MULTI-LEVEL MULTI-OBJECTIVE PROGRAMMING AND OPTIMIZATION FOR INTEGRATED AIR DEFENSE SYSTEM DISRUPTION

DISSERTATION

Aaron M. Lessin, Major, USAF

AFIT-ENS-DS-18-S-035

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

DISTRIBUTION STATEMENT A
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this document are those of the author and do not reflect the official policy or position of the United States Air Force, the United States Department of Defense or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENS-DS-18-S-035

MULTI-LEVEL MULTI-OBJECTIVE PROGRAMMING AND OPTIMIZATION FOR INTEGRATED AIR DEFENSE SYSTEM DISRUPTION

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy in Operations Research

Aaron M. Lessin, BS, MS

Major, USAF

September 2018

DISTRIBUTION STATEMENT A
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT-ENS-DS-18-S-035

MULTI-LEVEL MULTI-OBJECTIVE PROGRAMMING AND OPTIMIZATION FOR INTEGRATED AIR DEFENSE SYSTEM DISRUPTION

Aaron M. Lessin, BS, MS
Major, USAF

Committee Membership:

Brian J. Lunday, PhD
Chair

Raymond R. Hill, PhD
Member

Kenneth M. Hopkinson, PhD
Member

Adedeji B. Badiru, PhD
Dean, Graduate School of Engineering and Management

AFIT-ENS-DS-18-S-035

Abstract

The U.S. military's ability to project military force is being challenged. This dissertation develops, and demonstrates the application of, three respective sensor location, relocation, and network intrusion models to provide the mathematical basis for the strategic engagement of emerging technologically advanced, highly-mobile, Integrated Air Defense Systems. Herein, this research addresses each of these related problems via three distinct modeling and analysis efforts, each building upon the previous work.

First, a bilevel mathematical programming model is proposed for locating a heterogeneous set of sensors to maximize the minimum exposure of an intruder's penetration path through a defended region. This formulation also allows a defender to specify minimum probabilities of coverage for a subset of the located sensors (e.g., the most valuable sensors) and for high-value asset locations in the defended region. The bilevel program is reformulated to a single-level optimization problem for which instances can be readily solved using a commercial solver. Given the locations of a defender's sensors, three alternative path identification models are formulated, each corresponding to conceptually-motivated intrusion-path metrics. A test instance is examined for the air defense of a border region against intrusion by an enemy aircraft; upon identifying the optimal, respective defender asset location and intruder routing solutions, intruder-optimal solutions corresponding to each of three alternative metric-specific paths are examined, illustrating the relative impact of an intruder choosing an inappropriate metric. Sensitivity analyses are conducted to examine the effect of several model parameters on solution quality and required computational effort.

Next, consider a set of sensors having varying capabilities and respectively located to maximize an intruder's minimal expected exposure to traverse a defended border region. Given two subsets of the sensors that have been respectively incapacitated or degraded, a multi-objective, bilevel optimization model is formulated to relocate surviving sensors to maximize an intruder's minimal expected exposure to traverse a defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. This formulation also allows the defender to specify minimum preferential coverage requirements for high-value asset locations and emplaced sensors. Adopting the ε-constraint method for multi-objective optimization, a single-level reformulation is subsequently developed that enables the identification of non-inferior solutions on the Pareto frontier and, consequently, identifies trade-offs between the competing objectives. The aforementioned model and solution procedure are demonstrated for a scenario in which a defender is relocating surviving air defense assets to inhibit intrusion by a fixed-wing aircraft.

Lastly, this research considers an attacker seeking an optimal intrusion path through a region defended by a sensor network, as measured by the expected exposure of the intruding attacker to the defender's sensors. Herein, a trilevel mathematical programming formulation is presented in which an attacker respectively identifies a subset of the defender's heterogeneous sensors to incapacitate and a subset of the defender's network to degrade, subject to budget constraints; a defender subsequently relocates the surviving sensors, considering multiple, competing objectives; and in the third level, the attacker selects an optimal intrusion path to traverse through the defender's sensor network. A bilevel reformulation is derived, new heuristics are developed and tested, and the performance of the heuristics on synthetic-but-representative scenarios is reported.

To my Grandpa, my hero,

whose shoes I always wanted to fill and path I sought to follow.

Acknowledgements

I would like to extend a sincere thank you to my advisor, Dr. Brian Lunday, for his unwavering support and guidance throughout this research. His passion for learning and pursuit of excellence has been a constant inspiration, and this work would not have been possible without his mentorship.

Thanks also to the other members of my research committee, Dr. Raymond Hill and Dr. Kenneth Hopkinson, for their support and assistance which helped bring this academic endeavor to fruition.

Aaron M. Lessin

Table of Contents

Page

Abstract iv

Acknowledgements vii

List of Figures x

List of Tables xi

I. Introduction 1

1.1 Motivation 1
1.2 Research Focus and Organization 6

II. A Bilevel Exposure-oriented Sensor Location Problem for Border Security 8

2.1 Introduction 8
2.1.1 Literature Review 10
2.1.2 Major Contributions and Organization 16
2.2 Model & Methodology 17
2.2.1 Assumptions 17
2.2.2 Model 19
2.2.3 Alternative Intrusion Paths 25
2.3 Testing, Results, & Analysis 31
2.3.1 Illustrative Instance for Air Defense of a Border Region 31
2.3.2 Test Instance Generation 33
2.3.3 Results 35
2.3.4 Sensitivity Analysis 39
2.4 Conclusions & Recommendations 43

III. A Multi-objective, Bilevel Sensor Relocation Problem for Border Security 45

3.1 Introduction 45
3.1.1 Literature Review 47
3.1.2 Major Contributions & Organization 53
3.2 Model & Methodology 54
3.2.1 Assumptions 54
3.2.2 Model 57
3.2.3 Methodology 62
3.3 Testing, Results, & Analysis 65

Page

3.3.1 Representative Scenario for Air Defense of a Border Region . . . 65
3.3.2 Results . . . 69
3.3.3 Sensitivity Analysis . . . 77
3.4 Conclusions & Future Work . . . 80

IV. A Multi-objective, Trilevel Sensor Network Intrusion Problem . . . 83

4.1 Introduction . . . 83
4.1.1 Literature Review . . . 85
4.1.2 Major Contributions & Paper Organization . . . 92
4.2 Model & Methodology . . . 93
4.2.1 Assumptions . . . 94
4.2.2 Model Formulation . . . 97
4.3 Heuristic Solution Methods . . . 105
4.3.1 Heuristic 1 (H1): Piecewise incapacitation and degradation strategy determination . . . 105
4.3.2 Heuristic 2 (H2): Sequential incapacitation and degradation strategy determination . . . 113
4.4 Testing, Results, & Analysis . . . 115
4.4.1 Representative Scenario for the Intrusion of an Air Defense Network . . . 115
4.4.2 Results . . . 120
4.5 Conclusions & Recommendations . . . 125

V. Conclusion . . . 127

5.1 Contributions . . . 127
5.2 Recommendations for Future Research . . . 129

Appendix A. 2018 WDSI Proceedings: *A Multi-objective Bilevel Optimization Model for the Relocation of Integrated Air Defense System Assets* . . . 132

Bibliography . . . 139

List of Figures

Figure		Page
1	Hexagonal tessellation example	19
2	Probability-of-kill curve for each SAM battery type	33
3	Baseline Maximin Exposure Problem solution	35
4	Exposure values by path edge for four alternative intrusion paths	38
5	Probability-of-kill curve for each SAM battery type	67
6	Initial IADS layout	69
7	Initial IADS layout before asset relocations showing incapacitated and degraded assets	70
8	Multi-Objective Sensor Relocation Problem solution with $\varepsilon_2, \varepsilon_3$ unrestricted	71
9	Optimal minimal exposure values for discretized $(\varepsilon_2, \varepsilon_3)$-combinations	72
10	Percentage of maximum recoverable minimal exposure achievable for $(\varepsilon_2, \varepsilon_3)$-combinations	74
11	Pareto optimal relocation solution with $(\varepsilon_2, \varepsilon_3) = (1, 1)$	76
12	Pareto optimal relocation solution with $(\varepsilon_2, \varepsilon_3) = (2.5, 4)$	77
13	Effect of SAM battery spacing level on problem size.	79
14	Effect of d_{hex} and A_{BR} on LB_{hex}	80
15	Initial IADS layout	117
16	Heuristic 1 solution to Instance 3	122
17	Heuristic 1 solution to Instance 2	124
18	Heuristic 2 solution to Instance 2	125

List of Tables

Table		Page
1	Intrusion results by path metric and type	39
2	Effect of potential SAM battery location spacing on minimal exposure and computation times	40
3	Exposure values for the weighted exposure ($w^t = [1, 0.5, 0.2]$) solution	42
4	Differences in exposure for the equally and unequally weighted exposure instances	43
5	Pareto optimal solutions	75
6	Effect of potential SAM battery location spacing on instance size and computation time.	78
7	Test instance attacker incapacitation and degradation budget parameter values	116
8	SAM battery probability-of-kill functions	118
9	Heuristic 1 attacker objective function values for each test instance	121
10	Comparison of heuristic solution quality and computation time	122

MULTI-LEVEL MULTI-OBJECTIVE PROGRAMMING AND OPTIMIZATION FOR INTEGRATED AIR DEFENSE SYSTEM DISRUPTION

I. Introduction

1.1 Motivation

A key to the United States military's overwhelming historical success is due in large part to its ability to achieve and maintain air superiority. For the past half century, the United States has conducted combat operations relatively unimpeded, projecting power across the globe at will. However, this level of success has not gone unnoticed, and enemy nations have been forced to reassess their strategies in hope of achieving future success. As a result, many nations have adopted an antiaccess/area-denial (A2/AD) strategy to inhibit the United States' ability to penetrate their borders and project military power.

Unfortunately, past performance does not guarantee future success for the United States military. The operational environment is changing, and the United States' future military success will also depend on its own ability to adapt. This level of concern has risen to the highest ranks within the U.S. Air Force. In August 2016, during his "State of the Air Force" address, Air Force Chief of Staff General David Goldfein expressed his concern, stating that "air superiority is not an American birthright. It's actually something you have to fight for and maintain" (Goldfein & James, 2016).

Current U.S. doctrine for the suppression of enemy air defenses (SEAD) in Joint Publication (JP) 3-01, *Countering Air and Missile Threats* (specifically, Chapter 4, "Offensive Counterair Planning and Operations") highlights the need for a serious

reassessment of our strategy. JP 3-01 acknowledges that "potential adversaries' IADS [Integrated Air Defense Systems] have become increasingly complex and needs to be analyzed in-depth with an eye to potential strengths and weaknesses" (United States Joint Chiefs of Staff, 2012b). The document also discusses the change in mobility and effectiveness of enemy IADS as compared to past technologies. "SAM [Surface to Air Missile] forces have become more mobile and lethal, with some systems demonstrating a 'shoot-and-move' time in minutes rather than hours or days" (United States Joint Chiefs of Staff, 2012b). Although current doctrine recognizes the emergence of a more effective, modern A2/AD threat, JP 3-01 fails to provide a comprehensive approach to defeat such a threat.

In its section on "Suppression of Enemy Air Defenses," JP 3-01 details three categories of SEAD execution, namely (1) area of responsibility/joint operations area-wide (AOR/JOR-wide) air defense (AD) system suppression, (2) localized suppression, and (3) opportune suppression. AOR/JOR-wide air defense system suppression targets "high payoff AD assets that result in the greatest degradation of the enemy's total system," focusing on the destruction of "key C2 [Command and Control] nodes" (United States Joint Chiefs of Staff, 2012b). Unfortunately, enemy IADS command and control networks are becoming highly dispersed, decentralized, and redundant. Therefore, this category of SEAD execution will become much less effective in the future. The second category of SEAD, localized suppression, is focused on escort operations that are "normally confined to geographic areas associated with specific targets or transit routes for a specific time" (United States Joint Chiefs of Staff, 2012b). Under this category are two subcategories - planned localized suppression and immediate localized suppression. Planned localized suppression is a bottom-up, reactive approach whereby "localized suppression requests are processed from the lowest echelon of command to to the highest using the appropriate air control sys-

tem" (United States Joint Chiefs of Staff, 2012b). Immediate localized suppression is similar to its counterpart except with the added necessity of an immediate response, "similar to immediate requests for CAS [Close Air Support]" (United States Joint Chiefs of Staff, 2012b). It is clear that both subcategories of localized suppression are highly reactive as opposed to a deliberate, offensive approach. The final category of SEAD, opportune suppression, is also "unplanned and includes aircrew self-defense and attack against surface-AD targets of opportunity" (United States Joint Chiefs of Staff, 2012b). Included under the opportune suppression category of SEAD are also the following four subcategories: aircrew self-defense, targets of opportunity, targets acquired by observers or controllers, and targets acquired by aircrews. Again, a common theme characterized by a defensive and reactive strategy is present, complicated by the "proliferation of highly mobile AD weapon systems, coupled with deception and defensive tactics" (United States Joint Chiefs of Staff, 2012b).

Recognizing the gap in U.S. doctrine for defeating an ever developing and increasingly modern IADS threat, Lt Elliot Bucki recently proposed the addition of a new category of SEAD, termed "planned opportune suppression" (Bucki, 2016). This category of SEAD would combine the "planned nature of localized suppression and the tactics of opportune suppression" to produce a strategy that is more offensive-minded and proactive as opposed to the current doctrine which is more defensive and reactive (Bucki, 2016). This strategy makes three key assumptions about the nature of the new IADS threat which helps focus and shape its approach. First, it assumes that "almost all IADS components will be mobile and linked together in a system with considerable redundancy" (Bucki, 2016). Second, it assumes that non-stealth aircraft or those aircraft not equipped with long range standoff weapons will be "outranged" by technologically advanced IADS threats (Bucki, 2016). Third, it assumes that modern IADS will be "inherently resistant to jamming and electronic attack"

(Bucki, 2016). All of these assumptions help provide a realistic assessment of the modern IADS threat the U.S. is certain to face in an A2/AD environment.

It is important to note that Bucki's SEAD category of planned opportune suppression also accounts for the important temporal aspect in engaging an enemy IADS. By adding planned opportune suppression to JP 3-01, U.S. SEAD doctrine would contain a proactive approach that offers flexibility in attacking a highly mobile enemy IADS threat, providing a strategy that focuses on "planned on-call targets," while still offering the necessary flexibility to handle time critical targets of opportunity (United States Joint Chiefs of Staff, 2012b).

There has also been recent doctrinal development on the part of the Joint Chiefs of Staff as found in their "Joint Operational Access Concept (JOAC)" (United States Joint Chiefs of Staff, 2012a). Recognizing the "dramatic improvement and proliferation of weapons and other technologies," the document proposes a new concept for achieving *operational access* against an increasingly capable enemy that has adopted an antiaccess/area-denial strategy (United States Joint Chiefs of Staff, 2012a). Operational access is defined as "the ability to project military force into an operational area with sufficient freedom of action to accomplish the mission" (United States Joint Chiefs of Staff, 2012a). The JOAC doctrine notes that "the ability to ensure operational access in the future is being challenged - and may well be the most difficult operational challenge U.S. forces will face over the coming decades" (United States Joint Chiefs of Staff, 2012a).

In order to combat this emerging threat, the document lists multiple precepts describing how future joint forces could achieve operational access in the face of armed opposition. Some suggestions include: (1) "conduct operations based on the requirements of the broader mission, while also designing subsequent operations to lessen access challenges, (2) seize the initiative by deploying and operating on multiple, inde-

pendent lines of operations, (3) create pockets or corridors of local domain superiority to penetrate the enemy's defenses and maintain them as required to accomplish the mission, (4) maneuver directly against key operational objectives from strategic distance, (5) attack enemy antiaccess/area-denial defenses in depth rather than rolling back those defenses from the perimeter, and (6) maximize surprise through deception, stealth, and ambiguity to complicate enemy targeting" (United States Joint Chiefs of Staff, 2012a). This verbiage is strikingly different than the current SEAD doctrine found in JP 3-01. Here, a set of precepts outlines the development of a comprehensive operational concept for conducting planned, offensive operations in support of achieving the broader strategic objectives in a highly contested A2/AD environment.

In order to aid counter-A2/AD efforts, the JOAC recommends that future joint forces leverage "*cross-domain synergy* - the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of the others - to establish superiority in some combination of domains that will provide the freedom of action required by the mission" (United States Joint Chiefs of Staff, 2012a). Whereas synergy between joint forces has historically been a U.S. military strength, the unity of effort required for cross-domain synergy will require a higher level of integration, acting across domains and at lower echelons. This will allow the joint forces to exploit "fleeting local opportunities for disrupting the enemy system" because the temporal aspect of warfare will be critical in achieving cross-domain success. The days of overwhelming air supremacy will be far less likely, and air superiority as mentioned in the JOAC may not be "widespread or permanent; it more often will be local and temporary" (United States Joint Chiefs of Staff, 2012a).

1.2 Research Focus and Organization

Although the U.S. has taken significant steps in identifying the gaps in doctrine and proposing concepts for confronting a highly mobile, technologically advanced A2/AD enemy threat, the greater difficulty will be in operationally implementing these new concepts. This research provides a mathematical lens to analyze the emerging A2/AD threat with the aim of understanding how to engage and defeat future adversaries. To accomplish this task, this dissertation focuses on three main avenues of research, each building upon the previous work.

To ultimately defeat an advanced A2/AD threat, it is critical to first understand how an enemy may construct (i.e., layout) an air defense network consisting of a set of ground-based air defense assets to prevent intrusion of a defended region. To wit, Chapter II presents a bilevel math programming model to determine the optimal layout of a given set of heterogeneous assets to maximize the minimum exposure of an intruder's penetration path through a defended border region.

Considering the rapid increase in air defense asset mobility, it is also important to determine how an enemy may reposition surviving ground-based IADS assets following an attack. Given two subsets of the assets that have been respectively incapacitated or degraded, Chapter III formulates a multi-objective, bilevel optimization model to relocate surviving assets to maximize an intruder's minimal expected exposure to traverse a defended border region, minimize the maximum asset relocation time, and minimize the total number of assets requiring relocation.

Once a better understanding has been achieved regarding how an enemy may optimally locate and relocate ground-based elements of an A2/AD IADS, the research herein shifts its focus to the ultimate goal of the dissertation - determining how to optimally attack and penetrate an enemy air defense system. To accomplish this, Chapter IV proposes a trilevel mathematical programming formulation in which an

attacker respectively identifies a subset of the defender's heterogeneous sensors to incapacitate and a subset of the defender's network to degrade, subject to budget constraints; a defender subsequently relocates their sensors to maximize the attacker's minimal exposure, minimize the maximum relocation time, minimize the maximum number of sensors requiring relocation, and minimize the under coverage of high-value assets and emplaced sensors; in the third level, the attacker selects an optimal intrusion path through the defender's sensor network.

For each of the three main research efforts presented in Chapters II, III, and IV, detailed solution techniques are presented, and their application is demonstrated via a representative air defense scenario. A discussion of selected analyses is also provided therein. Chapter V concludes with a summary of the contributions and recommendations for future research.

By accomplishing each of these research goals, this dissertation provides a basis for the operational implementation of the concepts outlined in the JOAC and the proposed improvements to JP 3-01 to provide the strategic planning that will be necessary to effectively engage and defeat the emerging A2/AD IADS threat.

II. A Bilevel Exposure-oriented Sensor Location Problem for Border Security

2.1 Introduction

National, group, and individual sovereignty requires protection against threats. At the national level, potential threats include the illegal or unauthorized movement of people, weapons, or drugs. At the group level, corporations seek to defend their computer networks against malicious code. Individual sovereignty concerns include protection of a residence against burglary. The defense against such threats begins at a border or boundary of the region under a defender's control, whether it be physical or virtual. Moreover, the defense against threats occurs within a *border region*, wherein a defender will locate and use assets to detect and/or interdict a would-be intruder.

Evidence of the growing requirement for border security can be seen in a 2017 memorandum from the U.S. Department of Homeland Security (DHS) which indicates "the surge of illegal immigration at the southern border has overwhelmed federal agencies and resources and has created a significant national security vulnerability to the United States" (Kelly, 2017). As a result, the U.S. House of Representatives Homeland Security Committee passed a $10 billion bill (McCaul, 2017) to "deter, impede, and detect illegal activity" through the use of integrated surveillance and intrusion detection assets such as the Integrated Fixed Tower (IFT) System and the Remote Video Surveillance System (RVSS). IFTs are fixed sensors that provide long-range, persistent surveillance by automatically detecting and tracking targets of interest. Similarly, RVSS assets are fixed sensors that use cameras, radio, and microwave transmitters to "provide short-, medium-, and long-range persistent surveillance mounted on stand-alone towers, or other structures" (Alles et al., 2016). The bill also sets aside $10 million to implement Vehicle and Dismount Exploitation Radars

(VADER) in border security operations (McCaul, 2017). Since 2006, unmanned systems equipped with VADER sensors have been credited with interdicting over "13,144 pounds of cocaine and 321,330 pounds of marijuana worth an estimated $1.8 billion" (Alles et al., 2016).

Oriented against aerial threats to border security, ground-based air defense weapons are emplaced as part of an antiaccess/area-denial (A2/AD) strategy to defend against enemy aircraft attempting to penetrate a country's border region during active conflict. Many countries have adopted A2/AD strategies (Schmidt, 2016) and significantly advanced their Surface to Air Missile (SAM) technology. Over the last 10 years, Russia has developed and fielded the S-400 Triumf air defense weapon system which can destroy aerial targets at ranges of 40-400 km (Foss & O'Halloran, 2014). This highly-effective SAM system is capable of engaging the world's most premier aircraft, as well as cruise missiles and ballistic missiles. Recent reports indicate the Russian military currently operates 39 S-400 battalions, with each battalion consisting of eight launchers and up to 112 missiles, along with radar systems and a command post (Gady, 2017). China, Turkey, India, and Saudi Arabia have all signed contracts for the purchase of multiple S-400 systems from Russia (TAS, 2017). Motivated by this trend in air defense posturing, in this study we construct an air defense test instance as an illustrative border security application.

Border security is no longer limited to physical borders but now includes virtual, software-defined borders, creating vulnerabilities from the economic market to the energy sector. Due to recent threats "targeting government entities and organizations in the energy, nuclear, water, aviation, and critical manufacturing sectors" the DHS and the Federal Bureau of Investigation (FBI) released an alert "to educate network defenders and enable them to identify and reduce exposure to malicious activity" (DHS, 2017). This emerging threat is not simply a U.S. problem; in December 2015,

a cyberattack on the Ukrainian power grid left over 225,000 people without power (Lee et al., 2016). Daniel Tobok, CEO and co-owner of Toronto-based Cytelligence, estimates that cyberattacks "cost Canada $3 billion to $5 billion per year in proceeds to criminals, adding one Calgary energy company was forced to pay $200,000 in ransom three years ago to regain control of its corrupted digital production systems" (Healing, 2017). In his 2017 State of the Union Address, European Commission President Jean-Claude Juncker said that "cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks" (Juncker, 2017).

Common to each of these border security applications is that a defender must decide where to locate a set of assets to prevent an adversary from traversing through a region; the defender's assets may also have differing capabilities to detect or engage the adversary; some defensive assets may be important enough to the defender because of their high cost or limited supply to warrant protection, once emplaced; specific locations of the defended region may require preferential coverage due to their importance; and an adversary will be able to observe the location of defender assets and select a route through the border region to minimize their likelihood of detection.

2.1.1 Literature Review.

Our modeling efforts for this research focus on implementing and extending previous work in facility location. Schilling et al. (1993) presented a detailed overview of covering problems in facility location. They classified models as either a Set Covering Problem (SCP) or a Maximal Covering Location Problem (MCLP), where coverage is either required or optimized, respectively. The MCLP was first introduced by Church & ReVelle (1974) to maximize the amount of demand covered within a specified service distance by locating a fixed number of facilities. White & Case (1974) extended the work of Church & ReVelle (1974) by considering equal weights on all

demand points. Church (1984) later introduced the MCLP on a planar surface using Euclidean and rectilinear distance measures, where potential facility locations are no longer discrete (and finite).

One of the main assumptions of the MCLP is that coverage is binary. That is, a demand point is either fully covered or not covered at all by a located facility. However, this assumption is often unrealistic. Berman & Krass (2002) extended the MCLP to the Generalized Maximal Covering Location Problem (GMCLP), allowing for "partial coverage of customers, with the degree of coverage being a non-increasing step function of the distance to the nearest facility." Additionally, Berman et al. (2003) extended the GMCLP by way of a gradual covering decay model. Drezner et al. (2004) also solved the gradual covering problem on a planar surface.

Traditional facility location models do not address the need to prevent the passage of an adversary into friendly territory, which is the main concern for border security applications. However, a related field of research pertaining to the location of sensors in a Wireless Sensor Network (WSN) presents coverage models designed specifically for such a purpose. One of the three main coverage problems discussed in WSNs is *barrier coverage* (Cardei & Wu, 2006). In the context of WSNs, "a given belt region is said to be *k-barrier covered* with a sensor network if all crossing paths through the region are *k-covered*, where a crossing path is any path that crosses the width of the region completely" (Kumar et al., 2005). A path is said to be *k-covered* if it intersects at least k sensors' sensing ranges (Huang & Tseng, 2005).

As the defender, the goal of a barrier coverage model is to locate a set of sensors S such that some chosen measure of coverage is maximized. Alternatively, an attacker seeks to interdict or locate areas of the region where the value of the coverage measure is minimized. One such measure of coverage often used in WSN models is *exposure*. First introduced by Meguerdichian et al. (2001), exposure can informally be thought

of as the "expected average ability of observing a target in the sensor field." More formally, exposure is defined as "an integral of a sensing function that generally depends on distance from sensors on a path from a starting point p_S to destination point p_D" (Meguerdichian et al., 2001). Unlike some coverage metrics, the element of time is important for exposure, since the ability of a sensor to detect a target can improve as the sensing time (i.e., exposure) increases.

For a sensor s, the general sensing model S at an arbitrary point p is:

$$S(s,p) = \frac{\lambda}{[d(s,p)]^K}, \tag{1}$$

where $d(s,p)$ is the Euclidean distance between the sensor s and the point p, and positive constants λ and K are technology-dependent parameters (Meguerdichian et al., 2001). The parameter λ can be thought of as the energy emitted by a target, and K is an energy decay factor, typically ranging from 2 to 5 (Amaldi et al., 2008).

The *exposure* of an object in the sensor field during the interval $[t_1, t_2]$ along the path $p(t)$ is defined by Meguerdichian et al. (2001) as:

$$E(p(t), t_1, t_2) = \int_{t_1}^{t_2} I\Big(F, p(t)\Big) \left| \frac{dp(t)}{dt} \right| dt, \tag{2}$$

wherein the sensor field intensity $I\big(F, p(t)\big)$ is implemented using an *All-Sensor Field Intensity* model or a *Closest-Sensor Field Intensity* model, depending on the application and types of sensors used. The *All-Sensor Field Intensity* model is a summation of the sensing function values (1) from target p to *all* sensors in the sensor network, defined as $I_A(F,p) = \sum_{i=1}^{n} S(s_i, p)$, whereas the *Closest-Sensor Field Intensity* model only utilizes the sensing function value of the *closest* sensor to the target (Meguerdichian et al., 2001).

Using the definition of exposure, Meguerdichian et al. (2001) presented an algo-

rithm to find the *minimal exposure path* in a sensor network. The algorithm first transforms the problem into a discrete domain utilizing a generalized grid approach and then creates an edge-weighted graph. The algorithm then applies Dijkstra's single-source shortest-path algorithm (Dijkstra, 1959) to find the minimal exposure path from the source point p_S to the destination point p_D. Meguerdichian et al. (2001) also extended this initial work by developing a localized minimal exposure path algorithm using Voronoi diagrams.

Understanding that signals traveling from a target to a sensor are often corrupted by noise, Clouqueur et al. (2002) added an Adaptive White Gaussian Noise term $N_i, i = 1, ..., n$, to the initial sensor model in Equation (1). Clouqueur et al. (2002) also presented the concepts of *value fusion* and *decision fusion* as alternative techniques for collaborating sensors to decide whether a target is actually present in the field to avoid false alarms. In the same paper, Clouqueur et al. (2002) developed a multi-phase random deployment strategy to minimize the cost of sensor deployment while achieving a desired detection performance. Adlakha & Srivastava (2003) determined the minimum number of randomly deployed sensors required to guarantee a given exposure level. Veltri et al. (2003) presented a localized algorithm that enables a sensor network to determine its minimal exposure path. More recently, Amaldi et al. (2008) formulated two exposure-based optimization problems to respectively minimize the number of sensors required while guaranteeing a minimum exposure and, alternatively, to maximize the exposure of the least exposed path subject to a budget constraint on the sensors' installation cost. Tian et al. (2014) presented a motion-planning scheme to direct the movement of mobile sensors for better detecting "smart" intruders. Lastly, Feng et al. (2016) proposed a minimal exposure path problem that requires the passage of a path around the boundary of an inaccessible region, and is solved using a hybrid genetic algorithm.

Another metric used to evaluate the quality of service provided by a WSN is *maximal breach*, first proposed by Meguerdichian et al. (2001). Given a field A with n sensors $s_i \in S = \{1, ..., n\}$ located at (x_i, y_i), let points I and F be initial and final locations, respectively, of an intruder traveling through A. Given a path P connecting I to F, *breach* is defined as the minimum Euclidean distance from P to any sensor in S (Megerian et al., 2005). Furthermore, among all possible paths connecting I and F, the path that has the maximum breach value is called the *maximal breach path*, P_B (Duttagupta et al., 2007). For an intruder, the *breach* of P_B represents the closest the intruder will be to any sensor in A when traveling from point I to F. For the defender, breach represents how close to a sensor the intruder is guaranteed to travel, no matter which path the intruder traverses through the field for a given sensor layout.

In many WSN models wherein the objectives involve partial, if not complete, coverage of all grid points, the number of sensors available for deployment is typically not limited. However, in some situations resources may be limited and must be optimally allocated across a vast geographical area. WSN algorithms that make use of Voronoi diagrams and breach values are often better suited for this purpose. Meguerdichian et al. (2001) demonstrated how the critical edges of a maximal breach path could be used as a guide for determining where to add sensors in order to improve overall coverage. Duttagupta et al. (2007) developed a sensor insertion-based heuristic procedure to achieve the maximum possible improvement in average breach. This procedure provides an approach that builds up a sensor network by successively adding sensors to reduce the breach value as much as possible. Cavalier et al. (2007) presented a heuristic based on Voronoi diagrams to locate a finite number of sensors to detect an event in a given planar region where the objective is to minimize the maximum probability of non-detection. Recently, Karabulut et al. (2017) presented a mixed-integer

linear bilevel programming formulation, called the Maximal Breach Path Coverage Problem (MBPCP), along with three Tabu search heuristics; the defender determines the best sensor locations to maximize security, and the intruder reacts by destroying a subset of the sensors to increase the probability of evading detection, as computed using a maximal breach path approach.

There are several important distinctions that should be made between minimal exposure and maximal breach coverage models. Exposure models incorporate the element of time, assuming that sensors are more likely to detect an intruder given a longer period of observation. The minimal exposure problem seeks a path between points p_S and p_D such that the *total* exposure acquired from the sensors by the moving target is minimized. Alternatively, the maximal breach problem seeks a path from point p_S to p_D such that the maximum exposure to the sensors at *any* given point is minimized (Veltri et al., 2003). This is a key distinction between the two approaches. In terms of exposure, it may be beneficial to move closer to a sensor for a period of time to shorten the total path length and decrease the total exposure.

From the defender's perspective, our goal is to determine the optimal sensor layout to prevent an intruder from crossing a defended region of interest. We employ a minimal exposure path approach, and our objective is to maximize the intruder's minimal exposure. We are not concerned with forcing a specified probability of coverage during at least one segment of the intrusion path, but we instead seek to maximize the intruder's total exposure across the entire path. If we were to adopt a maximal breach path approach to solve this problem, our objective would be to minimize the intruder's maximal breach. That is, we would want to guarantee that, at some point in the traversal of the defended region, the intruder is within a certain distance of a sensor. However, it is unlikely, if not impossible, that we could force an intruder to always be within the coverage range across the entire space; we would be seeking to

ensure at least one opportunity exists for which the intruder is within the coverage range of a sensor. As the defender, an exposure-based approach may offer many more opportunities to engage an intruder relative to a maximal breach path approach.

2.1.2 Major Contributions and Organization.

A majority of the research implementing breach- and exposure-coverage metrics focuses on determining the maximal breach path or calculating the minimal exposure path for a given sensor layout. Our chief concern, however, is to find the optimal deployment of a given set of sensors to maximize the minimal exposure of an intruder's traversal of a defended region. Extending the work of Amaldi et al. (2008), this paper develops the notion of weighted exposure, considering a set of heterogeneous sensor types. The exposure weights represent the defender's sensor preferences in terms of which sensors the defender prefers to employ when interdicting the intruder. Our formulation also allows the defender to specify required minimum probabilities of coverage for a subset of the located sensors (e.g., the most valuable sensors) and for high-value asset locations in the defended region (e.g., fielded force locations, population centers, command and control centers, etc.), balancing the exposure objective with the protection of sensors and high-value asset locations. We also demonstrate the robustness of the exposure metric for border protection by formulating and analyzing three additional alternative intrusion path metrics. That is, the optimal objective value of the minimal exposure solution results in the worst-case exposure of an intruder's traversal of the defended region, regardless of the intruder's chosen metric for intrusion path determination.

Section 2.2 presents the bilevel mathematical formulation for solving the sensor location problem as well as a single-stage reformulation, and it proposes three conceptually-motivated, alternative intrusion path metrics an intruder might con-

sider adopting. Section 2.3 provides a military air defense scenario as an illustrative example for the application of the model, and it details the test instance generation, presents solutions, and provides sensitivity analysis results. Section 2.4 concludes with a summary of our findings and recommendations for future research.

2.2 Model & Methodology

In this section, we present a baseline formulation for the optimal sensor location problem, extending a modeling approach presented by Amaldi et al. (2008) wherein the authors seek to maximize the exposure of the least exposed path subject to a budget on the sensor installation cost. Unlike Amaldi et al. (2008), our model includes a heterogeneous set of sensors, and we introduce the notion of weighted exposure, allowing for defender-specified preferences between sensor types. We also add constraints to ensure defender-specified minimum probabilities of coverage for a set of high-value asset locations the defender seeks to protect. Considering instances where the loss of a sensor is highly undesirable, we include additional constraints to provide minimum probabilities of coverage for located sensors, by sensor type. Therefore, given a specified set of heterogeneous sensors, we determine the optimal layout that maximizes the minimal expected exposure of an intruder attempting to traverse the region, while ensuring adequate coverage of emplaced sensors and high-value asset locations.

2.2.1 Assumptions.

We make several assumptions related to the defender's objectives and sensors. Regarding the objectives, we assume that, in addition to constructing a sensor network to inhibit an adversary traversing the defended region, the defender also wants to provide specific coverage of a set of high-value asset locations (e.g., population centers,

command and control centers, etc.) and a subset of the located sensors (e.g., the most valuable sensors). A minimum probability of protection is specified for each high-value asset location of interest and for each sensor type. The overall objective is to determine the location of sensors to maximize the ability to intercept intruding targets while protecting the high-value asset locations and a subset of the located sensors.

In many instances, points within a sensor coverage ring are not *fully* covered, whereas points outside remain completely uncovered. Rather, a probability of coverage exists for a target located at a given distance from a sensor location. As the distance from target to sensor decreases, the probability of coverage increases. Instead of assuming binary sensor coverage (i.e., covered/not covered), we implement a probability-of-coverage curve as a function of the distance from target to sensor, for each of the heterogeneous sensor types. Furthermore, we assume the defender's incoming threat is a single target with a specified constant velocity.

To formulate instances of our model, we construct a hexagonal tessellation over the border region of interest, as shown in Figure 1. The intruding target traverses the arcs of the graph, traveling from artificial origination node o on the left side of the hexagonal grid to the artificial destination node d on the right. Potential sensor locations are positioned at the center of each hexagon in the grid. We choose to discretize the border region using a mesh of uniformly-sized regular hexagons, as Yousefi & Donohue (2004) demonstrated it to be superior to alternative uniform tessellation means (e.g., square, rhombus, triangle) as it provides more freedom of movement for the intruder.

Lastly, we assume the adversaries know each others' capabilities, and the intruder has sufficiently capable intelligence to know the defender's sensor locations.

