NAVAL POSTGRADUATE SCHOOL

MONTEREY CALIFORNIA

THESIS

STOCHASTIC NETWORK INTERDICTION FOR DEFENSIVE COUNTER AIR OPERATIONS PLANNING

by

Charalampos I. Tsamtsaridis

December 2011

Thesis Advisor: Javier Salmeron
Second Reader: Johannes O. Royset

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Stochastic Network Interdiction for Optimizing Defensive Counter Air Operations Planning		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Charalampos I. Tsamtsaridis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis describes a stochastic, network interdiction optimization model to guide defensive, counter-air (DCA) operations planning. We model a layered, integrated air-defense system, which consists of fighter and missile engagement zones. We extend an existing two-stage, stochastic, generalized-network interdiction model by Pan, Charlton and Morton, and adapt it to DCA operations planning. The extension allows us to handle multiple-type interdiction assets, and constrain the attacker's flight path by the maximum allowable traveled distance. The defender selects the locations to install multiple interceptor types, with uncertainty in the attacker's origin and destination, in order to minimize the probability of evasion, or the expected target value collected by the evader. Then, the attacker reveals an origin-destination pair (independent of the defender's decision), and sends a strike package along a path (through the interdicted network) that maximizes his probability of evasion. By adding a small persistence penalty we ensure the plans are consistent in presence of minor variations in the number of interceptors. We present computational results for several instances of a test case consisting of the airspace over a 360-by-360 nautical miles area. The computational time ranges from some seconds to ten minutes, which is acceptable for operational use of this model.

14. SUBJECT TERMS Stochastic Optimization, Defender-Attacker Sequential Model, Mixed Integer Programming, Defensive Counter Air Operations, Integrated Air Defense System, Decision Aid			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

STOCHASTIC NETWORK INTERDICTION FOR OPTIMIZING DEFENSIVE COUNTER AIR OPERATIONS PLANNING

Charalampos I. Tsamtsaridis
Lieutenant Colonel, Hellenic Air Force
B.S., Hellenic Air Force Academy, 1992

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Charalampos I. Tsamtsaridis

Approved by: Dr. Javier Salmeron
Thesis Advisor

Dr. Johannes O. Royset
Second Reader

Dr. Robert F. Dell
Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis describes a stochastic, network interdiction optimization model to guide defensive, counter-air (DCA) operations planning. We model a layered, integrated air-defense system, which consists of fighter and missile engagement zones. We extend an existing two-stage, stochastic, generalized-network interdiction model by Pan, Charlton and Morton, and adapt it to DCA operations planning. The extension allows us to handle multiple-type interdiction assets, and constrain the attacker's flight path by the maximum allowable traveled distance. The defender selects the locations to install multiple interceptor types, with uncertainty in the attacker's origin and destination, in order to minimize the probability of evasion, or the expected target value collected by the evader. Then, the attacker reveals an origin-destination pair (independent of the defender's decision), and sends a strike package along a path (through the interdicted network) that maximizes his probability of evasion. By adding a small persistence penalty we ensure the plans are consistent in presence of minor variations in the number of interceptors. We present computational results for several instances of a test case consisting of the airspace over a 360-by-360 nautical miles area. The computational time ranges from some seconds to ten minutes, which is acceptable for operational use of this model.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. BACKGROUND....1
1. Air Defense Doctrine Preliminaries. 1
B. THESIS OBJECTIVES....4
C. LITERATURE REVIEW 5
D. THESIS ORGANIZATION....7

II. MATHEMATICAL MODEL....9
A. STOCHASTIC PROGRAMMING....9
B. DEFENSIVE, COUNTER—AIR OPTIMIZATION PROBLEM 11
C. IADS MODEL DESCRIPTION....12
1. Overview....12
2. Deterministic Model for Multiple Interceptor Types....12
a. Networks with Gains....12
b. Deterministic Model Description....13
c. Formulation 14
3. Stochastic Model for Multiple Interceptor Types....20
a. Model description....20
b. Formulation 21
4. Side Constraints in the Second-Stage Problem....25
a. Explicit Side Constraints 25
b. Heuristic Approach....27

III. COMPUTATIONAL RESULTS....29
A. TEST SCENARIO 29
1. Baseline Case Description 29
2. Baseline Case Assumptions and Modeling 31
3. Network reduction 33
B. PERSISTENCE....34
C. NUMERICAL RESULTS 35
1. Output Display 35
2. Changing the Amount of Interceptors 36
3. Changing the Number of Interceptor Types 37
4. Changing the Number of Scenarios....38
5. Considering High-Value Targets....40
6. Persistence 42

IV. CONCLUSIONS AND FUTURE DEVELOPMENT....47
A. CONCLUSIONS 47
B. FUTURE DEVELOPMENT....48

LIST OF REFERENCES....51

INITIAL DISTRIBUTION LIST....53

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. The framework of counter air operations, from Joint Publication 3-0.1 (From [3].).....2

Figure 2. Patriot SAM system, from Joint Publication 3-01 (From [3]).....3

Figure 3. An F-16C block52 fighter. [Picture by author, 2006].....3

Figure 4. The baseline case considers an area 360-by-360 nautical miles, including three location types: sources, FEZ or MEZ areas, and target nodes. Each rectangular area represents a FEZ or MEZ of 60-by-80 nautical miles, which includes the corresponding entering and leaving nodes. When a target (or targets) is located in a FEZ or MEZ, the target and area nodes are consolidated, and then the resulting node is separated. We also indicate the way the nodes are linked. Interdictable arcs link the separated nodes inside the FEZ and MEZ areas.....30

Figure 5. Comparison of the computational effort among three instances of the baseline case, with equal number of resources, but with one, two, and three types of interceptors. The horizontal axis represents the budget range b_r for one interceptor type. The respective budget range for two types is $(b_{r1}, b_{r2}) = \{(2,1),(2,2),(3.2),...,(12,12)\}$, and for three types is $(b_{r1}, b_{r2}, b_{r3}) = \{(1,1,1),(2,1,1),(2,2,1),...,(8,8,8)\}$. The more interceptor types we model, the more the computational time is needed for the same total number of interceptors.....38

Figure 6. For select budget cases, that the probability of attacker's evasion is increased as the number of scenarios $|\Omega|$ is increases.....39

Figure 7. For select budget cases, the computational effort is not increasing in $|\Omega|$.....39

Figure 8. The graph compares the computational effort in seconds, between the baseline case (with equal-value targets) and a case that involves five higher-value targets (out of 15), as a function of interceptor budget (b_{r1}, b_{r2}, b_{r3}). The computational time, on average, is slightly increased in the high-value target case.....40

Figure 9. Interceptor optimal allocation for the baseline case, considering all targets have value one, and the available budget is $(b_{r1}, b_{r1}, b_{r3}) = (4,4,4)$.....41

Figure 10. We modify the baseline case by assuming targets T3, T7, T12, T13, T14 are high-valued. The available budget is $(b_{r1}, b_{r1}, b_{r3}) = (4,4,4)$. The new optimal interceptor allocation is influenced by those targets.....42

Figure 11. The graph compares the total computational time, in minutes, for 22 sequential runs of the program, with budget values ranging from (1,1,1) to (8,8,8), and persistence penalty factors δ = 0.000, 0.001, and 0.003. The "persistent" solutions require less computational effort.....43

Figure 12. The graph compares the number of interceptor relocations, among three persistence penalty factor cases. For each case δ = 0.000, 0.001, and 0.003,

respectively, we enumerate the interceptor relocations, for different budget levels, where each optimal solution is compared to the next budget level for persistence. $\delta = 0.000$ provides optimal but not persistent solutions. $\delta = 0.003$ induces significantly fewer interceptor relocations. 44

Figure 13. The graph compares the probability of the attacker's evasion among three cases with persistence penalty factors $\delta = 0.000$, 0.001, and 0.003 respectively, as a function of the available interceptor resources. δ=0.001 and 0.003 cause a negligible increase in the probability of evasion, compared to the benefit of providing persistent solutions. 45

LIST OF TABLES

Table 1. The evasion probabilities q_{ijr} depend on: (i) the type of interceptor, (ii) the number of missiles against a 20-ship strike package, and (iii) the probability of kill of the loaded missiles.....32

Table 2. The cost of allocating an aircraft formation in a FEZ area depends on the available time over station, or on the distance to the nearest refueling point. For example, the cost for an area $(i, j) \in AI$ is one if an aircraft formation can stay on combat air patrol for 60 minutes, but it increases to three if it can only stay for 20 min, because we need three formations to cover that area for 60 minutes.....33

Table 3. Number of decision variables and constraints, in both first and second stages.....33

Table 4. The output displays the optimal interceptor allocation, as well as the attacker's flight path, the final attacking force on target and the distance $s^{\omega} - t^{\omega}$ for scenario ω_6. Budget vector is $(b_{r1}, b_{r2}, b_{r3}) = (2,2,2)$ interceptors.....36

Table 5. Numerical results testing the baseline case, including computational time in seconds, and the optimal solution (attacker's probability of evasion), as the available defender's budget (b_{r1}, b_{r2}, b_{r3}) is sequentially increased from (1,1,1) to (8,8,8).....37

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAA	anti aircraft artillery
AFDD	Air Force doctrine document
CA	counter air
CAP	combat air patrol
DCA	defensive counter air
F-16C	multi-role fighter aircraft
FEZ	fighter engagement zone
GAMS	general algebraic modeling system
IADS	integrated air defense system
IAMD	integrated air and missile defense
MEZ	missile engagement zone
OCA	offensive counter air
SAM	surface-to- air missile
SNIP	stochastic network interdiction problem

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis describes a stochastic network interdiction model to optimize the defensive counter-air (DCA) operations planning. DCA involves all those operations undertaken to defend friendly assets against enemy air and missile threats. Warfare operations, in most cases, start with defensive and offensive counter-air operations conducted to achieve air superiority, or at least a favorable air situation, which are prerequisites for further land, sea, and air operations. Control of the air is the first objective in every armed conflict—and successful employment of DCA operations is essential to achieve it.

We model a layered integrated air-defense system (IADS) structure, which consists of fighter and missile engagement zones (FEZ and MEZ, respectively), in order guide DCA planning. To do that, we adapt a two-stage, stochastic, network interdiction model by Pan, Charlton and Morton used to identify the location of detectors against nuclear smuggling. This model is based on a generalized network where an arc's gain (actually loss) for the evader represent his probability of evasion should he traverse the arc.

In the adapted attacker-defender model, the defender selects the locations to install interceptors, with uncertainty in the attacker's origin and destination. The defender's goal is to minimize the probability of evasion, or the expected target value collected by the evader. The attacker reveals an origin-destination pair (independent of the defender's decision), and sends a strike package along a path (through the interdicted network) that maximizes his probability of evasion. We extend the original model in order to handle multiple types of interdiction assets, and to constrain the attacker's flight path by a mission metric. We handle the latter by modifying the network gains to reflect dependence on the arcs' lengths, and using an adequate Lagrangian multiplier as a penalty.

The suggested defensive plans are further enhanced by adding a small persistence penalty which guarantees consistency in presence of small variations in the number of assets available to the defender. Moreover, these solutions are computed even faster than the fully optimized ones.

We employ commercial optimization software to solve an instance of the problem consisting of the airspace over a 360-by-360 nautical miles notional area. The test case includes 24 FEZ and MEZ areas, and 15 destinations, which correspond to our scenarios. (An aggregated super-source node is used to give the attacker the benefit of possible air-refueling option.) We combine three interceptors: two fighter types and one surface-to-air missile system.

We show that the computational effort to solve the IADS model is mainly affected by the number of interceptor types, for the same total amount of interceptors. Another factor that affects the computational time is the number of interdictable arcs. We also find that the computational effort is not necessarily increasing with the number of scenarios, whereas the probability of attacker's evasion is roughly proportional to the number of scenarios. Cases that involve larger-size networks (over 100 nodes and a few hundred arcs) with a combination of large values of the above parameters can make the problem intractable for tactical use, requiring several hours to solve.

Realistic air-defense problems can be modeled using networks of the size and characteristics similar to the one analyzed in this work because, for example, a FEF or MEZ (representing an interdictable arc) covers a 60-by-80 nautical miles area, whereas an interceptor unit represents four to eight fighters or a surface-to-air missile system battery. Thus, the stochastic IADS model presented in this work can contribute to the preparation phase of the DCA operations and both the operational and tactical levels of the air-war campaign.

ACKNOWLEDGMENTS

I would like to thank Professor Javier Salmeron for giving me the inspiration to conduct this work and for his generous help and guidance throughout this learning process. I would also like to thank Professor Johannes Royset for his valuable feedback to improve this thesis.

I thank my family, Aphrodite, Sofia and Dimitra. Without their presence I would have not been able to finish my postgraduate studies.

Finally, I thank Hellenic Air Force and my Country, for giving me the opportunity to study my Master's degree at Naval Postgraduate School.

Dedicated to the "Three Hundred" guarding Thermopylae.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

1. Air Defense Doctrine Preliminaries

Nowadays, most warfare operations between two adversaries start as a duel between the integrated air defense system (IADS) of one side and the suppression of enemy air defense campaign of the other. Both sides conduct Counter Air (CA) operations to achieve air superiority, or at least a favorable air situation, which are required for further land, sea, or air operations. CA operations have the goal of gaining and maintaining the necessary level of control in the air battle theater, as stated in [1]. In other words, control of the air and, furthermore, the space, is the first and ultimate objective in every armed conflict—and successful employment of CA operations is a prerequisite to achieve it. CA operations are divided into offensive counter air (OCA) and Defensive Counter Air (DCA) operations. Integrated air and missile defense (IAMD) operations are a component of OCA and DCA, according to Air Force Doctrine Document (AFDD) 2-1.1 [2]. OCA includes all of the offensive operations conducted with the objective to decrease the enemy's air power. This thesis focuses on the active DCA, and its IAMD operations component. Figure 1 shows the framework of the CA operations.

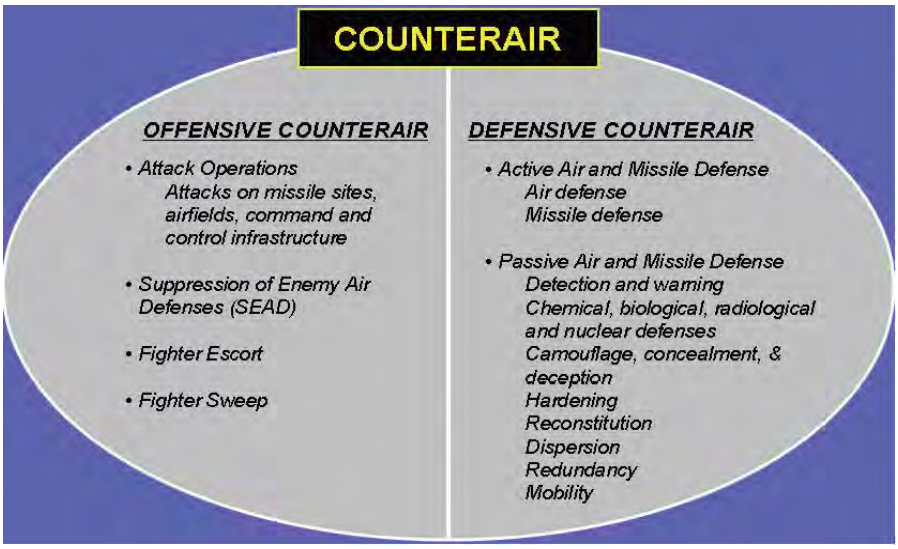

Figure 1. The framework of counter air operations, from Joint Publication 3-0.1 (From [3].)

DCA is synonymous to air defense and involves all those actions undertaken to defend friendly assets and forces (most times over a friendly territory) against enemy air and missile threats, according to Joint Publication 3-0.1 [3]. DCA is further categorized into active and passive operations. The objective of active DCA is to destroy, negate, or reduce the effectiveness of enemy attacks by engaging them with multiple air-defense weapons systems consisting of fighters, surface-to-air missiles (SAMs), or anti-aircraft artillery (AAA), as stated in AFDD 2-1.1 [2]. The targeting of enemy aircraft with multiple types of air-defense assets must be well coordinated and integrated in order to optimize combat power, minimize unengaged threats (and their effectiveness), and avoid fratricide.

An IADS synthesizes all anti-aircraft assets under a common system of command, control, communication and intelligence. The first known operational IADS occurred in the Battle of Britain and was derived manually (without computer assistance) by brilliant defensive planners, Bungay [4]. A modern IADS has multiple layers of sensors and systems. Defense in depth presupposes mutually supporting defensive positions designed to attrite and progressively weaken the enemy's air strike force, where the issues of integration, mutual support, and deconfliction of the deployed air-defense assets are

critical. Figures 2 and 3 show two different interceptor types: a Patriot SAM system; and, a F-16C block52 fighter, respectively.

Figure 2. Patriot SAM system, from Joint Publication 3-01 (From [3]).

Different air defense systems have both strengths and weaknesses. For example, fighters have the greatest range and mobility, but they have limited endurance to provide continuous coverage over a target. On the other hand, AAA and short-range SAMs provide continuous coverage, but only over limited range. Thus, efficient air-defense planning must combine and integrate multiple types of systems.

Figure 3. An F-16C block52 fighter. [Picture by author, 2006]

Point defense is a defensive tactic concept designed to protect single, vital targets, mainly employing AAA and SAM's. Area defense is planned with missile and fighter engagement zones (MEZ and FEZ, respectively), in order to protect clusters of friendly assets. Coordination of FEZ and MEZ operations present the enemy threats with the dilemma to react against two vastly different systems, which deteriorate their survivability (see Joint Publication 3–52 [5]). Additionally, the combination of area defense and point defense allows the defender to deploy more efficient tactics and protect more friendly assets with fewer resources, promoting the war principles of economy and unity of the effort. An IADS may incorporate AAA and short-range SAM systems for point defense, and fighters, long-range SAM's, and maritime forces for point or area defense.