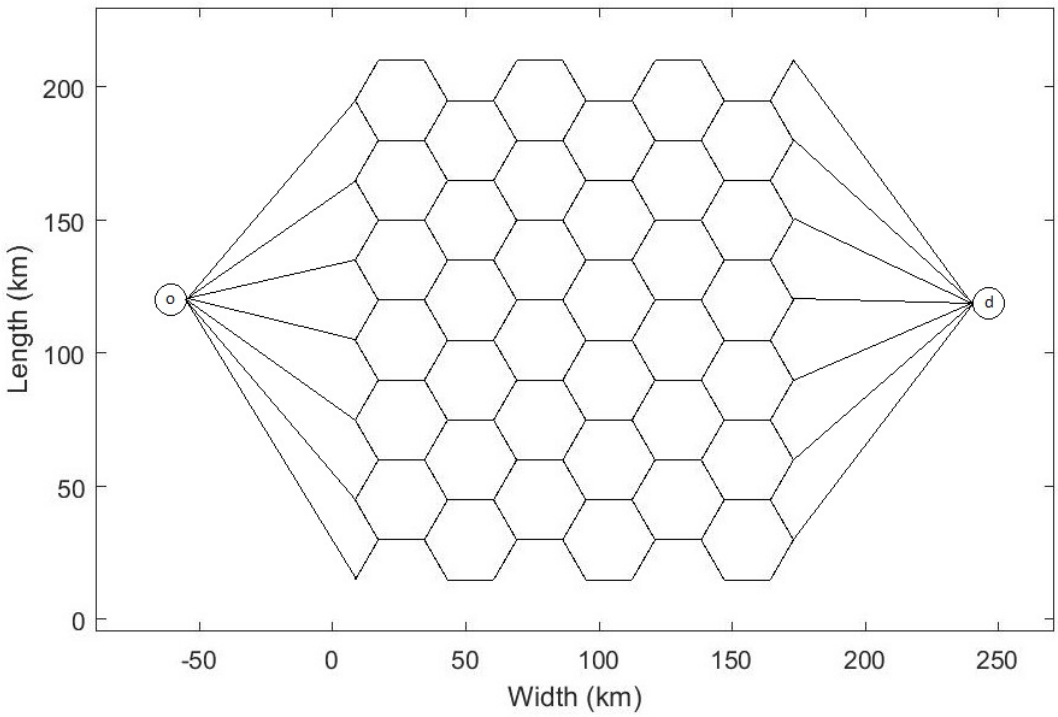


Figure 1. Hexagonal tessellation example

2.2.2 Model.

The following list of sets, parameters, and decision variables are used to formulate the mathematical programming models considered herein.

Sets:

T : the set of all types of sensors available to locate, indexed by t.

S : the set of all sites where sensors can be located, indexed by s.

F : the set of all sites where high-value assets are located, indexed by f.

A : the set of arcs over which an intruding target can traverse, indexed by (i, j).

N : the set of all nodes at which arcs intersect and through which an intruding target can traverse, indexed by n.

$G = (N, A)$: the graph over which an intruding target will traverse, as induced by the set of potential sensor sites $s \in S$.

Parameters:

w^t : the exposure weight for sensor type $t \in T$.

e_{ij}^{st} : the exposure time of a target traversing arc $(i, j) \in A$ to a sensor of type $t \in T$ located at site $s \in S$.

B^t : the maximum number of type $t \in T$ sensors available to locate.

p_{sp}^t : the probability that a sensor of type $t \in T$ located at site $s \in S$ can cover the point p.

C^f : the minimum probability of coverage required for each high-value asset location $f \in F$.

C^t: the minimum probability of coverage required for each located sensor of type $t \in T$.

Decision Variables:

x_s^t : 1 if the defender locates a type $t \in T$ sensor at site $s \in S$, and 0 otherwise.

y_{ij} : 1 if the intruder traverses arc $(i, j) \in A$, and 0 otherwise.

Given our assumptions, the game theoretic view of this problem is that of a two-player, extensive-form, two-stage, zero-sum game with perfect and complete information. In the upper-level problem, the defender determines the locations of a set of heterogeneous sensors. Observing this decision, the intruder reacts in the lower-level problem by selecting arcs to traverse the region. The defender and intruder seek

to respectively maximize and minimize the total expected weighted exposure of the least exposed path. Leveraging the aforementioned notation, we formulate the bilevel **Maximin Exposure Problem (MmEP)** corresponding to this Stackelberg game as follows:

$$\textbf{MmEP}: \max_{\boldsymbol{x}} \min_{\boldsymbol{y}} \sum_{(i,j)\in A} \left(\sum_{s\in S} \sum_{t\in T} w^t e_{ij}^{st} x_s^t \right) y_{ij} \tag{3}$$

$$\text{s.t.} \sum_{s\in S} x_s^t = B^t, \ \forall t \in T, \tag{4}$$

$$\sum_{t\in T} x_s^t \leq 1, \ \forall s \in S, \tag{5}$$

$$\sum_{s\in S} \sum_{t\in T} \ln\left(1 - p_{sf}^t\right) x_s^t \leq \ln\left(1 - C^f\right), \ \forall f \in F, \tag{6}$$

$$\sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} \ln\left(1 - p_{s\bar{s}}^t\right) x_s^t \leq \ln\left(1 - C^t\right) x_{\bar{s}}^t, \ \forall \bar{s} \in S, t \in T \tag{7}$$

$$\sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N \setminus \{o, d\}, \end{cases} \qquad \forall i \in N, \tag{8}$$

$$y_{ij} \geq 0, \ \forall (i,j) \in A, \tag{9}$$

$$x_s^t \in \{0,1\}, \ \forall s \in S, t \in T. \tag{10}$$

The objective function (3) maximizes the total expected weighted exposure of the intruder's minimal exposure path, where $\sum_{s\in S} \sum_{t\in T} w^t e_{ij}^{st} x_s^t$ represents the expected weighted exposure of a target traversing a given arc $(i,j) \in A$ to sensors of type $t \in T$ emplaced (i.e., $x_s^t = 1$) at locations $s \in S$. The exposure weights w^t account for the defender's preferences of sensors for engaging the intruder. We propound that cardinality weighting is appropriate for most applications, as it results in an objective calculation of exposure times for an intruder. However, we retain the general

model having w^t-parameters for a special case wherein the defender may exhibit preferences over the sensor types $t \in T$. As a defender-focused model, the purpose of these weights is to determine the optimal location of the sensors, *given the defender's sensor preferences*. For a given set of w^t-parameter values, the resulting formulation corresponds to the framework of a zero-sum game with perfect and complete information. Were the intruder to assume any other set of weights than the actual ones adopted by a defender, a different intrusion path may result; however, such a different path can only yield a better objective function value for the defender. If the intruder does perceive the defenders priorities correctly, the optimal solution identified via our model represents the worst-case solution from the defender's perspective.

For example, the defender could specify exposure weights of 1.0, 0.5, and 0.2 for a model with three different sensor types. For such a case, the defender would prefer to use the first sensor type over all other sensor types to engage the intruder. Alternatively, exposure weights may be parameterized to account for qualitative differences in sensor effectiveness not captured by the quantitative differences inherent in the sensor probability functions. Qualitative differences in sensor performance may result from factors such as insufficient sensor operator training or operational technical complexity of a given sensor type. Under this interpretation, the defender may be half as effective at employing the second type of sensor against a target compared to using the first sensor type.

Constraint (4) specifies the number of each type of sensor the defender can locate. Constraint (5) prevents more than one sensor from being located at the same site. Constraint (6) ensures that all high-value asset locations receive the required coverage. The form of Constraint (6) results from a logarithmic transformation of the constraint

$$1 - \prod_{s \in S} \prod_{t \in T} \left(1 - p_{sf}^t\right)^{x_s^t} \geq C^f, \ \forall f \in F, \tag{11}$$

wherein independence is assumed among the probabilities of coverage, p_{sf}^t over sensor locations, $s \in S$, and sensor types, $t \in T$. (Implied is the assumption that $C^f < 1$, which is appropriate for this probabilistic metric wherein certain coverage is not attainable.) Likewise, Constraint (7) provides for the coverage of emplaced sensors by other sensors, as may be required by specific applications to protect valuable sensors. That is, for every site $\bar{s} \in S$, if a defender locates a sensor of type $t \in T$ (i.e., $x_{\bar{s}}^t = 1$), Constraint (7) requires a specified level of coverage, C^t, via the effects of *other* sensors the defender chooses to locate (i.e., $x_s^t, \forall s \in S \setminus \{\bar{s}\}$). In contrast, if a defender does not locate a sensor of type $t \in T$ at a site $\bar{s} \in S$ (i.e., $x_{\bar{s}}^t = 0$), then the constraint effectively requires at least $C^t = 0$ (i.e., no coverage requirement). Constraint (8) induces the flow balance constraints for the path from the intruder's point of origin, o, to destination point, d. Constraint (9) is the non-negativity constraint associated with the minimal exposure path variables, and Constraint (10) enforces binary restrictions on the sensor location decision variables.

Adopting an approach similar to Wood (1993), Colson et al. (2007), and Amaldi et al. (2008), we reformulate the bilevel MmEP (3)-(10) by replacing the lower-level problem with its dual formulation, enabling the identification of an optimal solution via direct optimization using a commercial solver. Treating the upper-level variables x_s^t as parameters, the lower-level minimization problem becomes a shortest path problem in which the exposure objective is minimized, subject to Constraints (8) and (9). Replacing the primal, lower-level problem with its dual in Equations (12)-(15),

$$\max_{\boldsymbol{\pi}} \ \pi_d - \pi_o \tag{12}$$

$$\text{s.t.} \ -\pi_i + \pi_j \leq \sum_{s \in S} \sum_{t \in T} w^t e_{ij}^s x_s^t, \ \forall (i,j) \in A, \tag{13}$$

$$\pi_o = 0, \tag{14}$$

$$\pi_i \text{ unrestricted}, \forall i \in N \setminus \{o\}, \tag{15}$$

where π_i is the dual variable associated with the i^{th} Constraint (8), we obtain the following single-level reformulation of the MmEP:

$$\max_{\boldsymbol{x},\boldsymbol{\pi}} \ \pi_d - \pi_o \tag{16}$$

$$\text{s.t.} \sum_{s\in S} x_s^t = B^t, \ \forall t \in T, \tag{17}$$

$$\sum_{t\in T} x_s^t \leq 1, \ \forall s \in S, \tag{18}$$

$$\sum_{s\in S}\sum_{t\in T} \ln\left(1 - p_{sf}^t\right) x_s^t \leq \ln\left(1 - C^f\right), \ \forall f \in F, \tag{19}$$

$$\sum_{s\in S\setminus\{\bar{s}\}}\sum_{t\in T} \ln\left(1 - p_{s\bar{s}}^t\right) x_s^t \leq \ln\left(1 - C^t\right) x_{\bar{s}}^t, \ \forall \bar{s} \in S, t \in T \tag{20}$$

$$-\pi_i + \pi_j \leq \sum_{s\in S}\sum_{t\in T} w^t e_{ij}^{st} x_s^t, \ \forall (i,j) \in A, \tag{21}$$

$$\pi_o = 0 \tag{22}$$

$$\pi_i \text{ unrestricted}, \ \forall i \in N \setminus \{o\}, \tag{23}$$

$$x_s^t \in \{0,1\}, \ \forall s \in S, t \in T. \tag{24}$$

The sensor location formulation presented in Equations (16)-(24) provides a baseline model to determine the optimal location of sensors to maximize the exposure of the least exposed intruder path. Although our focus is on border security, the model is easily generalizable for surveillance or coverage of any type of region by any type of device (e.g., cameras, police units, air defense batteries, cell phone towers, etc.). Numerous model enhancements can be added to the above formulation to incorporate other situation-specific requirements. For example, if sensors represent police units, the defender may want to specify the maximum (or minimum) distance between any two sensor locations to ensure backup coverage for officer safety concerns. The defender may also need to prevent the placement of sensors in certain locations for

geographical or political reasons.

2.2.3 Alternative Intrusion Paths.

For a given instance, the MmEP not only determines the optimal sensor locations, but it also identifies an intruder's minimal exposure path. However, we recognize that an intruder may not adopt such an exposure metric when determining its intrusion path, but may instead consider the maximal breach metric or some other metric of choice. Accordingly, for a fixed sensor location solution to the MmEP, we also identify three alternative intrusion paths: the maximal breach path, the maximal weighted breach path, and the maximum probability of survival path.

As a defender-focused model, the goal of the bilevel programming formulation is to determine the optimal sensor locations to maximize the exposure of an intruder. For the worst-case scenario, the intruder adopts the same exposure-oriented metric as the defender. This scenario corresponds to a zero-sum game that is represented by our baseline MmEP formulation. Should the intruder adopt a different metric, the defender will do no worse with respect to their objective function for a given (i.e., fixed) sensor location strategy and, as demonstrated via our test results, may yield a markedly better outcome.

Should the defender assume (correctly or otherwise) that the intruder adopts a different metric, the solution to a modified bilevel programming formulation may identify a better outcome for the defender. However, if that defenders assumption is incorrect, the sensor location solution will not address the worst-case scenario, yielding a suboptimal solution for the defender, for whom the exposure metric is of paramount importance.

As such, we contend that the adopted framework should not be set aside for a defender to change their strategy based on assumptions about the intruders metric

in lieu of considering the worst-case scenario.

Defining d_{ij}^s as the minimum Euclidean distance between arc $(i,j) \in A$ and the sensor located at site $s \in S$, we develop the following multi-objective, binary **Maximal Breach Path (MBP)** programming model to determine the intruder's maximal breach path, given a defender's sensor layout solution to the MmEP:

$$\textbf{MBP}: \max_{d_{min}, \boldsymbol{y}} f(d_{min}, \boldsymbol{y}) = \Big(f_1(d_{min}), -f_2(\boldsymbol{y}) \Big) \tag{25}$$

$$\text{s.t. } f_1(d_{min}) = d_{min}, \tag{26}$$

$$f_2(\boldsymbol{y}) = \sum_{(i,j) \in A} y_{ij}, \tag{27}$$

$$d_{min} \leq d_{ij}^s \Bigg(\sum_{t \in T} x_s^t \Bigg) y_{ij} + M \Bigg(1 - \Bigg(\sum_{t \in T} x_s^t \Bigg) y_{ij} \Bigg), \ \forall (i,j) \in A, s \in S, \tag{28}$$

$$\sum_{j:(i,j) \in A} y_{ij} - \sum_{j:(j,i) \in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N \setminus \{o, d\}, \end{cases} \qquad \forall i \in N, \tag{29}$$

$$y_{ij} \in \{0,1\}, \ \forall (i,j) \in A. \tag{30}$$

Traditional maximal breach path approaches in the literature are single-objective formulations which seek to maximize the minimum distance between the intruder's path and any sensor in the region. These formulations determine a path that typically identifies one critical arc in the intruder's path (i.e., the arc with the maximal breach value). The other non-critical arcs are therefore insignificant in that they do not affect the maximal breach objective value, yielding many alternative optimal solutions. Without the inclusion of additional constraints or path length objectives, single-objective maximal breach formulations can yield (alternative optimal) intruder

paths that wander throughout a region and are unrealistic for many practical applications. This solution characteristic motivates our construction of a multi-objective maximal breach path approach to preemptively maximize the metric corresponding to the intruder's maximal breach path, d_{min}, and subsequently differentiate among alternative optimal solutions by minimizing the total path length, $f_2(\boldsymbol{y})$. Constraint (28) bounds d_{min} based on the intruder path selected, wherein the values of the location decisions x_s^t are fixed parameters from the optimal solution to the MmEP. Constraint (**??**) induces the flow balance constraints for the path from the intruder's point of origin, o, to destination point, d. Constraint (30) enforces binary restrictions on the path traversal decision variables.

Instead of solving the MBP (25)-(30) using a weighted sum or lexicographic approach, we implement the ε-constraint method and reformulate the MBP as follows:

$$\mathbf{MBP}_{\boldsymbol{\varepsilon}}\text{:} \max_{\boldsymbol{y}} d_{min} \tag{31}$$

$$\text{s.t.} \sum_{(i,j)\in A} y_{ij} \leq \varepsilon_2, \tag{32}$$

$$\text{Constraints (28)} - \text{(30)},$$

wherein we utilize Constraint (32) to bound our second objective, the minimization of the intruder path length, to be no more than ε_2, a maximum path length. We do not specify the value used for ε_2 because it is a tunable parameter for which the appropriate value is instance-specific. Its purpose is to inhibit the generation of solutions having intruder paths that wander, in that any routing that is not affected by the binding constraint is otherwise allowable in an optimal solution. During initial testing, setting ε_2 equal to the intruder path length corresponding to the optimal solution to Problem MmEP was effective, but it may not hold for every instance, and tuning may be required. Since we discretized the defended region using a uniformly-

sized regular hexagon tessellation, the intruder's path length is simply the number of arcs in the maximal breach path. More generally, we could include the length l_{ij} of each arc $(i,j) \in A$ in Constraints (27) and (32) to minimize the intruder's path length for tessellation schemes having disparate arc lengths.

If the entire sensor network consisted of a homogeneous set of sensors, the maximal breach path would indeed remain as far away from every sensor as possible across the intrusion path. However, since a sensor network may consist of sensors having different capabilities, an intruder will most likely seek to remain further away from more capable sensors. We captured this effect by examining two additional intruder path-selection metrics: the maximal weighted breach path and the maximum probability of survival path.

Using a maximal weighted breach path approach, we weight the breach distances from sensor location to intruder path by sensor type, using a weighting scheme based on the maximum effective sensor range ($r_{\max}$) of each sensor type. For example, consider a sensor network with three types of sensors with maximum effective ranges of $r_{\max} = [250, 20, 6]$ km. We then assign the following breach distance weights:

$$\gamma_t = \left[1.0, \frac{r_{\max_1}}{r_{\max_2}}, \frac{r_{\max_1}}{r_{\max_3}}\right] = \left[1.0, \frac{250}{20}, \frac{250}{6}\right] = \left[1.0, 12.5, 41.\bar{6}\right], \tag{33}$$

for the first ($t = 1$), second ($t = 2$), and third ($t = 3$) sensor types, respectively. Modifying the MBP formulation (25)-(30) by incorporating the breach distance weights, γ_t, we obtain the following multi-objective **Maximal Weighted Breach Path (MWBP)** formulation:

$$\textbf{MWBP}: \max_{d_{min}, \boldsymbol{y}} f(d_{min}, \boldsymbol{y}) = \Big(f_1(d_{min}), -f_2(\boldsymbol{y})\Big) \tag{34}$$

$$\text{s.t. } f_1(d_{min}) = d_{min}, \tag{35}$$

$$f_2(\boldsymbol{y}) = \sum_{(i,j)\in A} y_{ij}, \tag{36}$$

$$d_{min} \leq d_{ij}^s \left(\sum_{t\in T} \gamma_t x_s^t \right) y_{ij} + \cdots$$

$$\cdots + M\left(1 - \left(\sum_{t\in T} x_s^t\right) y_{ij}\right), \ \forall (i,j) \in A, s \in S, \tag{37}$$

$$\sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N \setminus \{o, d\}, \end{cases} \qquad \forall i \in N, \tag{38}$$

$$y_{ij} \in \{0, 1\}, \ \forall (i,j) \in A. \tag{39}$$

Moreover, adopting the ε-constraint method results in the following ε-constrained MWBP formulation:

$$\mathbf{MWBP}_{\boldsymbol{\varepsilon}}\text{:} \ \max_{\boldsymbol{y}} \ d_{min} \tag{40}$$

$$\text{s.t.} \sum_{(i,j)\in A} y_{ij} \leq \varepsilon_2, \tag{41}$$

$$\text{Constraints } (37) - (39),$$

Alternatively, we determined the path that maximizes the intruder's probability of survival during sensor network traversal, using the probability-of-coverage function for each sensor type as a proxy weighting scheme. Assuming independence among sensors and arcs $(i,j) \in A$, an intruder's probability of not surviving across an intrusion path is:

$$\bar{p} = 1 - p = 1 - \prod_{(i,j)\in A} \prod_{s\in S} \prod_{t\in T} \left[1 - p_{sij}^t\right]^{x_s^t y_{ij}}, \tag{42}$$

where $\bar{p}$ is the probability of not surviving and p_{sij}^t is the probability of being covered (i.e., not surviving) along arc $(i,j) \in A$ by a sensor of type $t \in T$ located at site

$s \in S$.

Such a modeling construct is erroneous for a defender to adopt; compared to the Minimal Exposure Path, a so-called "Maximum Probability of Survival Path" does not account for the time spent traversing any given arc in the network. However, its conceptual simplicity portends that an adversary may consider it, so we examine it as an alternative intrusion path metric within this study.

Imposing a logarithmic transformation, maximizing the probability of survival is equivalent to maximizing:

$$\ln(p) = \sum_{(i,j)\in A} \sum_{s\in S} \sum_{t\in T} \left(\ln\left[1 - p_{sij}^{t}\right] x_s^t\right) y_{ij}. \tag{43}$$

To determine the maximum probability of survival path, we solved the following binary programming **Maximum Probability of Survival Path (MPSP)** problem:

$$\textbf{MPSP}: \max_{\boldsymbol{y}} \sum_{(i,j)\in A} \sum_{s\in S} \sum_{t\in T} \left(\ln\left[1 - p_{sij}^{t}\right] x_s^t\right) y_{ij} \tag{44}$$

$$\text{s.t.} \sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N \setminus \{o, d\}, \end{cases} \qquad \forall i \in N, \tag{45}$$

$$y_{ij} \in \{0, 1\},\ \forall (i,j) \in A. \tag{46}$$

Since the values of the location decisions x_s^t are fixed parameters from the optimal solution of the MmEP (3)-(10), we could replace the objective function (44) with $\min_{\boldsymbol{y}} \sum_{(i,j)\in A} c_{ij} y_{ij}$, where $c_{ij} = -\sum_{s\in S} \sum_{t\in T} \ln\left[1 - p_{sij}^{t}\right] x_s^t$, and the MPSP problem (44)-(46) is equivalent to a shortest path problem.

In addition to providing the defender with knowledge of potential alternative intruder path locations, analyzing the exposure values associated with each of the

alternative intrusion paths provides the defender with an assessment of the robustness of the MmEP sensor location solution. We demonstrate the MmEP solution approach and provide alternative intrusion path analysis via an air defense application example in the following section.

2.3 Testing, Results, & Analysis

We solve the mixed integer linear reformulation (16)-(24) of the bilevel Maximin Exposure Problem (3)-(10) on a 3.2 GHz PC with 6 GB of RAM, using the commercial solver IBM ILOG CPLEX 12.7. The following subsections present the chosen border security application, discuss test instance generation, and provide numerical results of the testing.

2.3.1 Illustrative Instance for Air Defense of a Border Region.

Adopting the viewpoint of a defender, we illustrate via a representative test instance the applicability of our MmEP formulation and solution approach to the border security application of locating ground-based assets within an Integrated Air Defense System (IADS).

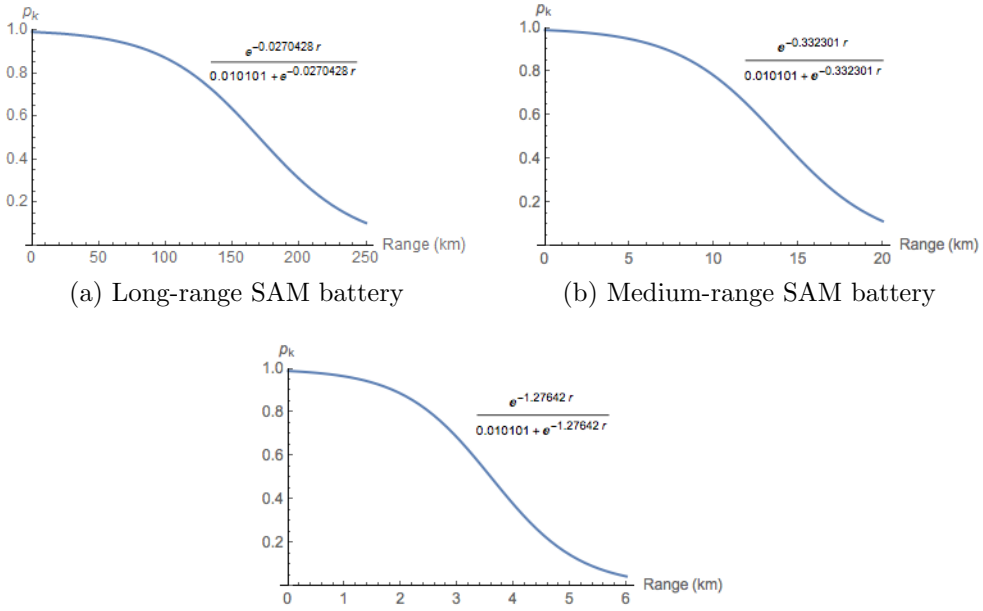
Given a 600 km long by 520 km wide border region, the defender's objective is to optimally locate two long-range (e.g., SA-21 Growler), four medium-range (e.g., SA-22 Greyhound), and six short-range (e.g., SA-24 Grinch) SAM battery assets (i.e., $B^t = [2, 4, 6]$) to maximize the ability to intercept intruding aircraft (Foss & O'Halloran, 2014). The defender also seeks to protect three high-value assets (e.g., fielded force locations, population centers, command and control centers, etc.) located at $F = \{(375, 420), (405, 30), (450, 565)\}$, with minimum probabilities of protection of $C^f = [0.75, 0.5, 0.5]$. Additionally, the defender requires the long-range SAM batteries to be protected with a minimum probability of 0.7 (i.e., $C^t = [0.7, 0, 0]$). Given the

defender's air defense asset location solution, the intruder's objective is to determine the least exposed intrusion path.

Instead of assuming binary SAM battery coverage (i.e., covered/not covered), we implement a representative probability-of-kill curve as a function of the distance from target to SAM battery, for each SAM battery type. Capabilities of these weapons for parameterizing model instances in this study are obtained from an open-source, unclassified reference (Foss & O'Halloran, 2014). The construction of the probability-of-kill curves for instances herein is notional but representative; we utilized a logit model for the probability of kill as a function of the range, assuming a probability of 0.99 for a range of zero and a probability of between 0.04 and 0.11 at the maximum effective range (r_{max}) (Foss & O'Halloran, 2014). To artificially induce different interceptor performance, we specified a probability of 0.55 at 65% of r_{max} for the long-range SAM batteries, a probability of 0.2 at 90% of r_{max} for the medium-range SAM batteries, and a probability of 0.5 at 60% of r_{max} for the short-range SAM batteries. The probability-of-kill function for each SAM battery type is depicted in Figure 2. These functions are used to calculate the exposure values for each arc resulting from the hexagonal tessellation of the border region.

In addition to the aforementioned SAM battery types, the long-range assets require separate targeting and tracking radars to engage a target. However, to simplify the model, we assume that each SAM battery possesses the required radar coverage to engage enemy targets.

Furthermore, we assume for this study the defender's incoming threat consists only of aircraft, as opposed to a wide range of threats not limited to, but including, cruise missiles and ballistic missiles. This assumption determines the coverage capabilities for each SAM battery instead of requiring the model to account for a myriad of target types. The intrusion aircraft travel at a constant velocity of 1,800 km/hr (i.e.,



(a) Long-range SAM battery

(b) Medium-range SAM battery

(c) Short-range SAM battery

Figure 2. Probability-of-kill curve for each SAM battery type

$|v| = 1,800$ km/hr). For the baseline instance, we further assume equal exposure weights (i.e., $w^t = [1, 1, 1]$). That is, the defender does not wish to specify preferences between SAM battery types for engaging the intruder.

2.3.2 Test Instance Generation.

Test instances for our analysis are generated by first constructing a hexagonal grid with potential sensor (i.e., SAM battery) locations positioned in the center of each hexagon. Neighboring hexagon centers are located at a defender-specified distance (in km) from each other. Herein, we adopt a distance of 30 km for initial testing in Section 2.3.3 and explore alternatives through sensitivity analyses in Section 2.3.4. The granularity of grid construction is easily adapted to suit a given situation or modeler's needs for fidelity.

The intruder's goal is to traverse the border region from an artificial origination

node, o, on the (w.l.o.g.) Western side of the border region to an artificial destination node, d, on the (w.l.o.g.) Eastern side of the border region, where these nodes are connected by arcs to the leftmost and rightmost hexagon arc nodes, respectively.

Unlike previous definitions of exposure in the literature which utilize the standard sensing model (1), we leverage the specific probability-of-kill functions depicted in Figure 2, as well as the target's velocity. That is, for a type $t \in T$ SAM battery located at site $s \in S$, the sensing model for a target located at the point l on arc $(i, j) \in A$ is:

$$S^t(s, l) = p^t(s, l), \tag{47}$$

where $p^t(s, l)$ is the probability of kill for a target located at the Euclidean distance from SAM battery $s \in S$ of type $t \in T$ to the point l on arc $(i, j) \in A$.

Given a target's location as a function of time, denoted $l(\tau)$, the cumulative exposure time of a target traversing arc $(i, j) \in A$ from SAM battery $s \in S$ of type $t \in T$ is represented as a function of either time or distance via Equation (48), wherein τ_1 and τ_2 indicate the respective times at which a target starts and completes the arc traversal, corresponding to points l_1 and l_2 for a given constant target velocity, $|v|$.

$$e_{ij}^{st} = \int_{\tau_1}^{\tau_2} S^t(s, l(\tau))d\tau = \int_{\tau_1}^{\tau_2} p^t(s, l(\tau))d\tau = \int_{l_1}^{l_2} \frac{p^t(s, l)}{|v|}dl \tag{48}$$

This exposure calculation within Equation (48) differs slightly from that used by Meguerdichian et al. (2001), wherein the author calculates cumulative exposure *intensity* vis-à-vis cumulative exposure *time*, the metric of interest for the parameter e_{ij}^{st}.

The exposure value for each arc is calculated via numerical integration and included as a model parameter. The numerical integration requires an assumed, constant speed of the intruder and the probability of kill (i.e., detection) at each of a set

of discrete points along the arc. The specific probability-of-kill values at each point are determined by the probability-of-kill functions for each of the three sensor types, $t \in T$, shown in Figure 2 and the Euclidean distance between the point l and sensor location s. Therefore, we can interpret the objective function (3) as the total expected time the defender can intercept an intruder, which the defender and intruder seek to maximize and minimize, respectively.

2.3.3 Results.

Figure 3 depicts the solution to the single-level MmEP reformulation (16)-(24) for this instance, using a 30 km spacing between potential SAM battery locations. It further depicts the four respective intruder paths, each of which is optimal for its given metric.

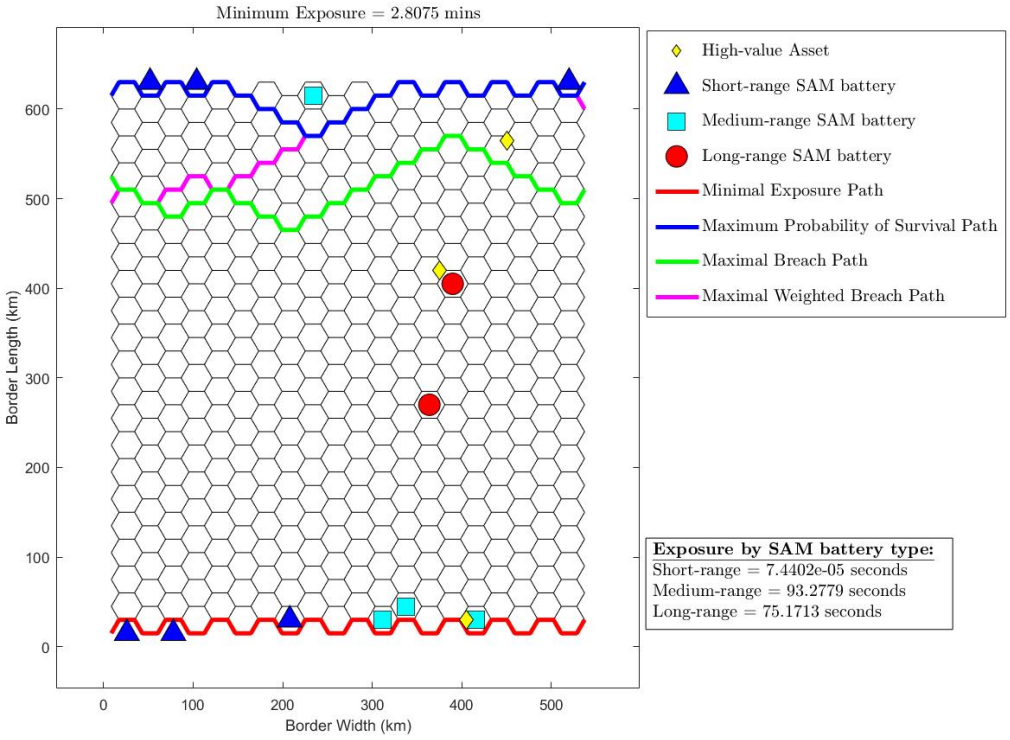


Figure 3. Baseline Maximin Exposure Problem solution

The two long-range SAM batteries are located near the center of the border re-

gion, while the medium-range and short-range SAM batteries provide coverage of the northern and southern edges of the border region. This IADS layout results in a minimal exposure of 2.8075 minutes, divided between the long-range, medium-range, and short-range SAM batteries which induce 75-second, 93-second, and 7.44×10^{-5}-second exposures, respectively. The minimal exposure is the total expected time the defender will have to engage an enemy aircraft traversing the minimal exposure path. This represents the worst-case exposure the defender will experience for a given IADS layout; any other path chosen by the intruder will result in an equal or greater exposure value, which can only benefit the defender. This effect is observed in the resulting exposure values for the MBP, the MWBP, and the MPSP, as displayed in Figure 4 and reported in Table 1.

The disparity in exposure values between the alternative intrusion paths results from the distinct differences in path location. The minimal exposure path traverses the southern edge of the border region, remaining as far away from the long-range SAM batteries as possible since they result in the largest exposure values. The maximum probability of survival path travels along the northern edge of the border region, but moves away from the more capable medium-range SAM battery located near the northern border. This path corresponds to a 0.0024 probability of survival for the intruder, and it also results in a 0.92% (i.e., 1.54 second) increase in exposure compared to the minimal exposure path. Alternatively, the maximal breach path seeks to remain as far away from *all* IADS assets as possible without regard to differing asset capabilities, splitting the distance between the long-, medium-, and short-range SAM batteries in the northern part of the border region. Similarly, the maximal weighted breach path also attempts to remain as far away from the IADS assets as possible; however, this path seeks to remain furthest from the long-range assets, traveling closer to the less capable SAM batteries. This behavior is showcased by the magenta path

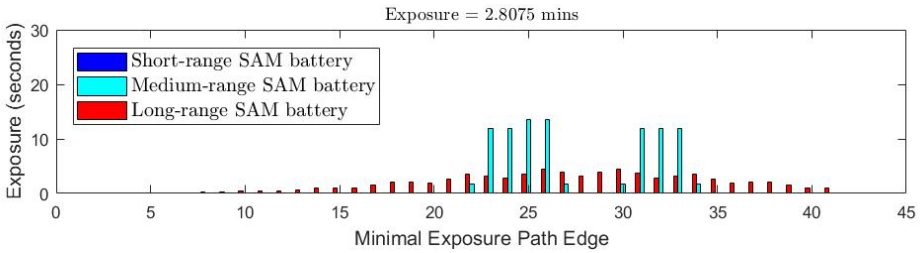
in the northern part of the border region in Figure 3. Instead of splitting the distance between the three SAM battery types, the maximal weighted breach path travels closer to the medium-range and short-range SAM batteries while remaining further away from the more capable, long-range SAM battery.

Due to the relatively small number of IADS assets available to the defender, the optimal objective value for the MBP and the MWBP remained unchanged for varying values of ε_2 in the MBP_ε and MWBP_ε. Therefore, the breach path solutions shown in Figure 3 represent the maximal breach solution with the minimum feasible path length (i.e., $f_2(\boldsymbol{y}) = 41$).