There are many implications if two or more interceptors are assigned to engage enemy air-threats in the same area. Thus, deconfliction is one of the key requirements in air defense. In some cases, joint engagement zones are planned where a mix of defensive systems (i.e., fighters and missiles) are assigned to act in the same area, either accepting a certain probability of fratricide, or relying on identification (friend or foe) and other electronics to avoid it, according to Joint Publication 3–52 [5].

Military publications (see, e.g., Joint Airspace Control 3–52 [5]) view airspace as a "network" integrating specific critical points, routes, areas of interest (airspace control order), and weapons systems that are assigned to protect friendly assets in order to optimize the air-defense effort in the entire region. The lethality and the variety of the contemporary air threats dictate the necessity for optimizing the entire air-defense planning and execution effort, and the military operational analysis that can contribute to that goal.

B. THESIS OBJECTIVES

This thesis focuses on the active DCA operations' planning that integrates FEZ and MEZ areas into a layered IADS structure. We research in which warfare campaign level, tactical or operational, can an optimization model aid a commander with this type of air-defense planning.

We extend the stochastic network interdiction of Pan, Charlton, and Morton [6] to handle multiple types of interdiction assets, add an additional distance constraint, and adapt the resulting mathematical program to model the airspace covered by an IADS consisting of FEZ and MEZ of multiple weapons systems. We use commercial optimization software to implement and solve an instance of the problem assuming the relevant airspace over an area of 360-by-360 nautical miles, and present computational results and insights. Primarily, the network interdiction model studied in this thesis can help military planners to determine the optimal allocation of multiple types of air defense assets into FEZ and MEZ comprising a layered IADS structure. Secondly, the model presents the evader's optimal routing for every strike package scenario consisting of an origin-destination pair.

C. LITERATURE REVIEW

Network interdiction models can be employed to disrupt an adversary's ability to traverse, or send flow through a network, between two given nodes. Some of the early military applications of network interdiction appeared during the Vietnam War when McMasters and Mustin [7] developed deterministic models to optimize interdiction on enemy supply lines. Network interdiction applications include fighting against the smuggling of drugs or other illicit materials—as in Pan et al. [6] and Washburn and Wood [8], and critical infrastructure defense—as in Brown et al. [9], among others.

Stochastic network interdiction allows for some of the problem data (such as the origin and destination of the adversary) to be only known in terms of a probability distribution, as in Cormican et al. [10] and Pan et al. [6]. Two classical stochastic network interdiction problems involve removing arcs from the network in order to maximize the evader's shortest path—as in Israeli and Wood [11] , or reducing their flow capacity—as in Janjarassuk and Linderoth [12], and Wood [13].

This thesis extends the stochastic, network interdiction model described by Pan, Charlton, and Morton [6], to handle multiple types of interdiction assets. They develop a stochastic program for interdicting smuggled nuclear material, identifying locations for installing nuclear detectors to minimize the probability a smuggler can travel through a transportation network undetected. This model is stochastic because the evader's origin

and destination are unknown at the time the detectors are installed by the defender. However, the origin-destination pair (scenario) is assumed to be governed by a known probability mass function. For each possible scenario, the evader maximizes the probability of avoiding detection knowing the arcs in which detectors have been installed. The evasion probabilities for interdicted and non-interdicted arcs in the network are also assumed to be known by both the evader and the defender. This model is a leader-follower Stackelberg (sequential) game, as described in [14], because the evader decides his path after the interdictor reveals his defensive strategy.

Washburn and Wood [8] view the network interdiction problem as a simultaneous, two-person, zero-sum game, and analyze simple extensions of the basic model (including instances with undirected networks, node interdiction, multiple sources and sinks, or more complicated generalizations which allow multiple interdictors).

Cormican, Morton, and Wood [10] introduce a stochastic network interdiction model to minimize the maximum expected flow of the adversary. Here, the edge capacities are not known with certainty, and each interdiction outcome is a Bernoulli random variable (corresponding to successfully destroying an edge or failing to do so). Janjarassuk and Linderoth [12] employ a parallel decomposition algorithm on a distributed computing platform to improve the efficiency of the sampling optimization approach.

Another category of relevant work has been carried out to optimize the attacker's offensive operations, developing models, algorithms, and applications like auto-routers or mission planners for strike aircraft. For example, Royset, Carlyle, and Wood [15] develop a discrete, constrained shortest-path model for routing manned or unmanned aircraft, minimizing the risk from missile threats, while constraints limit the fuel consumption and/or flight time. The above model assumes the aircraft strike package is only subject to ground-based threats, like SAM and AAA, and the missiles effective range is represented by concentric circles. In contrast, this thesis considers that the main threat for the strike package is the fighters, as this is generally the case of similar-strength adversaries.

D. THESIS ORGANIZATION

In Chapter II we describe the DCA planning problem, and formulate the deterministic and stochastic version of our mathematical programs. In Chapter III we outline our test cases and present the computational results. Chapter IV presents our conclusions and proposes future development areas.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MATHEMATICAL MODEL

In this Chapter, we first introduce basic stochastic programming concepts and modeling approaches. Then, we introduce our IADS problem, and propose a mathematical formulation to address it.

A. STOCHASTIC PROGRAMMING

Although deterministic optimization problems assume all the addressed parameters to be known with certainty, in most real-world situations some aspects of the problem are unknown at the time when a decision needs to be made. Stochastic programming (see, e.g., Birge and Louveaux [16]) deals with optimization problems in the presence of uncertain parameters. Formulation of stochastic models depends on a number of assumptions related to the nature of the uncertainty, the degree to which that uncertainty can be modeled, and the relation between decisions and uncertain parameter realizations.

Some of the stochastic programming models take advantage of the fact that discrete probability distributions governing the uncertain parameters are known or can be estimated, for example, from historical data, as stated in Shapiro et al. [17]. Often these models are applied in cases where decisions are essentially repeated under the same conditions, and the goal is to make a decision that will perform well on average. That is, the objective is to find a solution which is feasible for all (or almost all) possible discrete cases, and optimizes the expected objective function of decisions and random variables [18]. For example, consider a simple process of minimizing the expected value of a linear function F, with a decision vector x, and a discrete random vector Y (whose probability distribution is known), where the decision has to be made before the realization of the random variable:

$$\min_{x \in X} \mathrm{E}\left[F(x;Y)\right] \tag{1}$$

In what follows, we shall assume that Y is finite, with potential outcomes (scenarios) $\Omega = \{\omega_1, ..., \omega_n\}$, and probabilities $\Pr(\omega) = P^\omega$, where $\sum_{\omega \in \Omega} P^\omega = 1$. If the decision making

process repeats itself many times, then a certain x will be optimal on average, and model (1) seeks to find that decision vector.

Stochastic programming can also be applied to cases in which we need to make a one-time decision. The complication in this case is the choice of objective function. For example, minimizing expected cost as in (1) is less legitimate in this case given that many individual scenarios may result in much worse outcomes. Thus, the measure and/or control of risk that we adopt play an important role in the outcome of our model (see Shapiro et al. [17]).

If the random vector Y is replaced by its mean μ_Y, then the modified problem is a deterministic instance:

$$\min_{x \in X} F(x, \mu_Y) \ , \tag{2}$$

whose optimal solution may be very different from that of the original stochastic problem (1), because formulation (2) does not take into account the variability of random vector Y [18]. For example, if F is convex, according to Jensen's inequality: $\min_{x \in X} F(x; \mu_Y) \leq \min_{x \in X} \mathrm{E}\left[F(x; Y)\right]$.

A common model of stochastic programming is the two-stage linear program with recourse actions. In these models, the decision-maker's initial decision, x, occurs in a first stage, before the random event $\omega \in \Omega$ occurs. Then, he can still make a retrospective decision in a second stage, which will offset some of the negative impact that may have been recorded as a result of the first decision. For each x in the first-stage, there is a set of recourse decisions, because a different action may need to be taken for each random outcome $\omega \in \Omega$ [17]. The expected value $\mathrm{E}\left[F(x; Y)\right]$ is calculated as the weighted sum of the n discrete scenarios, and the stochastic problem (1) is modeled as a deterministic equivalent:

$$\min_{x \in X} \sum_{\omega \in \Omega} P^{\omega} h(x; \omega) \tag{3}$$

where the expression (3) is the first-stage problem, and

$$h(x; \omega) \tag{4}$$

represents the deterministic, second-stage problem for scenario realization $\omega \in \Omega$.

Stochastic problems are usually very large, and therefore much of the research effort has been devoted to developing algorithms that exploit their structure. For example, if the second stage is a convex problem, the stochastic problem can be solved by Benders' Decomposition: For any given value of the first-stage (complicating) variables we may solve (and retrieve duals from) the second stage problem, which is also separable for each scenario $\omega \in \Omega$.

Although two-stage, linear programs with recourse are often regarded as the classic example of stochastic optimization; stochastic programming has expanded to include a wide range of models and approaches. An alternative approach uses the so-called chance constraints. Here, constraints are required to be satisfied only with certain probability, which provides a significant relaxation to an optimization problem; see Birge and Louveaux [16].