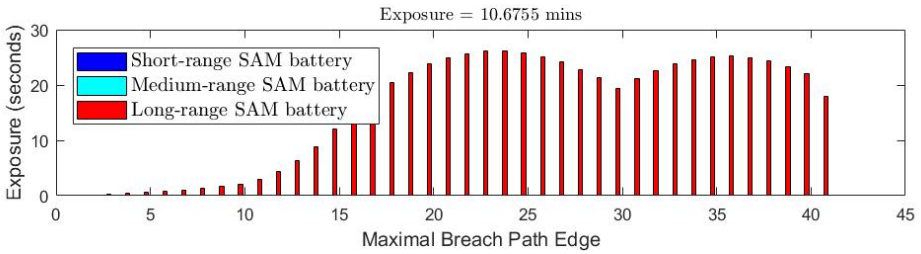
Figure 4 depicts the exposure of an attacking aircraft to each type of located SAM battery as it traverses its intrusion path, as it corresponds to each of the four metrics (and paths) considered. These exposure plots illustrate the differences in exposure values by SAM battery type across the four alternative intrusion paths analyzed.

Not only do we observe the difference in overall exposure values, but the plots also show the differences in exposure across each edge of the intruder's flight profile. As the defender, these plots reveal the points in the flight path that offer the most opportune times for engaging the intruder. For the intruder, these plots highlight the riskiest portions of the mission profile. For example, if the intruder decides to operate along the minimal exposure path, the intruder is most exposed between edges 23-33 of the flight profile, as depicted in Figure 4(a).

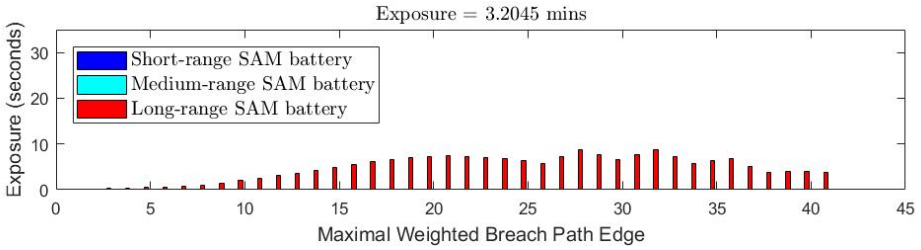
The defender determined the location of the IADS assets under the assumption that the attacker would adopt a minimal exposure path for intrusion. Even if this assumption does not hold, the results in Figure 4 validate this approach for metric selection. Moreover, if the intruder instead chose to use the breach metric for intrusion path selection, the results show that intruder the would experience a 280% increase in exposure. Table 1 further details the differences in solution quality for the alternative



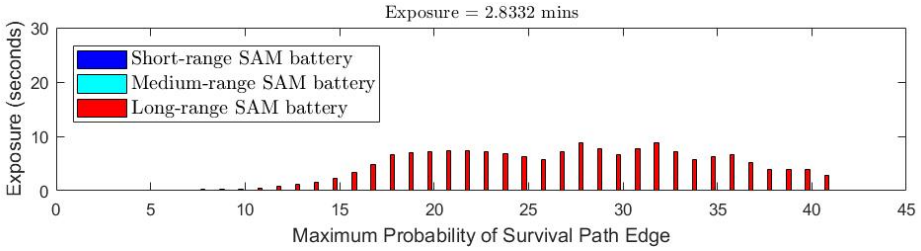
(a) Minimal Exposure Path



(b) Maximal Breach Path



(c) Maximal Weighted Breach Path



(d) Maximum Probability of Survival Path

Figure 4. Exposure values by path edge for four alternative intrusion paths

intrusion paths based on the four metrics for intrusion path selection (i.e., exposure, breach, weighted breach, and probability of survival).

The minimal exposure path indeed provides a worst-case bound on the expected exposure. All three alternative intrusion paths result in an increased exposure, which benefits the defender. As expected, we also observe that each path performs best

Table 1. Intrusion results by path metric and type

Intrusion Path Type	Intrusion Path Metric			
	Exposure (min)	Breach (km)	Weighted Breach (km)	Probability of Survival
Minimal Exposure Path	2.8075	15.0	187.5	4.0E-04
Maximal Breach Path	10.6755	113.6	138.6	3.3E-13
Maximal Weighted Breach Path	3.2045	15.0	210.7	1.2E-03
Maximum Probability of Survival Path	2.8332	15.0	210.7	2.4E-03

for its respective metric. In terms of the probability of survival, all paths result in a near-zero probability of survival for this specific instance. However, this calculation presumes that a defender engages an intruding aircraft with an interceptor from every IADS asset as it traverses each arc. This is indeed a pessimistic metric and not one we recommend adopting. This metric could be adjusted by making additional assumptions regarding the number of weapon engagements the defender could employ for each SAM battery, as well as decision rules to determine when a defender would engage a target.

2.3.4 Sensitivity Analysis.

We conducted a sensitivity analysis to examine the effect of several model parameters on solution quality and required computational effort. When modeling the MmEP, there are several important modeling parameters that can affect the minimal exposure objective. We chose to investigate the respective effect of (1) the separation distance between potential SAM battery locations and (2) the exposure weights assigned to each SAM battery type on the minimal exposure objective value. Specifically, we considered potential SAM battery separations of 25, 30, 40, and 50 km, and we examined exposure weights $w^t \in (0, 1]$ for each SAM battery type.

Although each SAM battery spacing alternative yields a unique layout, several trends emerged for this test instance. The long-range SAM batteries remained cen-

trally located in the border region, whereas the medium-range and short-range SAM batteries were most often dispersed along the northern and southern edges of the border region. Perhaps of greater interest, however, are the effects on solution quality and computation time, as reported in Table 6. A decrease in the distance between potential SAM battery locations from 40 km to 30 km (i.e., an increase in granularity of the hexagonal grid) yields a relative increase of 9.5% in the minimal exposure for an intruder. However, this result does not portend a monotonically increasing relationship, as an additional decrease to 25 km corresponds to a relative decrease of 12.7% from the exposure attained from a 30 km tessellation. We postulate but do not examine further herein that such relative decreases with increased granularity result merely from the altered feasible set of locations for SAM battery sites, S, specific to a given instance.

Table 2. Effect of potential SAM battery location spacing on minimal exposure and computation times

Distance Between Potential SAM Batteries (km)	Number of Potential SAM Battery Locations	Number of Arcs	Minimal Exposure (min)	Computation Time (sec)
25	600	1825	2.4507	28,558.5
30	420	1281	2.8075	107.1
40	210	645	2.5641	7.8
50	156	481	1.6165	4.0

Moreover, the 25 km spacing instance required nearly 8 hours to solve, whereas the 30 km instance required under 2 minutes. While further testing may be conducted to determine if this trend holds in general, there is indeed a practical spacing value to maximize the minimal exposure objective. For this instance, we recommend using a 30 km spacing of potential SAM batteries. One may even be able to construct a general spacing rule that results in a superlative solution found with reasonable computational effort.

If the potential SAM battery spacing is too large, the model may not obtain

a feasible solution. For example, in the 50 km instance, the medium-range SAM batteries were no longer capable of satisfying the high-value asset coverage constraints because their effective ranges were too small. One could remedy this situation by increasing the number of potential SAM battery locations for a set hexagon size or by reducing the minimum high-value asset and/or SAM battery coverage requirements. The 50 km instance, for example, required reducing the coverage requirements by 10% in order to obtain a feasible solution.

Although the model specifies exact locations for each SAM battery, in real-world applications, commanders of air defense units should be given the latitude to adjust the prescribed locations of their specific SAM batteries within the associated hexagon region while still satisfying the coverage requirements. For example, there may be local terrain restrictions or other aspects indiscernible from a high-level modeling standpoint that need to be considered during implementation of a specific IADS layout solution.

If a defender prefers to engage an enemy aircraft using certain SAM batteries over others, our model allows for the specification of exposure weights (w^t) to capture these preferences. Instead of equally weighting the exposure values (i.e., $w^t = [1, 1, 1]$) as in the baseline solution shown in Figure 3, the defender may prefer to assign exposure weights of $w^t = [1, 0.5, 0.2]$, for example. That is, the defender is half as effective at employing the medium-range SAM battery against an enemy aircraft as compared to using the long-range SAM battery. Likewise, the defender considers their forces to be five times more effective at employing a long-range SAM battery than a short-range SAM battery. Table 3 details the change in exposure values for each of the alternative intrusion paths, using the exposure weights $w^t = [1, 0.5, 0.2]$.

Compared to the baseline solution in Figure 3, the minimal weighted exposure solution locates all the medium-range SAM batteries on the southern edge of the

Table 3. Exposure values for the weighted exposure ($w^t = [1, 0.5, 0.2]$) solution

Intrusion Path Type	Exposure (min)	Percent Change (%)*
Minimal Weighted Exposure Path	2.3898	-14.9
Maximal Breach Path	12.5862	17.9
Maximal Weighted Breach Path	2.4656	-23.1
Maximum Probability of Survival Path	2.3898	-15.7

*compared to the baseline instance solution with $w^t = [1, 1, 1]$

border region and transfers an additional short-range SAM battery near the northern edge of the border region. As a result, the locations of the intrusion paths also change. More importantly, this layout produces a minimal exposure value of 2.3898 minutes. This represents a 14.9% decrease in the minimal exposure, as compared to the baseline solution. Even though the defender may prefer using one SAM battery over another, the solution is actually worse if the model is forced to comply with the defender's additional exposure weights; the model produces a better solution in terms of minimal exposure when allowed to determine SAM battery placement using equally weighted exposure values.

To further examine the effect of exposure weighting, we fixed the long-range exposure weight at 1 and systematically decreased the medium-range and short-range exposure weights at the same rate (i.e., $w^1 = 1$ and $w^2 = w^3 : 1 \rightarrow 0$). Our results confirmed that the equally weighted, baseline exposure model results in an optimal IADS layout that maximizes the minimal exposure. Additional exposure weights imposed by the defender (i.e., weights less than 1) produced suboptimal minimal exposure objective values for all test instances analyzed. However, if the defender prefers a non-equal weighting, the model does offer such flexibility and will identify the optimal solution corresponding to such user-imposed weights. For example, the defender may choose to implement a weighted exposure scheme to account for differences in crew training or expertise between various SAM battery types. Although the overall exposure decreases in the weighted instance, Table 4 indeed shows that the

IADS solution using weighted exposures $w^t = [1, 0.5, 0.2]$ produces an increase in the long-range SAM battery exposure and a decrease in the medium-range SAM battery exposure, as desired by the defender.

Table 4. Differences in exposure for the equally and unequally weighted exposure instances

Exposure Weights	Total Exposure (minutes)	Exposure by SAM Battery Type (seconds)		
		Long-range	Medium-range	Short-range
$w^t = [1, 1, 1]$	2.8075	75.2	93.3	7.4E-05
$w^t = [1, 0.5, 0.2]$	2.3898	143.4	1.1E-80	7.4E-05

2.4 Conclusions & Recommendations

Using the minimal exposure metric, we formulated a heterogeneous sensor location model for border security, developing the notion of weighted exposure to incorporate defender preferences among different sensor types. Our formulation also allows the defender to specify required minimum probabilities of coverage for a subset of the located sensors (e.g., the most valuable sensors) and for high-value asset locations in the defended region. Moreover, for a given defender location solution, we formulated intruder path identification models corresponding to each of three conceptually-motivated, alternative intrusion path metrics. We showcased our formulation and solution approach via a representative air defense asset location instance. Upon identifying the optimal, respective defender asset location and intruder routing solutions, we examined the intruder-optimal solutions corresponding to each of the alternative metric-specific paths, illustrating the relatively greater exposure incurred to an intruder by choosing an inappropriate metric. We also conducted a sensitivity analysis to examine the effects of exposure weights, along with varying potential sensor location spacing, on the minimal exposure objective value.

Future research could be conducted to increase model fidelity by accounting for

the placement of hierarchical sensors or by considering multiple intrusion targets with disparate capabilities. We could also refine the sensor probability-of-coverage functions to account for location-specific effects such as terrain and altitude, depending on the application of interest. Alternatively, a follow-on study could set aside the discrete expectation framework for identifying an intruder exposure-minimizing path, instead embedding the routing problem within a simulation (e.g., see Ryan et al. (1998, 1999)); however, such an approach would preclude the identification of an optimal sensor location solution via a single-stage optimization problem, and the use of a response surface methodology would be more appropriate.

III. A Multi-objective, Bilevel Sensor Relocation Problem for Border Security

3.1 Introduction

Defense against threats to a sensor network begin at a border or boundary of a defender's network, whether it be physical or virtual. Moreover, the defense against such threats occurs within a *border region*, wherein a defender will locate sensors to detect and/or interdict an intruder and relocate sensors to adjust to disruptions or unexpected changes. Location decisions for the sensors are often made using static assumptions. In practice, however, subsequent decisions may be required to respond to changes, whether internal or external, to the decision space. Within the context of sensor networks, such changes within a network may result from random sensor failures, planned sensor outages, direct adversarial attacks, or temporary decreases in sensor performance due to malicious attacks. Changes external to the sensor network, such as unexpected increases in demand or the need to provide backup coverage, may require the adjustment of sensor locations to improve the level of coverage. Relocation models are designed to respond to such changes by adjusting initial location decisions.

Applications of relocation problems that account for possible changes affecting initial location decisions can be found throughout the public, private, and government sectors. Natural disasters that destroy power generation and delivery components and cause power outages or create critical shortages of basic supplies, necessitate the relocation of electrical generators and emergency response resources (FEMA, 2017). In the wake of recent hurricanes, such as the one in Puerto Rico that left over 3.5 million people without electricity, the U.S. Secretary of Energy is considering plans to relocate air transportable nuclear power plants as a rapid response solution to minimize the impact of future disasters (Adams, 2017). Temporary relocation of

cell phone towers may be required to perform maintenance on permanent towers or to support high-volume demands for major sporting events, concerts, Presidential inaugurations (Baig, 2017), or even solar eclipses (Banse, 2017). Taxi companies such as Uber relocate vehicles based on historical data to meet forecasted demands or accommodate significant short-term increases in service requests (Laptev et al., 2017). Police units, ambulance companies, and fire stations (Lincoln, 2014) may relocate individual units or entire stations to decrease response times or adapt to changing demands as the coverage area increases or the distribution and/or likelihood of events in a given location changes over time (Macaulay, 2017).

An application of particular interest within this study relates to military defense of airspace. To counter aerial threats to border security, ground-based air defense weapons are positioned as part of an Integrated Air Defense System (IADS) to defend against enemy aircraft attempting to penetrate a country's border region during active conflict. Unlike previously fielded air defense systems, emerging air defense assets are highly mobile, "with some systems demonstrating a 'shoot-and-move' time in minutes rather than hours or days" (United States Joint Chiefs of Staff, 2012b). We construct an air defense test instance as an illustrative border security application, showcasing the sensor relocation formulation and solution approach developed herein.

The objective of this paper is to provide an exact solution method for the sensor relocation problem to prevent intrusion through a defended border region. We accomplish this via the formulation and solution of a bilevel, multi-objective optimization model. Given an initial layout of heterogeneous sensors, we simulate a disruption to the sensor network by incapacitating (i.e., interdicting) a subset of sensors and degrading (i.e., partially interdicting) the effectiveness of another subset of sensors, wherein an incapacitation is enduring for an affected sensor whereas a degradation is limited to a geographic region and sensor type (i.e., moving an incapacitated sensor

does not recover its capability, but moving a degraded sensor out of an affected region will). We then determine the optimal response to these events by relocating the available sensors, considering multiple, competing objectives. Specifically, we seek to maximize an intruder's minimal expected exposure to traverse the defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation.

3.1.1 Literature Review.

Our modeling efforts apply and extend previous techniques in facility relocation and bilevel, multi-objective optimization, particularly as they relate to border security. Ehrgott (2006) provides a comprehensive presentation of multi-objective optimization modeling approaches and solution techniques "to compute so called efficient, or Pareto optimal, or compromise solutions that - unlike traditional mathematical programming methods - take the contradictory nature of the criteria into account." Unlike single-objective problems, we no longer achieve a single optimal solution but rather a set of Pareto optimal solutions. A solution is called Pareto optimal (or efficient) if no single objective function can improve without deteriorating the objective function value of at least one of the other objectives (Ehrgott, 2006).

Most multi-objective optimization problems in the literature focus on problems with continuous decision variables. However, many facility location models incorporate binary location decision variables. Ulungu & Teghem (1994) and Ehrgott & Gandibleux (2000) provide surveys of multi-objective combinatorial optimization (MOCO). Greco et al. (2005) provide a collection of state of the art multi-criteria survey papers that includes a chapter of specific interest by Nickel et al. (2005), which presents a broad overview of multi-criteria location problems.

Defender-attacker optimization problems in the literature often employ bilevel

mathematical programming models to represent extensive form games. With a view to protect fixed sites, Brown et al. (2006) examined and illustrated models to defend nodes on critical infrastructure networks such as petroleum refinement and electrical supply. Bricha & Nourelfath (2013) adopted a non-zero-sum approach to protect supply nodes, wherein both the defender and attacker have multiple objectives (i.e., respective player action costs and their collective impact on the resulting defender's supply system capabilities). From a facility location-oriented approach, Scaparra & Church (2008) developed models to fortify facilities and maintain the best p-median coverage of demands, whereas Losada et al. (2012) proposed a similar coverage protection model but with an emphasis on the restoration of coverage over time, and Aliakbarian et al. (2015) examined hierarchical facility protection having a similar p-median coverage structure. Alternatively, other works examine bilevel defender-attacker models to protect networks rather than fixed sites. For example, Qiao et al. (2007) modeled a defender's allocation of resources to maximize an attacker's cost of inflicting damage to water supply network components, and Cappanera & Scaparra (2011) sought to identify the components in a transportation network to protect from disruption so as to maintain the shortest path between a supply and demand node pair. The problem considered herein differs from the aforementioned literature in that it seeks to relocate a subset of the defender's assets rather than emplace new assets. Moreover, the defender's objective function in the proposed model is not only coverage-focused, but it also integrates an exposure-based metric to directly counter the intruder's penetration-oriented objective.

Many such protection models have been extended via a trilevel mathematical programming framework to account for an additional stage. Because such a framework is beyond what is necessary for the current study, we refrain from providing a complete review of this literature, but we refer an interested reader to the works of Brown

et al. (2006), San Martin (2007), Smith et al. (2007), Yao et al. (2007), Alderson et al. (2011), Liberatore et al. (2012), Yuan et al. (2014), and Lozano & Smith (2017). In a parallel to the aforementioned bilevel models, the majority of these works model the protection or fortification of sites, although a select few examine network components, in general.

Although related in their two-player, game theoretic structure, several attacker-defender models in the literature also adopt a bilevel mathematical programming model (e.g., see Wood, 1993; Washburn & Wood, 1995; Cormican et al., 1998; Lim & Smith, 2007; Lunday & Sherali, 2012). However, these attacker-focused frameworks do not notably inform the current work that adopts a defender-attacker sequence of decisions.

A plethora of multi-objective location modeling examples and applications exist in the literature. Badri et al. (1998) proposed a multi-objective model for the location of fire stations that incorporates 11 different strategic objectives. Raisanen & Whitaker (2005) determined where to place antennae in a cellular wireless network to maximize service while minimizing cost. Kulturel-Konak et al. (2007) considered a bi-objective approach to solve the manufacturing facility relayout problem, minimizing material handling costs and relayout costs. A model to determine the locations of park-and-ride facilities is developed by Farhan & Murray (2008) to cover as much potential demand as possible, while integrating new facilities as close as possible to major roadways in an existing transit system.

A majority of facility relocation problems in the literature are applied to the relocation of fire companies (Kolesar & Walker, 1974), ambulances (Brotcorne et al., 2003; Gong & Batta, 2007), and emergency vehicles (Gendreau et al., 2006). Many of these works have been extended from single-objective to multi-objective formulations as well. Sathe & Miller-Hooks (2005) set forth a model to locate military units,

police forces, and first responders, and to relocate idle units in response to an event, maximizing secondary coverage and minimizing cost. Melachrinoudis & Min (2000) presented a multi-objective application involving the relocation and phase-out of a combined manufacturing plant and warehousing facility. The location and relocation of mobile servers in a transportation network was considered by Berman & Rahnama (1985), wherein the authors sought to balance coverage, response time, and relocation costs. Recently, Paul et al. (2016) provided a multi-objective, maximal conditional covering location problem applied to the relocation of hierarchical emergency response facilities to respond to large-scale emergencies.

Traditional facility location models are focused on the coverage of specific demand points within an area of interest and do not address the need to prevent the passage of an adversary into friendly territory, which is the main concern for border security applications. However, a related field of research pertaining to the location of sensors in a Wireless Sensor Network (WSN) presents coverage models designed specifically for such a purpose. One of the three main coverage problems discussed in WSNs is *barrier coverage* (Cardei & Wu, 2006). In the context of WSNs, "a given belt region is said to be *k-barrier covered* with a sensor network if all crossing paths through the region are *k-covered*, where a crossing path is any path that crosses the width of the region completely" (Kumar et al., 2005). A path is said to be *k-covered* if it intersects at least k sensors' sensing ranges (Huang & Tseng, 2005).

As the defender, the goal of a barrier coverage model is to locate a set of sensors S such that some chosen measure of coverage is maximized. Alternatively, an attacker seeks to interdict or locate areas of the region where the value of the coverage measure is minimized. One such measure of coverage often used in WSN models is *exposure*. First introduced by Meguerdichian et al. (2001), exposure can informally be thought of as the "expected average ability of observing a target in the sensor field." More

formally, exposure is defined as "an integral of a sensing function that generally depends on distance from sensors on a path from a starting point p_S to destination point p_D" (Meguerdichian et al., 2001). Unlike some coverage metrics, the element of time is important for exposure, since the ability of a sensor to detect a target can improve as the sensing time (i.e., exposure) increases.

For a sensor s, the general sensing model S at an arbitrary point p is:

$$S(s,p) = \frac{\lambda}{[d(s,p)]^K}, \tag{49}$$

where $d(s,p)$ is the Euclidean distance between the sensor s and the point p, and positive constants λ and K are technology-dependent parameters (Meguerdichian et al., 2001). The parameter λ can be thought of as the energy emitted by a target, and K is an energy decay factor, typically ranging from 2 to 5 (Amaldi et al., 2008). The sensing function represents the energy received by a sensor s from the target p. Furthermore, the *exposure* of an object in the sensor field during the interval $[t_1, t_2]$ along the path $p(t)$ is defined by Meguerdichian et al. (2001) as:

$$E(p(t), t_1, t_2) = \int_{t_1}^{t_2} I\Big(F, p(t)\Big) \left| \frac{dp(t)}{dt} \right| dt, \tag{50}$$

wherein the sensor field intensity $I\big(F, p(t)\big)$ is implemented using an *All-Sensor Field Intensity* model or a *Closest-Sensor Field Intensity* model, depending on the application and types of sensors used. The *All-Sensor Field Intensity* model is a summation of the sensing function values (49) from target p to *all* sensors in the sensor network, defined as $I_A(F,p) = \sum_{i=1}^{n} S(s_i, p)$, whereas the *Closest-Sensor Field Intensity* model only utilizes the sensing function value of the *closest* sensor to the target (Meguerdichian et al., 2001).

Using the definition of exposure, Meguerdichian et al. (2001) presented an algo-

rithm to find the *minimal exposure path* in a sensor network. The algorithm first transforms the problem into a discrete domain utilizing a generalized grid approach and then creates an edge-weighted graph. The algorithm then applies Dijkstra's single-source shortest-path algorithm (Dijkstra, 1959) to find the minimal exposure path from the source point p_S to the destination point p_D. Meguerdichian et al. (2001) also extended this initial work by developing a localized minimal exposure path algorithm using Voronoi diagrams. We utilize the exposure coverage metric for border security in this paper since we are concerned with maximizing the coverage of an intruder's path across a sensor network.

Numerous solution techniques exist to solve multi-objective optimization and facility relocation problems, ranging from the Weighted Sum and ε-constraint Methods to genetic algorithms and other metaheuristics. The Weighted Sum Method involves selecting weights for each objective that represent their relative importance and subsequently optimizing the resulting weighted objective function (Ehrgott, 2006). However, prespecifying appropriate weights for each objective may be unrealistic, and the objectives may be incommensurable (Sherali & Soyster, 1983). Detailed surveys of systematic weight selection techniques are presented by Eckenrode (1965), Hobbs (1980), and Hwang & Yoon (2012). Similarly, the Lexicographic Method requires preemptively ranking the objectives in order of importance such that an incremental improvement in a particular objective preempts arbitrarily large improvements in the less important objectives (Sherali & Soyster, 1983). This method iteratively solves a sequence of single-objective problems, optimizing one objective at a time and assigning previously determined optimal objective function values as constraints (Ehrgott, 2006). Alternatively, one can develop preemptive weights for a single objective function that includes all objectives as shown by Sherali & Soyster (1983), but potential scaling issues in practice may induce premature termination in a commercial solver,

resulting in the identification of a solution that is not Pareto optimal. As such, herein we utilize the ε-constraint Method, which bounds the respective values for all but one of the objective function values while optimizing the remaining objective. The respective bounds may be iteratively relaxed (w.l.o.g.) with the corresponding identification of optimal solutions for each combination of bounds used to identify non-inferior solutions (Mavrotas, 2009). Additionally, goal programming has been applied to multi-objective optimization and facility relocation problems, such as in research conducted by by Min (1988), Bhattacharya et al. (1993), and Badri (1999). Goal programming requires specification of goals for each objective function, upon which the total absolute deviation from the goals is typically minimized (Marler & Arora, 2004). Lee & Olson (1999) provide a review of goal programming formulations and applications.

3.1.2 Major Contributions & Organization.

This paper provides the only known exposure-based solution to the heterogeneous sensor relocation problem, extending the work of Lessin et al. (2018a) to optimally respond to the incapacitation and/or degradation of sensors and their respective capabilities within a sensor network. Our multi-objective formulation and subsequent single-level reformulation captures system disruptions to the sensor network via model parameters developed herein. Our model also provides the defender-focused flexibility to specify minimum probabilities of protection for emplaced sensors and high-value asset locations, and specific capabilities of sensors via probability-of-coverage functions and transit speeds for each sensor type. Our modeling framework also allows the defender to quantify qualitative differences in sensor preferences in terms of which sensors the defender prefers to employ when interdicting an intruder.

Section 3.2 presents the bilevel mathematical formulation and a single-level refor-

mulation that enables the identification of non-inferior solutions on the Pareto frontier using a commercial solver. Section 3.3 provides a military air defense scenario as an illustrative borer security application of the model, and it details the test instance generation, presents solutions, and discusses the results of selected analyses. Section 3.4 summarizes our findings and suggests potential avenues for future research.

3.2 Model & Methodology

In this section, we present a mathematical programming formulation for the optimal relocation of sensors, following an attack. Given a specified set of surviving assets and a location-and-asset-type degradation, we determine the optimal layout that maximizes the minimum expected exposure of an intruder to prevent access across a defended border region, minimizes the maximum sensor relocation time, and minimizes the total number of sensors requiring relocation, while also ensuring adequate preferential coverage of high-value asset locations and a subset of the located sensors.

3.2.1 Assumptions.

We make several assumptions related to the defender's objectives and sensors. Regarding the objectives, we assume that, in addition to constructing a sensor network to inhibit an adversary traversing the border region, we also seek to minimize the maximum time required to relocate sensors, as well as minimize the number of sensors requiring relocation. Additionally, we desire protection of a specified set of high-value asset locations and a subset of the located sensors (e.g., the most valuable sensors). A minimum probability of protection is specified for each high-value asset location of interest and for each sensor type. We assume a given allocation of a heterogeneous set of sensors. For testing purposes, our problem instance includes a combination of

three types of sensors with varying capabilities.

In many instances, binary sensor coverage is unrealistic or unrepresentative of actual sensor capabilities. Rather, a probability of coverage exists for targets located at a given distance from a sensor location. As the distance from target to sensor increases, the probability of coverage decreases. Instead of assuming binary sensor coverage (i.e., covered/not covered), we implement a notional probability-of-coverage function for each of the heterogeneous sensor types, as a function of the distance from target to sensor.

Furthermore, we assume the defender's incoming threat is a single target with a known, constant velocity. Our model addresses a single intruder who will identify and traverse a single path through the border region. This assumption is valid because, although the identified optimal solution to our formulation identifies a single intrusion path, any alternative path taken by an intruder will yield an expected exposure that is the same or higher. Because our model seeks to identify the best relocation solution for the defender's sensors, we are not concerned with the specific path an intruder will traverse, merely the least expected exposure an intruder can attain via any of the paths. Within our model testing, we assume a constant velocity for the intruder. A variable velocity could be considered when computing expected exposure times for arc-sensor combinations, and the model set forth in Section **??** can be readily parameterized for such a case. The consideration of a variable intruder velocity would be appropriate to account for terrain (e.g., traveling faster when terrain does not mask an intruder from sensors) but, for testing on a terrain-agnostic instance herein, there is no compelling reason to consider it.

Moreover, we assume sensors that are attacked by the intruder are either completely incapacitated or their performance is degraded by a specified percentage. Relocating an incapacitated sensor will not recover its capability and is therefore not

considered for relocation in our model. However, we allow the relocation of sensors to sites of incapacitated sensors (i.e., a defender may move surviving sensors to sites where other sensors were destroyed by the intruder). Degraded sensors experience a proportional reduction in system effectiveness across the system's operating range but can be relocated to reduce the level of degradation.

To formulate instances of our model, we first tessellate the continuous planar space representing the border region via regular hexagons for computational tractability. Hexagonal tessellations are computationally easier to construct because they allow clustering in every direction and mitigate the directional restrictions to travel vis-à-vis other regular shapes (Yousefi & Donohue, 2004). Although we choose a uniformly-sized tessellation of the border region to evenly space the potential sensor relocation positions, this approach is not strictly required for our model; unequally-sized tessellations can be applied to vary the density of potential senor locations for situation-specific reasons (e.g., to align with the effects of instance-specific terrain).

Given this discretization of the solution space, we restrict the location of sensors to the centroid of each hexagon, whereas the edges of the hexagonal mesh comprise the induced network over which an intruder may traverse, traveling from artificial origination node o on the (w.l.o.g.) left side of the hexagonal grid to the artificial destination node d on the right. Moreover, as a defender-focused model, we are not concerned with the intruder's actions outside the defended border region of interest. We make no assumptions regarding the number or location of the intruder's final destination(s), other than their existence outside the defended border region by way of the artificial destination node d.

Lastly, given the state of today's intelligence capabilities, especially for various nation-states in defense-related applications, it is reasonable to assume that an intruder knows the location of sensors that a defender has emplaced, as well as their

capabilities. Likewise, a defender will have reasonable estimates for the capabilities of intruding targets. Together, this level of assumed intelligence on adversaries entails a perfect information game framework. With rapid advancements in persistent and effective intelligence, surveillance, and reconnaissance, we can also assume that adversaries will be aware of each other's previous decisions. Subject to the strength of this assumption, this framework constitutes a complete information game as well.

3.2.2 Model.

The following list of sets, parameters, and decision variables are used to formulate the mathematical programming models considered herein.

Sets:

T : the set of all types of sensors available to locate, indexed by t.

S : the set of all sites where sensors can be located, indexed by s.

$\bar{S}$: the set of all sites where sensors are initially located (i.e., $\bar{S} = \{s \mid x_s^t = 1, \forall s \in S, t \in T\}$), indexed by $\bar{s}$.

F : the set of all sites where high-value assets are located, indexed by f.

A : the set of arcs in the graph that are equidistant from adjacent potential sensor sites $s \in S$, and over which an intruding target can traverse, indexed by (i, j).

N : the set of all nodes at which arcs intersect and through which an intruding target can traverse, indexed by n.

$G = (N, A)$: the graph over which an intruding target will traverse, as induced by the set of potential sensor sites $s \in S$.

Parameters:

λ_s^t : the percent effectiveness of a sensor of type $t \in T$ located at site $s \in S$, due to intruder countermeasures. For example, if a type $t \in T$ sensor located at site $s \in S$ is degraded by 20%, then $\lambda_s^t = 0.8$.

w^t : the exposure weight for sensor type $t \in T$.

e_{ij}^{st} : the exposure time of a target traversing arc $(i, j) \in A$ to a sensor of type $t \in T$ located at site $s \in S$.

$d_{\bar{s}s}$: the Euclidean distance between sensor sites $\bar{s} \in \bar{S}$ and $s \in S$.

r^t : the transit speed of sensor type $t \in T$.

$v_{\bar{s}}^t$: 1 if a type $t \in T$ sensor is initially located at site $\bar{s} \in \bar{S}$, and 0 otherwise.

$z_{\bar{s}}^t$: 1 if the intruder incapacitates a type $t \in T$ sensor initially located at site $\bar{s} \in \bar{S}$, and 0 otherwise.

B^t : the maximum number of type $t \in T$ sensors the defender can locate.

p_{sp}^t : the probability that a sensor of type $t \in T$ located at site $s \in S$ can cover the point p.

C^f : the minimum probability of coverage required for each high-value asset location $f \in F$.

C^t: the minimum probability of coverage required for each located sensor of type $t \in T$.

Decision Variables:

$x_{\bar{s}s}^t$: 1 if the defender relocates a type $t \in T$ sensor from site $\bar{s} \in \bar{S}$ to site $s \in S$, and 0 otherwise.

y_{ij} : 1 if the intruder traverses arc $(i,j) \in A$, and 0 otherwise.

ψ_{max} : the maximum time (in hrs) required to complete sensor relocations.

Given our assumptions, the game theoretic view of this problem is that of a two-player, two-stage, zero-sum game with perfect and complete information. In the upper-level problem, the defender determines the locations of a set of heterogeneous sensors, given an intruder-induced incapacitation and degradation of a subset of the initially located sensors. Observing this decision, the intruder reacts in the lower-level problem by selecting arcs to traverse the region. The defender seeks to maximize the total expected weighted exposure of the intruder's least exposed path across the defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. The defender seeks to minimize the total expected weighted exposure of the least exposed path. Leveraging the aforementioned notation, we formulate the multi-objective, bilevel program **Multi-Objective Sensor Relocation Problem (MOSRP)**, alternatively denoted **Problem P1** herein, corresponding to this Stackelberg game as follows:

$$\textbf{P1}: \max_{\boldsymbol{x},\psi_{max}} \quad f(\boldsymbol{x},\boldsymbol{y},\psi_{max}) = \Big(f_1(\boldsymbol{x},\boldsymbol{y}), -f_2(\psi_{max}), -f_3(\boldsymbol{x})\Big) \tag{51}$$

$$\text{s.t.} \quad f_1(\boldsymbol{x},\boldsymbol{y}) = \sum_{(i,j)\in A} \Bigg(\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda_s^t w^t e_{ij}^{st} x_{\bar{s}s}^t \Bigg) y_{ij}, \tag{52}$$

$$f_2(\psi_{max}) = \psi_{max}, \tag{53}$$

$$f_3(\boldsymbol{x}) = \sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x_{\bar{s}s}^t, \tag{54}$$

$$\frac{d_{\bar{s}s}}{r^t} x_{\bar{s}s}^t \leq \psi_{max}, \forall \bar{s}\in\bar{S}, s\in S, t\in T, \tag{55}$$

$$\sum_{s\in S} x_{\bar{s}s}^t = v_{\bar{s}}^t - z_{\bar{s}}^t, \forall \bar{s}\in\bar{S}, t\in T, \tag{56}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} x_{\bar{s}s}^t = B^t - \sum_{\bar{s}\in\bar{S}} z_{\bar{s}}^t, \ \forall t\in T, \tag{57}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{t\in T} x^t_{\bar{s}s} \leq 1,\ \forall s \in S, \tag{58}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{sf}\Big)x^t_{\bar{s}s} \leq \ln\Big(1-C^f\Big),\ \forall f \in F, \tag{59}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S\setminus\{\hat{s}\}}\sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{s\hat{s}}\Big)x^t_{\bar{s}s} \leq \ln\Big(1-C^t\Big)x^t_{\bar{s}\hat{s}},\ \forall \hat{s} \in S, t \in T, \tag{60}$$

$$x^t_{\bar{s}s} \in \{0,1\},\ \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{61}$$

where $\boldsymbol{y}$ represents the optimal solution to the lower-level problem:

$$\min_{\boldsymbol{y}} \quad f_1(\boldsymbol{x},\boldsymbol{y}) \tag{62}$$

$$\text{s.t.} \quad \sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N\setminus\{o,d\}, \end{cases} \qquad \forall i \in N, \tag{63}$$

$$y_{ij} \geq 0,\ \forall (i,j) \in A. \tag{64}$$

The objective function (51) maximizes the total expected weighted exposure of the minimal exposure path (52), minimizes the maximum sensor relocation time (53), and minimizes the total number of relocated sensors (54). The expected weighted exposure of a target traversing a given arc $(i,j) \in A$ to sensors of type $t \in T$ relocated (i.e., $x^t_{\bar{s}s} = 1$) from site $\bar{s} \in \bar{S}$ to site $s \in S$ is represented by $\sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} \lambda^t_s w^t e^{st}_{ij} x^t_{\bar{s}s}$, where the λ^t_s-parameters account for the degradation of sensor capability due to intruder countermeasures. A sensor of type $t \in T$ located at site $s \in S$ experiences a $(1-\lambda^t_s)\times 100\%$ system degradation, which proportionally reduces the system effectiveness across a sensor's operational range.