A natural generalization of the two-stage model is the multi-stage model. In this case, each stage consists of a decision followed by a series of observations of uncertain parameters that are emerging gradually over time. In this context, stochastic programming is closely related to decision analysis, stochastic control theory, Markov processes, and dynamic programming; see, e.g., Ruszczynski and Shapiro [18].

B. DEFENSIVE, COUNTER—AIR OPTIMIZATION PROBLEM

The optimization problem addressed in this thesis involves two adversaries, an evader (attacker) and an interdictor (defender). The area of operations is designed as a directed network $G(N,A)$ where N and A are the sets of nodes and arcs, respectively. The attacker executes OCA operations that consist of sending an aircraft strike package from a specific origin point s, traversing a path through the network defensive positions, and reaching the desired target t, in order to hit its target. Node s represents the aircraft package base (or its last air refueling point into friendly territory), whereas t represents the target (or a weapons release point against that target) that the defender is trying to protect. On the other hand, the defender designs his air defense plan to obtain the maximum survivability for his assets, by maximizing the attrition rate of the strike

package. The defender's decisions include how to organize point and area defense, and how to allocate limited resources to the planned MEZ and FEZ layered IADS structure in order to optimize DCA operations. The resources include different types of air-defense weapons systems. The attacker, having being fully informed of the adversary's DCA plan, selects the strike package path that ensures a minimum attrition rate (maximum probability of evasion) through all encountered defensive systems to the target. We assume that all air-defense assets are visible to the attacker, which is common given the capabilities of modern detection systems.

In the deterministic version of the problem, we consider that the defender knows the strike package's origin and destination exactly, and that he adjusts his defensive plan to that particular scenario. In contrast, when the defender is uncertain about the adversary's plan, he has to account for every feasible origin-destination scenario. In that case, he decides a single plan that minimizes the probability of a strike package evasion (perhaps prioritized by target value) over all possible scenarios.

C. IADS MODEL DESCRIPTION

1. Overview

Pan et al. [6] formulate a Stochastic Network Interdiction Problem (SNIP) for identifying locations where nuclear detectors can be installed in order to combat nuclear smuggling. Their model is a two-stage, stochastic, mixed-integer program. We extend the SNIP, which assumes a single detector type, to allow several types of air-defense interceptors. We then constrain the attacker's second-stage problem (shortest path in terms of the probability of interception) on a mission-specific metric, to a maximum allowable traveled distance. For clarity, we first describe the deterministic version of the model, and then continue with the stochastic one.

2. Deterministic Model for Multiple Interceptor Types

a. Networks with Gains

Network flow models can be roughly divided into two broad categories: pure (or ordinary) and generalized (or "with gains") models. Consider a directed network

$G(N, A)$. Pure network flow models assume conservation of the flow in all nodes or arcs, which means that the flow arriving at a node equals the flow exiting that node, or similarly, the flow entering an arc leaves that arc in its entirety, as described in Bertsekas [19]. Respectively, the generalized network models assign a gain (or loss) factor (i.e., a positive multiplier g_{ij}) to every arc $(i, j) \in A$, such that the flow passing the arc will be augmented (or, more frequently in practice, diminished) after it is multiplied by that factor. Therefore, after flow y_{ij} leaves node *i,* it arrives to node *j* as $g_{ij} y_{ij}$, and the associated conservation of flow constrains are:

$$\sum_{(i,j)\in RS(i)} y_{ij} - \sum_{(j,i)\in FS(i)} g_{ij} y_{ij} = s_i \quad \forall i \in N,$$

where *FS*(*i*) and *RS*(*i*) are the set of arcs leaving and entering node *i* respectively, and s_i is the divergence of node *i* [19]. The relaxation of the flow conservation assumption is very useful to model some problems, but it also complicates the solvability of the models. The generalized network flow approach is the key feature that allows the extension of SNIP to model the air-defense problem with multiple interceptor types.

b. Deterministic Model Description

The deterministic model assumes the airspace over the area of operations is represented by a directed network $G(N, A)$. The attacker sends an aircraft strike package departing from a specific origin node $s \in N$ to a specific destination node $t \in N$ through the network. The defender allocates his interception resources to the arcs of the network in order to minimize the probability of evasion (maximize the attrition rate) of the strike package, knowing its origin-destination pair. If the defender has allocated an interceptor of type $r \in R$ on an arc (i, j), then the probability of strike package evasion (if that arc is traversed) is q_{ijr}. If no interceptor has been installed on arc (i, j), the nominal probability of evasion is p_{ij} (where $p_{ij} < q_{ijr} \quad \forall (i, j) \in A, \ \forall r \in R$). In other words, p_{ij} and q_{ijr} are the network gain (actually loss) factors used to model the attrition rate of the attacker's force. We also follow Pan et al.'s [6] assumption that the

probabilities of the strike package being intercepted at the successive arcs, in a selected path, are independent. We discuss the consequences of this assumption later in this thesis.

c. Formulation

We use the following notation to formulate the deterministic model:

Indices and index sets:

$G(N, A)$	directed network with node set N and arc set A
$(i, j) \in A$	arcs in $G(N, A)$
$s, t \in N$	source and sink nodes (evader's origin and destination, respectively)
$FS(i)$	set of arcs leaving node i ("forward star")
$RS(i)$	set of arcs entering node i ("reverse star")
$AI \subset A$	set of arcs where an interceptor of any type can be installed
$r \in R$	interceptor types, e.g., $R = \{r_1, r_2, r_3\}$ is used in all of our test cases

Data [units]:

b_r	number of available interceptors of type $r \in R$ [interceptors]
c_{ijr}	number of interceptors of type $r \in R$ to cover arc $(i, j) \in AI$ for the duration of the planning horizon [interceptors]
p_{ij}	nominal probability of evasion if the attacker traverses an arc $(i, j) \in A$ where no interceptor is installed
q_{ijr}	probability of evasion if the attacker traverses an arc $(i, j) \in AI$ where an interceptor of type $r \in R$ is installed

Defender's decision variables:

x_{ijr} takes value 1 if an interceptor of type $r \in R$ is installed on arc $(i, j) \in AI$, and 0 otherwise

Attacker's decision variables:

y_{ij} takes a positive value only if the attacker traverses arc $(i, j) \in A$ and no interceptor is installed on that arc, and represents the probability of evasion up to arc (i, j)

z_{ijr} takes a positive value only if the attacker traverses arc $(i, j) \in AI$ and an interceptor of type $r \in R$ is installed on that arc, and represents the probability of evasion up to arc (i, j)

$\tilde{y}_t$ probability of evasion up to target node

Deterministic IADS model formulation:

$$\min_{x \in X} \; h\left(x;(s,t)\right) \tag{1.1a}$$

subject to

$$X = \left\{ x: \begin{array}{ll} \sum\limits_{(i,j)\in AI} c_{ijr} x_{ijr} \le b_r & \forall r \in R \\ \sum\limits_{r \in R} x_{ijr} \le 1 & \forall (i,j) \in AI \\ x_{ijr} \in \{0,1\} & \forall (i,j) \in AI, \;\; \forall r \in R \end{array} \right\}, \tag{1.1b}$$

where:

$$h\left(x;(s,t)\right) = \max_{\tilde{y},\mathbf{y},\mathbf{z}} \tilde{y}_t \tag{1.2a}$$

s.t.:

$$\sum_{(s,j)\in FS(s)} y_{sj} + \sum_{(s,j)\in FS(s)\cap AI} \sum_{r \in R} z_{sjr} = 1 \tag{1.2b}$$

$$\sum_{(i,j)\in FS(i)} y_{ij} + \sum_{(i,j)\in FS(i)\cap AI} \sum_{r\in R} z_{ijr}$$

$$- \sum_{(j,i)\in RS(i)} p_{ji} y_{ji} - \sum_{(j,i)\in RS(i)\cap AI} \sum_{r\in R} q_{jir} z_{jir} = 0 \qquad \forall i \in N \setminus \{s,t\} \tag{1.2c}$$

$$\tilde{y}_t - \sum_{(j,t)\in RS(t)} p_{jt} y_{jt} + \sum_{(j,t)\in RS(t)\cap AI} \sum_{r\in R} q_{jtr} z_{jtr} = 0 \tag{1.2d}$$

$$0 \le y_{ij} \le 1 - x_{ijr} \quad \forall (i,j) \in AI, \quad \forall r \in R \tag{1.2e}$$

$$0 \le z_{ijr} \le x_{ijr} \quad \forall (i,j) \in AI, \quad \forall r \in R \tag{1.2f}$$

$$\tilde{y}_t \text{ unrestricted}, \; y_{ij}, \; z_{ijr} \ge 0, \; \forall (i,j) \in A, \; \forall r \in R \tag{1.2g}$$

Formulations (1.1) and (1.2) represent the mixed-integer, linear problem of the defender, and the linear problem of the attacker, respectively. The objective function (1.1a) minimizes the probability of attacker's evasion, while (1.2a) maximizes that probability. The set of the feasible interceptor allocations on the arcs $(i,j) \in AI$ are defined by (1.1b) which comprise budget and deconfliction (at most one interceptor in each arc) constraints.

The attacker's subproblem (1.2) follows the generalized network flow modeling approach. Each interdictable arc $(i,j) \in AI$ may be thought of as multiple arcs between *i* and *j* (one arc for no interceptor, and one arc for each interceptor type). If an interceptor of type $r \in R$ is installed on arc $(i,j) \in AI$ (that is, if $x_{ijr} = 1$), then the flow z_{ijr} will only traverse the relevant interceptor's arc. If no interceptor is located on arc $(i,j) \in A,$ then (1.2e) and (1.2f) ensure that $x_{ijr} = 0$, and the flow y_{ij} will only traverse the "no interceptor" arc with nominal (typically low) probability of attrition. The initial unity flow that the attacker sends from node *s* to node *t* is decreased by factors p_{ij} and q_{ijr}, along the selected path. The fraction of the flow that arrives at the end node *t* represents the overall probability of attacker's evasion. Its value, $\tilde{y}_t$, is given by:

$$\tilde{y}_t = \prod_{(i,j)\in A\setminus AI} p_{ij} \prod_{(i,j)\in AI} \left[\left(p_{ij}(1 - \sum_{r\in R} x_{ijr}) \right) + \left(\sum_{r\in R} q_{ijr} x_{ijr} \right) \right],$$

but its correct calculation is ensured by constraints (1.2b)–(1.2d).

The assumption that the attacker solves his optimization shortest-path problem before selecting a path is pessimistic for the defender, but necessary in the absence of additional information.

The min-max structure of the model does not allow us to solve it as a standard optimization problem. A possible solution approach consists of taking the dual attacker's linear subproblem, in order to formulate a model that simultaneously minimizes over the defender's primal variables and the attacker's dual variables.

An issue in taking the dual of subproblem (1.2) and, specifically, dualizing constraints (1.2e) and (1.2f), is that nonlinear terms arise involving the defender's decision variables x_{ijr} and the duals of those constraints. We follow the technique of Pan et al. [6], who relax problem (1.2) by eliminating constraints (1.2e) and (1.2f), and add a penalty into the objective function (1.2a) when these constraints are violated. So the attacker's subproblem (1.2) is restated as follows:

Relaxation of the attacker's subproblem:

$$\max_{\tilde{y}_t,\mathbf{y},\mathbf{z}} \tilde{y}_t - \sum_{(i,j)\in AI} \lambda_{ij} \left[\left(y_{ij} - \sum_{r\in R} \left(1 - x_{ijr}\right) \right)^+ + \sum_{r\in R} \left(z_{ijr} - x_{ijr} \right)^+ \right], \tag{1.3a}$$

which can be restated as:

$$\max_{\tilde{y}_t,\mathbf{y},\mathbf{z}} \tilde{y}_t - \sum_{(i,j)\in AI} \lambda_{ij} \left[\left(\sum_{r\in R} x_{ijr} \right) y_{ij} + \sum_{r\in R} \left(1 - x_{ijr}\right) z_{ijr} \right] \tag{1.3b}$$

s.t.: Duals

$$\sum_{(s,j)\in FS(s)} y_{sj} + \sum_{(s,j)\in FS(s)\cap AI} \sum_{r\in R} z_{sjr} = 1 \qquad [\pi_s] \tag{1.3c}$$

$$\sum_{(i,j)\in FS(i)} y_{ij} + \sum_{(i,j)\in FS(i)\cap AI} \sum_{r\in R} z_{ijr} - \sum_{(j,i)\in RS(i)} p_{ji} y_{ji} - \sum_{(j,i)\in RS(i)\cap AI} \sum_{r\in R} q_{jir} z_{jir} = 0 \qquad \forall i \in N \setminus \{s,t\} \qquad [\pi_i] \tag{1.3d}$$

$$\tilde{y}_t - \sum_{(j,t)\in RS(t)} p_{jt} y_{jt} + \sum_{(j,t)\in RS(t)\cap AI} \sum_{r\in R} q_{jtr} z_{jtr} = 0 \qquad [\pi_t] \tag{1.3e}$$

$\tilde{y}_t$ unrestricted, y_{ij}, $z_{ijr} \geq 0$, $\forall (i,j) \in A$, $\forall r \in R$ (1.3f)

We impose a penalty only when the eliminated constraints are violated (that is, only when the relevant terms in (1.3a) take positive values). The objective function (1.3b) results from (1.3a) because of the binary nature of the decision variable x_{ijr}. Therefore:

$$\left[y_{ij} - \sum_{r \in R} \left(1 - x_{ijr}\right) \right]^+ = \left(\sum_{r \in R} x_{ijr} \right) y_{ij} \text{ and } \sum_{r \in R} \left(z_{ijr} - x_{ijr} \right)^+ = \sum_{r \in R} \left(1 - x_{ijr}\right) z_{ijr} \quad \forall (i,j) \in AI .$$

A valid value for the Lagrangian multiplier λ_{ij} in the objective function (1.3a) is one because the duals of the respective constraints (1.2e) and (1.2f) cannot exceed that value, given that the network gains p_{ij}, q_{ijr} $\forall (i,j) \in A$, $\forall r \in R$ are at most one. This multiplier could be made tighter (i.e., smaller) based on the problem characteristics, strengthening the subsequent formulation of the defender's problem.

Next, we take the dual of the relaxed attacker's subproblem:

Dual of the attacker's subproblem:

$$\min_{\pi} \pi_s \qquad (1.4a)$$

s.t.: Duals

$$\pi_i - p_{ij}\pi_j \geq 0 \quad \forall (i,j) \in A \setminus AI \qquad [y_{ij}] \qquad (1.4b)$$

$$\pi_i - p_{ij}\pi_j \geq -\lambda_{ij} \sum_{r \in R} x_{ijr} \quad \forall (i,j) \in AI \qquad [y_{ij}] \qquad (1.4c)$$

$$\pi_i - q_{ijr}\pi_j \geq -\lambda_{ij} \left(1 - x_{ijr}\right) \quad \forall (i,j) \in AI, \quad \forall r \in R \qquad [z_{ijr}] \qquad (1.4d)$$

$$\pi_t = 1 \qquad [\tilde{y}_t] \qquad (1.4e)$$

$$\pi_i \text{ unrestricted } \forall i \in N \qquad (1.4f)$$

By strong duality, model (1.4a)–(1.4f) is another expression of $h\left(x;(s,t)\right)$, provided either model possesses an optimal solution. By construction, this is always the case. Dual decision variable π_i is interpreted as the conditional probability the attacker traverses a path from a node *i* to the destination node *t* without being intercepted, given he has arrived the node *i* without being intercepted, as in Pan et al. [6]. Thus, π_s represents the probability of the attacker's interception for the selected *s*-*t* path, while the objective function (1.4a) minimizes that probability, and constraints (1.4b)–(1.4d) ensure its correct computation. Constraint (1.4b) refers to the non-interdictable arcs, whereas constraints (1.4c) and (1.4d) affect the interdictable ones. The expressions (1.4c) and (1.4d) are controlled by the binary nature of the defender's decision variable x_{ijr}. When $x_{ijr}=1$, that is, when an interceptor of type $r \in R$ has been located on arc $(i,j) \in AI$, constraint (1.4c) is void, because the flow follows the interceptor arc. Similarly, when no interceptor has been located on arc $(i,j) \in AI$, the flow proceeds through the "no interceptor" arc, and the expression (1.4d) is void. Constraint (1.4e) defines the conditional probability that the attacker will not be intercepted, given he reaches destination node *t* without being intercepted, as equal to one.

Finally, the original deterministic optimization problem (1.1) is restated as the following minimization, mixed-integer, linear program:

<u>Deterministic IADS model reformulation as a mixed-integer, linear program:</u>

$$\min_{x,\pi} \quad \pi_s \tag{1.5a}$$

s.t.:

$$X = \left\{ x: \begin{array}{ll} \displaystyle\sum_{(i,j)\in AI} c_{ijr} x_{ijr} \le b_r & \forall r \in R \\ \displaystyle\sum_{r\in R} x_{ijr} \le 1 & \forall (i,j) \in AI \\ x_{ijr} \in \{0,1\} & \forall (i,j) \in AI, \ \forall r \in R \end{array} \right\} \tag{1.5b}$$

Duals

$$\pi_i - p_{ij}\pi_j \geq 0 \qquad \forall (i,j) \in A \setminus AI \qquad \left[y_{ij} \right] \quad (1.5c)$$

$$\pi_i - p_{ij}\pi_j + \lambda_{ij} \sum_{r \in R} x_{ijr} \geq 0 \qquad \forall (i,j) \in AI \qquad \left[y_{ij} \right] \quad (1.5d)$$

$$\pi_i - q_{ijr}\pi_j + \lambda_{ij}(1 - x_{ijr}) \geq 0 \qquad \forall (i,j) \in AI \qquad \left[z_{ijr} \right] \quad (1.5e)$$

$$\pi_t = 1 \qquad \left[\tilde{y}_{t^\omega} \right] \quad (1.5f)$$

$$\pi_i \text{ unrestricted } \forall i \in N \quad (1.5g)$$

Formulation (1.5) addresses the deterministic problem as a standard minimization problem, in which we are simultaneously optimizing over both the defender's and attacker's decision variables. Its solution can be obtained via standard mixed-integer programming algorithms, and/or by using commercially available optimization software.