The exposure weights w^t may be parameterized to account for qualitative differences in sensor effectiveness not captured by the quantitative differences inherent in

the sensor probability functions, p_{sp}^t. Qualitative differences in sensor performance may result from factors such as insufficient sensor operator training or operational technical complexity of a given sensor type. For example, the defender could specify exposure weights of 1.0, 0.5, and 0.2 for a model having three different sensor types, thereby affecting a relative preference over the set of sensors within the model formulation. Under this interpretation, the defender is half as effective at employing the second type of sensor against a target as compared to the first sensor type.

Constraint (55) provides lower bounds on the maximum relocation time, ψ_{max}. Constraint (56) ensures we can only relocate sensors that are initially located and not incapacitated. Constraint (57) determines the number of each type of sensor the defender can relocate. Constraint (58) prevents more than one sensor from being relocated to the same site. Constraint (59) ensures that all high-value asset locations receive the required coverage. The form of Constraint (59) results from a logarithmic transformation of the constraint:

$$1 - \prod_{s \in S} \prod_{t \in T} \left(1 - \lambda_s^t p_{sf}^t\right)^{x_{\bar{s}s}^t} \geq C^f, \ \forall f \in F,$$

wherein independence is assumed among the probabilities of coverage, p_{sf}^t, over sensor locations, $s \in S$, and sensor types, $t \in T$. (Implied is the assumption that $C^f < 1$, which is appropriate for this probabilistic metric wherein certain coverage is not attainable.) Likewise, Constraint (60) provides for the coverage of emplaced sensors by other sensors, as may be required by specific applications to protect valuable sensors. That is, for every site $\hat{s} \in S$, if a defender relocates a sensor of type $t \in T$ from site $\bar{s} \in \bar{S}$ to site $\hat{s} \in S$ (i.e., $x_{\bar{s}\hat{s}}^t = 1$), Constraint (60) requires a specified level of coverage, C^t, via the effects of *other* sensors the defender chooses to locate (i.e., $x_{\bar{s}s}^t, \forall \bar{s} \in \bar{S}, s \in S \setminus \{\hat{s}\}$). In contrast, if a defender does not relocate a sensor of type $t \in T$ from site $\bar{s} \in \bar{S}$ to site $\hat{s} \in S$ (i.e., $x_{\bar{s}\hat{s}}^t = 0$), then the constraint induces

no coverage requirement (i.e., an upper bound on the constraint that corresponds to $C^t = 0$). Constraint (61) enforces binary restrictions on the sensor relocation decision variables. The lower-level objective function (62) seeks to minimize the total expected weighted exposure of the intruder's minimal exposure path (52). Constraint (63) induces the flow balance constraints for the path from the intruder's point of origin, o, to destination point, d. Lastly, Constraint (64) is the non-negativity constraint associated with the minimal exposure path variables.

3.2.3 Methodology.

Instead of solving an MOSRP instance using a weighted sum or lexicographic approach, we utilize the ε-constraint method to identify a set of non-inferior solutions. We first reformulate Problem P1 (i.e., MOSRP) to **Problem P2** as follows:

$$\textbf{P2}: \max_{\boldsymbol{x},\psi_{max}} \min_{\boldsymbol{y}} \quad \sum_{(i,j)\in A} \left(\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda_s^t w^t e_{ij}^{st} x_{\bar{s}s}^t \right) y_{ij} \tag{65}$$

$$\text{s.t.} \quad \psi_{max} \leq \varepsilon_2, \tag{66}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x_{\bar{s}s}^t \leq \varepsilon_3, \tag{67}$$

$$\text{Constraints (55)} - \text{(61) and (63)} - \text{(64)}.$$

In this reformulation, we replaced the objective function (51) with the defender and intruder objectives of maximizing and minimizing the total expected weighted exposure of the minimal exposure path (52), respectively. We utilize Constraint (66) to bound our second objective, the minimization of the maximum sensor relocation time, to be no more than ε_2, a maximum relocation time. Likewise, Constraint (67) bounds our third objective, the minimization of the total number of sensor relocations, to be no more than ε_3, an allowed number of relocations.

Similar to Wood (1993), Colson et al. (2007), Amaldi et al. (2008), and Lessin et al. (2018a), we reformulate the bilevel Problem P2 by replacing the lower-level problem with its dual formulation. Treating the upper-level variables $x^t_{\bar{s}s}$ as parameters, the lower-level minimization problem becomes a shortest path problem in which the expected weighted exposure objective is minimized, subject to Constraints (63) and (64). Replacing the primal, lower-level problem with its dual formulation as represented in Equations (68)-(71),

$$\max_{\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{68}$$

$$\text{s.t.} \quad -\pi_i + \pi_j \leq \sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda^t_s w^t e^{st}_{ij} x^t_{\bar{s}s}, \ \forall (i,j) \in A, \tag{69}$$

$$\pi_o = 0, \tag{70}$$

$$\pi_i \text{ unrestricted}, \forall i \in N \setminus \{o\}, \tag{71}$$

where π_i is the dual variable associated with the i^{th} Constraint (63), we obtain the following single-level reformulation of Problem P2, denoted **Problem P3**:

$$\textbf{P3}: \max_{\boldsymbol{x},\psi_{max},\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{72}$$

$$\text{s.t.} \quad \psi_{max} \leq \varepsilon_2, \tag{73}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x^t_{\bar{s}s} \leq \varepsilon_3, \tag{74}$$

$$\frac{d_{\bar{s}s}}{r^t} x^t_{\bar{s}s} \leq \psi_{max}, \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{75}$$

$$\sum_{s\in S} x^t_{\bar{s}s} = v^t_{\bar{s}} - z^t_{\bar{s}}, \forall \bar{s} \in \bar{S}, t \in T, \tag{76}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} x^t_{\bar{s}s} = B^t - \sum_{\bar{s}\in\bar{S}} z^t_{\bar{s}}, \ \forall t \in T, \tag{77}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{t\in T} x^t_{\bar{s}s} \leq 1, \ \forall s \in S, \tag{78}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T}\ln\left(1-\lambda_s^t p_{sf}^t\right)x_{\bar{s}s}^t \le \ln\left(1-C^f\right),\ \forall f\in F, \tag{79}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S\setminus\{\hat{s}\}}\sum_{t\in T}\ln\left(1-\lambda_s^t p_{s\hat{s}}^t\right)x_{\bar{s}s}^t \le \ln\left(1-C^t\right)x_{\bar{s}\hat{s}}^t,\ \forall \hat{s}\in S, t\in T, \tag{80}$$

$$-\pi_i+\pi_j \le \sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T}\lambda_s^t w^t e_{ij}^{st} x_{\bar{s}s}^t,\ \forall (i,j)\in A, \tag{81}$$

$$\pi_o = 0, \tag{82}$$

$$\pi_i \text{ unrestricted}, \forall i\in N\setminus\{o\}, \tag{83}$$

$$x_{\bar{s}s}^t\in\{0,1\},\ \forall \bar{s}\in\bar{S}, s\in S, t\in T. \tag{84}$$

Problem P3 provides a baseline, single-level model to determine the relocation of a heterogeneous set of surviving sensors following an attack to maximize the exposure of the intruder's least exposed path, minimize the maximum time required for any sensor relocation, and minimize the number of sensor relocations. We initially set $\varepsilon_2 = \max\limits_{\bar{s}\in\bar{S},s\in S}\{d_{\bar{s}s}\}/\min\limits_{t\in T}\{r^t\}$ and $\varepsilon_3 = \sum\limits_{\bar{s}\in\bar{S}}\sum\limits_{t\in T}(v_{\bar{s}}^t - z_{\bar{s}}^t)$ as upper bounds on the second and third objectives, respectively. Given these values for ε_2 and ε_3, we solve Problem P3 to determine the maximum minimal exposure solution. We can then set ε_2 and ε_3 to the values from the initial optimal solution to Problem P3 to tighten Constraints (73) and (74). By iteratively decreasing the value of ε_2 and/or ε_3 and re-solving Problem P3, we develop a set of non-inferior solutions on the Pareto frontier that identify the trade-offs between the competing objectives of maximizing the intruder's minimal exposure, minimizing the maximum sensor relocation time, and minimizing the total number of sensor relocations.

3.3 Testing, Results, & Analysis

We explore the Pareto frontier of efficient solutions by iteratively solving the reformulated Problem P3 for an illustrative instance of Problem P1 on a 3.2 GHz PC with 6 GB of RAM, using the commercial solver IBM ILOG CPLEX 12.7. The following subsections present a selected border security application, discuss test instance generation, and provide numerical results of the testing.

3.3.1 Representative Scenario for Air Defense of a Border Region.

We demonstrate the applicability of the MOSRP (51)-(64) formulation and our solution approach to the border security problem with an illustrative air defense test instance. This application is representative of the general problem class in that a decision maker has a set of sensors (i.e., air defense batteries), some of which have been incapacitated (i.e., rendered inert by kinetic or non-kinetic attack) or degraded (e.g., made less capable due to electronic countermeasures), and wherein the decision maker seeks to relocate the sensors to optimize multiple, competing objectives, at least one of which relates directly to the goal of the intruder.

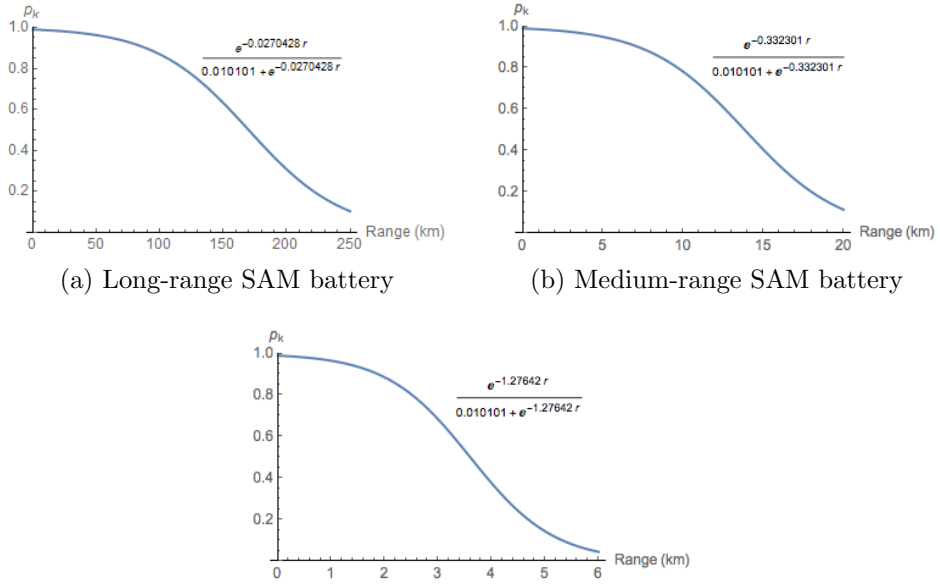
Adopting the viewpoint of a defender, we seek to relocate surviving ground-based assets of an Integrated Air Defense System (IADS) following the incapacitation and degradation of a subset of the air defense assets. We assume a given allocation of long-range (e.g., SA-21 Growler), medium-range (e.g., SA-22 Greyhound), and short-range (e.g., SA-24 Grinch) Surface to Air Missile (SAM) batteries (Foss & O'Halloran, 2014). Although these weapons do not represent the full range of SAM technologies a defender could encounter, they are representative of the various threats that countries employing antiaccess/area-denial (A2/AD) strategies are likely to possess and employ (Schmidt, 2016).

Given a 600 km long by 520 km wide border region with an initial IADS layout

consisting of two long-range, five medium-range, and five short-range SAM batteries (i.e., $B^t = [2, 5, 5]$), we seek to optimally relocate surviving air defense assets following the incapacitation of two medium-range and one short-range SAM batteries, as well as a single degradation attack resulting in a 10% decrease in system effectiveness for the two long-range assets. We require protection of three high-value assets located at $F = \{(500, 100), (350, 400), (500, 550)\}$, with minimum probabilities of protection of $C^f = [0.75, 0.5, 0.5]$, respectively. We also require the long-range SAM batteries to be protected with a minimum probability of 0.5 (i.e., $C^t = [0.5, 0, 0]$). Additionally, we assume transit speeds of $r^t = [50, 70, 90]$ km/hr for the long-range, medium-range, and short-range SAM batteries, respectively. For this baseline instance, we further assume equal exposure weights (i.e., $w^t = [1, 1, 1]$), an intrusion aircraft velocity of 1,800 km/hr (i.e., $|v| = 1,800$ km/hr), and a 30 km spacing between potential SAM battery locations.

We also specify a probability-of-kill function for each SAM battery type, based on representative SAM battery capabilities found in Foss & O'Halloran (2014). The construction of the probability-of-kill curves for instances herein is notional but representative; we utilized a logit model for the probability of kill as a function of the range, assuming a probability of 0.99 for a range of zero and a probability of between 0.04 and 0.11 at the maximum effective range (r_{max}) (Foss & O'Halloran, 2014). To artificially induce different interceptor performance, we specified a probability of 0.55 at 65% of r_{max} for the long-range SAM batteries, a probability of 0.2 at 90% of r_{max} for the medium-range SAM batteries, and a probability of 0.5 at 60% of r_{max} for the short-range SAM batteries. The probability-of-kill function for each SAM battery type is depicted in Figure 5. These functions are used to calculate the exposure values for each arc resulting from the hexagonal tessellation of the border region.

In addition to the aforementioned SAM battery types, the long-range assets re-



(a) Long-range SAM battery

(b) Medium-range SAM battery

(c) Short-range SAM battery

Figure 5. Probability-of-kill curve for each SAM battery type

quire separate targeting and tracking radars to engage a target. For this illustrative scenario, we assume that each SAM battery possesses the required radar coverage to engage intruding targets. We make this assumption to avoid an increase in model complexity necessary to include the radar location decisions within the current framework. Alternatively, the radar location problem could be solved as a separate covering location problem (or relocation problem, as appropriate); given a SAM battery relocation solution from our formulation, one could subsequently solve a radar location problem to determine the optimal radar locations.

Furthermore, we assume for this study the defender's incoming threat consists only of aircraft, as opposed to a wide range of threats not limited to, but including, cruise missiles and ballistic missiles. This assumption determines the coverage capabilities for each SAM battery instead of requiring the model to account for a myriad of target types. This assumption is made to demonstrate a solution for an illustrative scenario, but it is appropriate for two reasons. First, a single intruder is considered

as representative of a strike package, a technique for organizing multiple attacking aircraft in a single sortie (e.g., see McLemore, 2010). Second, any alternative path taken by an intruder will yield an exposure that is not less than the identified minimal exposure path.

Moreover, we assume IADS assets that are attacked by the intruder are either completely incapacitated via kinetic or non-kinetic effects or degraded due to effects such as, but not limited to, electronic warfare. Relocating an incapacitated asset will not recover its capability and is therefore not considered for relocation in our model. However, we allow the relocation of surviving assets to sites of incapacitated assets. Degraded assets experience a proportional reduction in system effectiveness across the system's operating range.

The adoption of a two-dimensional network for aircraft traversal implicitly assumes an intruder flies below (or at) a given altitude ceiling. Such an assumption is reasonable if either (a) the intruder utilizes such tactics within their doctrinal framework or (b) if the ground-based air defense assets are complemented within the IADS by interceptor aircraft that operate at high altitudes. Given the precepts of Energy-Maneuverability Theory (Boyd et al., 1966), the doctrinal employment of interceptors conducting Combat Air Patrols (CAPs) requires the aircraft to patrol at (and begin maneuvers from) relatively high altitudes, reinforcing the division of effort among air- and ground-based assets within an IADS by altitude and, hence, the validity of the two-dimensional modeling assumption.

Test instances for our analysis were generated by first constructing a hexagonal grid with potential sensor (i.e., SAM battery) locations positioned at the center of each hexagon. Neighboring hexagon centers are located at a defender-specified distance (in km) from each other. Herein, we adopt a distance of 30 km for initial testing in Section 3.3.2. The granularity of grid construction is easily adapted to suit a given

situation or modeler's desired fidelity.

The intruder's goal is to traverse the border region from an artificial origination node, o, on the (w.l.o.g.) Western side of the border region to an artificial destination node, d, on the (w.l.o.g.) Eastern side of the border region, where these nodes are connected by arcs to the leftmost and rightmost hexagon arc nodes, respectively.

3.3.2 Results.

Figure 6 depicts the initial IADS layout for this instance found by solving the Maximin Exposure Problem (MmEP) as presented by Lessin et al. (2018a).

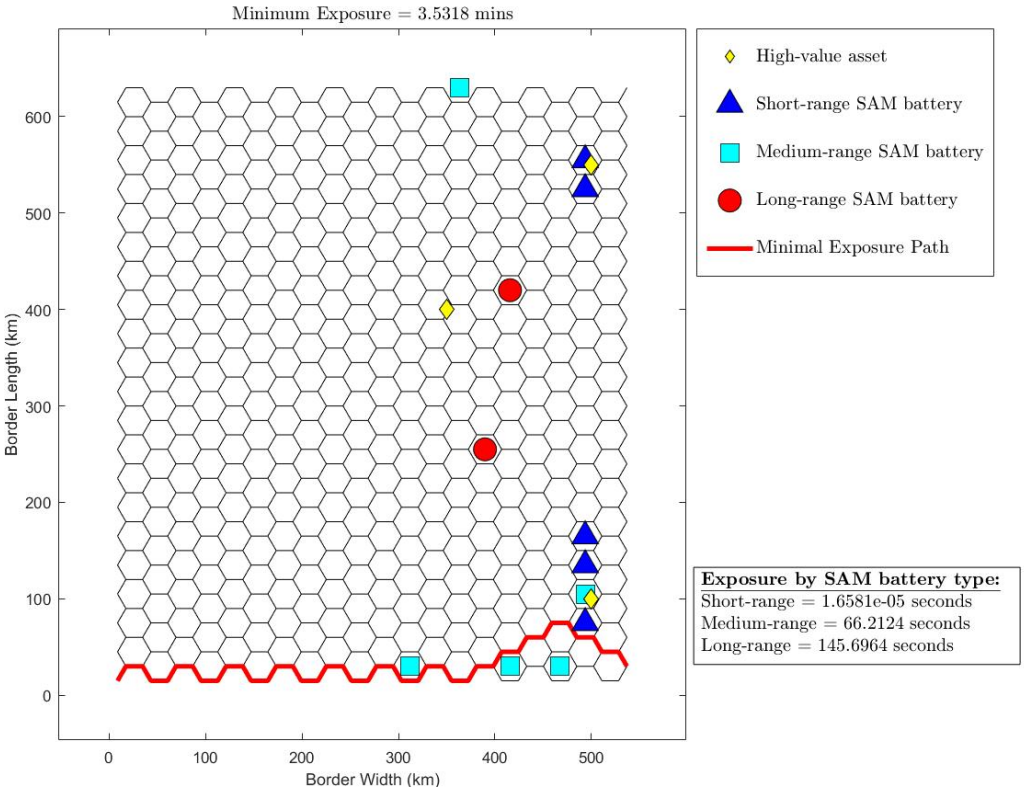


Figure 6. Initial IADS layout

Considering the initial IADS layout, we determine which assets to incapacitate and where to locate specific degradation effects, based on SAM battery type. For this study, we select three IADS assets (two medium-range and one short-range SAM

battery) in the Southeast corner of the border region to incapacitate. Additionally, a representative degradation event (e.g., electronic warfare) is created to affect the performance of long-range SAM batteries located within the shaded hexagons near the center of the border region, ranging from 40% (i.e., assets located at the center of the affected area) to 10% degradation in capability (e.g., the two long-range assets located at the outermost ring of the affected area). Figure 7 shows the incapacitated assets and degradation locations for the initial IADS layout.

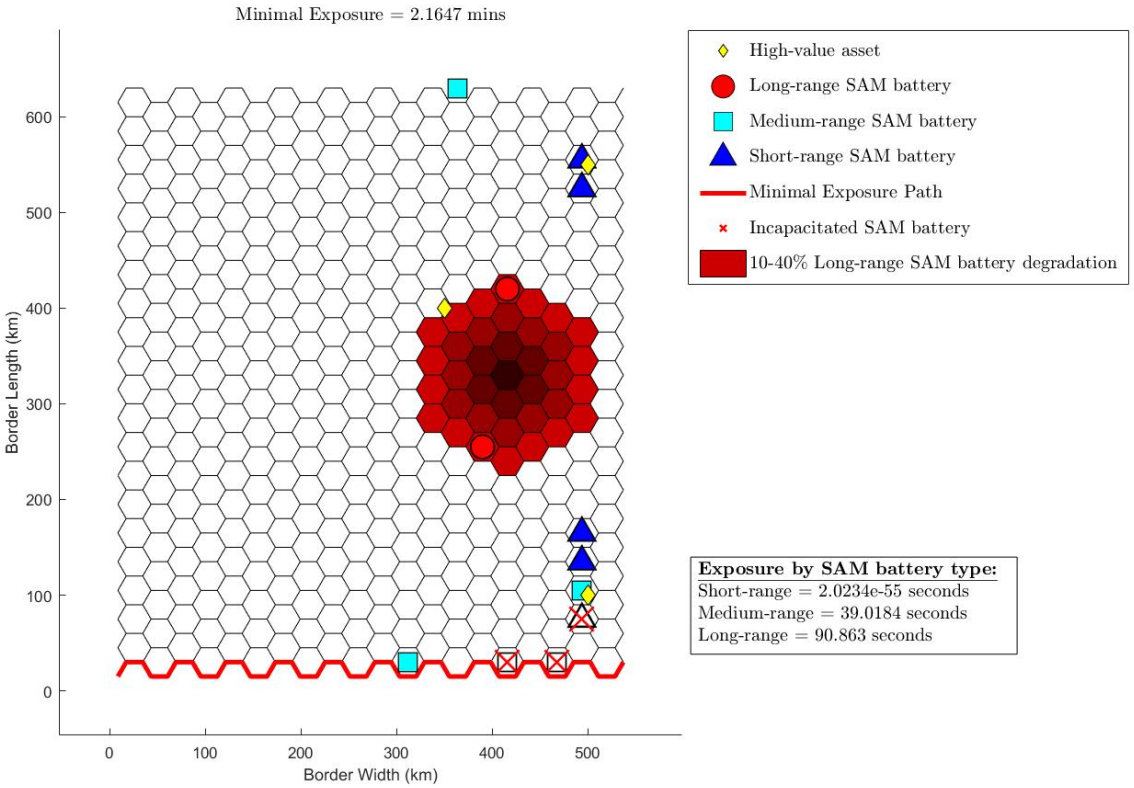


Figure 7. Initial IADS layout before asset relocations showing incapacitated and degraded assets

Assuming no assets are relocated, the incapacitation and degradation of the affected SAM batteries decreases the intruder's expected minimal exposure from 3.5318 minutes to 2.1647 minutes, representing a 38.7% reduction in exposure to the IADS assets accumulated during traversal of the minimal exposure path. However, this solution is no longer feasible for the defender because the long-range asset degradation

reduces the probability of coverage for the long-range assets to 0.4676, which is less than the required coverage probability of 0.5 (i.e., $C^t = [0.5, 0, 0]$).

We can determine an upper bound on the intruder's minimal exposure following the relocation of surviving IADS assets by solving Problem P3, placing no restrictions on the maximum relocation time or the number of assets allowed to relocate (i.e., ε_2 and ε_3 are unrestricted, respectively). This relocation solution is depicted in Figure 8 and yields a minimal exposure of 2.4939 minutes, allowing the defender to recover up to 24.1% of the minimal exposure lost due to the intruder's incapacitation and degradation efforts.

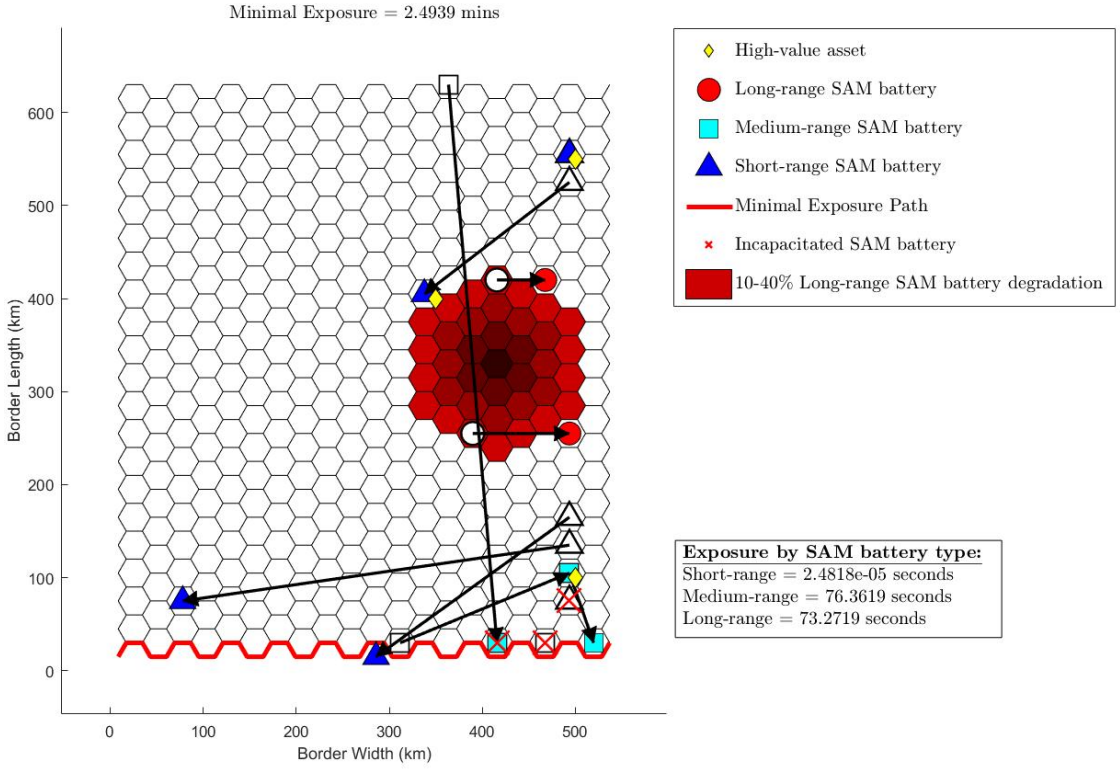


Figure 8. Multi-Objective Sensor Relocation Problem solution with $\varepsilon_2, \varepsilon_3$ unrestricted

Note that, at optimality, this solution requires $f_2 = 8.6$ hours and $f_3 = 8$ asset relocations for the defender to accomplish. However, this asset relocation solution may be impractical due to operational time constraints or physical restrictions on

IADS asset mobility. Therefore, it is important to examine the trade-offs between the competing objectives and to identify more practical relocation options.

Given that a defender may need to accomplish all asset relocations in a limited amount of time (e.g., $\varepsilon_2 \leq 4$ hours) or may not be able to relocate as many surviving assets (i.e, $\varepsilon_3 \leq 9$), we analyzed the defender's maximization of the intruder's minimal exposure over numerous $(\varepsilon_2, \varepsilon_3)$-combinations. Specifically, we solved Problem P3 with $\varepsilon_2 = \{1, 1.5, 2, ..., 4\}$ hours and $\varepsilon_3 = \{1, 2, ..., 9\}$ asset relocations, with results depicted in Figure 9, to generate a subset of operationally feasible solutions for the $(\varepsilon_2, \varepsilon_3)$-combinations, among which a subset of non-inferior solutions can be identified (i.e., denoted Points A-E in Figures 9 and 10).

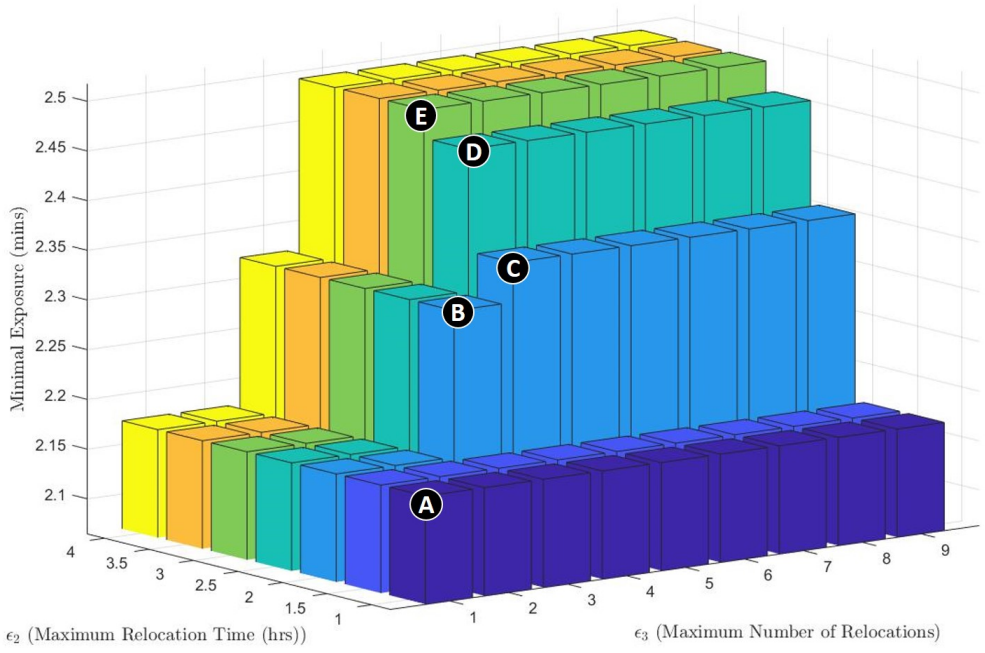


Figure 9. Optimal minimal exposure values for discretized $(\varepsilon_2, \varepsilon_3)$-combinations

We note that, hereafter, solutions denoted as non-inferior or Pareto optimal are only assured to hold this property within the granularity of the $(\varepsilon_2, \varepsilon_3)$-values exam-

ined for the solution space. It is possible that a higher fidelity examination of the $(\varepsilon_2, \varepsilon_3)$-values will identify the existence of additional non-inferior solutions and/or solutions that (weakly) dominate those identified as Pareto optimal within the context of this examination. However, a higher resolution mapping is not practical for the current application, the defense against an aerial threat, as the solutions depicted in Figures 9 and 10 required approximately 39 hours of CPU time to compute. Such a defense plan is typically conducted over several days or weeks as part of the contingency planning process prior to adversarial engagements. Accordingly, the approximately 39 hours required to identify the 63 solutions over a realistic solution set of values for both ε_2 and ε_3 and to explore the Pareto frontiers depicted in Figures 9 and 10 is not computationally prohibitive for the application of interest. Moreover, should computational effort be of concern, upper bounds on ε_2 and ε_3 may be further constrained, resulting in the need to solve fewer instances for the same discrete step size of the bounded objectives (i.e., f_2 and f_3). Alternatively, a larger step size for one or both of the objectives' bounds may suffice; depending on the application of interest, a single, operationally-acceptable upper bound on ε_3 may be justified and affixed, requiring an examination of only a two-dimensional Pareto front corresponding to a set of ε_2-values.

Alternatively, we can examine the relocation solution for each $(\varepsilon_2, \varepsilon_3)$-combination in terms of the percentage of recoverable minimal exposure, as illustrated in Figure 10. These values represent the percentage of the maximum recoverable minimal exposure (i.e., 2.4939 minutes) the defender can achieve for a given $(\varepsilon_2, \varepsilon_3)$-combination, where the baseline recovery is the optimal objective value associated with the solution resulting from the minimum feasible relocation time (i.e., $f_2 = 0.6$ hours) and the minimum feasible number of relocated assets (i.e., $f_3 = 1$ relocation); this baseline recovery is represented by the $(\varepsilon_2, \varepsilon_3) = (1, 1)$ relocation solution, denoted as Point A

in Figures 9 and 10, which results in a minimal expected exposure of 2.1733 minutes, as depicted in Figure 11.

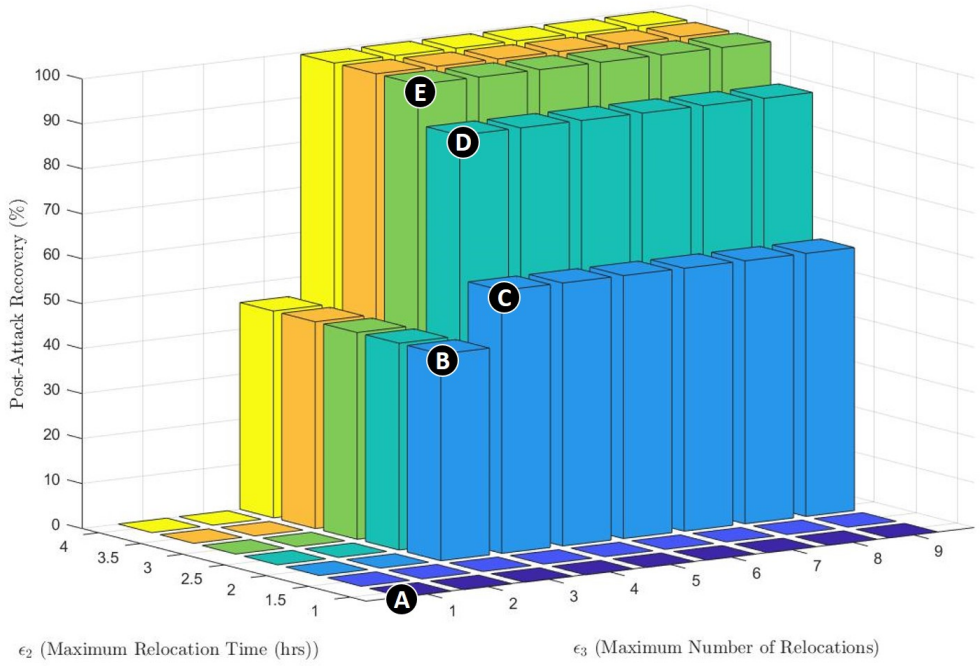


Figure 10. Percentage of maximum recoverable minimal exposure achievable for $(\varepsilon_2, \varepsilon_3)$-combinations

As the bounds on the maximum asset relocation time (ε_2) and/or the number of asset relocations (ε_3) increase, the intruder's minimal exposure and the defender's percentage of maximum recoverable minimal exposure increases, as seen in Figures 9 and 10, respectively. This behavior highlights the conflicting nature of the defender's objectives. As the defender, we can use either of these plots to make an informed asset relocation decision. Specifically, by inspecting Figure 9 we see that the five solutions represented by the $(\varepsilon_2, \varepsilon_3)$-combinations $(1, 1), (2, 3), (2, 4), (2.5, 4)$, and $(3, 4)$, and respectively labeled Points A-E, are the Pareto optimal solutions for this test instance, with solution-specific results presented in Table 5. Considering the operational constraints on relocation time and the number of asset relocations, the Pareto

optimal solutions in Table 5 represent the defender's best response to the intruder's incapacitation and degradation efforts, given the chosen ε_2 discretization.

Table 5. Pareto optimal solutions

Point	(ε_2,ε_3)	Minimal Exposure (minutes)	Percentage of Minimal Exposure Recovered (%)
A	(1,1)	2.1733	N/A*
B	(2,3)	2.3207	46.0
C	(2,4)	2.3608	58.5
D	(2.5,4)	2.4637	90.6
E	(3,4)	2.4923	99.5

*Minimum feasible relocation solution

Note that for a given pair of Pareto optimal solutions $(\varepsilon_2, \varepsilon_3) = (a, b)$ and $(\varepsilon_2, \varepsilon_3) = (c, d)$ where $a < c$ or $b < d$, it is not necessarily true that $(a, b) \subset (c, d)$. That is, the asset relocations associated with solution (a, b) may not be a subset of the asset relocations for solution (c, d). For example, the long-range asset relocation in Figure 11 for Pareto optimal solution Point A is not included in the asset relocations for Pareto optimal solution Point D in Figure 12. Therefore, one cannot consider a subset of Pareto optimal solutions (e.g., with $a < c$ or $b < d$) as a series of solutions to be implemented in turn. Rather, a defender must select one solution appropriate for a reasonable $(\varepsilon_2, \varepsilon_3)$-combination, given the tactical situation.

Although the unrestricted $(\varepsilon_2, \varepsilon_3)$-solution depicted in Figure 8 results in the maximum expected exposure for the intruder, the defender may decide to implement one of the alternative Pareto optimal solutions. For example, during active combat, the defender may need to reposition unaffected air defense batteries as fast as possible to satisfy the minimum coverage requirements of the high-value assets and long-range SAM batteries. In this situation, the defender would implement the $(\varepsilon_2, \varepsilon_3) = (1, 1)$ relocation solution Point A to recover a feasible defense posture requiring only one, 36-minute, long-range SAM battery relocation. However, if more time is available

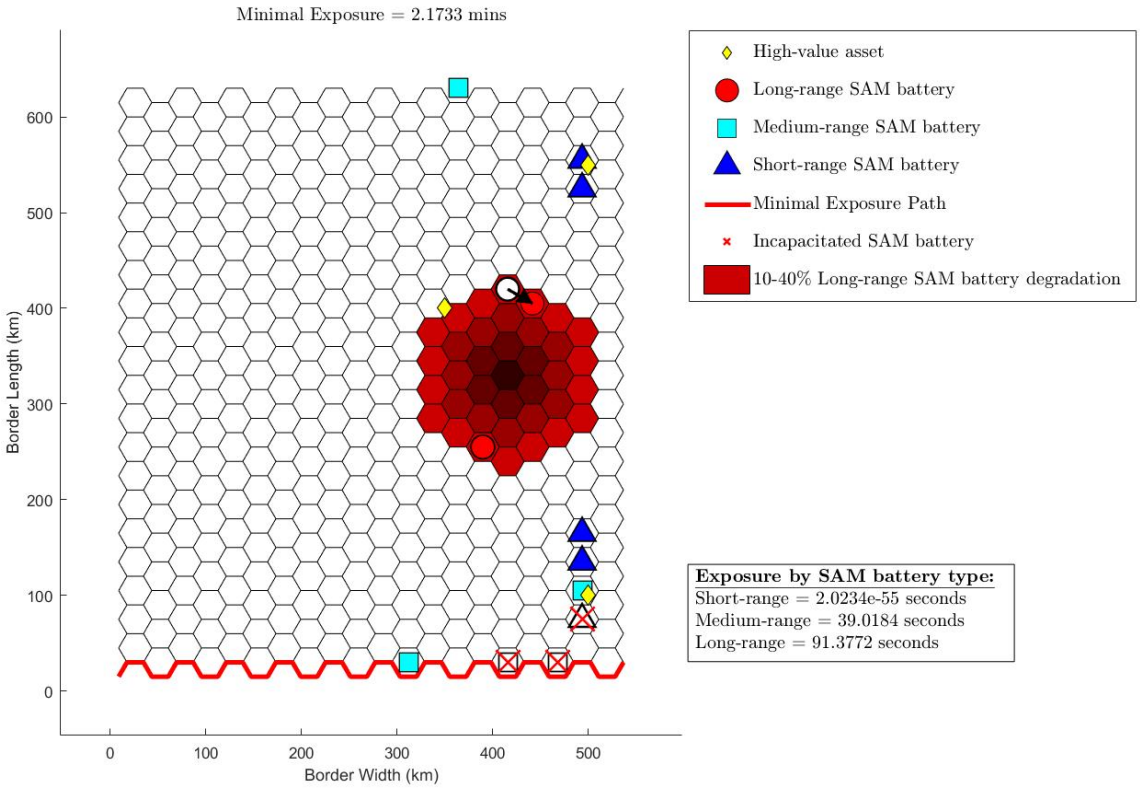


Figure 11. Pareto optimal relocation solution with $(\varepsilon_2, \varepsilon_3) = (1, 1)$

or a higher level of coverage is desired, the defender may choose to implement the $(\varepsilon_2, \varepsilon_3) = (2.5, 4)$ relocation solution Point D for example, which requires $f_2 = 2.14$ hours and $f_3 = 4$ relocations and results in a minimal exposure of 2.4637 minutes. This solution (shown in Figure 12) achieves 90.6% of the maximum recoverable minimal exposure time with a 75.1% reduction in relocation time and a 50.0% reduction in the number of assets relocated.

However, since the defender seeks to minimize the number of relocations, the $(\varepsilon_2, \varepsilon_3) = (2, 3)$ Pareto optimal relocation solution Point B offers the largest increase in the intruder's minimal exposure per unit increase in allowable relocation time, as evidenced in Table 5 and Figure 10.

It is worth noting that practical instances may exist wherein the defender is restricted to a specific $(\varepsilon_2, \varepsilon_3)$-combination that results in no feasible relocation solution

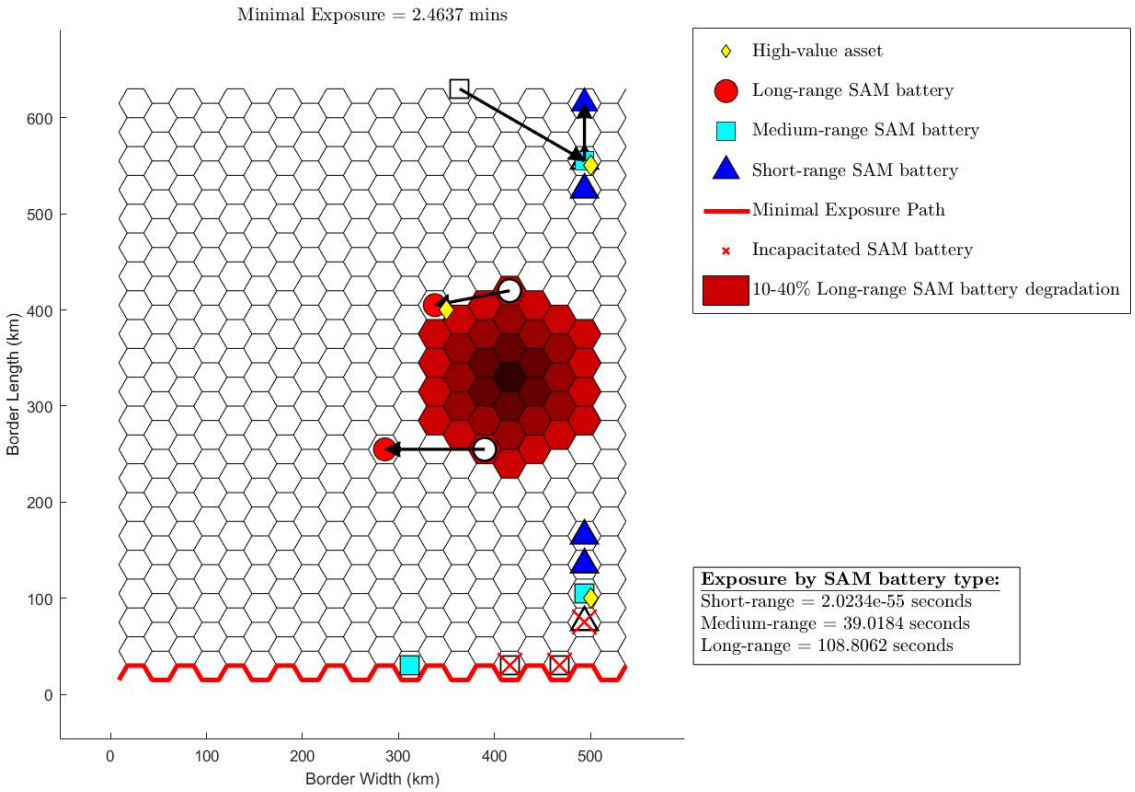


Figure 12. Pareto optimal relocation solution with $(\varepsilon_2, \varepsilon_3) = (2.5, 4)$

because the defender may be unable to provide the minimum required coverage for either SAM batteries or high-value assets (i.e., C^t or C^f, respectively). In such instances, the defender has several recourses within the MOSRP modeling framework, to include incrementally reducing the infeasible minimum required coverage level until a feasible solution can be identified or removing the coverage requirement altogether. The resulting solutions, although not satisfying the defender's initial coverage requirements, would yield feasible relocation solutions for realistic, operationally-constrained scenarios.

3.3.3 Sensitivity Analysis.

Anecdotal testing found that the required computational effort to solve a single instance of Problem P3 for the illustrative scenario was most sensitive to the granu-

larity of the tessellation imposed upon the border region. Given this research requires the solution of multiple instances via the ε-constraint Method to explore the Pareto frontier for a single scenario, we examine herein the effect of tessellation granularity on the required computational effort to solve for the Pareto frontier in Figures 9 and 10, for each of four potential SAM battery spacing levels (i.e., 25, 30, 40, and 50 km). Reported in Table 6 is the effect of SAM battery spacing on the problem size for an instance of Problem P3 and the required computation time for the entire Pareto frontier, consisting of 63 instances of Problem P3, as determined by the $(\varepsilon_2, \varepsilon_3)$-discretization adopted in Figures 9 and 10.

Table 6. Effect of potential SAM battery location spacing on instance size and computation time.

Distance Between Potential SAM Batteries (km)	Number of Potential SAM Battery Locations	Number of Arcs	Number of Decision Variables	Number of Constraints	Pareto Frontier Computation Time (min)
25	600	1,875	23,285	49,683	10,011.6
30	420	1,323	16,005	34,171	2,374.8
40	210	675	8,445	18,043	319.1
50	156	507	6,389	13,659	132.1

Figure 13 depicts the effect of SAM battery spacing on the number of decision variables and constraints for an instance of Problem P3 for the illustrative scenario presented in Section 3.3.1. As the distance between potential SAM battery locations decreases, the numbers of decision variables and constraints for an instance of Problem P3 both increase exponentially.

Several instance parameters notably affect the respective numbers of decision variables and constraints for an instance of Problem P3. The number of arcs (i.e., $|A|$) in the induced hexagonal tessellation, G, as it affects the number of constraints in (81), is linearly bounded by the number of potential sensor locations (i.e., $|S|$). More specifically, the regular hexagonal tessellation yields $\lim_{|S|\to 1} |A| = 6|S|$ and $\lim_{|S|\to\infty} |A| = 3|S|$. More notable is the effect of $|S|$ on the size of the instance, as manifest both via the

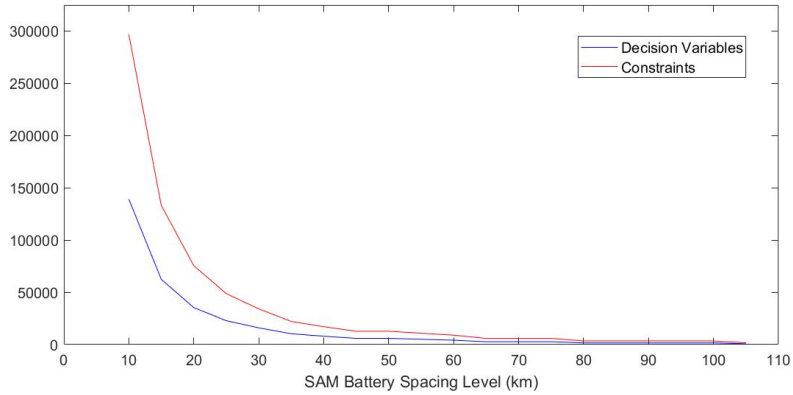


Figure 13. Effect of SAM battery spacing level on problem size.

correspondingly indexed decision variables and several constraints within Problem P3.

However, the magnitude of $|S|$ results from the granularity adopted for the tessellation. Let d_{hex} and A_{BR} respectively denote the distance between centroids of adjacent hexagons (i.e., hexagons sharing a side) and the area of the defended border region. For the corresponding area of $\left(\sqrt{3}\ d_{hex}^2\right)/2$ for each identical hexagon, the border region requires a minimum of

$$LB_{hex} = \left(\frac{2\sqrt{3}}{3}\right)\frac{A_{BR}}{d_{hex}^2}, \tag{85}$$

hexagons in the tessellation (i.e., $|S|$). Figure 14 illustrates the effect of both d_{hex} and A_{BR} on LB_{hex} over a range of values that includes the scenario examined in Section 3.3.1.

More readily visible in Figure 14 than depicted via Equation (85) is the contrast between the linear effect of A_{BR} and the greater-than-linear effect of d_{hex} on the lower bound on $|S|$. The latter relationship explains the rapid increase in Pareto frontier computation times reported in Table 6. Therefore, the defender must be mindful when selecting the sensor spacing level, especially for instances in which computation

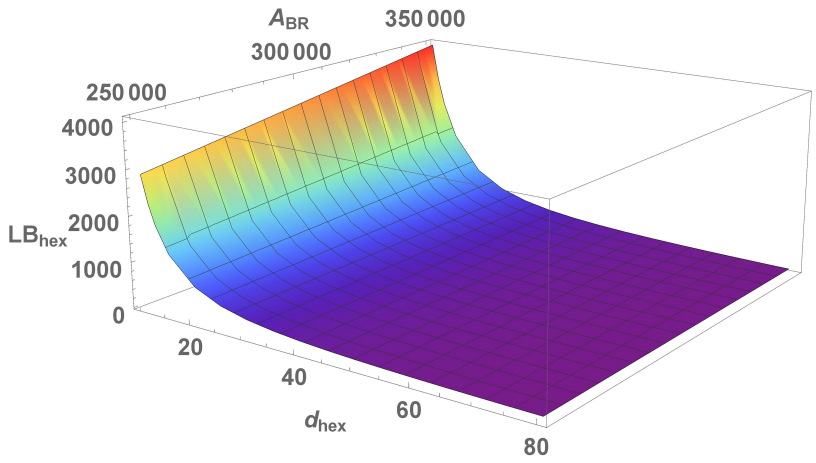


Figure 14. Effect of d_{hex} and A_{BR} on LB_{hex}

time is of utmost importance.

3.4 Conclusions & Future Work

Given an initial sensor network and two subsets of sensors that have been incapacitated or degraded, we demonstrated the ability to formulate and solve a multi-objective, bilevel optimization model to relocate surviving sensors to respectively maximize an intruders minimal expected exposure to traverse a defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. Adopting the ε-constraint method, we developed a single-level reformulation that enabled the identification of non-inferior solutions on the Pareto frontier and, consequently, identified trade-offs between the competing objectives. Our formulation also allows the defender to specify minimum coverage requirements for high-value asset locations and emplaced sensors. Additionally, our modeling framework provides the defender with the ability to quantify qualitative differences in sensor preferences in terms of which sensors the defender prefers to employ when interdicting an intruder. We showcased our formulation and solution approach via a representative air defense asset relocation instance.

Of note, our model assumes that the intruder threat corresponds to an attempt to penetrate the border region that is deliberate rather than persistent. To wit, the defender seeks to maximize an intruder's minimum expected exposure upon the completion of sensor relocation, while minimizing both the number of relocations and the time required to complete the relocations. The degradation in sensor coverage during the relocations is not examined, as our solution approach presumes the defender can make an assumption about the maximum time until an intrusion attempt may occur, during which a degradation to sensor coverage is acceptable. Should a reader seek to apply the model to scenarios wherein degraded coverage is of concern, an iterative application of our model with small bounds on the allowable time for relocations can generate a suitable sequence of successive asset relocations. Alternatively, a temporal relocation model could be adapted to enable the defender to implement time-phased sensor relocation strategies. Compared to an iterative application of the model examined in this study, a temporal model would seek to identify a global optimal solution of phased relocations, yet may be computationally cumbersome for practical implementation.

Future research could be conducted to increase model fidelity by accounting for the placement of hierarchical sensors and by considering multiple intruder targets with varying capabilities. We could also incorporate location-specific sensor probability-of-coverage functions, thereby accounting for effects such as terrain and altitude. Alternative intruder path selection metrics could also be considered to examine model robustness. Lastly, this model, combined with an effective solution methodology, could be embedded within a two-player, three-stage game, wherein an attacker seeks to identify effective interdiction and degradation efforts, respectively, to predict a defender's likely sensor relocation responses with the intent of penetrating the border region. More specifically, for a given sensor layout, the intruder would first select a

bounded number of sensors to incapacitate and locations for a fixed number of sensor degradation effects. Observing the intruder's decision, the defender would then react in the second stage by determining the optimal relocation of the surviving sensors and, observing the defender's relocation decision, the intruder would subsequently react in the third stage by selecting the optimal intrusion path.

IV. A Multi-objective, Trilevel Sensor Network Intrusion Problem

4.1 Introduction

We live in an age of heightened security in both the physical and virtual world (Wong, 2016; Dennison et al., 2018; Jansen, 2018). Existing networks have implemented increasingly advanced methods for detecting intrusive and illicit attacks that threaten network integrity (Alles et al., 2016; Ashford, 2016). Construction of new networks focuses heavily on secure network design to prevent or mitigate network disruptions (Bodeau & Graubart, 2017; Crosman, 2018; James, 2018). Such disruptions can be intentional (e.g., terrorist or cyber attacks) or unintentional (e.g., power outages due to severe weather). Given these trends, attackers have been forced to reassess their strategies to decrease their likelihood of detection and increase their probability of achieving a successful attack. This research focuses on the attack of defended sensor networks, from the attacker's perspective.

To decrease the probability of detection, an intelligent attacker must carefully examine and understand the physical (or virtual) layout of a defender's sensors and their relationship to the attacker's available penetration paths through the defended network or region. However, an attacker may not be limited to simple observation of a defended network prior to identifying a path to traverse. Rather, an attacker may have the ability to conduct an attack on some or all of the defender's sensors as well as regions within the defended network to decrease the likelihood of detection and consequently increase the probability of successful network penetration. To wit, an attacker may be capable of incapacitating (i.e., physically destroying or rendering completely ineffective) or degrading (i.e., decreasing the effectiveness) some subset of the defender's sensors.

Sensor networks are increasingly interconnected. With information regarding individual sensor health and status readily available across a network through an Internet-of-Things (IoT) approach, defenders now have the ability to quickly react to changes within the network. Therefore, if sensors are destroyed or degraded, a defender may have near-instant knowledge of such events and be able to react to improve the network's security. For example, in a physical network, a defender may choose to relocate sensors to more advantageous locations.

However, knowledge of network changes is not necessarily limited to the defender. Technological advances in adversarial surveillance and reconnaissance may allow an attacker to observe the defender's adjustments to the sensor network. This level of intelligence allows the attacker to make a more informed decision regarding the ultimate attack strategy.

This paper provides a solution method for the sensor network intrusion problem to respectively incapacitate a subset of the defender's sensors and degrade a subset of the defender's network, after which the surviving sensors may be relocated, and the attacker subsequently determines the optimal intrusion path through the defender's sensor network. We address this problem via the formulation and solution of a trilevel, multi-objective optimization model utilizing new heuristics developed herein. Given an initial layout of heterogeneous sensors, the attacker first incapacitates (i.e., interdicts) a subset of sensors and degrades (i.e., partially interdicts) the effectiveness of another subset of sensors, wherein an incapacitation is enduring for an affected sensor whereas a degradation is limited to a geographic region and is based on sensor type (i.e., moving an incapacitated sensor does not recover its capability, but moving a degraded sensor out of an affected region can improve the sensor's effectiveness). We then determine the defender's optimal response to these events by relocating the surviving sensors, considering multiple, competing objectives. Specif-

ically, the defender seeks to maximize the attacker's minimal expected exposure to traverse the defended border region, minimize the maximum sensor relocation time, minimize the total number of sensors requiring relocation, and minimize the under coverage of high-value assets and emplaced sensors. After the defender's sensor relocations, the attacker selects the intrusion path that minimizes the expected exposure to the defender's sensors.

4.1.1 Literature Review.

The modeling efforts in this paper represent an amalgamation of work from various fields of study, including, but not limited to, facility location and relocation, interdiction modeling, network intrusion, Wireless Sensor Networks (WSNs), trilevel programming, multi-objective optimization, and goal programming.

The foundation of the modeling examined in this research is derived from the published facility location literature. Schilling et al. (1993) presented a detailed overview of covering problems in facility location. They classified models as either a Set Covering Problem (SCP) or a Maximal Covering Location Problem (MCLP), where coverage is either required or optimized, respectively. The MCLP was first introduced by Church & ReVelle (1974) to maximize the amount of demand covered within a specified service distance by locating a fixed number of facilities. White & Case (1974) extended the work of Church & ReVelle (1974) by considering equal weights on all demand points. Church (1984) later introduced the MCLP on a planar surface using Euclidean and rectilinear distance measures, where potential facility locations are no longer discrete (and finite). For a more recent review of covering problems in facility location, see Farahani et al. (2012).

One of the main assumptions of the MCLP is that coverage is binary. That is, a demand point is either fully covered or not covered by a located facility. However,

this assumption is often unrealistic. Berman & Krass (2002) extended the MCLP to the Generalized Maximal Covering Location Problem (GMCLP), allowing for "partial coverage of customers, with the degree of coverage being a non-increasing step function of the distance to the nearest facility." Additionally, Berman et al. (2003) extended the GMCLP by way of a gradual covering decay model wherein the authors define two critical distances; within the lower distance demand points are completely covered, whereas demand points beyond the further distance receive no coverage. For demand points within the critical distances, coverage gradually decreases from full coverage to no coverage. Drezner et al. (2004) solved the gradual covering problem on a planar surface. Although the coverage radius is typically an exogenously determined parameter, Suzuki & Drezner (2003) and Berman et al. (2009) considered the variable radius problem, treating the coverage radii as decision variables. Instead of demand points receiving coverage from the single nearest facility, Berman et al. (2009) developed a cooperative cover model in which each facility transmits a "signal" that decays over distance, and the amount of coverage provided at each demand point is aggregated across all facilities. Most recently, Colombo et al. (2016) proposed a Multimode Covering Location Problem which locates a fixed number of facilities of varying types, with limits on the number of co-located facilities. For demand coverage considered in this paper and presented in the models that follow, the defender employs a cooperative, multimode, gradual-covering decay framework.

Interdiction models can be thought of as a natural extension of facility location models with a leader-follower framework, wherein the leader (i.e., the attacker) seeks to destroy and/or degrade a subset of nodes (i.e., facilities) or arcs, and the follower subsequently seeks to optimize a given objective function (e.g., maximizing flow or minimizing traversal distance). Wollmer (1964) was the first to model the interdiction of a fixed number of arcs to maximize the reduction in the maximum flow between

an origin and destination node pair across a network. Interdiction using the minimum cost network flow model was also examined by Fulkerson & Harding (1977) and Golden (1978), allowing for partial interdiction of arcs. Node interdiction was considered by Corley Jr & Chang (1974) and Whiteman (1999) to respectively interdict a fixed number of vital network nodes and select the optimal set of military targets. Motivated by the desire to disrupt drug smuggling traffic, Wood (1993) and Washburn & Wood (1995) developed bilevel models to respectively minimize the maximum flow of drug traffic and maximize the probability of detecting an evader. Cormican et al. (1998) extended this work by considering a stochastic network interdiction model to minimize the expected maximum flow through a network when interdiction successes are binary random variables. Lim & Smith (2007) developed complete and partial arc interdiction models on multicommodity flow networks, wherein an attacker destroys a set of network arcs to minimize the maximum profit that can be obtained from shipping commodities across the network. Examining various forms of superadditive synergy effects of arc interdiction resources, Lunday & Sherali (2012) solved the network interdiction problem of minimizing the maximum flow between two network nodes, where the net interdictive effect of the resources on a given arc may be greater than the sum of their independent effects. In a more recent work, Rashidi et al. (2018) proposed an attacker-defender model to suppress the spread of wildfires, for which they develop and test a decomposition algorithm to solve the corresponding bilevel program.

Although related in their two-player, game theoretic structure, defender-attacker models have focused on identifying and protecting critical infrastructure assets from intentional and unintentional disruptions (e.g., see Brown et al., 2006; Qiao et al., 2007; Scaparra & Church, 2008; Cappanera & Scaparra, 2011; Losada et al., 2012; Bricha & Nourelfath, 2013; Aliakbarian et al., 2015). However, these defender-focused

frameworks do not notably inform the current work because the problem considered herein features a defender who seeks to relocate assets following an attack, rather than identify or protect vulnerable assets from a future attack. Moreover, the defender's objective function in the proposed model is not only coverage-focused; it also considers a metric to directly counter the intruder's penetration-oriented objective.

Most of the facility location and network interdiction models, including those previously mentioned, feature objective functions that focus on maximizing flow, minimizing path length, or minimizing the probability of detection. However, the objective functions for the models developed in this study adopt an exposure-based metric found more commonly in a related field of research pertaining to the location of sensors in a Wireless Sensor Network (WSN). First introduced by Meguerdichian et al. (2001), exposure can be thought of informally as the "expected average ability of observing a target in the sensor field." More formally, exposure is defined as "an integral of a sensing function that generally depends on distance from sensors on a path from a starting point p_S to destination point p_D" (Meguerdichian et al., 2001). Unlike some coverage metrics, the element of time is important for exposure because the ability of a sensor to detect a target can improve as the sensing time (i.e., exposure) increases.

For a sensor s, the general sensing model S at an arbitrary point p is:

$$S(s,p) = \frac{\lambda}{[d(s,p)]^K}, \tag{86}$$

where $d(s,p)$ is the Euclidean distance between the sensor s and the point p, and positive constants λ and K are technology-dependent parameters (Meguerdichian et al., 2001). The parameter λ can be thought of as the energy emitted by a target, and K is an energy decay factor, typically ranging from 2 to 5 (Amaldi et al., 2008). The sensing function represents the energy received by a sensor s from the target p.

Furthermore, the *exposure* of an object in the sensor field during the interval $[t_1, t_2]$ along the path $p(t)$ is defined by Meguerdichian et al. (2001) as:

$$E(p(t), t_1, t_2) = \int_{t_1}^{t_2} I\Big(F, p(t)\Big) \left| \frac{dp(t)}{dt} \right| dt, \tag{87}$$

wherein the sensor field intensity $I\big(F, p(t)\big)$ is implemented using an *All-Sensor Field Intensity* model or a *Closest-Sensor Field Intensity* model, depending on the application and types of sensors used. The *All-Sensor Field Intensity* model is a summation of the sensing function values (86) from target p to *all* sensors in the sensor network, defined as $I_A(F, p) = \sum_{i=1}^{n} S(s_i, p)$, whereas the *Closest-Sensor Field Intensity* model only utilizes the sensing function value of the *closest* sensor to the target (Meguerdichian et al., 2001).

Using the definition of exposure, Meguerdichian et al. (2001) presented an algorithm to find the *minimal exposure path* in a sensor network. The algorithm first transforms the problem into a discrete domain utilizing a generalized grid approach and then creates an edge-weighted graph. The algorithm next applies Dijkstra's single-source shortest-path algorithm (Dijkstra, 1959) to find the minimal exposure path from the source point p_S to the destination point p_D. Meguerdichian et al. (2001) extended this initial work by developing a localized minimal exposure path algorithm using Voronoi diagrams. We utilize the exposure coverage metric since the attacker is concerned with incapacitating and/or degrading the defender's sensors to minimize the defender's coverage of the attacker's penetration path across the sensor network.

The modeling framework developed herein combines an upper-level interdiction model with a bilevel, defender-attacker (i.e., facility relocation-network intrusion) model. This framework ultimately requires the adoption of a trilevel programming formulation. Although many of the bilevel attacker-defender problems have been

extended to include an additional first-stage defender problem (e.g., see Brown et al., 2006; San Martin, 2007; Smith et al., 2007; Yao et al., 2007; Alderson et al., 2011; Liberatore et al., 2012; Yuan et al., 2014; Lozano & Smith, 2017), there are few, if any, attacker-defender-attacker (ADA) models in the literature. In a defender-attacker-defender (DAD) framework, the defender first determines which facilities to fortify to minimize future damage. In the second level, the attacker selects the most damage-inducing elements to attack, and the defender reacts to the destruction in the third level to minimize the resulting damage to the system. Alternatively, in a proposed ADA framework, the attacker acts first to determine the most damage-inducing elements to attack. The defender then responds to the attack in the second level to minimize the effectiveness of the attack. Observing the defender's response, the attacker makes a final decision in the third level to optimize a specific objective function. Within the DAD framework, the defender is often referred to as a system operator in the third level. By comparison, within an ADA model, the attacker could be considered the *system exploiter*, using the defender's system against their will for the attacker's advantage. For example, in a network model, the attacker could seek to penetrate the defender's network in the third stage, while minimizing the probability of being detected.

In a trilevel, two-player, ADA scenario, it is unlikely that the attacker and defender seek to optimize the same objective function (albeit from opposite perspectives). Either player may seek to optimize objectives that are of no concern to the other. As such, this necessitates the implementation of a multi-objective programming approach at one or more stages of the decision space. Numerous solution techniques exist to solve multi-objective optimization and facility relocation problems, ranging from the Weighted Sum (Ehrgott, 2006) and ε-constraint (Mavrotas, 2009) Methods to genetic algorithms (Holland, 1975) and other metaheuristics. The Weighted

Sum Method involves selecting weights for each objective that represent their relative importance and subsequently optimizing the resulting weighted objective function (Ehrgott, 2006). However, prespecifying appropriate weights for each objective may be unrealistic, and the objectives may be incommensurable (Sherali & Soyster, 1983). Detailed surveys of systematic weight selection techniques are presented by Eckenrode (1965), Hobbs (1980), and Hwang & Yoon (2012). Similarly, the Lexicographic Method requires preemptively ranking the objectives in order of importance such that an incremental improvement in a particular objective preempts arbitrarily large improvements in the less important objectives (Sherali & Soyster, 1983). This method iteratively solves a sequence of single-objective problems, optimizing one objective at a time and assigning previously determined optimal objective function values as constraints (Ehrgott, 2006). Alternatively, one can develop preemptive weights for a single objective function that includes all objectives as shown by Sherali & Soyster (1983), but potential scaling issues in practice may induce premature termination in a commercial solver, resulting in the identification of a solution that is not Pareto optimal. As such, herein we utilize the ε-constraint Method, which bounds the respective values for all but one of the defender's multiple objective function values while optimizing the remaining objective. The respective bounds may be iteratively relaxed, without loss of generality (w.l.o.g.), with the corresponding identification of optimal solutions for each combination of bounds used to identify non-inferior solutions (Mavrotas, 2009).

Additionally, goal programming has been applied to multi-objective optimization and facility relocation problems, such as in research conducted by Min (1988), Bhattacharya et al. (1993), and Badri (1999). Goal programming requires specification of goals for each objective function, upon which the total absolute deviation from the goals is typically minimized (Marler & Arora, 2004). Lee & Olson (1999) provide

a review of goal programming formulations and applications. The heuristic solution approaches we develop apply a preemptively weighted goal programming approach to maximize the defender's preeminent exposure-based objective while simultaneously minimizing the failure to satisfy relatively less important coverage goals.

This research specifically builds upon and extends the work of Lessin et al. (2018a,b). In their initial work, Lessin et al. (2018a) developed a bilevel mathematical programming model to locate a heterogeneous set of sensors to maximize the minimum exposure of an intruder's penetration path through a defended region. In a subsequent work, given an initial sensor layout and two subsets of the sensors that have been respectively incapacitated or degraded, Lessin et al. (2018b) formulated and solved a defender-attacker, multi-objective, bilevel optimization model to relocate the surviving sensors subject to multiple, competing objectives. Specifically, the defender seeks to maximize an intruder's minimal expected exposure to traverse a defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. The two previous avenues of research inform the second and third levels of the ADA modeling framework developed herein.

4.1.2 Major Contributions & Paper Organization.

This paper provides the only known attacker-defender-attacker solution to the heterogeneous sensor network intrusion problem, extending the work of Lessin et al. (2018a,b) to optimally incapacitate a subset of the defender's sensors and degrade a subset of the defender's network to ultimately determine the attacker's optimal penetration path through the defended network. A trilevel, multi-objective formulation and subsequent bilevel reformulation is developed, the latter of which is solved via new heuristics. Our model allows flexibility for defender-imposed minimum probabilities of protection for emplaced sensors and high-value asset locations and considers

specific capabilities of sensors via probability-of-coverage functions and transit speeds for each sensor type. Our model also permits the defender to quantify qualitative differences in sensor preferences in terms of which sensors the defender prefers to employ when interdicting an attacker.

Section 4.2 presents a trilevel mathematical programming formulation in which an attacker respectively identifies a subset of the defender's heterogeneous sensors to incapacitate and a subset of the defender's network to degrade, subject to budget constraints; a defender subsequently relocates their sensors to maximize the attacker's minimal exposure, minimize the maximum relocation time, minimize the maximum number of sensors requiring relocation, and minimize the under coverage of high-value assets and emplaced sensors; in the third level, the attacker selects an optimal intrusion path through the defendor's sensor network. Section 4.3 presents a bilevel reformulation and new heuristics. Section 4.4 details the representative scenario used to illustrate the solution approach, presents solutions attained via the respective heuristics, and discusses the results of selected analyses. Section 4.5 summarizes our findings and suggests recommendations for future research.

4.2 Model & Methodology

In this section, we present a trilevel mathematical programming formulation for the optimal intrusion of a heterogeneous sensor network. Given a sensor layout, the attacker first determines the optimal subset of sensors to incapacitate and the optimal subset of the defender's network to degrade to minimize the expected weighted exposure of the resulting minimal exposure path through the defended region. Observing the attacker's decision, the defender reacts by relocating surviving sensors to maximize the minimum expected weighted exposure of an attacker to prevent access across a defended border region, minimize the maximum sensor relocation time, minimize

the total number of sensors requiring relocation, and minimize the under coverage of high-value assets and emplaced sensors. Lastly, the attacker determines the minimal exposure path through the region.

4.2.1 Assumptions.

With respect to the attacker's objectives, we assume that the attacker is solely focused on the intrusion metric; the damage affected to a defender's sensors is a means to that end, not an objective to be optimized. We also assume that the attacker will use all assets budgeted for incapacitation and degradation, respectively; effectiveness is of paramount importance, whereas efficiency is not.

We also make several assumptions related to the defender's objectives and sensors. Regarding the objectives, we assume that, in addition to constructing a sensor network to inhibit an adversary traversing the border region, the defender also seek to minimize the maximum time required to relocate sensors, minimize the number of sensors requiring relocation, and minimize the under coverage of high-value assets and emplaced sensors (e.g., the most valuable sensors). Minimum probabilities of desired protection are specified for each high-value asset location of interest and for each sensor type. We assume the defender has a given initial layout of heterogeneous sensors; for testing purposes, we consider a combination of three types of sensors with varying capabilities.

For many applications binary sensor coverage is unrealistic or unrepresentative of actual sensor capabilities. Rather, a probability of coverage exists for targets located at a given distance from a sensor location. As the distance from target to sensor increases, the probability of coverage decreases. Instead of assuming binary sensor coverage (i.e., covered/not covered), we assume a probability-of-coverage function for each of the heterogeneous sensor types, as an explicit function of the distance from

target to sensor, which we parameterize for testing in Section 4.4 using notional, synthetic sensor data.

Furthermore, we assume the defender's incoming threat is a single target with a known, constant velocity. Our model addresses a single attacker who will identify and traverse a single path through the border region. This assumption is valid because, although the identified optimal solution to our formulation identifies a single intrusion path, any alternative path taken by an attacker will yield an expected exposure that is the same or higher. The defender is not concerned with the specific path an attacker will traverse, merely the least expected exposure an attacker can attain via *any* of the paths. Within our model testing, we assume a constant velocity for the attacker. A variable velocity could be considered when computing expected exposure times for arc-sensor combinations, and we now comment on how this can be applied. Such an approach would be appropriate to account for terrain (e.g., traveling faster when terrain does not mask an attacker from sensors) but, for testing on a terrain-agnostic instance herein, there is no compelling reason to consider a variable attacker velocity.

Similarly, our model assumes that the attacker threat corresponds to an attempt to penetrate the border region that is deliberate rather than persistent. The degradation in sensor coverage during the relocations is not examined, as our solution approach presumes the defender can make an assumption about the time until an intrusion may occur, during which a degradation to sensor coverage is acceptable.

Moreover, we assume sensors that are incapacitated by the attacker are rendered completely ineffective. Relocating an incapacitated sensor will not recover its capability, and so our model does not consider the relocation of incapacitated sensors. Alternatively, sensors that are degraded by the attacker experience a decrease in effectiveness as a function of the distance between the sensor and the degradation location, wherein the decrease in coverage capability is also dependent upon the spe-

cific sensor type. Unlike incapacitated sensors, degraded sensors can be relocated to reduce the level of degradation due to the adjusted proximity of the sensor to the geographic center of the degradation attack. Moreover, we allow the relocation of degraded sensors to sites at which other sensors have been incapacitated.