3. Stochastic Model for Multiple Interceptor Types

a. Model description

In the stochastic problem we assume that the defender is not aware of the (*s,t*) choice made by the attacker. However, he can enumerate a number of possible scenarios $\omega \in \Omega$ and assign probabilities P^ω to each of them based, for example, on intelligence reports, or analysis of the current operational and tactical situation. The attacker's origin and destination is considered a random vector (S,T), whose realization (s^ω, t^ω) is revealed only after the defender's decisions, x_{ijr}, $\forall (i,j) \in AI$, $\forall r \in R$, have been made. The attacker's model selects the optimum path after each (s^ω, t^ω) realization in order to maximize the probability of evasion under that scenario. The defender's objective is to find a solution that performs well for all scenarios, on average, without subordinating the decisions to any particular one. We also assign a value V^ω to target t^ω in order to

prioritize the targets to protect: an evader traversing the network and reaching this target with probability $\tilde{y}_{t^\omega}$ is assumed to collect $\tilde{y}_{t^\omega} V^\omega$ units of value.

We next formulate the problem of minimizing the expected value collected as a function of defender's decisions over all the possible outcomes of random vector (S,T).

b. Formulation

We add the below notation in order to formulate the stochastic IADS model.

Additional notation for the stochastic IADS model:

$\omega \in \Omega$	scenario set, assumed to be finite
P^ω	probability of scenario ω
(s^ω, t^ω)	realization of random origin-destination pair for scenario ω
V^ω	a value assigned to the target t^ω of scenario ω

Stochastic IADS model formulation:

$$\min_{x \in X} F\left(x;(S,T)\right) =$$

$$\min_{x \in X} \sum_{\omega \in \Omega} h\left(x;(s^\omega,t^\omega)\right) P^\omega V^\omega \tag{2.1a}$$

s.t.:

$$X = \left\{ x: \begin{array}{ll} \sum\limits_{(i,j)\in AI} c_{ijr} x_{ijr} \le b_r & \forall r \in R \\ \sum\limits_{r \in R} x_{ijr} \le 1 & \forall (i,j) \in AI \\ x_{ijr} \in \{0,1\} & \forall (i,j) \in AI, \ \forall r \in R \end{array} \right\}, \tag{2.1b}$$

where:

$$h\left(x;(s^\omega,t^\omega)\right) = \max_{\tilde{y}_{t^\omega}, \mathbf{y}, \mathbf{z}} \tilde{y}_{t^\omega} \tag{2.2a}$$

s.t.:

$$\sum_{(s^\omega,j)\in FS(s^\omega)} y_{s^\omega j} + \sum_{(s^\omega,j)\in FS(s^\omega)\cap AI} \sum_{r\in R} z_{s^\omega jr} = 1 \tag{2.2b}$$

$$\sum_{(i,j)\in FS(i)} y_{ij} + \sum_{(i,j)\in FS(i)\cap AI} \sum_{r\in R} z_{ijr}$$

$$- \sum_{(j,i)\in RS(i)} p_{ji} y_{ji} - \sum_{(j,i)\in RS(i)\cap AI} \sum_{r\in R} q_{jir} z_{jir} = 0 \qquad \forall i \in N \setminus \{s^\omega, t^\omega\} \tag{2.2c}$$

$$\tilde{y}_{t^\omega} - \sum_{(j,t^\omega)\in RS(t^\omega)} p_{jt^\omega} y_{jt^\omega} + \sum_{(j,t^\omega)\in RS(t^\omega)\cap AI} \sum_{r\in R} q_{jt^\omega r} z_{jt^\omega r} = 0 \tag{2.2d}$$

$$0 \le y_{ij} \le 1 - x_{ijr} \quad \forall (i,j) \in AI, \quad \forall r \in R \tag{2.2e}$$

$$0 \le z_{ijr} \le x_{ijr} \quad \forall (i,j) \in AI, \quad \forall r \in R \tag{2.2f}$$

$$\tilde{y}_{t^\omega} \text{ unrestricted, } y_{ij}, \ z_{ijr} \ge 0, \ \forall (i,j) \in A, \ \forall r \in R \tag{2.2g}$$

Formulation (2.2) models the attacker's second stage problem, which is linear as in the deterministic subproblem (1.2), for every scenario $\omega \in \Omega$. The objective function (2.2a) now maximizes the conditional probability of attacker's evasion, given $(S,T) = (s^\omega, t^\omega)$. The objective function (2.1a) is the expected value collected across the targets the evader can reach, where the expectation is taken over all possible scenarios.

The set X in (2.1b) defines the feasible interceptor allocations as in the deterministic version. The expressions (2.2b)-(2.2g) restrict the attacker's linear subproblem, and have the same interpretation as in the deterministic version, because they refer to each possible (s^ω, t^ω) realization separately.

The stochastic version of the problem is also a sequential game. First, the defender decides how to allocate his interceptors. Second, the attacker solves the problem for a (s^ω, t^ω) realization and decides the optimal path that minimizes the probability of being intercepted.

Next, we derive the relaxation of the attacker's second stage problem by eliminating constraints (2.2e) and (2.2f), and then take the dual of that relaxed problem.

Relaxation of the attacker's second-stage problem:

$$\max_{\tilde{y}_{t^\omega},\mathbf{y},\mathbf{z}} \tilde{y}_{t^\omega} - \sum_{(i,j)\in AI} \lambda_{ij} \left[\left(y_{ij} - \sum_{r\in R} \left(1 - x_{ijr}\right) \right)^+ + \sum_{r\in R} \left(z_{ijr} - x_{ijr} \right)^+ \right]$$

which can be restated as:

$$\max_{\tilde{y}_{t^\omega},\mathbf{y},\mathbf{z}} \tilde{y}_{t^\omega} - \sum_{(i,j)\in AI} \lambda_{ij} \left[\left(\sum_{r\in R} x_{ijr} \right) y_{ij} + \sum_{r\in R} \left(1 - x_{ijr}\right) z_{ijr} \right] \quad (2.3a)$$

s.t.: Duals

$$\sum_{(s^\omega,j)\in FS(s^\omega)} y_{s^\omega j} + \sum_{(s^\omega,j)\in FS(s^\omega)\cap AI} \sum_{r\in R} z_{s^\omega jr} = 1 \qquad \left[\pi_{s^\omega}\right] \quad (2.3b)$$

$$\sum_{(i,j)\in FS(i)} y_{ij} + \sum_{(i,j)\in FS(i)\cap AI} \sum_{r\in R} z_{ijr} - \sum_{(j,i)\in RS(i)} p_{ji} y_{ji} - \sum_{(j,i)\in RS(i)\cap AI} \sum_{r\in R} q_{jir} z_{jir} = 0 \qquad \forall i \in N \setminus \{s^\omega, t^\omega\} \qquad \left[\pi_i\right] \quad (2.3c)$$

$$\tilde{y}_{t^\omega} - \sum_{(j,t^\omega)\in RS(t^\omega)} p_{jt^\omega} y_{jt^\omega} + \sum_{(j,t^\omega)\in RS(t^\omega)\cap AI} \sum_{r\in R} q_{jt^\omega r} z_{jt^\omega r} = 0 \qquad \left[\pi_{t^\omega}\right] \quad (2.3d)$$

$\tilde{y}_{t^\omega}$ unrestricted, y_{ij}, $z_{ijr} \geq 0$, $\forall (i,j) \in A$, $\forall r \in R$ (2.3e)

The rationale for the Lagrangian multiplier λ_{ij} and the resulting penalty term in the objective function (2.3a) are the same as those described in the deterministic version of the problem, see equation (1.3a). Formulation (2.3) is an instance of model (1.3) for each scenario $\omega \in \Omega$.

The dual of the relaxed attacker's second stage problem is as follows:

Dual of the attacker's second-stage problem:

$$\min_{\pi} \ \pi_{s^\omega} \quad (2.4a)$$

s.t.: Duals

$$\pi_i - p_{ij}\pi_j \geq 0 \quad \forall (i,j) \in A \setminus AI \qquad [y_{ij}] \quad (2.4b)$$

$$\pi_i - p_{ij}\pi_j \geq -\lambda_{ij} \sum_{r\in R} x_{ijr} \quad \forall (i,j) \in AI \qquad [y_{ij}] \quad (2.4c)$$

$$\pi_i - q_{ijr}\pi_j \geq -\lambda_{ij} \left(x_{ijr} - 1\right) \quad \forall (i,j) \in AI, \quad \forall r \in R \qquad [z_{ijr}] \quad (2.4d)$$

$$\pi_{t^\omega} = 1 \quad \forall \omega \in \Omega \qquad \left[\tilde{y}_{t^\omega}\right] \quad (2.4e)$$

π_i unrestricted $\forall i \in N$ (2.4f)

The inner sub-problem (2.4) has the same optimal solution as (2.3). The interpretation of the dual decision variables, $\pi_i, \pi_{s^\omega}, \pi_{t^\omega}$, is the same as that given for π_i, π_s, π_t in model (1.4).