To formulate instances of our model, we first tessellate the continuous planar space representing the border region via regular hexagons for computational tractability. Hexagonal tessellations are computationally easier to construct since they allow clustering in every direction and mitigate the directional restrictions to travel that are more prevalent when using other regular shapes (e.g., square, rhombus, triangle), as discussed by Yousefi & Donohue (2004). Although we chose a uniformly-sized tessellation of the border region to evenly space the potential sensor relocation positions, this approach is not strictly required; unequally-sized tessellations can be used to vary the density of potential senor locations for situation-specific reasons (e.g., to align with the effects of instance-specific terrain).

Given this discretization of the solution space, we restrict the location of sensors to the centroid of each hexagon, whereas the edges of the hexagonal mesh comprise the induced network over which an attacker may traverse, traveling from artificial origination node o on the (w.l.o.g.) left side of the hexagonal grid to the artificial destination node d on the right. Moreover, we are not concerned with the attacker's actions outside the defended border region of interest; we make no assumptions regarding the number or location of the attacker's final destination(s), other than their existence outside the defended border region by way of the artificial destination node d.

Lastly, given the state of today's intelligence capabilities, especially for various nation-states in defense-related applications, it is reasonable to assume that an attacker knows the locations of sensors a defender has emplaced, as well as their ca-

pabilities. Likewise, a defender will have reasonable estimates for the capabilities of intruding targets. Together, these respective levels of assumed intelligence on adversaries makes the game a perfect information game. With rapid advancements in persistent and effective intelligence, surveillance, and reconnaissance, we can also assume that adversaries will be aware of each other's previous decisions. Subject to the strength of this assumption, this model constitutes a complete information game as well.

4.2.2 Model Formulation.

The following list of sets, parameters, and decision variables are used to formulate the mathematical programming models considered herein.

Sets:

T : the set of all types of sensors available to locate, indexed by t.

S : the set of all potential sites where sensors can be located, indexed by s.

$\bar{S}$: the set of all sites where sensors are initially located (i.e., $\bar{S} = \{s \mid x_s^t = 1, \forall s \in S, t \in T\}$), indexed by $\bar{s}$.

K : the set of all potential sites where sensor degradation attacks can be centered, indexed by k.

F : the set of all sites where high-value assets are located, indexed by f.

A : the set of arcs in the graph that are equidistant from adjacent potential sensor sites $s \in S$, and over which an intruding target can traverse, indexed by (i, j).

N : the set of all nodes at which arcs intersect and through which an intruding attacker can traverse, indexed by n.

$G = (N, A)$: the graph over which an intruding attacker will traverse, as induced by the set of potential sensor sites $s \in S$.

Parameters:

w^t : the exposure weight for sensor type $t \in T$.

e_{ij}^{st} : the exposure time of a target traversing arc $(i, j) \in A$ to a sensor of type $t \in T$ located at site $s \in S$.

τ^t: the degradation power constant for sensors of type $t \in T$, where $\tau^t \in \mathbb{R}$.

d_{sp} : the Euclidean distance between site $s \in S$ and site p.

θ : the degradation decay factor, where $\theta \in \mathbb{R}^+$.

ζ^t : the maximum number of sensors of type $t \in T$ the attacker can incapacitate (i.e., render completely ineffective) via kinetic or non-kinetic measures.

Δ : the maximum number of degradation attacks the attacker can employ.

r^t : the transit speed of sensor type $t \in T$.

$x_{\bar{s}}^t$: 1 if a type $t \in T$ sensor is initially located at site $\bar{s} \in \bar{S}$, and 0 otherwise.

B^t : the number of initially located defender sensors of type $t \in T$.

p_{sp}^t : the probability that a sensor of type $t \in T$ located at site $s \in S$ can cover the point p.

C^f : the minimum probability of coverage desired for each high-value asset location $f \in F$.

C^t: the minimum probability of coverage desired for each located sensor of type $t \in T$.

Decision Variables:

$z_{\bar{s}}^t$: 1 if the attacker incapacitates a type $t \in T$ sensor initially located at site $\bar{s} \in \bar{S}$, and 0 otherwise.

δ_k : 1 if the attacker centers a sensor degradation attack at site $k \in K$, and 0 otherwise.

λ_s^t : the percent effectiveness of a sensor of type $t \in T$ located at site $s \in S$, due to degradation attacks. For example, if a type $t \in T$ sensor located at site $s \in S$ is degraded by 20%, then $\lambda_s^t = 0.8$.

$x_{\bar{s}s}^t$: 1 if the defender relocates a type $t \in T$ sensor from site $\bar{s} \in \bar{S}$ to site $s \in S$, and 0 otherwise.

ψ_{max} : the maximum time (in hrs) required to complete sensor relocations.

y_{ij} : 1 if the attacker traverses arc $(i, j) \in A$, and 0 otherwise.

Given our assumptions and leveraging the aforementioned notation, we formulate the multi-objective, trilevel **Sensor Network Intrusion Problem (SNIP)** as follows:

$$\textbf{SNIP}: \min_{\boldsymbol{z},\boldsymbol{\delta},\boldsymbol{\lambda}} \quad f_1(\boldsymbol{x}, \boldsymbol{y}) = \sum_{(i,j)\in A} \left(\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda_s^t w^t e_{ij}^{st} x_{\bar{s}s}^t \right) y_{ij} \tag{88}$$

$$\text{s.t.} \quad \lambda_s^t = 1 - \min\left\{ \sum_{k\in K} \frac{\tau^t}{\left(d_{sk}\right)^\theta} \delta_k, 1 \right\}, \forall s \in S, t \in T, \tag{89}$$

$$\sum_{\bar{s}\in\bar{S}} z_{\bar{s}}^t \leq \zeta^t, \forall t \in T, \tag{90}$$

$$\sum_{k\in K} \delta_k \leq \Delta, \tag{91}$$

$$z_{\bar{s}}^t \in \{0, 1\}, \ \forall \bar{s} \in \bar{S}, t \in T, \tag{92}$$

$$\delta_k \in \{0,1\},\ \forall k \in K, \tag{93}$$

$$\max_{\boldsymbol{x},\psi_{max},u^f,u^{\hat{s}t}} \quad f(\boldsymbol{x},\boldsymbol{y},\psi_{max},u^f,u^{\hat{s}t}) = \cdots$$

$$\cdots = \Big(f_1(\boldsymbol{x},\boldsymbol{y}), -f_2(\psi_{max}), -f_3(\boldsymbol{x}), -f_4(u^f,u^{\hat{s}t})\Big) \tag{94}$$

$$\text{s.t.} \quad f_2(\psi_{max}) = \psi_{max}, \tag{95}$$

$$f_3(\boldsymbol{x}) = \sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x^t_{\bar{s}s}, \tag{96}$$

$$f_4(u^f,u^{\hat{s}t}) = \sum_{f\in F} u^f + \sum_{\hat{s}\in S} \sum_{t\in T} u^{\hat{s}t}, \tag{97}$$

$$\frac{d_{\bar{s}s}}{r^t} x^t_{\bar{s}s} \le \psi_{max}, \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{98}$$

$$\sum_{s\in S} x^t_{\bar{s}s} = x^t_{\bar{s}} - z^t_{\bar{s}}, \forall \bar{s} \in \bar{S}, t \in T, \tag{99}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} x^t_{\bar{s}s} = B^t - \sum_{\bar{s}\in\bar{S}} z^t_{\bar{s}},\ \forall t \in T, \tag{100}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{t\in T} x^t_{\bar{s}s} \le 1,\ \forall s \in S, \tag{101}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{sf}\Big) x^t_{\bar{s}s} + o^f - u^f = \ln\Big(1-C^f\Big),$$

$$\forall f \in F, \tag{102}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\hat{s}\}} \sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{s\hat{s}}\Big) x^t_{\bar{s}s} + o^{\hat{s}t} - u^{\hat{s}t} = \cdots$$

$$\cdots = \sum_{\bar{s}\in\bar{S}} \ln\Big(1-C^t\Big) x^t_{\bar{s}\hat{s}}, \forall \hat{s} \in S, t \in T, \tag{103}$$

$$x^t_{\bar{s}s} \in \{0,1\},\ \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{104}$$

$$o^f, u^f \ge 0,\ \forall f \in F, \tag{105}$$

$$o^{\hat{s}t}, u^{\hat{s}t} \ge 0,\ \forall \hat{s} \in S, t \in T, \tag{106}$$

$$\min_{\boldsymbol{y}} \quad f_1(\boldsymbol{x},\boldsymbol{y}) \tag{107}$$

$$\text{s.t.} \quad \sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i = o, \\ -1, & i = d, \\ 0, & i = N \setminus \{o, d\}, \end{cases}$$

$$\forall i \in N, \quad (108)$$

$$y_{ij} \geq 0, \ \forall (i,j) \in A. \quad (109)$$

The attacker's upper-level objective (88) minimizes the total expected weighted exposure of the minimal exposure path by incapacitating and/or degrading a subset of the defender's sensors. The λ_s^t-parameters in the objective function account for the degradation of SAM battery capability due to the attacker's employment of sensor degradation attacks. A sensor of type $t \in T$ located at site $s \in S$ experiences a $(1 - \lambda_s^t) \times 100\%$ system degradation, which proportionally reduces the sensor's effectiveness across its operational range. The effect of multiple degradation attacks are additive and bounded by complete sensor degradation (i.e., $\lambda_s^t = 0$). Note, however, that degraded sensors are permitted to relocate, regardless of the level of degradation. The percent effectiveness values are calculated via Constraint (89), where τ^t is the degradation power constant associated with each sensor of type $t \in T$ and θ is the degradation decay factor. That is, each degradation attack centered at site $k \in K$ has a different effect on each type of sensor as a result of the respective degradation power constant. Constraint (90) bounds the number of defender sensors the attacker can incapacitate, by asset type. Likewise, Constraint (91) bounds the number degradation attacks the attacker can employ. Constraints (92) and (93) enforce binary restrictions on the sensor incapacitation and degradation location decision variables, respectively.

The defender's objective function (94) maximizes the total expected weighted exposure of the attacker's minimal exposure path (88), minimizes the maximum sensor

relocation time (95), minimizes the total number of relocated sensors (96), and minimizes the under coverage of high-value assets and emplaced sensors (97), following the attacker's incapacitation and degradation efforts. The expected weighted exposure of an intruder traversing a given arc $(i, j) \in A$ to sensors of type $t \in T$ relocated (i.e., $x^t_{\bar{s}s} = 1$) from site $\bar{s} \in \bar{S}$ to site $s \in S$ is represented by $\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda^t_s w^t e^{st}_{ij} x^t_{\bar{s}s}$, with sensor effectiveness parameters, λ^t_s, defined in Constraint (89).

The exposure weights w^t may be parameterized to account for qualitative differences in sensor effectiveness not captured by the quantitative differences inherent in the sensor probability functions, p^t_{sp}. Qualitative differences in sensor performance may result from factors such as insufficient sensor operator training or operational technical complexity of a given sensor type. For example, the defender could specify exposure weights of 1.0, 0.5, and 0.3 for a model having three different sensor types, thereby affecting a relative preference over the set of sensors within the model formulation. Under this interpretation, the defender is twice as effective at employing the first type of sensor against a target as compared to the second sensor type.

Constraint (98) provides lower bounds on the maximum relocation time, ψ_{max}. Constraint (99) ensures the defender can only relocate sensors that are initially located and not incapacitated. Constraint (100) determines the number of each type of sensor the defender can relocate. Constraint (101) prevents more than one sensor from being relocated to the same site. Constraint (102) ensures that all high-value asset locations receive the required coverage. The form of Constraint (102) results from a logarithmic transformation of the constraint

$$1 - \prod_{s\in S} \prod_{t\in T} \left(1 - \lambda^t_s p^t_{sf}\right)^{x^t_{\bar{s}s}} \geq C^f, \ \forall f \in F,$$

wherein independence is assumed among the probabilities of coverage, p^t_{sf}, over sensor locations, $s \in S$, and sensor types, $t \in T$. (Implied is the assumption that $C^f < 1$,

which is appropriate for this probabilistic metric wherein certain coverage is not attainable.) Likewise, Constraint (103) provides for the coverage of emplaced sensors by other sensors, as may be required by specific applications to protect valuable sensors. That is, for every site $\hat{s} \in S$, if a defender relocates a sensor of type $t \in T$ from site $\bar{s} \in \bar{S}$ to site $\hat{s} \in S$ (i.e., $x^t_{\bar{s}\hat{s}} = 1$), Constraint (103) requires a specified level of coverage, C^t, via the effects of *other* sensors the defender chooses to relocate (i.e., $x^t_{\bar{s}s}, \forall \bar{s} \in \bar{S}, s \in S \setminus \{\hat{s}\}$). In contrast, if a defender does not relocate a sensor of type $t \in T$ from site $\bar{s} \in \bar{S}$ to site $\hat{s} \in S$ (i.e., $x^t_{\bar{s}\hat{s}} = 0$), then the constraint induces no coverage requirement (i.e., an upper bound on the constraint that corresponds to $C^t = 0$). Constraint (104) enforces binary restrictions on the sensor relocation decision variables. Constraints (105) and (106) are the non-negativity constraints for the over and under coverage of high-value assets and emplaced sensors, respectively.

Following the incapacitation and degradation attacks on the defender's sensors and the defender's subsequent relocation of surviving sensors, the attacker's lower-level objective function (107) seeks to minimize the total expected weighted exposure of the minimal exposure path (88) through the defended region. Constraint (108) induces the flow balance constraints for the path from the attacker's point of origin, o, to destination point, d. Lastly, Constraint (109) is the non-negativity constraint associated with the minimal exposure path variables.

Multi-level optimization problems are inherently difficult to solve. With multiple binary decision variables in the first and second-level problems, solving an instance of the SNIP via an enumerative approach is combinatorially complex. Consider, for example, an instance where the defender has $B^t = [2, 5, 5]$ sensors of which the attacker can incapacitate $\zeta^t = [1, 2, 3]$ sensors and additionally locate $\Delta = 3$ degradation attacks across 400 potential locations. This relatively small instance results in $\binom{2}{1}\binom{5}{2}\binom{5}{3}\binom{400}{3} = 2,117,360,000$ possible incapacitation/degradation combinations for

the attacker in the upper-level problem alone. For each of these feasible upper-level solutions, the defender could have up to $\binom{400}{1}\binom{399}{3}\binom{396}{2} = 328,713,470,316,000$ possible sensor relocation combinations. Hence, it would be computationally burdensome, or altogether impractical, to enumerate the first and second-level attacker and defender decision spaces, respectively, and then solve the resulting third-level, defender routing problem, for each feasible first and second-level solution combination.

Another alternative to find an exact solution is to reformulate the SNIP to a single-level optimization problem using one of several available techniques. There exist two often used methods to transform a multilevel mathematical programming formulation into a mathematical programming formulation having fewer levels (preferably only one level) to consider. One may replace the third-level optimization problem, the attacker's shortest path problem, with its Karush-Kuhn-Tucker (KKT) necessary (and sufficient) optimality conditions. Alternatively, if the second-level problem bounds the values of objectives (95), (96), and (97) while maximizing objective (88), one can take the dual of the third-level optimization problem. In either case, a bilevel optimization problem results.

However, with binary restricted defender variables, we cannot take the dual of the resulting lower-level optimization problem within the corresponding bilevel program to further transform the problem into a single-level formulation. Unfortunately, an integer-valued solution is also not guaranteed if we relax the binary restrictions on the defender's sensor relocation variables because covering Constraints (102) and (103) preclude the defender's problem from being totally unimodular. Likewise, we cannot replace the second-level problem with its necessary (and sufficient) KKT optimality conditions for its linear relaxation, as an integer-valued optimal solution is not assured. Moreover, we considered and found a decomposition approach unsuitable due to the combinatorial nature of the upper-level decisions within the trilevel

programming framework. As a result, we propose two heuristic solution methods in the following section.

4.3 Heuristic Solution Methods

In the absence of a computationally tractable, exact solution method to solve the SNIP, we develop two heuristics using a game theoretic, tree search technique. The SNIP can be seen as a two-player, three-stage game with perfect and complete information. In the first-level problem, the attacker selects a subset of the defender's sensors to incapacitate and determines where to locate a limited number of sensor degradation attacks. The defender subsequently determines where to locate the surviving sensors to maximize the expected exposure of the attacker's minimal exposure path, which is determined in the third-level problem. The optimal solution to SNIP is represented by the set of attacker-defender-attacker (i.e., incapacitate and/or degrade $\rightarrow$ relocate $\rightarrow$ route) strategies in which neither player's objective function value (i.e., expected exposure) can improve by a change in either player's strategy.

4.3.1 Heuristic 1 (H1): Piecewise incapacitation and degradation strategy determination.

Although it is theoretically possible to search the entire game tree corresponding to a SNIP instance and determine the subgame perfect Nash equilibrium, the combinatorial nature of even small SNIP instances is cumbersome and renders this approach computationally impractical. Therefore, we consider an enumeration technique only for the attacker's upper-level problem, and solve a reformulation of the second and third-level optimization problems for each of the attacker's fixed upper-level decisions.

However, even an enumeration of the upper level decision space is challenging; whereas the number of possible incapacitation strategies is limited by the available

resources for attack and the number (and location) of sensors, the number of sensor degradation strategies corresponds to the granularity of the instance, as the decision for each sensor degradation relates to the location for the center of the attack, and it is not restricted to the current location of sensors. To limit the number of upper-level attacker strategies enumerated, we consider a partial enumeration technique; we enumerate only the attacker's upper-level incapacitation strategies. We then decompose the problem of identifying the optimal attacker strategy (i.e., a sensor incapacitation/degradation location combination) into a sequence of problems for each potential incapacitation strategy, the first of which is identifying the defender's optimal relocation strategy for the fixed incapacitation strategy, in the absence of degradations; the second is to identify the attacker's optimal degradation strategy, given the fixed incapacitation strategy and the previously identified relocation strategy; and the third of which is to identify the defender's optimal relocation strategy, given the the fixed incapacitation strategy and the previously identified degradation strategy. Although this heuristic represents a decrease in the computational burden of finding an optimal solution via game tree enumeration, such a piecewise approach is not guaranteed to identify an optimal solution to the original problem. For that reason, we test H1 in the following section with respect to solution quality and required computational effort, and we compare it with a heuristic that manifests an even greater level of problem decomposition.

To reformulate the second and third-level problems of the SNIP as a single-level optimization problem for implementation in the solution heuristic, we utilize the ε-constraint method and first reformulate the two lower-level problem formulations to **Problem P2** as follows:

$$\mathbf{P2}\text{:} \max_{\boldsymbol{x},\psi_{max},u^f,u^{\hat{s}t}} \min_{\boldsymbol{y}} \quad \sum_{(i,j)\in A} \left(\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda_s^t w^t e_{ij}^{st} x_{\bar{s}s}^t \right) y_{ij} \tag{110}$$

$$\text{s.t.} \quad \psi_{max} \leq \varepsilon_2, \tag{111}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x^t_{\bar{s}s} \leq \varepsilon_3, \tag{112}$$

$$\sum_{f\in F} u^f + \sum_{\hat{s}\in S} \sum_{t\in T} u^{\hat{s}t} \leq \varepsilon_4, \tag{113}$$

$$\text{Constraints (98)} - \text{(106)}, \text{ and (108)} - \text{(109)}.$$

Similar to Wood (1993), Colson et al. (2007), Amaldi et al. (2008), and Lessin et al. (2018a), we reformulate Problem P2 by replacing the attacker's lower-level problem with its dual formulation. Treating the defender variables $x^t_{\bar{s}s}$ as parameters, the attacker's lower-level minimization problem becomes a shortest path problem in which the expected weighted exposure objective is minimized, subject to Constraints (108) and (109). Replacing the attacker's primal, lower-level problem with its dual formulation as represented in Equations (114)-(117),

$$\max_{\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{114}$$

$$\text{s.t.} \quad -\pi_i + \pi_j \leq \sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \lambda^t_s w^t e^{st}_{ij} x^t_{\bar{s}s}, \ \forall (i,j) \in A, \tag{115}$$

$$\pi_o = 0, \tag{116}$$

$$\pi_i \text{ unrestricted}, \forall i \in N \setminus \{o\}, \tag{117}$$

where π_i is the dual variable associated with the i^{th} Constraint (108), we obtain the following single-level reformulation of Problem P2, denoted **Problem P3**:

$$\textbf{P3}: \max_{\boldsymbol{x},\psi_{max},u^f,u^{\hat{s}t},\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{118}$$

$$\text{s.t.} \quad \psi_{max} \leq \varepsilon_2, \tag{119}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x^t_{\bar{s}s} \leq \varepsilon_3, \tag{120}$$

$$\sum_{f\in F} u^f + \sum_{\hat{s}\in S}\sum_{t\in T} u^{\hat{s}t} \leq \varepsilon_4, \tag{121}$$

$$\frac{d_{\bar{s}s}}{r^t} x^t_{\bar{s}s} \leq \psi_{max}, \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{122}$$

$$\sum_{s\in S} x^t_{\bar{s}s} = x^t_{\bar{s}} - z^t_{\bar{s}}, \forall \bar{s} \in \bar{S}, t \in T, \tag{123}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S} x^t_{\bar{s}s} = B^t - \sum_{\bar{s}\in\bar{S}} z^t_{\bar{s}},\ \forall t \in T, \tag{124}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{t\in T} x^t_{\bar{s}s} \leq 1,\ \forall s \in S, \tag{125}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{sf}\Big) x^t_{\bar{s}s} + o^f - u^f = \ln\Big(1-C^f\Big), \quad \forall f \in F, \tag{126}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S\setminus\{\hat{s}\}}\sum_{t\in T} \ln\Big(1-\lambda^t_s p^t_{s\hat{s}}\Big) x^t_{\bar{s}s} + o^{\hat{s}t} - u^{\hat{s}t} = \cdots$$

$$\cdots = \sum_{\bar{s}\in\bar{S}} \ln\Big(1-C^t\Big) x^t_{\bar{s}\hat{s}}, \forall \hat{s} \in S, t \in T, \tag{127}$$

$$-\pi_i + \pi_j \leq \sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} \lambda^t_s w^t e^{st}_{ij} x^t_{\bar{s}s},\ \forall (i,j) \in A, \tag{128}$$

$$\pi_o = 0, \tag{129}$$

$$\pi_i \text{ unrestricted}, \forall i \in N \setminus \{o\}, \tag{130}$$

$$x^t_{\bar{s}s} \in \{0,1\}, \forall \bar{s} \in \bar{S}, s \in S, t \in T, \tag{131}$$

$$o^f, u^f \geq 0,\ \forall f \in F, \tag{132}$$

$$o^{\hat{s}t}, u^{\hat{s}t} \geq 0,\ \forall \hat{s} \in S, t \in T. \tag{133}$$

Problem P3 provides a single-level model formulation to determine the defender's optimal relocation of the surviving sensors to maximize the exposure of the attacker's least exposed path, minimize the maximum time required for any sensor relocation, minimize the number of sensor relocations, and minimize the under coverage of high-value assets and emplaced sensors, wherein the latter three objectives can be explored

by imposing varying bounds via ε_2, ε_3, and ε_4, respectively. The attacker's decision variables $z_{\bar{s}}^t$ and λ_s^t are fixed input parameters from the first-level SNIP problem. To further simplify our solution approach, we make two additional assumptions which allow the attacker to plan for the worst-case defender relocations, from the attacker's perspective. First, we set $\varepsilon_2 = \gamma$ as an upper bound on the defender's second objective, where γ is the minimum amount of time until the attacker will traverse back through the defended region. This parameter setting ensures the defender accomplishes all sensor relocations before needing to reengage the attacker. Second, we set $\varepsilon_3 = \sum_{\bar{s}\in\bar{S}} \sum_{t\in T} (x_{\bar{s}}^t - z_{\bar{s}}^t)$ as upper bounds on the third objective, allowing the defender to relocate all surviving sensors, if desired.

Instead of bounding the defender's fourth objective of under coverage of high-value assets and emplaced sensors via ε_4 in (121), we propose a hybrid approach wherein the defender preemptively weights the exposure objective (118) and the coverage goal (97), while maintaining ε-bounded constraints for the sensor relocation oriented objectives (95) and (96). Removing ε-constraint (121), and adding preemptive, defender specified weights w_1 and w_2 to the objective function, results in the hybrid model, denoted **Problem P3***:

$$\textbf{P3*}: \max_{\boldsymbol{x},\psi_{max},u^f,u^{\hat{s}t},\boldsymbol{\pi}} \quad w_1(\pi_d - \pi_o) - w_2\left(\sum_{f\in F} u^f + \sum_{\hat{s}\in S}\sum_{t\in T} u^{\hat{s}t}\right) \tag{134}$$

$$\text{s.t.} \quad \text{Constraints (119)} - \text{(120)}, \text{ and (122)} - \text{(133)},$$

wherein weights w_1 and w_2 are specified based on the defender's preferences between the exposure and coverage oriented objectives. For example, the defender may seek to achieve a bounded trade-off between the exposure objective and the coverage penalty objective where $w_1 = \epsilon$ and $w_2 = 1-\epsilon$, for $0 < \epsilon < 1$. Alternatively, the defender may wish to impose a large penalty for failing to meet the minimum coverage requirements

C^f and C^t, thereby setting $w_2 = M$ (i.e., where M is a large positive value) and $w_1 = 1$.

Although the reformulation of Problem P3 to the hybrid model P3* appears defender-focused in its intent, the impetus for constructing P3* is indeed attacker-focused. When trying to determine the attacker's optimal sensor incapacitation and degradation strategy for intrusion of a defended border region, instances can exist wherein, for a given incapacitation/degradation strategy, a defender-feasible solution does not exist for Problem P3 because of the inability to meet the minimum respective coverage requirements for high-value assets and/or emplaced sensors. Model P3* therefore enables the determination of a defender-feasible solution for instances in which strictly imposed defender coverage requirements are unattainable. This hybrid approach to objectives (118) and (97) provides the attacker with the ability to identify (potentially optimal) strategies that otherwise would not be found.

For a fixed attacker incapacitation strategy and the defender's relocation solution from Problem P3*, we solve the following variant of a covering location problem, denoted **Problem P4**, to determine the attacker's optimal sensor degradation locations.

$$\mathbf{P4}\text{: } \max_{\boldsymbol{\lambda},\boldsymbol{\delta}} \quad \sum_{s\in S}\sum_{t\in T}\left(\sum_{(i,j)\in A}\sum_{\bar{s}\in\bar{S}} w^t e_{ij}^{st} x_{\bar{s}s}^t y_{ij}\right)(1-\lambda_s^t) \tag{135}$$

$$\text{s.t.} \quad 1-\lambda_s^t \le 1,\ \forall s\in S, t\in T \tag{136}$$

$$1-\lambda_s^t \le \sum_{k\in K}\frac{\tau^t}{\left(d_{sk}\right)^\theta}\delta_k,\ \forall s\in S, t\in T, \tag{137}$$

$$\sum_{k\in K}\delta_k \le \Delta, \tag{138}$$

$$\delta_k \in \{0,1\},\ \forall k\in K. \tag{139}$$

where $(1-\lambda_s^t)$ represents the percent degradation of a type $t\in T$ sensor located at

site $s \in S$, resulting from a degradation attack located at site $k \in K$.

If we let the expected weighted exposure of a type $t \in T$ sensor located at site $s \in S$ be denoted as:

$$e_s^t = \sum_{(i,j)\in A} \sum_{\bar{s}\in\bar{S}} w^t e_{ij}^{st} x_{\bar{s}s}^t y_{ij}, \forall s \in S, t \in T,$$

and denote the percent degradation of a type $t \in T$ sensor located at site $s \in S$ as $(1 - \lambda_s^t) = v_s^t$, then Problem P4 is equivalent to **Problem P5** below:

$$\textbf{P5}: \max_{\boldsymbol{v},\boldsymbol{\delta}} \quad \sum_{s\in S} \sum_{t\in T} e_s^t v_s^t \tag{140}$$

$$\text{s.t.} \quad v_s^t \leq 1, \ \forall s \in S, t \in T \tag{141}$$

$$v_s^t \leq \sum_{k\in K} \frac{\tau^t}{\left(d_{sk}\right)^\theta} \delta_k, \ \forall s \in S, t \in T, \tag{142}$$

$$\sum_{k\in K} \delta_k \leq \Delta, \tag{143}$$

$$\delta_k \in \{0, 1\}, \ \forall k \in K. \tag{144}$$

The formulation in Problem P5 is an extension of the gradual covering decay model introduced by Berman et al. (2003) where, in this case, the attacker seeks to maximize the degradation of the defender's sensors whereby each degradation attack location (i.e., facility) provides a specified level of degradation (i.e., demand coverage) for each of the defender's sensors based on the sensor (i.e., demand) type. To the best of our knowledge, this is the only known covering problem in facility location in which facilities provide coverage of a heterogeneous set of demand points, and the coverage level associated with each demand point is dependent upon the specific demand type and the distance from each demand point.

After solving Problem P4 (or P5) to determine the attacker's optimal sensor degra-

dation attack locations, we re-solve Problem P3*, given the attacker's sensor degradation solution $\delta_k, \forall k \in K$, to determine the defender's optimal sensor relocation decision and the attacker's minimal exposure path decision. A detailed description of **Heuristic 1** is presented below.

Heuristic 1: Piecewise incapacitation and degradation strategy determination

Step 1. Enumerate attacker sensor incapacitation combinations,
$\boldsymbol{Z} = \left\{ z^t_{\bar{s}_a}, \forall \bar{s} \in \bar{S}, t \in T | a = 1, ..., n = \binom{\beta^1}{\zeta^1} \cdots \binom{\beta^t}{\zeta^t} \right\}$.
Set $(\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}) = (\emptyset, \emptyset, \emptyset, \emptyset)$ and $\nu\left[(\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}})\right] = 0$.
Set $a \leftarrow 1$.
Step 2. Initialize: Let $\delta_k = \{\emptyset\}, \forall k \in K$.
while $(a < n)$ **do**
  Step 3. Solve Problem P3* $(\boldsymbol{z^t_{\bar{s}_a}}, \boldsymbol{\delta_k})$.
    Input : The attacker's sensor incapacitation decision $z^t_{\bar{s}_a}, \forall \bar{s} \in \bar{S}, t \in T$ and sensor degradation locations $\delta_k, \forall k \in K$
    Output: The defender's sensor relocation decision $x^t_{\bar{s}s}, \forall \bar{s} \in \bar{S}, s \in S, t \in T$, and the attacker's minimal exposure path decision $y_{ij}, \forall (i,j) \in A$

  Step 4. Solve Problem P4 $(\boldsymbol{x^t_{\bar{s}s}}, \boldsymbol{y})$.
    Input : The defender's sensor relocation decision $x^t_{\bar{s}s}, \forall \bar{s} \in \bar{S}, s \in S, t \in T$, and the attacker's minimal exposure path decision $y_{ij}, \forall (i,j) \in A$
    Output: The attacker's degradation location decision $\delta_k, \forall k \in K$

  Step 5. Re-solve Problem P3* $(\boldsymbol{z^t_{\bar{s}_a}}, \boldsymbol{\delta_k})$.
    if $\nu\left[(\boldsymbol{z}, \boldsymbol{\delta}, \boldsymbol{x}, \boldsymbol{y})\right] < \nu\left[(\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}})\right]$ **then**
      Set $(\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}) \leftarrow (\boldsymbol{z}, \boldsymbol{\delta}, \boldsymbol{x}, \boldsymbol{y})$.
    end
    Set $a \leftarrow a + 1$. Go to Step 2.
end
Return solution $(\tilde{\boldsymbol{z}}, \tilde{\boldsymbol{\delta}}, \tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}})$.

4.3.2 Heuristic 2 (H2): Sequential incapacitation and degradation strategy determination.

As a baseline for comparing solution approaches, we develop an alternative, greedy construction heuristic to solve an instance of the SNIP. We sequentially identify the sensors to incapacitate and degrade, respectively, in two stages. Within each category of attack, we iteratively identify individual sensors for either incapacitation or degradation, as appropriate, allowing the defender to relocate sensors after each decision. Such an approach does not entail an actual relocation of sensors by the defender; rather, it identifies the defender's best response to all previous attacker decisions, allowing the determination of the best subsequent attacker decision.

In the first stage of H2, given an attacker's type-specific sensor incapacitation budget, $\zeta^t,\ \forall\ t \in T$, we iteratively determine the most advantageous sensor to incapacitate in each of $\sum_{t \in T} \zeta^t$ iterations, assuming a preemptive incapacitation by sensor type according to decreasing capability over the sensor types. For example, if type $t = 1$ is a more capable sensor than type $t = 2$, then H2 will iteratively identify the ζ^1 sensors of type $t = 1$ to incapacitate, then iteratively identify the ζ^2 sensors of type $t = 2$ to incapacitate.

The selection of the first sensor to incapacitate considers the initial sensor layout. Each subsequent selection considers the optimal relocation solution to Problem P3*, given previously identified incapacitation decisions.

Given a sensor layout and an iteration-specific sensor type for incapacitation, $\bar{t} \in T$, H2 solves the following mathematical program to determine which sensor $z^{\bar{t}}_{\bar{s}},\ \forall\ \bar{s} \in \bar{S}$, to incapacitate in the current iteration:

$$\mathbf{GCH_{\boldsymbol{z}}}\colon \max_{\boldsymbol{z}} \quad \sum_{(i,j) \in A} \sum_{\bar{s} \in \bar{S}} w^{\bar{t}} e^{\bar{s}\bar{t}}_{ij} x^{\bar{t}}_{\bar{s}} y_{ij} z^{\bar{t}}_{\bar{s}} \tag{145}$$

$$\text{s.t.} \quad \sum_{\bar{s}\in\bar{S}} z_{\bar{s}}^{\bar{t}} = 1, \tag{146}$$

$$z_{\bar{s}}^{\bar{t}} \in \{0,1\},\ \forall \bar{s} \in \bar{S}. \tag{147}$$

Within this formulation, the attacker seeks to identify the sensor that has the greatest contribution to the expected exposure calculation in (145).

In the second stage of H2, we determine the attacker's sensor degradation strategy. Given an attacker's sensor degradation budget, we determine the most advantageous sensor degradation location in each of Δ iterations by solving the following modification of Problem P4:

$$\mathbf{GCH_{\delta}}\text{:} \max_{\boldsymbol{\lambda},\boldsymbol{\delta}} \quad \sum_{(i,j)\in A} \sum_{\bar{s}\in\bar{S}} \sum_{t\in T} w^t e_{ij}^{\bar{s}t} x_{\bar{s}}^t y_{ij} (1-\lambda_{\bar{s}}^t) \tag{148}$$

$$\text{s.t.} \quad 1-\lambda_{\bar{s}}^t \leq 1,\ \forall \bar{s} \in \bar{S}, t \in T, \tag{149}$$

$$1-\lambda_{\bar{s}}^t \leq \sum_{k\in K} \frac{\tau^t}{\left(d_{\bar{s}k}\right)^{\theta}} \delta_k,\ \forall \bar{s} \in \bar{S}, t \in T, \tag{150}$$

$$\delta_k \in \{0,1\},\ \forall k \in K, \tag{151}$$

where the attacker seeks to maximize the defender's degradation in expected attacker exposure, where $(1-\lambda_{\bar{s}}^t)$ represents the percent degradation of a type $t \in T$ sensor located at site $\bar{s} \in \bar{S}$, resulting from a degradation attack δ_k located at site $k \in K$ in a given iteration. For each successive iteration, one additional degradation location is selected and the previous degradation location decisions remain unchanged. That is, in each iteration $q \in [1,\ldots,\Delta]$, $\sum_{k\in K} \delta_k = q$ and $\delta_{k(q-1)} \leq \delta_{kq}, \forall k \in K,\ q \in [2,\ldots,\Delta]$, where δ_{kq} represents the attacker's degradation decision in iteration q. The combined sensor incapacitation and degradation decisions found via $\text{GCH}_{\boldsymbol{z}}$ and GCH_{δ}, constitute the greedy sensor attack strategy.

4.4 Testing, Results, & Analysis

We solve the SNIP (88)-(109) using H1 and H2 for an illustrative scenario on a 2.5 GHz PC with 192 GB of RAM, using the commercial solver IBM ILOG CPLEX 12.7. We compare the results of the heuristics for three attacker sensor incapacitation instances. The following subsections present a representative network intrusion application, discuss test instance generation, and provide numerical results of the testing.

4.4.1 Representative Scenario for the Intrusion of an Air Defense Network.

We demonstrate the applicability of the SNIP (88)-(109) formulation and our heuristic solution approaches to the sensor network intrusion problem with an illustrative and representative air defense network intrusion scenario. This application is representative of the general problem class in that an attacker has a limited budget with which to incapacitate (i.e., by kinetic or non-kinetic attack) and degrade (e.g., render less capable due to electronic countermeasures) a subset of the defender's sensors (i.e., air defense batteries), after which the defender can relocate the surviving sensors subject to assumed constraints on the maximum sensor relocation time and the maximum number of sensors which can be relocated. Following the defender's sensor relocations, the attacker determines the optimal intrusion path through the defended sensor network to minimize the expected exposure to the defender's sensors.

Adopting the viewpoint of an attacker, we seek to incapacitate and degrade a subset of the defender's ground-based assets of an Integrated Air Defense System (IADS), and the defender subsequently relocates the surviving assets to prevent the attacker's intrusion through the defended border region. We assume the attacker has a limited incapacitation and degradation budget for the defender's initially located

long-range (e.g., SA-21 Growler), medium-range (e.g., SA-22 Greyhound), and short-range (e.g., SA-24 Grinch) Surface to Air Missile (SAM) batteries (Foss & O'Halloran, 2014). Although these weapons do not represent the full range of SAM technologies an attacker could encounter, they are representative of the various threats that countries employing antiaccess/area-denial (A2/AD) strategies are likely to possess and employ (Schmidt, 2016).

Given a 600 km long by 520 km wide border region with an initial IADS layout consisting of two long-range, five medium-range, and five short-range SAM batteries (i.e., $B^t = [2, 5, 5]$), the attacker seeks to optimally incapacitate and degrade a subset of the defender's air defense batteries, and after the defender's relocation of surviving assets, determine the optimal intrusion path through the region.

Figure 15 depicts the initial IADS layout for this instance found by solving the Maximin Exposure Problem (MmEP) as presented by Lessin et al. (2018a).

To facilitate the solution of the illustrative scenario in Figure 15, we enumerate the set of possible attacker incapacitation decisions for three budget-constrained attack instances, as detailed in Table 7.

Table 7. Test instance attacker incapacitation and degradation budget parameter values

Instance	**Number of Incapacitations, ζ^t**			**Number of Degradations, Δ**
	Long-range ($t = 1$)	Medium-range ($t = 2$)	Short-range ($t = 3$)	
1	1	2	0	2
2	0	3	0	2
3	1	1	0	1

In each of the three instances, the attacker is respectively limited to the destruction of $\zeta^t = [1, 2, 0]$, $\zeta^t = [0, 3, 0]$, and $\zeta^t = [1, 1, 0]$ of the defender's initially located air defense assets. We make these operationally-constrained incapacitation assumptions to scope the attacker's incapacitation search space. This results in 20, 10, and 10 unique H1 incapacitation strategies $z_{\bar{s}}^t$ for each of the respective instances. For each

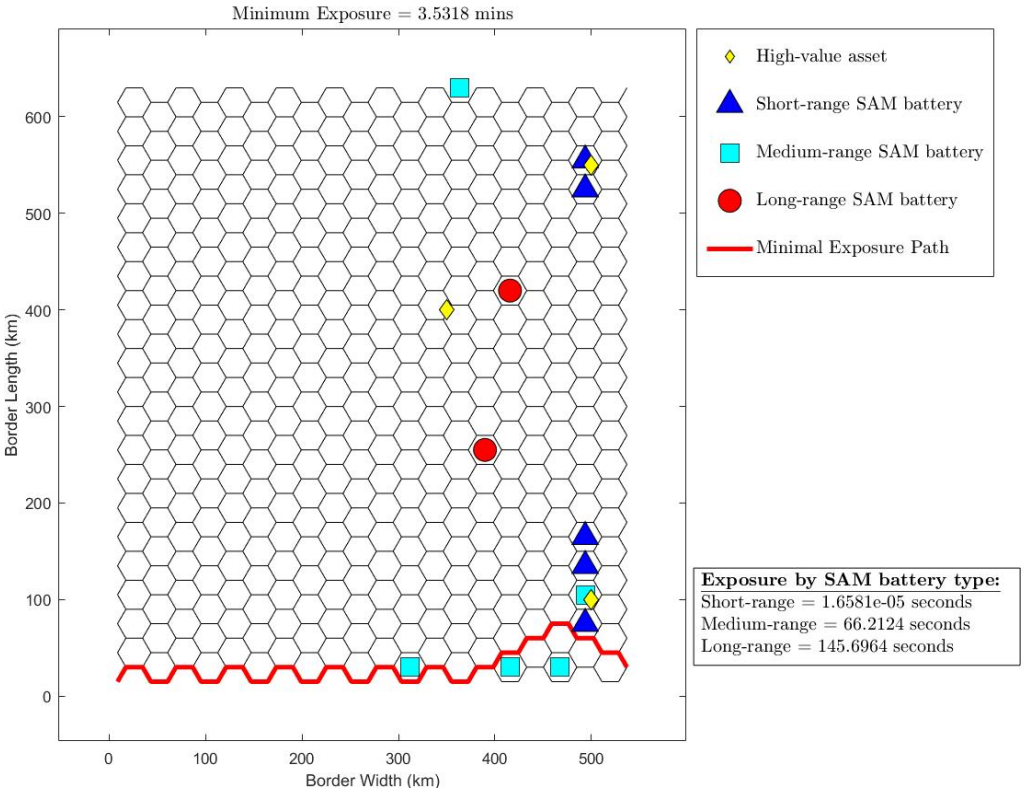


Figure 15. Initial IADS layout

potential incapacitation strategy, the attacker determines the optimal locations of $\Delta = 2$ sensor degradations in the first two instances and $\Delta = 1$ sensor degradation in the third instance, via the solution of H1.

Following the attacker's incapacitation and degradation decisions, the defender relocates the surviving air defense assets. We operationally constrain the defender to relocate at most $\varepsilon_3 = 8$ air defense assets within $\varepsilon_2 = 3$ hours. Degraded assets experience a proportional reduction in system effectiveness across the system's operating range, based on the distance from the affected asset to the degradation center, as determined by constraints (136) and (137). We assume degradation power constant values of $\tau^t = [800, 1500, 2000]$ for each air defense asset of type $t \in T$ and a degradation decay factor of $\theta = 1.5$. The defender seeks to protect three high-value assets located at $F = \{(500, 100), (350, 400), (500, 550)\}$, with minimum probabilities

of protection of $C^f = [0.75, 0.5, 0.5]$, respectively. The defender also seeks to protect long-range SAM batteries with a minimum probability of 0.5 (i.e., $C^t = [0.5, 0, 0]$). Additionally, we assume transit speeds of $r^t = [50, 70, 90]$ km/hr for the long-range, medium-range, and short-range SAM batteries, respectively. We further assume equal exposure weights (i.e., $w^t = [1, 1, 1]$).

We also specify a probability-of-kill function for each SAM battery type, based on representative SAM battery capabilities found in Foss & O'Halloran (2014). The construction of the probability-of-kill curves for instances herein is notional but representative; we utilized a logit model for the probability of kill as a function of the range, assuming a probability of 0.99 for a range of zero and a probability of between 0.04 and 0.11 at the maximum effective range (r_{max}) (Foss & O'Halloran, 2014). To artificially induce different interceptor performance, we specified a probability of 0.55 at 65% of r_{max} for the long-range SAM batteries, a probability of 0.2 at 90% of r_{max} for the medium-range SAM batteries, and a probability of 0.5 at 60% of r_{max} for the short-range SAM batteries. The probability-of-kill function for each SAM battery type is listed in Table 8. These functions are used to calculate the exposure values for each arc resulting from the hexagonal tessellation of the border region and mirror the parameterization used in previous studies (Lessin et al., 2018a,b).

Table 8. SAM battery probability-of-kill functions

SAM Battery Type	p_{sp}^t
Long-range ($t = 1$)	$\frac{e^{-0.0270428 d_{sp}}}{0.010101 + e^{-0.0270428 d_{sp}}}$
Medium-range ($t = 2$)	$\frac{e^{-0.332301 d_{sp}}}{0.010101 + e^{-0.332301 d_{sp}}}$
Short-range ($t = 3$)	$\frac{e^{-1.27642 d_{sp}}}{0.010101 + e^{-1.27642 d_{sp}}}$

In addition to the aforementioned SAM battery types, the long-range assets require separate targeting and tracking radars to engage a target. For this illustrative

scenario, we assume that each SAM battery possesses the required radar coverage to engage intruding targets. We make this assumption to avoid the increase in model complexity to include the radar location decisions within the current framework.

Furthermore, we assume for this study the defender's incoming threat consists only of an aircraft with velocity of 1,800 km/hr (i.e., $|v| = 1,800$ km/hr), as opposed to a wide range of threats not limited to, but including, cruise missiles and ballistic missiles. This assumption determines the coverage capabilities for each SAM battery instead of requiring the model to account for a myriad of target types. This assumption is made to demonstrate the solution for an illustrative scenario, but it is appropriate for two reasons. First, a single attacker is considered as representative of a strike package, a technique for organizing multiple attacking aircraft in a single sortie (e.g., see McLemore, 2010). Second, any alternative path taken by an attacker will yield an exposure that is no lesser and most likely much greater.

Test instances for our analysis were generated by first constructing a hexagonal grid with potential sensor (i.e., SAM battery) locations positioned at the centroid of each hexagon. Neighboring hexagon centroids (i.e., potential SAM battery locations) are located at a defender-specified distance (in km) from each other. Herein, we adopt a distance of 30 km for testing in Section 4.4.2 and as depicted in Figure 15. The granularity of grid construction is easily adapted to suit a given situation or modeler's desired fidelity. The adoption of a two-dimensional network for aircraft traversal implicitly assumes an attacker flies below (or at) a given altitude ceiling. Such an assumption is reasonable if either (a) the attacker utilizes such tactics within their doctrinal framework or (b) if the ground-based air defense assets are complemented within the IADS by interceptor aircraft that operate at high altitudes. Given the precepts of Energy-Maneuverability Theory (Boyd et al., 1966), the doctrinal employment of interceptors conducting Combat Air Patrols (CAPs) requires the air-

craft to patrol at (and begin maneuvers from) relatively high altitudes, reinforcing the division of effort among air- and ground-based assets within an IADS by altitude and, hence, the validity of the two-dimensional modeling assumption.

The attacker's goal is to traverse the border region from an artificial origination node, o, on the (w.l.o.g.) west side of the border region to an artificial destination node, d, on the (w.l.o.g.) east side of the border region, where these nodes are connected by arcs to the leftmost and rightmost hexagon arc nodes, respectively. For each possible instance-specific, attacker incapacitation strategy, the attacker determines the combined sensor incapacitation and degradation strategy via H1 and selects the strategy with the minimum expected exposure objective function (88) value as optimal, for each test instance in Table 7. The attacker also determines the optimal combined sensor incapacitation and degradation strategy via H2 for each of the three test instances. The instance-respective solutions identified by H1 and H2 are then compared with respect to solution quality and required computation time.

4.4.2 Results.

Table 9 shows the attacker's minimal exposure objective function (88) values for the solutions identified via H1, for each of the test instances.

We note from the results presented in Table 9 that, over Instances 1-3, respectively, the best identified strategy attained an expected exposure that was 5.6, 59.7, and 15.6 seconds, on average, lesser than identified by the alternative incapacitation strategies. Moreover, when compared to the best reported strategy, the worst incapacitation strategy for each of the instances corresponded respectively to increases in the expected exposure time to the attacker by 15.7, 80.6, and 35.1 seconds. Also of note within Instance 2, both Incapacitation Strategies 3 and 9 yielded the same objective function value and, although not depicted here, identical intrusion paths as

Table 9. Heuristic 1 attacker objective function values for each test instance

Incapacitation Strategy+	Expected Exposure (seconds)		
	Instance 1	Instance 2	Instance 3
1	0.587	129.225	2.967
2	1.410	129.225	36.232
3	8.838	63.769*	1.696
4	11.883	133.573	1.161*
5	0.591	140.529	4.861
6	3.795	144.393	9.049
7	0.090	83.130	15.511
8	0.328	83.130	36.232
9	2.375	63.769*	11.438
10	1.410	144.394	33.177
11	9.732		
12	9.516		
13	15.815		
14	1.163		
15	8.399		
16	11.883		
17	2.784		
18	5.691		
19	0.090*		
20	11.883		

*Best instance-specific incapacitation strategy
+An Incapacitation Strategy number is specific to each instance, not common across instances.

well. Thus, alternative best solutions are possible and should be examined, as external circumstances not represented within the math programming formulation (e.g., relative risk to the attacker's asset that implements the incapacitation strategy) may warrant a preference among them.

As an example depiction of the best solution for one of the test instances, Figure 16 illustrates the solution identified by H1 for Instance 3, corresponding to a minimal expected exposure of 1.161 seconds for the attacker. The associated intrusion path shown in Figure 16 represents the optimal attacker path through the defender's air defense network, following the defender's sensor relocations subsequent to the attacker's initial $\zeta^t = [1, 1, 0]$ asset incapacitations and $\Delta = 1$ degradation attack.

Table 10 compares the best solution identified by H1 for each test instance with the

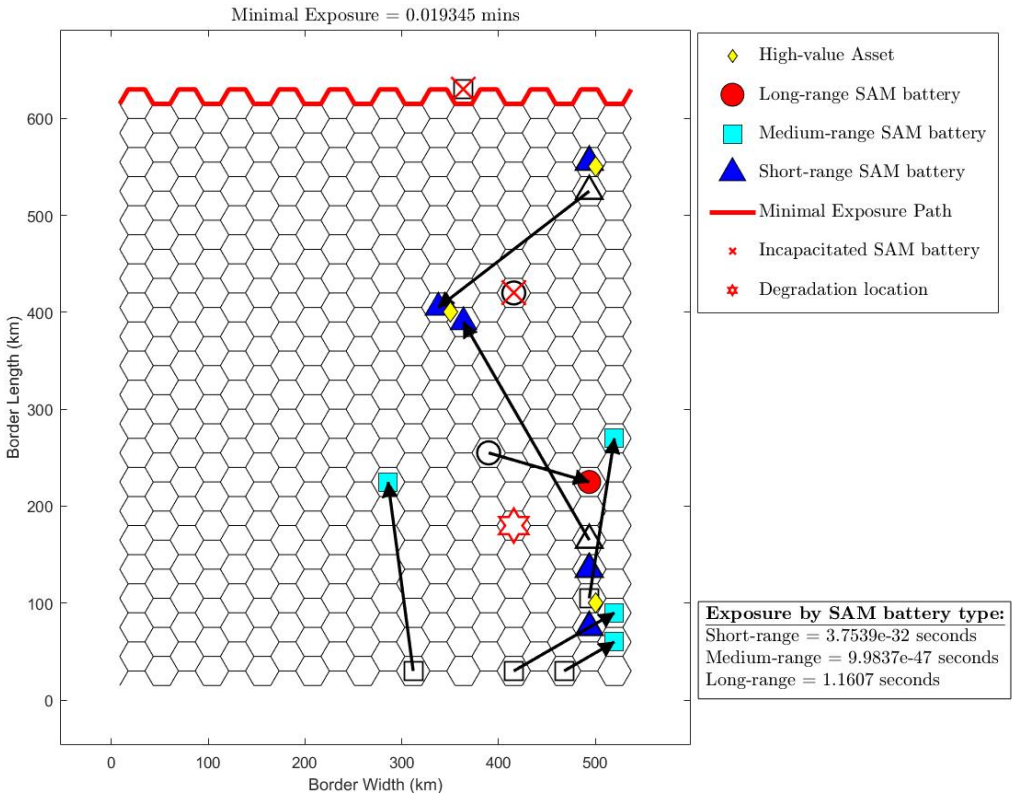


Figure 16. Heuristic 1 solution to Instance 3

corresponding solution identified via H2, both with respect to solution quality (i.e., the attacker's minimal expected exposure objective function value, f_1) and required computation time.

Table 10. Comparison of heuristic solution quality and computation time

Instance	Expected Exposure (seconds)		Computation Time (hours)	
	Heuristic 1	Heuristic 2	Heuristic 1	Heuristic 2
1	0.090	0.518	57.094	7.493
2	63.769	31.942	29.700	8.314
3	1.161	0.776	25.460	5.292

H2 yielded better solutions than H1 for the attacker in all but the first test instance analyzed herein. Moreover, H2 was less computationally burdensome than H1, obtaining solutions in 79.4% less time, on average; whereas H2 iteratively constructs one incapacitation strategy before iteratively identifying the degradation strategy,

the combinatorial nature of H1 requires the identification of the optimal degradation strategy for every possible incapacitation strategy, for a given attacker incapacitation budget, ζ^t. As the attacker's incapacitation budget increases, the combinatorial nature of the instance's complexity increases the number of incapacitation strategies that must be considered, and the disparity in computation time between the two heuristics increases as well. Of course, this combinatorial effect also decreases beyond a certain point, where the attacker incapacitation budget approaches the respective cardinalities for the set of targets (e.g., if the attacker can interdict every sensor, then only one incapacitation strategy exists).

Figures 17 and 18 comparatively illustrate the solutions respectively identified by H1 and H2 for Instance 2. Whereas H1 yielded an attacker's minimal expected exposure of 63.8 seconds, H2 identified a solution having 31.9 seconds of expected exposure, a 49.4% decrease in defender coverage to the attacker's advantage.

Examining Figures 17 and 18, we note that both heuristics selected the same attacker incapacitation strategies and network routing decisions. However, the sensor relocation decisions and the degradation strategies differ. Ultimately, the difference in degradation strategies has the greatest impact on the attacker's decrease in expected exposure. It's worth noting that, by its construct, H1 will necessarily consider the incapacitation strategy that H2 will select. Therefore, any difference in the heuristics' recommended solutions is attributable to the piecewise identification of the attacker's degradation strategy adopted in H2.

The difference in solutions for Instance 2 serve to highlight the underlying assumptions within the heuristics that affect different performance, particularly when developing a degradation strategy. In solving P4, H1 seeks to identify all degradations in one optimization problem, but it does so with respect to the intruder path for a fixed incapacitation strategy. In contrast, when iteratively identifying degradations

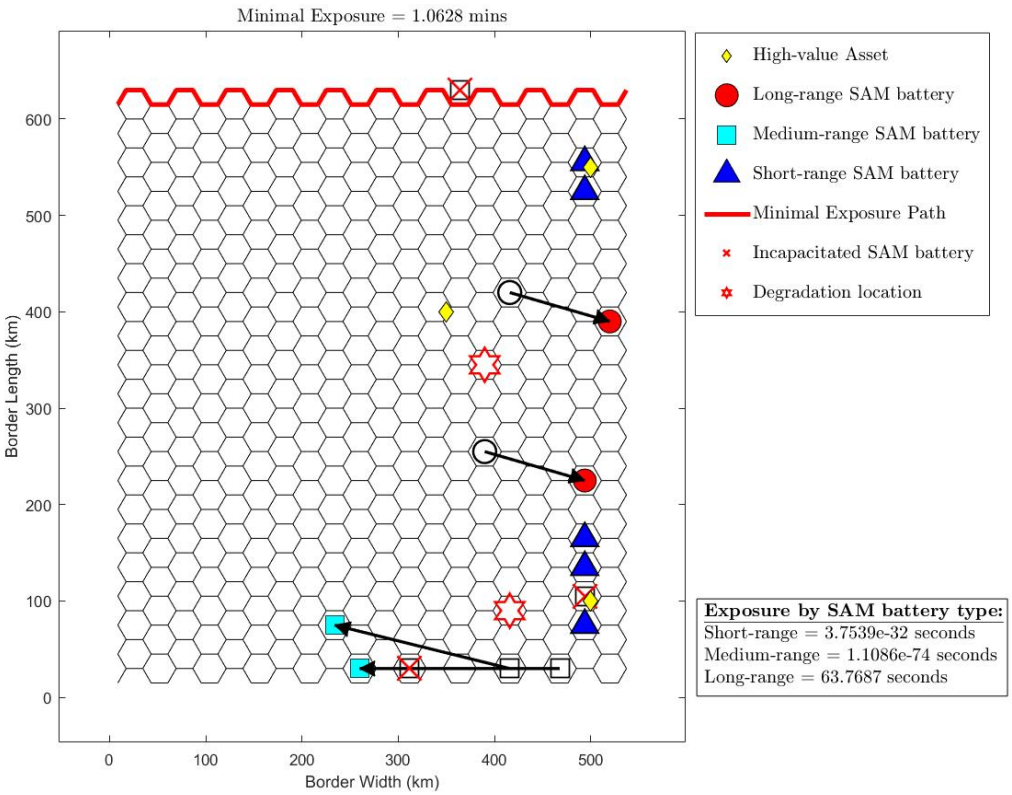


Figure 17. Heuristic 1 solution to Instance 2

to implement, H2 also iteratively identifies and considers the intruder path, given all previously identified incapacitation *and* degradation strategies (and corresponding defender relocations). Thus, H2 exhibits a greater consideration for the defender's adaptation to attacker decisions.

Both solutions procedures, as heuristics, are readily noted as unable to guarantee the identification of a global optimal solution by decomposing the SNIP optimization problem into a set of stepwise optimization subproblems. However, an optimizer's most likely conjecture would portend that a heuristic involving lesser decomposition (i.e., H1) would yield better solutions than one involving a greater degree of problem decomposition (i.e., H2), even though it would likely require a greater computational effort. For the problem instances tested herein, the implied assumption about the relative required computational held forth, but the conjecture about problem decom-

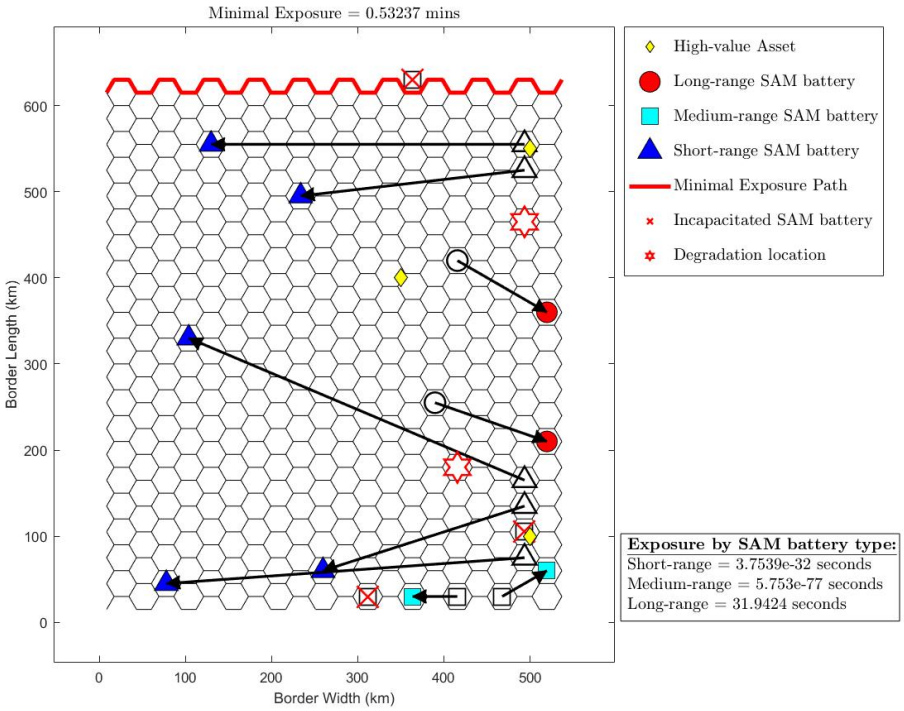


Figure 18. Heuristic 2 solution to Instance 2

position did not. This result motivates the study of alternative heuristics that may not comport with an optimizer's theoretical intuition.

4.5 Conclusions & Recommendations

Given a defender's initial sensor network, we formulated a trilevel mathematical programming model to identify a subset of the defender's heterogeneous sensors to incapacitate and a subset of the defender's network to degrade, subject to budget constraints. In the model, the defender subsequently responds to the attacker's initial sensor incapacitation and degradation attacks and relocates the surviving sensors, seeking to optimize multiple, competing objectives. Lastly, the attacker selects the optimal intrusion path through the defender's sensor network to minimize the expected exposure to the defender's sensors. We also derived a bilevel reformulation which we solved by developing two new heuristics. The heuristics were compared

based on solution quality and computation time and were examined via the solution of three different synthetic-but-representative test instances, for varying attacker incapacitation and degradation budgets. Due to the combinatorial complexity of the attacker's potential incapacitation strategies, H1 was more computationally burdensome than H2. Moreover, H2 yielded more favorable attacker solutions in terms of minimizing the exposure to the defender's sensors than H1 in 2 out of the 3 test instances considered herein.

Future research could be conducted to account for the stochastic nature of various aspects of the ADA modeling framework assumed to be deterministic in this study. For example, the exact number and/or location of defender assets may not be known. We could also consider incapacitation attacks with stochastic probabilities of success (i.e., an incapacitation decision would not necessarily result in the complete incapacitation of a defender's sensor, but may yield a partial decrease in the sensor's effectiveness, wherein the sensor could be allowed to relocate but would experience a decrease in capability). The attacker could also decide to make no defender-related coverage or sensor relocation assumptions, resulting in a single, exposure-focused objective function for the defender. A single objective ADA framework could generate alternative heuristic (or potentially exact) solution approaches that may decrease computation time and improve solution quality.

V. Conclusion

This research provides a mathematical lens to analyze the emerging A2/AD threat to understand how to engage and defeat air defense systems. To accomplish this task, this dissertation focused on three main avenues of research, each building upon the previous work. Chapter II proposed a bilevel math programming model for locating a heterogeneous set of sensors to maximize the minimum exposure of an intruder's penetration path through a defended region. Building upon the initial work in Chapter II, Chapter III formulated a multi-objective, bilevel optimization model to relocate surviving sensors to maximize an intruder's minimal expected exposure to traverse a defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. Finally, Chapter IV presented a trilevel, attacker-defender-attacker mathematical programming formulation for the heterogeneous sensor network intrusion problem to optimally incapacitate a subset of the defender's sensors and degrade a subset of the defender's network to ultimately determine the attacker's optimal penetration path through a defended network.

5.1 Contributions

The research presented in this dissertation represents an amalgamation and extension of work from various fields of study, including, but not limited to, facility location and relocation, Wireless Sensor Networks (WSNs), interdiction modeling, network intrusion, game theoretic bilevel and trilevel programming, multi-objective optimization, and goal programming.

A majority of the research implementing breach- and exposure-coverage metrics focuses on determining the maximal breach path or calculating the minimal exposure path for a given sensor layout. The first research goal, however, was to find

the optimal deployment of a given set of sensors to maximize the minimal exposure of an intruder's traversal of a defended region, extending the work of Amaldi et al. (2008). The notion of weighted exposure was also proposed herein, considering a heterogeneous set of sensors as opposed to utilizing only one sensor type. The benefit of exposure weights is that they allow the defender to account for qualitative differences in sensor effectiveness not captured by the quantitative differences inherent in the sensor probability functions. Qualitative differences in sensor performance may result from factors such as insufficient sensor operator training or operational technical complexity of a given sensor type. The Minimax Exposure Problem formulation also allows the defender to specify required minimum probabilities of coverage for a subset of the located sensors (e.g., the most valuable sensors) and for high-value asset locations in the defended region (e.g., fielded force locations, population centers, command and control centers, etc.), not considered by other works in the literature. This feature enables the balancing of the exposure objective with the protection of sensors and other high-value, defender locations. The robustness of the exposure metric for border protection was also demonstrated by formulating and analyzing three additional alternative intrusion path metrics. The optimal objective value of the minimal exposure solution was shown to result in the worst-case exposure of an intruder's traversal of the defended region, regardless of the intruder's chosen metric for intrusion path determination. This research highlights the importance of considering an exposure metric for determining the optimal intrusion path through an IADS.

This research also provided the only known exposure-based solution to the heterogeneous sensor relocation problem to optimally respond to the incapacitation and/or degradation of sensors and their respective capabilities within a sensor network. Most relocation problems in the literature are single-level problems, focused on optimizing some coverage-related objective function. Alternatively, the multi-objective, bilevel

modeling framework developed herein combined an upper-level problem that accounted for the defender's coverage and relocation related objectives and a lower-level attacker problem that determined an optimal intrusion path. The single-level reformulations presented in Chapters II and III enabled the determination of exact solutions using a commercial solver, as demonstrated with the representative air defense scenario considered herein.

Lastly, this dissertation presented the only known attacker-defender-attacker solution to the heterogeneous sensor network intrusion problem to optimally incapacitate a subset of the defender's sensors and degrade a subset of the defender's network to ultimately determine the attacker's optimal penetration path through a defended network. There are few, if any, attacker-defender-attacker models in the literature. This research is the first of its kind (i.e., incapacitate and/or degrade $\rightarrow$ relocate $\rightarrow$ route) to address the problem of sensor network intrusion. As part of the heuristic solution approach constructed to determine the attacker's degradation strategy, an extension of the gradual covering decay model (Berman et al., 2003) was proposed where, in this case the attacker seeks to maximize the degradation of the defender's sensors whereby each degradation attack location (i.e., facility) provides a specified level of degradation (i.e., demand coverage) for each of the defender's sensors based on the sensor (i.e., demand) type. This is the only known covering problem in facility location in which facilities provide coverage of a heterogeneous set of demand points, and the coverage level associated with each demand point is dependent upon the specific demand type and the distance from each demand point.

5.2 Recommendations for Future Research

There are numerous aspects of the research conducted within this study that could be altered, extended, or combined with other avenues of research. Future research

could be conducted to increase model fidelity by accounting for the placement of hierarchical sensors, adopting alternative intrusion path metrics, or by considering multiple intrusion targets with disparate capabilities. A natural extension may be to pair the research conducted herein with the Weapon-Target Assignment (WTA) problem to determine the optimal assignment of a limited number of defender interceptor weapons to intruding targets. Sensor location solutions from the Maximin Exposure Problem (MmEP) or the Multi-Objective Sensor Relocation Problem (MOSRP) could be used as initial weapon employment locations for the WTA problem. Alternatively, a multi-level mathematical programming formulation could be developed wherein the MmEP or MOSRP is an upper-level problem to a lower-level WTA problem, since the optimal sensor location decisions are naturally linked to the WTA decision variables.

The sensor probability-of-coverage functions could also be refined to account for location-specific effects such as terrain and altitude, depending on the application of interest. The proposed models could be extended to consider a third dimension for the discretization of the defended region of interest, accounting for altitude. Alternative discretization schemes (e.g., truncated octahedrons) might also be considered, especially for a three dimensional discretization. Moreover, one might seek to forgo the discretization altogether and allow the intruder to operate in continuous space. Alternatively, a follow-on study could set aside the discrete expectation framework for identifying an intruder exposure-minimizing path, instead embedding the routing problem within a simulation (e.g., see Ryan et al. (1998, 1999)).

Considering an attacker that is persistent rather than deliberate wherein sensor coverage during relocations is of import, an iterative application of the relocation model with small bounds on the allowable time for relocations could be constructed to generate a suitable sequence of successive asset relocations. Alternatively, a temporal relocation model could be adapted to enable the defender to implement time-phased

sensor relocation strategies.

Various aspects of the modeling frameworks assumed to be deterministic in this research could instead be examined as stochastic. For example, the exact number and/or location of defender assets may not be known. Incapacitation attacks could instead be considered with stochastic probabilities of success (i.e., an incapacitation decision would not necessarily result in the complete incapacitation of a defender's sensor, but may yield a partial decrease in the sensor's effectiveness, wherein the sensor could be allowed to relocate but would experience a decrease in capability). The attacker could also decide to make no defender-related coverage or sensor relocation assumptions, resulting in a single, exposure-focused objective function for the defender. A single objective attacker-defender-attacker framework could generate alternative heuristic (or potentially exact) solution approaches that may decrease computation time and improve solution quality. Moreover, an exploration of appropriate meta-heuristic solution approaches (e.g., genetic algorithms) could be considered for any of the models proposed in this research.

Appendix A. 2018 WDSI Proceedings: *A Multi-objective Bilevel Optimization Model for the Relocation of Integrated Air Defense System Assets*

A MULTI-OBJECTIVE BILEVEL OPTIMIZATION MODEL FOR THE RELOCATION OF INTEGRATED AIR DEFENSE SYSTEM ASSETS

Aaron M. Lessin, Department of Operational Sciences, Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433, 937-255-6565 x6006, aaron.lessin@afit.edu
Brian J. Lunday, Department of Operational Sciences, Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433, 937-255-6565 x4624, brian.lunday@afit.edu

ABSTRACT

Given a subset of ground-based air defense weapon systems within an Integrated Air Defense System (IADS) that have been incapacitated, we formulate a multi-objective bilevel optimization model to relocate surviving assets to maximize an intruder's minimal exposure across a defended border region, minimize the maximum asset relocation time, and minimize the total number of assets requiring relocation. Our formulation also allows the defender to specify minimum coverage requirements for high-value asset locations and emplaced weapon systems. Adopting the ε-constraint method, we develop a single-level reformulation that enables the identification of Pareto-optimal solutions and identifies trade-offs between the competing objectives.

Keywords: Bilevel programming, Multi-objective optimization, Asset relocation, Minimal exposure path, Air defense

INTRODUCTION

Unlike previously fielded air defense systems, emerging antiaccess/area-denial (A2/AD) IADS assets will be highly mobile, "with some systems demonstrating a 'shoot-and-move' time in minutes rather than hours or days" [12]. Instead of planning only the first salvo of strategic attacks against an enemy IADS, it is important to investigate and understand how an enemy may reposition its assets so that we can predict reactions to intended disruption of an IADS. The objective of this paper is to formulate a multi-objective bilevel optimization model to relocate surviving ground-based elements of an IADS and develop a reformulation that enables direct solution via a commercial solver.

LITERATURE REVIEW

A majority of facility relocation problems in the literature are applied to the relocation of fire companies [7], ambulances [3], and emergency vehicles [6]. These works have also been extended from single-objective to multi-objective formulations. Sathe & Miller-Hooks [11] set forth a model to locate military units, police forces, and first responders, and to relocate idle units in response to an event, maximizing secondary coverage and minimizing cost. Melachrinoudis & Min [9] presented a multi-objective application involving the relocation and phase-out of a combined manufacturing plant and warehousing facility. The location and relocation of mobile servers in a transportation network were considered by Berman & Rahnama [2], wherein the authors sought to balance coverage, response time, and relocation costs. Recently, Paul et al. [10] provided a multi-objective, maximal conditional covering location problem applied to the relocation of hierarchical emergency response facilities to respond to large-scale emergencies. Incorporating ideas from facility relocation and multi-objective optimization will allow us to understand how an enemy IADS may adjust during conflict.

MODEL FORMULATION & SOLUTION METHODOLOGY

In this section, we present a baseline formulation for the optimal relocation of IADS assets following an enemy attack. Given a specified set of surviving IADS assets, we determine the optimal layout that maximizes the minimal exposure of an intruder to prevent access across the IADS, minimizes the maximum asset relocation time, and minimizes the total number of assets requiring relocation, while also ensuring adequate coverage of high-value asset locations and a subset of Surface to Air Missile (SAM) batteries.

Assumptions

We make several assumptions related to the defender's objectives and IADS assets. In addition to adjusting an IADS to inhibit an adversary traversing the border region, we also seek to minimize the maximum time required to relocate assets, as well as to minimize the number of assets requiring relocation. Additionally, we require protection of a specified set of high-value asset locations (e.g., fielded force locations, command and control centers, etc.) and a subset of the located assets (e.g., long-range SAM batteries). A minimum probability of protection will be specified for each high-value asset location and for each IADS asset type. We assume a given allocation of SAM batteries; specifically, our model includes a combination of long-range (e.g., SA-21), medium-range (e.g., SA-22), and short-range (e.g., SA-24) missile batteries. Although these weapons do not comprise the full range of SAM technologies the U.S. could encounter, they are representative of the various threats that countries employing A2/AD strategies are likely to possess and employ [5]. In addition to the aforementioned SAM battery types, the long-range assets will require separate targeting and tracking radars to engage a target. However, to simplify the model, we assume that each SAM battery possesses the required radar coverage to engage enemy targets.

Instead of assuming binary SAM battery coverage (i.e., covered/not covered), we implement a representative, but unclassified, probability-of-kill curve as a function of the distance from target to SAM battery, for each SAM battery type.