Stochastic IADS model reformulation as a two-stage, stochastic, mixed-integer, linear program:

$$\min_{x,\pi} \sum_{\omega \in \Omega} \pi_{s^\omega} P^\omega V^\omega \quad (2.5a)$$

s. t.:

$$X = \left\{ x: \begin{array}{l} \sum_{(i,j) \in AI} c_{ijr} x_{ijr} \le b_r \quad \forall r \in R \\ \sum_{r \in R} x_{ijr} \le 1 \quad \forall (i,j) \in AI \\ x_{ijr} \in \{0,1\} \quad \forall (i,j) \in AI, \ \forall r \in R \end{array} \right\} \quad (2.5b)$$

Duals

$\pi_i^\omega - p_{ij} \pi_j^\omega \ge 0 \qquad \forall (i,j) \in A \setminus AI, \ \forall \omega \in \Omega$ $\left[y_{ij}^\omega \right]$ (2.5c)

$\pi_i^\omega - p_{ij} \pi_j^\omega + \lambda_{ij} \sum_{r \in R} x_{ijr} \ge 0 \qquad \forall (i,j) \in AI, \ \forall \omega \in \Omega$ $\left[y_{ij}^\omega \right]$ (2.5d)

$\pi_i^\omega - q_{ijr} \pi_j^\omega + \lambda_{ij} (1 - x_{ijr}) \ge 0 \qquad \forall (i,j) \in AI, \quad \forall r \in R$ $\left[z_{ijr}^\omega \right]$ (2.5e)

$\pi_{t^\omega} = 1 \qquad \forall \omega \in \Omega$ $\left[\tilde{y}_{t^\omega} \right]$ (2.5f)

π_i unrestricted, $\forall i \in N$ (2.5g)

Formulation (2.5) is a stochastic linear mixed-integer program, which minimizes the maximum average expected value collected by the attacker over the defined scenarios $\omega \in \Omega$.

4. Side Constraints in the Second-Stage Problem

The attacker's second stage program is a shortest-path problem on a generalized network. This problem computes the unconstrained evader's shortest path, where the length of the path is considered his probability of evasion.

Some of the evader's shortest paths may be infeasible in a real-world situation due to, for example, flight distance, fuel, or time. We choose to constrain the model on a maximum allowable traveling distance given that fuel quantity and consumption is aircraft dependent, and flight time does not always reflect the distance traveled.

Generally, side constraints complicate the problem's solution because they cause a departure from the original network structure. In our problem, complications may arise from split flow (e.g., two fractional paths) for certain (s^{ω}, t^{ω}) pairs, i.e., the integer character of the computed solution may be lost, as described in Bertsekas [19]. We propose two options to constrain the second-stage attacker's problem: (a) explicitly add side constraints, and (b) follow an approximation solution (i.e., a heuristic).

a. Explicit Side Constraints

We add the below notation to: (i) impose additional side constraints to problem (2.2), which becomes a constrained, shortest-path problem; and, (ii) maintain integrality in our solution, by explicitly introducing integer constraints on the arc flows.

Variable:

ξ_{ij} a binary variable that takes value 1 if arc (i, j) is in the $s^{\omega} - t^{\omega}$ path (for the incumbent scenario $\omega \in \Omega$), and 0 otherwise

Data:

d_{ij} length of arc $(i, j) \in A$ [nautical miles]

D maximum allowable distance for all $s^{\omega} - t^{\omega}$ paths [nautical miles]

Formulation of additional side constraints for scenario $\omega \in \Omega$:

$$\sum_{(s^\omega, j) \in FS(s^\omega)} \xi_{s^\omega j} - \sum_{(j, s^\omega) \in RS(s^\omega)} \xi_{j s^\omega} = 1 \tag{2.2h}$$

$$\sum_{(i,j) \in FS(i)} \xi_{ij} - \sum_{(j,i) \in RS(i)} \xi_{ji} = 0 \quad \forall i \in N \setminus \left\{ s^\omega, t^\omega \right\} \tag{2.2i}$$

$$\sum_{(t^\omega, j) \in FS(t^\omega)} \xi_{t^\omega j} - \sum_{(j, t^\omega) \in RS(t^\omega)} \xi_{j t^\omega} = -1 \tag{2.2j}$$

$$0 \le y_{ij} \le \xi_{ij} \qquad \forall (i,j) \in A \tag{2.2k}$$

$$0 \le \sum_{r \in R} z_{ijr} \le \xi_{ij} \qquad \forall (i,j) \in AI, \quad \forall r \in R \tag{2.2l}$$

$$\sum_{(i,j) \in A} \xi_{ij} d_{ij} \le D \tag{2.2m}$$

$$\xi_{ij} \in \{0,1\} \qquad \forall (i,j) \in A \tag{2.2n}$$

Constraints (2.2h)-(2.2j) ensure the conservation of the flow for the new binary variables for every $s^\omega - t^\omega$ path. Constraints (2.2k) and (2.2l) force ξ_{ij} to be 1 whenever the y_{ij} or z_{ijr} decision variables take a positive value. Finally, constraint (2.2m) restricts the evader's optimal path, for every scenario ω, to not exceed the maximum distance D.

Pan et al. [6] prove that the SNIP model is NP-hard, while the related decision problem is NP-complete. Therefore, the same applies to the stochastic IADS model. In addition, if we pursue the described solution strategy by eliminating constraints (2.2k), (2.2l) and adding the respective penalty term into the objective function (2.2a), nonlinear terms (involving products of binary and continuous variables) appear. Unfortunately, taking the dual of the updated second-stage problem, the primal variables reappear in the dual problem's constraints. Even if we could linearize the non-linear terms in the resulting objective function, this solution approach is computationally limited by the rapid explosion in the model's size and the weakness in the linearization of the nonlinear terms. Given the inherent complexity of the model, we prefer to discard this approach and employ a heuristic approach.

b. Heuristic Approach

In this approach, similar to Bertsekas [19], we discard constraints (2.2h)-(2.2n) and use a heuristic to compensate for the violated maximum distance constraint (2.2n). Then, instead of correcting the arc lengths (probabilities of evasion) as in [19], we correct the network's gains $p_{ij}, q_{ijr} \quad \forall (i,j) \in A, \quad \forall r \in R$ to reflect a dependence on the arc coefficient d_{ij}. Let μ be the Lagrange multiplier for constraint (2.2m). The corrected network gains in the expressions (2.5c)-(2.5e) have the form:

$$\hat{p}_{ij} = p_{ij} - \mu d_{ij} \quad \forall (i,j) \in A \tag{3.1}$$

$$\hat{q}_{ijr} = q_{ijr} - \mu d_{ij} \quad \forall (i,j) \in AI, \quad \forall r \in R \tag{3.2}$$

In practice, we choose μ to be a small, positive penalty factor. We restrict the second-stage, shortest-path problem on a maximum allowable traveled distance, replacing the corrected network gains (3.1) and (3.2) into the (2.5) formulation.

The method is efficient because it can compensate for *k* constraints on *k* different resources without increasing the problem's complexity, while providing the desired constrained optimal solutions. For example, the expressions (3.1) and (3.2) can be generalized for *k* constraints on *k* resources as:

$$\hat{p}_{ij} = p_{ij} - \sum_{k=1}^{K} \mu^k d_{ij}^k \quad \forall (i,j) \in A \text{, and}$$

$$\hat{q}_{ijr} = q_{ijr} - \sum_{k=1}^{K} \mu^k d_{ij}^k \quad \forall (i,j) \in AI, \quad \forall r \in R$$

A difficulty arises in choosing μ, because we may need to evaluate different values until we find the smallest one that ensures that all the computed $s^{\omega} - t^{\omega}$ paths have distance less than the maximum allowable traveled distance *D*.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COMPUTATIONAL RESULTS

A. TEST SCENARIO

1. Baseline Case Description

The baseline case considers the airspace over a notional area of operations of 360-by-360 nautical miles. The defender covers part of the airspace with a layered IADS structure comprising FEZ and MEZ. Each of these covers an area of 60-by-80 nautical miles, from the ground up to 45,000 feet. A directed network (see, e.g., Figure 4) represents this topology and includes three locations types:

(1) The origins, representing the attacker's bases from which an aircraft strike package can depart, or last air-refueling point before the ingress phase.

(2) The destinations, representing the potential strike package's targets, or the weapons-release points against those targets.

(3) The planned FEZ and MEZ, where interceptors can be installed by the defender.