Furthermore, we assume for this study the defender's incoming threat consists only of aircraft, vis-à-vis a wide range of threats not limited to, but including, cruise missiles and ballistic missiles. This assumption will determine the coverage capabilities for each SAM battery instead of requiring the model to account for a myriad of target types. Additionally, we assume IADS assets that are attacked by the intruder are completely incapacitated. That is, no partial capability remains for the attacked assets. Incapacitated assets, therefore, cannot be relocated. However, we allow the model to relocate unaffected assets to sites of incapacitated assets.
To formulate instances of our model, we first construct a hexagonal tessellation over the border region of interest. We choose to discretize an IADS border region using a mesh of uniformly-sized regular hexagons, as Yousefi & Donohue [14] demonstrated it to be superior to alternative uniform tessellation means (e.g., square, rhombus, triangle). Intruding aircraft can traverse the arcs of the graph, traveling from an artificial origination node *o* on the (*w.l.o.g.*) left side of the hexagonal grid to the artificial destination node *d* on the right. Potential SAM battery locations will exist at the center of each hexagon in the grid.

Lastly, we assume the adversaries know each other’s capabilities, and the intruder has sufficiently capable intelligence to know the location of IADS assets, once emplaced. Our bilevel program is formulated as a zero-sum, two-player, extensive form, complete-and-perfect information game using the following notation.

Sets

T: the set of all types of IADS assets available to locate, indexed by t.

S: the set of all potential sites where SAM batteries can be located, indexed by s.

$\bar{S}$: the set of all sites where SAM batteries are initially located (i.e., $\bar{S} = \{S | x_{\bar{s}}^{t} = 1, \forall \bar{s} \in \bar{S}, t \in T\}$), indexed by $\bar{s}$.

$\hat{S}$: the set of all sites where SAM batteries are located following asset relocations (i.e., $\hat{S} = \{S | x_{\bar{s}s}^{t} = 1, \forall \bar{s} \in \bar{S}, s \in S, t \in T\}$), indexed by $\hat{s}$, where $x_{\bar{s}s}^{t} = 1$ indicates a decision to relocate a SAM battery of type $t \in T$ from site $\bar{s} \in \bar{S}$ to site $s \in S$.

F: the set of all sites where high-value assets are located, indexed by f.

A: the set of arcs in the graph that are equidistant from adjacent potential SAM battery sites $s \in S$, and over which an intruding aircraft can traverse, indexed by a.

N: the set of all nodes at which arcs intersect and through which an intruding aircraft can traverse, indexed by n.

$G(N, A)$: the graph over which an intruding aircraft will traverse, as induced by the set of potential SAM battery sites $s \in S$.

Parameters

w^{t}: the exposure weight for asset type $t \in T$.

e_{ij}^{st}: the exposure time of an aircraft traversing arc $(i, j) \in A$ to an asset of type $t \in T$ located at site $s \in S$.

$d_{\bar{s}s}$: the Euclidean distance between SAM battery sites $\bar{s} \in \bar{S}$ and $s \in S$.

r^{t}: the transit speed of IADS asset type $t \in T$.

$x_{\bar{s}}^{t}$: 1 if a type $t \in T$ IADS asset is initially located at site $\bar{s} \in \bar{S}$, and 0 otherwise.

$z_{\bar{s}}^{t}$: 1 if a type $t \in T$ IADS asset initially located at site $\bar{s} \in \bar{S}$ is incapacitated, and 0 otherwise.

B^{t}: the maximum number of type $t \in T$ IADS assets to locate.

p_{sp}^{t}: the probability that a SAM battery of type $t \in T$ located at site $s \in S$ can cover the point p.

C^{f}: the minimum probability of protection required for each high-value asset location $f \in F$.

C^{t}: the minimum probability of protection required for each located SAM battery of type $t \in T$.

Decision Variables

$x_{\bar{s}s}^{t}$: 1 if a type $t \in T$ IADS asset is relocated from site $\bar{s} \in \bar{S}$ to site $s \in S$; 0 otherwise.

y_{ij}: 1 if arc (i, j) is in the minimal exposure path; 0 otherwise.

ψ_{max}: the maximum time (in hours) required to complete asset moves.

Formulation

Given our assumptions and leveraging the aforementioned notation, we formulate the multi-objective, bilevel program **IADS Multi-Objective Asset Relocation Problem (IADS-MOARP)**, denoted **Problem P1**, as follows:

$$\max_{\boldsymbol{x}, \psi_{max}} \quad f(\boldsymbol{x}, \boldsymbol{y}, \psi_{max}) = \left(f_1(\boldsymbol{x}, \boldsymbol{y}), -f_2(\psi_{max}), -f_3(\boldsymbol{x})\right) \tag{1}$$

$$s.t. \quad f_1(\boldsymbol{x}, \boldsymbol{y}) = \sum_{(i,j) \in A} \left(\sum_{\bar{s} \in \bar{S}} \sum_{s \in S} \sum_{t \in T} w^{t} e_{ij}^{st} x_{\bar{s}s}^{t} \right) y_{ij}, \tag{2}$$

$$f_2(\psi_{max}) = \psi_{max}, \tag{3}$$

$$f_3(\boldsymbol{x}) = \sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\bar{s}\}} \sum_{t\in T} x_{\bar{s}s}^t, \tag{4}$$

$$\left(\frac{d_{\bar{s}s}}{r^t}\right) x_{\bar{s}s}^t \le \psi_{max}, \qquad \forall \bar{s}\in\bar{S}, s\in S, t\in T, \tag{5}$$

$$\sum_{s\in S} x_{\bar{s}s}^t = x_{\bar{s}}^t - z_{\bar{s}}^t, \qquad \forall \bar{s}\in\bar{S}, t\in T, \tag{6}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} x_{\bar{s}s}^t = B^t - \sum_{\bar{s}\in\bar{S}} z_{\bar{s}}^t, \qquad \forall t\in T, \tag{7}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{t\in T} x_{\bar{s}s}^t \le 1, \qquad \forall s\in S, \tag{8}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S} \sum_{t\in T} \ln\left(1-p_{sf}^t\right) x_{\bar{s}s}^t \le \ln(1-C^f), \qquad \forall f\in F, \tag{9}$$

$$\sum_{\bar{s}\in\bar{S}} \sum_{s\in S\setminus\{\hat{s}\}} \sum_{t\in T} \ln(1-p_{s\hat{s}}^t) x_{\bar{s}s}^t \le \ln(1-C^t), \qquad \forall \hat{s}\in\hat{S}, t\in T, \tag{10}$$

$$x_{\bar{s}s}^t \in \{0,1\}, \qquad \forall \bar{s}\in\bar{S}, s\in S, t\in T, \tag{11}$$

$$\min_{\boldsymbol{y}} \quad f_1(\boldsymbol{x},\boldsymbol{y}) \tag{12}$$

$$s.t. \sum_{j:(i,j)\in A} y_{ij} - \sum_{j:(j,i)\in A} y_{ji} = \begin{cases} 1, & i=o, \\ -1, & i=d, \\ 0, & i=N\setminus\{o,d\}, \end{cases} \quad \forall i\in N, \tag{13}$$

$$y_{ij} \ge 0, \qquad \forall (i,j)\in A. \tag{14}$$

The objective function (1) maximizes the total expected weighted exposure of the minimal exposure path (2), minimizes the maximum IADS asset relocation time (3), and minimizes the total number relocated IADS assets (4). Constraint (5) provides lower bounds on the maximum relocation time, ψ_{max}. Constraint (6) ensures we can only relocate assets that are initially located and not incapacitated. Constraint (7) determines the number of each type of IADS asset the defender can relocate. Constraint (8) prevents more than one SAM battery from being relocated to the same site. Constraint (9) ensures that all high-value asset locations receive the required coverage. The form of Constraint (9) results from a logarithmic transformation of the constraint

$$1 - \prod_{s\in S} \prod_{t\in T} \left(1-p_{sf}^t\right)^{x_{\bar{s}s}^t} \ge C^f, \ \forall f\in F,$$

wherein independence is assumed among the probabilities of coverage, p_{sf}^t, over SAM battery locations, $s\in S$, and SAM battery types, $t\in T$. (Implied is the assumption that $C^f < 1$, which is appropriate for this probabilistic metric wherein guaranteed coverage is not attainable.) Likewise, Constraint (10) provides for the coverage of SAM batteries by other SAM batteries. Constraint (11) enforces binary restrictions on the IADS asset relocation decision variables. The lower-level objective function (12) seeks to minimize the total expected weighted exposure of the minimal exposure path (2). Constraint (13) induces the flow balance constraints of the minimal exposure path from the intruder's point of origin, *o*, to destination point, *d*. Lastly, Constraint (14) is the non-negativity constraint associated with the minimal exposure path variables.

Methodology

Instead of solving IADS-MOARP (1)-(14) using a weighted sum or lexicographic approach, we utilize the ε-constraint method to identify a set of non-inferior solutions. We first reformulate Problem P1 (i.e., IADS-MOARP) to **Problem P2** as follows:

$$\max_{x,\psi_{max}} \min_{y} \quad \sum_{(i,j)\in A}\left(\sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} w^t e_{ij}^{st} x_{\bar{s}s}^t\right) y_{ij} \tag{15}$$

$$s.t. \quad \psi_{max} \le \varepsilon_2, \tag{16}$$

$$\sum_{\bar{s}\in\bar{S}}\sum_{s\in S\setminus\{\bar{s}\}}\sum_{t\in T} x_{\bar{s}s}^t \le \varepsilon_3, \tag{17}$$

Constraints (5)-(11) and (13)-(14).

In this reformulation, we replaced the objective function (1) with the defender and intruder objectives of maximizing and minimizing the total expected weighted exposure of the minimal exposure path (2), respectively. We utilize Constraints (16) and (17) to respectively bound our second and third objective functions: the maximum asset relocation time and the total number of asset relocations.

Similar to other bilevel math programming works [1][4][8][13], we reformulate the bilevel Problem P2 by replacing the lower-level problem with its dual formulation. Treating the upper-level variables $x_{\bar{s}s}^t$ as parameters, the lower-level minimization problem becomes a shortest path problem in which the expected weighted exposure objective is minimized, subject to Constraints (13) and (14). Replacing the primal, lower-level problem with its dual formulation as represented in Equations (18)-(21),

$$\max_{\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{18}$$

$$s.t. \quad -\pi_i + \pi_j \le \sum_{\bar{s}\in\bar{S}}\sum_{s\in S}\sum_{t\in T} w^t e_{ij}^{st} x_{\bar{s}s}^t, \qquad \forall (i,j) \in A, \tag{19}$$

$$\pi_o = 0, \tag{20}$$

$$\pi_i \text{ unrestricted}, \forall i \in N\setminus\{o\}, \tag{21}$$

where π_i is the dual variable associated with the i^{th} Constraint (13), we obtain the following reformulation of Problem P2, denoted **Problem P3**:

$$\max_{x,\psi_{max},\boldsymbol{\pi}} \quad \pi_d - \pi_o \tag{22}$$

$$s.t. \quad \text{Constraints (5)-(11), (16)-(17), and (19)-(21).}$$

Problem P3 provides a baseline, single-level model to determine the optimal relocation of surviving air defense assets following an attack.

CONCLUSION

Problem P3 can be solved directly using a commercial solver and iteratively while incrementally decreasing the values of ε_2 and ε_3 to map the efficient Pareto frontier for an instance of Problem P1, thereby examining the tradeoffs between the competing objectives of maximizing the intruder's minimal exposure, minimizing the maximum asset relocation time, and minimizing the total number of asset relocations.

REFERENCES

[1] E. Amaldi, A. Capone, M. Cesana, I. Filippini, Coverage planning of wireless sensors for mobile target detection, in: 2008 5th IEEE Int. Conf. Mob. Ad-Hoc Sens. Syst. MASS 2008, 2008: pp. 48–57.

[2] O. Berman, M.R. Rahnama, Optimal location-relocation decisions on stochastic networks, Transp. Sci. 19 (1985) 203–221.

[3] L. Brotcorne, G. Laporte, F. Semet, Ambulance location and relocation models, Eur. J. Oper. Res. 147 (2003) 451–463.

[4] B. Colson, P. Marcotte, G. Savard, An overview of bilevel optimization, Ann. Oper. Res. 153 (2007) 235–256.

[5] C.F. Foss, J.C. O'Halloran, IHS Jane's Land Warfare Platforms: Artillery and Air Defence, Jane's Information Group, United Kingdom, 2014.

[6] M. Gendreau, G. Laporte, F. Semet, The maximal expected coverage relocation problem for emergency vehicles, J. Oper. Res. Soc. 57 (2006) 22–28.

[7] P. Kolesar, W.E. Walker, An algorithm for the dynamic relocation of fire companies, Oper. Res. 22 (1974) 249–274.

[8] A. Lessin, Bilevel multi-objective programming and optimization for integrated air defense system disruption, Air Force Institute of Technology, 2017.

[9] E. Melachrinoudis, H. Min, The dynamic relocation and phase-out of a hybrid, two-echelon plant/warehousing facility: A multiple objective approach, Eur. J. Oper. Res. 123 (2000) 1–15.

[10] N.R. Paul, B.J. Lunday, S.G. Nurre, A multiobjective, maximal conditional covering location problem applied to the relocation of hierarchical emergency response facilities, Omega. 66 (2016) 147–158.

[11] A. Sathe, E. Miller-Hooks, Optimizing location and relocation of response units in guarding critical facilities, Transp. Res. Rec. J. Transp. Res. Board. (2005) 127–136.

[12] United States Joint Chiefs of Staff, Joint Publication 3-01: Countering Air and Missile Threats, (2012).

[13] R.K. Wood, Deterministic network interdiction, Math. Comput. Model. 17 (1993) 1–18.

[14] A. Yousefi, G. Donohue, Temporal and spatial distribution of airspace complexity for air traffic controller workload-based sectorization, in: AIAA 4th Aviat. Technol. Integr. Oper. Forum, 2004.

Bibliography

(2017). Alert (ta17-293a): Advanced persistent threat activity targeting energy and other critical infrastructure sectors. Available: https://www.us-cert.gov/ncas/alerts/TA17-293A. Accessed 27 November 2017.

(2017). Exports of Russia's S-400 missile systems. Available: http://tass.com/defense/969682. Accessed 27 November 2017.

Adams, R. (2017). Nuclear generator movable by cargo plane not only possible, but proven in the early 1960s. Available: http://www.theenergycollective.com/rodadams/2414142/nuclear-generator-movable-cargo-plane-not-possible-proven-early-1960s. Accessed 12 December 2017.

Adlakha, S. & Srivastava, M. (2003). Critical density thresholds for coverage in wireless sensor networks. In *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.*, volume 3, (pp. 1615–1620).

Alderson, D. L., Brown, G. G., Matthew, C. W., & Wood, R. K. (2011). Solving defender-attacker-defender models for infrastructure defense. In *Proceedings of the 12th INFORMS Computing Society Conference*, (pp. 28–49). INFORMS. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a582412.pdf. Accessed 28 May 2018.

Aliakbarian, N., Dehghanian, F., & Salari, M. (2015). A bi-level programming model for protection of hierarchical facilities under imminent attacks. *Computers & Operations Research*, *64*, 210–224.

Alles, R., Borkowski, M., & Vitiello, R. (2016). Border security gadgets, gizmos, and information: using technology to increase situational awareness

and operational control. Available: https://www.dhs.gov/news/2016/05/24/written-testimony-cbp-house-homeland-security-subcommittee-border-and-maritime. Accessed 27 November 2017.

Amaldi, E., Capone, A., Cesana, M., & Filippini, I. (2008). Coverage planning of wireless sensors for mobile target detection. In *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, (pp. 48–57).

Ashford, W. (2016). Hunters: a rare but essential breed of enterprise cyber defenders. Available: https://www.computerweekly.com/feature/Hunters-a-rare-but-essential-breed-of-enterprise-cyber-defenders. Accessed 11 July 2018.

Badri, M. A. (1999). Combining the analytic hierarchy process and goal programming for global facility location-allocation problem. *International Journal of Production Economics*, *62*(3), 237–248.

Badri, M. A., Mortagy, A. K., & Alsayed, C. A. (1998). A multi-objective model for locating fire stations. *European Journal of Operational Research*, *110*(2), 243–260.

Baig, E. (2017). Cell-phone providers roll out cows to handle massive surge on inauguration day. Available: https://www.usatoday.com/story/tech/columnist/baig/2017/01/19/cell-phone-providers-roll-out-cows-handle-massive-surge-inauguration-day/96786674/. Accessed 14 December 2017.

Banse, T. (2017). Wireless carriers deploy 'cell on wheels' to boost coverage in eclipse path. Available: http://nwpr.org/post/wireless-carriers-deploy-cell-wheels-boost-coverage-eclipse-path. Accessed 14 December 2017.

Berman, O., Drezner, Z., & Krass, D. (2009). Cooperative cover location problems: the planar case. *IIE Transactions*, *42*(3), 232–246.

Berman, O., Drezner, Z., Krass, D., & Wesolowsky, G. O. (2009). The variable radius covering problem. *European Journal of Operational Research*, *196*(2), 516–525.

Berman, O. & Krass, D. (2002). The generalized maximal covering location problem. *Computers & Operations Research*, *29*(6), 563–581.

Berman, O., Krass, D., & Drezner, Z. (2003). The gradual covering decay location problem on a network. *European Journal of Operational Research*, *151*(3), 474–480.

Berman, O. & Rahnama, M. R. (1985). Optimal location-relocation decisions on stochastic networks. *Transportation Science*, *19*(3), 203–221.

Bhattacharya, U., Rao, J., & Tiwari, R. (1993). Bi-criteria multi facility location problem in fuzzy environment. *Fuzzy Sets and Systems*, *56*(2), 145–153.

Bodeau, D. & Graubart, R. (2017). Cyber resiliency design principles. Technical Report MTR170001, MITRE. Available: `https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf`. Accessed 11 July 2018.

Boyd, J. R., Christie, T. P., & Gibson, J. E. (1966). Energy maneuverability. *Air Proving Ground Center Report APGC-TR-66-4 Vol*, *1*.

Bricha, N. & Nourelfath, M. (2013). Critical supply network protection against intentional attacks: A game-theoretical model. *Reliability Engineering & System Safety*, *119*, 1–10.

Brotcorne, L., Laporte, G., & Semet, F. (2003). Ambulance location and relocation models. *European Journal of Operational Research*, *147*(3), 451–463.

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

Bucki, E. M. (2016). Flexible, smart, and lethal: Adapting U.S. SEAD doctrine to changing threats. *Air & Space Power Journal*, *30*(2), 65.

Cappanera, P. & Scaparra, M. P. (2011). Optimal allocation of protective resources in shortest-path networks. *Transportation Science*, *45*(1), 64–80.

Cardei, M. & Wu, J. (2006). Energy-efficient coverage problems in wireless ad-hoc sensor networks. *Computer Communications*, *29*(4), 413–420.

Cavalier, T. M., Conner, W. A., del Castillo, E., & Brown, S. I. (2007). A heuristic algorithm for minimax sensor location in the plane. *European Journal of Operational Research*, *183*(1), 42–55.

Church, R. & ReVelle, C. (1974). The maximal covering location problem. *Papers of the Regional Science Association*, *32*(1), 101–118.

Church, R. L. (1984). The planar maximal covering location problem. *Journal of Regional Science*, *24*(2), 185–201.

Clouqueur, T., Phipatanasuphorn, V., Ramanathan, P., & Saluja, K. K. (2002). Sensor deployment strategy for target detection. In *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, (pp. 42–48)., New York, NY, USA. ACM.

Colombo, F., Cordone, R., & Lulli, G. (2016). The multimode covering location problem. *Computers & Operations Research*, *67*, 25–33.

Colson, B., Marcotte, P., & Savard, G. (2007). An overview of bilevel optimization. *Annals of Operations Research*, *153*(1), 235–256.

Corley Jr, H. & Chang, H. (1974). Finding the n most vital nodes in a flow network. *Management Science*, *21*(3), 362–364.

Cormican, K. J., Morton, D. P., & Wood, R. K. (1998). Stochastic network interdiction. *Operations Research*, *46*(2), 184–197.

Crosman, P. (2018). Banks underground data vault is evolving will it use blockchain next? Available: `https://www.americanbanker.com/news/banks-underground-data-vault-is-evolving-will-it-use-blockchain-next`. Accessed 11 July 2018.

Dennison, S., Franke, U. E., & Zerka, P. (2018). The nightmare of the dark: The security fears that keep europeans awake at night. Available: `http://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n`. Accessed 11 July 2018.

Dijkstra, E. W. (1959). A note on two problems in connexion with graphs. *Numerische Mathematik*, *1*(1), 269–271.

Drezner, Z., Wesolowsky, G. O., & Drezner, T. (2004). The gradual covering problem. *Naval Research Logistics (NRL)*, *51*(6), 841–855.

Duttagupta, A., Ghosh, A., Bishnu, A., & Sengupta, I. (2007). Maximal breach and support: Geometric characterisation and algorithms. Technical report, Indian Statistical Institute.

Eckenrode, R. T. (1965). Weighting multiple criteria. *Management Science*, *12*(3), 180–192.

Ehrgott, M. (2006). *Multicriteria optimization*. Springer Science & Business Media.

Ehrgott, M. & Gandibleux, X. (2000). A survey and annotated bibliography of multiobjective combinatorial optimization. *OR-Spektrum*, *22*(4), 425–460.

Farahani, R. Z., Asgari, N., Heidari, N., Hosseininia, M., & Goh, M. (2012). Covering problems in facility location: A review. *Computers & Industrial Engineering*, *62*(1), 368–407.

Farhan, B. & Murray, A. T. (2008). Siting park-and-ride facilities using a multi-objective spatial optimization model. *Computers & Operations Research*, *35*(2), 445–456.

FEMA (2017). Federal family continues response and relief operations following hurricane irma. Available: `https://www.fema.gov/news-release/2017/09/14/federal-family-continues-response-and-relief-operations-following-hurricane`. Accessed 14 December 2017.

Feng, H., Luo, L., Wang, Y., Ye, M., & Dong, R. (2016). A novel minimal exposure path problem in wireless sensor networks and its solution algorithm. *International Journal of Distributed Sensor Networks*, *12*(8), 1–15.

Foss, C. F. & O'Halloran, J. C. (2014). *IHS Jane's Land Warfare Platforms: Artillery and Air Defence*. United Kingdom: Jane's Information Group.

Fulkerson, D. R. & Harding, G. C. (1977). Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming*, *13*(1), 116–118.

Gady, F.-S. (2017). Russia inducts new s-400 missile air defense system. Available: `https://thediplomat.com/2017/10/russia-inducts-new-s-400-missile-air-defense-system/`. Accessed 27 November 2017.

Gendreau, M., Laporte, G., & Semet, F. (2006). The maximal expected coverage relocation problem for emergency vehicles. *Journal of the Operational Research Society*, *57*(1), 22–28.

Golden, B. (1978). A problem in network interdiction. *Naval Research Logistics (NRL)*, *25*(4), 711–713.

Goldfein, D. L. & James, D. L. (2016). Department of defense press briefing by secretary james and gen. goldfein on the state of the air force in the pentagon briefing room. `http://www.defense.gov/News/Transcripts/Transcript-View/Article/911083/department-of-defense-press-briefing-by-secretary-james-and-gen-goldfein-on-the`. Accessed 22 November 2016.

Gong, Q. & Batta, R. (2007). Allocation and reallocation of ambulances to casualty clusters in a disaster relief operation. *IIE Transactions*, *39*(1), 27–39.

Greco, S., Figueira, J., & Ehrgott, M. (2005). Multiple criteria decision analysis. *Springer's International Series*.

Healing, D. (2017). Cyberattacks pose serious threat to canadas automated resource firms. Available: `https://www.theglobeandmail.com/report-on-business/industry-news/energy-and-resources/cyberattacks-pose-serious-threat-to-canadas-automated-resource-firms/article37087705/`. Accessed 27 November 2017.

Hobbs, B. F. (1980). A comparison of weighting methods in power plant siting. *Decision Sciences*, *11*(4), 725–737.

Holland, J. H. (1975). *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence.* U Michigan Press.

Huang, C.-F. & Tseng, Y.-C. (2005). The coverage problem in a wireless sensor network. *Mobile Networks and Applications*, *10*(4), 519–528.

Hwang, C.-L. & Yoon, K. (2012). *Multiple attribute decision making: methods and applications a state-of-the-art survey*, volume 186. Springer Science & Business Media.

James, M. (2018). Secure by design: Improving the cyber security of consumer internet of things report. Technical report, Department for Digital, Culture, Media & Sport, United Kingdom. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf. Accessed 11 July 2018.

Jansen, B. (2018). TSA: Fliers will face more scrutiny for powders in carry-on bags. Available: https://www.usatoday.com/story/travel/flights/todayinthesky/2018/06/19/tsa-fliers-face-more-scrutiny-powders-carry-bags/715386002/. Accessed 07 July 2018.

Juncker, J.-C. (2017). State of the union address. Available: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm. Accessed 27 November 2017.

Karabulut, E., Aras, N., & Altnel, . K. (2017). Optimal sensor deployment to increase the security of the maximal breach path in border surveillance. *European Journal of Operational Research*, *259*(1), 19–36.

Kelly, J. (2017). Implementing the president's border security and immigration enforcement improvements policies. Available: https://www.dhs.gov/sites/default/files/publications/17_0220_S1_Implementing-the-Presidents-Border-Security-Immigration-Enforcement-Improvement-Policies.pdf. Accessed 27 November 2017.

Kolesar, P. & Walker, W. E. (1974). An algorithm for the dynamic relocation of fire companies. *Operations Research*, *22*(2), 249–274.

Kulturel-Konak, S., Smith, A. E., & Norman, B. A. (2007). Bi-objective facility expansion and relayout considering monuments. *IIE Transactions*, *39*(7), 747–761.

Kumar, S., Lai, T. H., & Arora, A. (2005). Barrier coverage with wireless sensors. In *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking*, (pp. 284–298)., New York, NY, USA. ACM.

Laptev, N., Smyl, S., & Shanmugam, S. (2017). Engineering extreme event forecasting at uber with recurrent neural networks. Available: `https://eng.uber.com/neural-networks/`. Accessed 12 December 2017.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber attack on the ukrainian power grid. Technical report, Electricity Information Sharing and Analysis Center, Washington, DC.

Lee, S. M. & Olson, D. L. (1999). Goal programming. In *Multicriteria Decision Making* (pp. 203–235). Springer.

Lessin, A. M., Lunday, B. J., & Hill, R. R. (2018a). A bilevel exposure-oriented sensor location problem for border security. *Computers & Operations Research*, *98*, 56–68.

Lessin, A. M., Lunday, B. J., & Hill, R. R. (2018b). A multi-objective, bilevel sensor relocation problem for border security. Technical Report AFIT-TR 18.01, Air Force Institute of Technology.

Liberatore, F., Scaparra, M. P., & Daskin, M. S. (2012). Hedging against disruptions with ripple effects in location analysis. *Omega*, *40*(1), 21–30.

Lim, C. & Smith, J. C. (2007). Algorithms for discrete and continuous multicommodity flow network interdiction problems. *IIE Transactions*, *39*(1), 15–26.

Lincoln Fire & Rescue (2014). Station optimization study. Technical Paper. Available: `http://lincoln.ne.gov/City/fire/pdf/relocate/optimum2.pdf`. Accessed 14 December 2017.

Losada, C., Scaparra, M. P., & OHanley, J. R. (2012). Optimizing system resilience: a facility protection model with recovery time. *European Journal of Operational Research*, *217*(3), 519–530.

Lozano, L. & Smith, J. C. (2017). A backward sampling framework for interdiction problems with fortification. *INFORMS Journal on Computing*, *29*(1), 123–139.

Lunday, B. J. & Sherali, H. D. (2012). Minimizing the maximum network flow: models and algorithms with resource synergy considerations. *Journal of the Operational Research Society*, *63*(12), 1693–1707.

Macaulay, T. (2017). How big data is changing the nature of policing from reactive to proactive. Available: `https://www.computerworlduk.com/data/how-big-data-is-moving-policing-from-reactive-proactive-approach-3655033/`. Accessed 14 December 2017.

Marler, R. T. & Arora, J. S. (2004). Survey of multi-objective optimization methods for engineering. *Structural and Multidisciplinary Optimization*, *26*(6), 369–395.

Mavrotas, G. (2009). Effective implementation of the ε-constraint method in multi-objective mathematical programming problems. *Applied Mathematics and Computation*, *213*(2), 455–465.

McCaul, M. (2017). Border security for america act of 2017, h. r. 3548. Available: https://www.congress.gov/bill/115th-congress/house-bill/3548/text#toc-H32171C617A904FEDBA741BB5ADC8F0F6. Accessed 27 November 2017.

McLemore, C. S. (2010). Strike package-target pairing: Real-time optimization for airborne battlespace command and control. Master's thesis, Naval Postgraduate School, Monterey, CA. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a531478.pdf. Accessed 28 May 2018.

Megerian, S., Koushanfar, F., Potkonjak, M., & Srivastava, M. B. (2005). Worst and best-case coverage in sensor networks. *IEEE Transactions on Mobile Computing*, *4*(1), 84–92.

Meguerdichian, S., Koushanfar, F., Potkonjak, M., & Srivastava, M. B. (2001). Coverage problems in wireless ad-hoc sensor networks. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213)*, volume 3, (pp. 1380–1387 vol.3).

Meguerdichian, S., Koushanfar, F., Qu, G., & Potkonjak, M. (2001). Exposure in wireless ad-hoc sensor networks. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, (pp. 139–150)., New York, NY, USA. ACM.

Meguerdichian, S., Slijepcevic, S., Karayan, V., & Potkonjak, M. (2001). Localized algorithms in wireless ad-hoc networks: location discovery and sensor exposure. In *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, (pp. 106–116)., New York, NY, USA. ACM.

Melachrinoudis, E. & Min, H. (2000). The dynamic relocation and phase-out of

a hybrid, two-echelon plant/warehousing facility: A multiple objective approach. *European Journal of Operational Research*, *123*(1), 1–15.

Min, H. (1988). The dynamic expansion and relocation of capacitated public facilities: A multi-objective approach. *Computers & Operations Research*, *15*(3), 243–252.

Nickel, S., Puerto, J., & Rodríguez-Chía, A. M. (2005). Mcdm location problems. In *Multiple criteria decision analysis: State of the art surveys* (pp. 761–787). Springer.

Paul, N. R., Lunday, B. J., & Nurre, S. G. (2016). A multiobjective, maximal conditional covering location problem applied to the relocation of hierarchical emergency response facilities. *Omega*, *66*, 147–158.

Qiao, J., Jeong, D., Lawley, M., Richard, J.-P. P., Abraham, D. M., & Yih, Y. (2007). Allocating security resources to a water supply network. *IIE Transactions*, *39*(1), 95–109.

Raisanen, L. & Whitaker, R. M. (2005). Comparison and evaluation of multiple objective genetic algorithms for the antenna placement problem. *Mobile Networks and Applications*, *10*(1-2), 79–88.

Rashidi, E., Medal, H., & Hoskins, A. (2018). An attacker-defender model for analyzing the vulnerability of initial attack in wildfire suppression. *Naval Research Logistics (NRL)*, *65*.

Ryan, J. L., Bailey, T. G., Moore, J. T., & Carlton, W. B. (1998). Reactive tabu search in unmanned aerial reconnaissance simulations. In *Proceedings of the 30th Conference on Winter Simulation*, (pp. 873–880). IEEE Computer Society Press.

Ryan, J. L., Bailey, T. G., Moore, J. T., & Carlton, W. B. (1999). Unmanned aerial vehicles (UAV) route selection using reactive tabu search. *Military Operations Research*, *4*(3), 5–24.

San Martin, P. A. (2007). Tri-level optimization models to defend critical infrastructure. Master's thesis, Naval Postgraduate School, Monterey, CA. Available: `https://calhoun.nps.edu/handle/10945/3343`. Accessed 28 May 2018.

Sathe, A. & Miller-Hooks, E. (2005). Optimizing location and relocation of response units in guarding critical facilities. *Transportation Research Record: Journal of the Transportation Research Board*, (1923), 127–136.

Scaparra, M. P. & Church, R. L. (2008). A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research*, *35*(6), 1905–1923.

Schilling, D. A., Jayaraman, V., & Barkhi, R. (1993). A review of covering problems in facility location. *Location Science*, *1*(1), 25–55.

Schmidt, A. (2016). Countering anti-access/area denial: future capability requirements in nato. *The Journal of the Joint Airpower Competence Centre*, *23*(8), 69–77.

Sherali, H. D. & Soyster, A. L. (1983). Preemptive and nonpreemptive multi-objective programming: Relationship and counterexamples. *Journal of Optimization Theory and Applications*, *39*(2), 173–186.

Smith, J. C., Lim, C., & Sudargho, F. (2007). Survivable network design under optimal and heuristic interdiction scenarios. *Journal of Global Optimization*, *38*(2), 181–199.

Suzuki, A. & Drezner, Z. (2003). Covering problem with variable radii and fixed centers. In *Proceedings of the international workshop on urban operations research, Seto, Japan, Nanzan University*, (pp. 34–35).

Tian, J., Wang, G., Yan, T., & Zhang, W. (2014). Detect smart intruders in sensor networks by creating network dynamics. *Computer Networks*, *62*, 182–196.

Ulungu, E. L. & Teghem, J. (1994). Multi-objective combinatorial optimization problems: A survey. *Journal of Multi-Criteria Decision Analysis*, *3*(2), 83–104.

United States Joint Chiefs of Staff (2012a). *Joint Operational Access Concept (JOAC)*.

United States Joint Chiefs of Staff (2012b). *Joint Publication 3-01: Countering Air and Missile Threats*.

Veltri, G., Huang, Q., Qu, G., & Potkonjak, M. (2003). Minimal and maximal exposure path algorithms for wireless embedded sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, (pp. 40–50)., New York, NY, USA. ACM.

Washburn, A. & Wood, K. (1995). Two-person zero-sum games for network interdiction. *Operations Research*, *43*(2), 243–251.

White, J. A. & Case, K. E. (1974). On covering problems and the central facilities location problem. *Geographical Analysis*, *6*(3), 281–294.

Whiteman, P. S. (1999). Improving single strike effectiveness for network interdiction. *Military Operations Research*, *4*(4), 15–30.

Wollmer, R. (1964). Removing arcs from a network. *Operations Research*, *12*(6), 934–940.

Wong, A. (2016). Cybersecurity: Threats, challenges, opportunities. Available: `https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf/`. Accessed 10 July 2018.

Wood, R. K. (1993). Deterministic network interdiction. *Mathematical and Computer Modelling*, *17*(2), 1–18.

Yao, Y., Edmunds, T., Papageorgiou, D., & Alvarez, R. (2007). Trilevel optimization in power network defense. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *37*(4), 712–718.

Yousefi, A. & Donohue, G. (2004). Temporal and spatial distribution of airspace complexity for air traffic controller workload-based sectorization. In *AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum*.

Yuan, W., Zhao, L., & Zeng, B. (2014). Optimal power grid protection through a defender–attacker–defender model. *Reliability Engineering & System Safety*, *121*, 83–89.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704–0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
14–09–2018	PhD Dissertation	Aug 2015 — Sep 2018

4. TITLE AND SUBTITLE

MULTI-LEVEL MULTI-OBJECTIVE PROGRAMMING AND OPTIMIZATION FOR INTEGRATED AIR DEFENSE SYSTEM DISRUPTION

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lessin, Aaron M., Maj, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENS-DS-18-S-035

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Sponsor wishes to remain anonymous.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The U.S. military's ability to project military force is being challenged. This research develops and demonstrates the application of three respective sensor location, relocation, and network intrusion models to provide the mathematical basis for the strategic engagement of emerging technologically advanced, highly-mobile, Integrated Air Defense Systems. First, we propose a bilevel mathematical programming model for locating a heterogeneous set of sensors to maximize the minimum exposure of an intruder's penetration path through a defended region. Next, we formulate a multi-objective, bilevel optimization model to relocate surviving sensors to maximize an intruder's minimal expected exposure to traverse a defended border region, minimize the maximum sensor relocation time, and minimize the total number of sensors requiring relocation. Lastly, we present a trilevel, attacker-defender-attacker formulation for the heterogeneous sensor network intrusion problem to optimally incapacitate a subset of the defender's sensors and degrade a subset of the defender's network to ultimately determine the attacker's optimal penetration path through a defended network.

15. SUBJECT TERMS

Bilevel programming, Facility location, Minimal exposure path, Wireless Sensor Networks, Border surveillance, Barrier coverage, Multi-objective optimization, Facility relocation, Trilevel programming, Network intrusion

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Brian J. Lunday, AFIT/ENS
U	U	U	U	166	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636, x4624; brian.lunday@afit.edu