The underlying infiltration network contains one node for each of these entities, excluding the case in which two or more entities are synthesized in one node, when one or more targets are located in a planned FEZ or MEZ. In that case the target (or targets) and the FEZ or MEZ comprise one node. Sequentially, these nodes are connected by directed arcs that represent the potential strike package's flight legs. Each feasible combination of origin-destination (in terms of distance) represents one of the finite scenarios $\omega \in \Omega$ of the model. The SNIP model locates the interdictors on the arcs [6], and following the same approach we split every FEZ and/or MEZ node into two nodes. Figure 4 illustrates the underlying test case with 6 origins, 24 FEZ and/or MEZ areas (including the 48 separated nodes), and 15 targets.

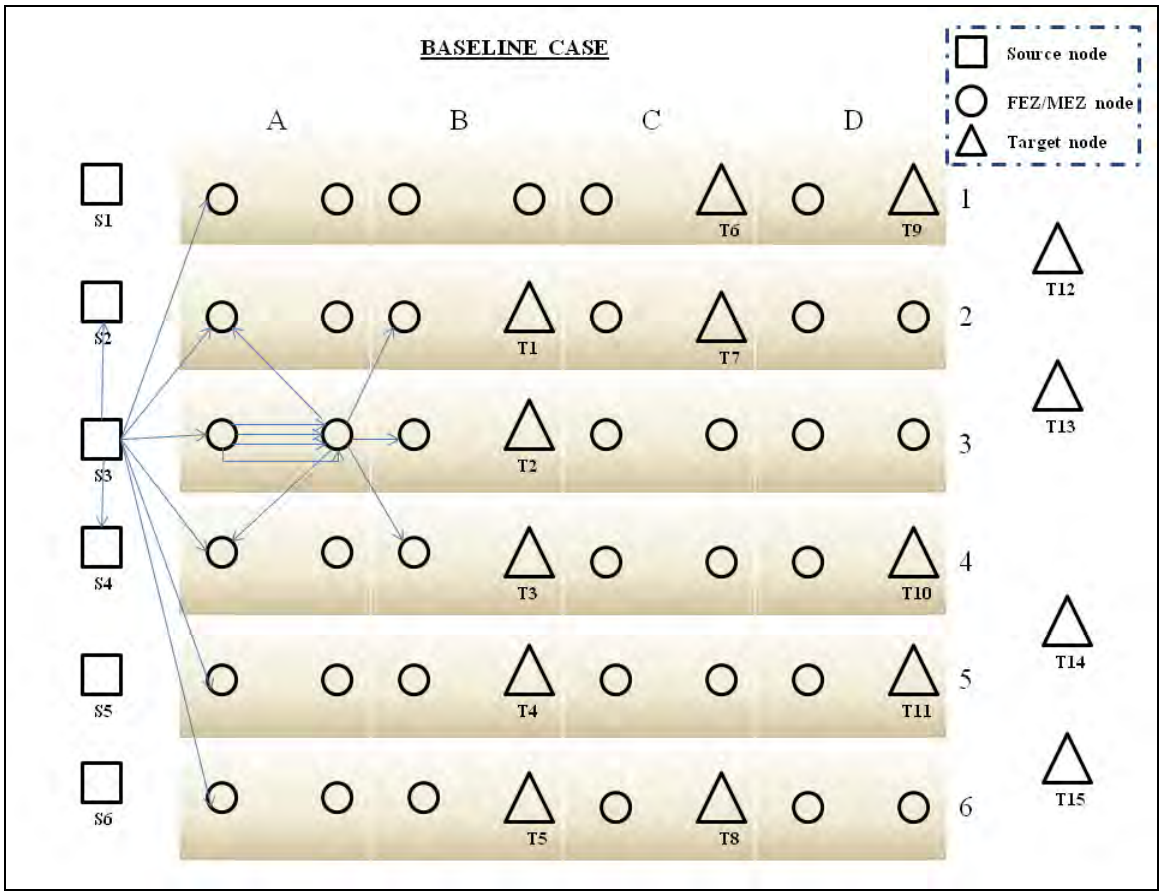

Figure 4. The baseline case considers an area 360-by-360 nautical miles, including three location types: sources, FEZ or MEZ areas, and target nodes. Each rectangular area represents a FEZ or MEZ of 60-by-80 nautical miles, which includes the corresponding entering and leaving nodes. When a target (or targets) is located in a FEZ or MEZ, the target and area nodes are consolidated, and then the resulting node is separated. We also indicate the way the nodes are linked. Interdictable arcs link the separated nodes inside the FEZ and MEZ areas.

The arcs that link the separated FEZ or MEZ nodes are the interdictable arcs $(i, j) \in AI$. We consider three types of interceptors: two types of fighters and one type of SAM system. In the IADS model the separated FEZ or MEZ nodes are linked with four arcs: one for each interceptor type and one for "no-interceptor." Nodes are linked as shown in the example for area A3. The area can be traversed (from left to right) on the nominal arc, if the area is not interdicted; or, on either one of the three other arcs depending on the type of interdiction. The route may continue upwards (to cell A2) or

downwards (to cell A4) using oblique arcs in the graph, which allow interdiction on either area (e.g., A2 and A4) if the evader needs to traverse them.

2. Baseline Case Assumptions and Modeling

We model only the ingress part of the strike package's flight path, because the objective for the defender is to prevent the attack against his assets. The current formulation provides the optimal allocation of multiple interceptor types, on average, for a finite number of origin-destination scenarios, as well as the optimal routing for the attacker through the defensive positions from each source to the targets. We do not explicitly model the egress part, but that extension can be accommodated easily. We assume that the maximum feasible traveled distance *D*, for every $s^{\omega} - t^{\omega}$ path, is 400 nautical miles (considering an average speed of eight nautical miles per minute and maximum flight time, at that speed, of 50 minutes for the ingress part of the mission).

The model represents the attacker's straight and level flight in two dimensions, and any altitude changes are not represented. The optimal solution for every scenario provides the FEZ or MEZ nodes that comprise the attacker's path but not specific way points inside these FEZ or MEZ areas. That is, any deviation (lateral or vertical maneuvering) from the straight and level flight is not accounted for in the distance penalty; accordingly, the computed solution is pessimistic for the defender.

By extending the SNIP formulation, we are still assuming independence among the interdiction at the successive arcs in the path the evader traverses. In our case, the layered structure of the network favors the defender, because the probability that a strike package will be intercepted is increased if it has already been intercepted at the preceding arcs. Thus, the optimal solution is, again, pessimistic for the defender.

In our baseline case, the nominal probability of evasion, p_{ij}, if the attacker traverses an arc $(i, j) \in A$, given no interceptor has been located on that arc, is assumed to be one. The probability of evasion q_{ijr}, if the attacker traverses an arc $(i, j) \in AI$, depends only on the efficiency of the installed interceptor type $r \in R$, and not on the arc $(i, j) \in AI$. In other words, we are assuming the defensive systems perform with the same

efficiency in every area. We roughly estimate q_{ijr}, considering that interceptors r_1, r_2 are fighter formations of type A and B respectively, whose efficiency is defined by the number and the probability of kill of the loaded air-to-air missiles. Interceptor r_3 is assumed to be a SAM system, and its efficiency depends on the number and the probability of kill of the loaded ground-to-air missiles. The strike package consists of 20 aircraft. Every time the strike package enters into a FEZ or MEZ where an interceptor has been located, it is interdicted, diminishing its force according to the installed type of interceptor. Specifics are shown in Table 1.

Interceptor	Type	Number of missiles	Probability of kill	q_{ijr}
r_1	Aircraft formation: Type-A	16	0.5	0.6
r_2	Aircraft formation: Type-B	8	0.75	0.7
r_3	SAM system	20	0.5	0.5

Table 1. The evasion probabilities q_{ijr} depend on: (i) the type of interceptor, (ii) the number of missiles against a 20-ship strike package, and (iii) the probability of kill of the loaded missiles.

The corrected gains $\hat{p}_{ij}\ \forall(i,j) \in A$ and $\hat{q}_{ijr}\ \forall(i,j) \in AI,\ \forall r \in R$ are determined by the equations (3.1) and (3.2), respectively. For both expressions, d_{ij} is the arc distance and μ is a Lagrangian multiplier, set as a small positive factor that ensures the attacker's optimal path remains under D=400 nautical miles $\forall \omega \in \Omega$. We use $\mu = 0.00033$ in all of our test cases.

Cost c_{ijr} represents the number of interceptors we need to cover a FEZ area for 60 minutes (combat air-patrol time), as indicated in Table 2. Consequently, for air interceptors with similar fuel consumption, it only depends on the distance to the nearest defender's air base or air refueling point, that is, on the arc $(i,j) \in AI$. The cost for the SAM system is considered $c_{ij"SAM"} = 1 \quad \forall(i,j) \in AI$.

FEZ cost	Combat air patrol time	Distance to the nearest refueling point
c_{ijr} =1	60 minutes	less than 80 nautical miles
c_{ijr} =1.5	40 minutes	less than 140 nautical miles
c_{ijr} =3	20 minutes	less than 200 nautical miles

Table 2. The cost of allocating an aircraft formation in a FEZ area depends on the available time over station, or on the distance to the nearest refueling point. For example, the cost for an area $(i, j) \in AI$ is one if an aircraft formation can stay on combat air patrol for 60 minutes, but it increases to three if it can only stay for 20 min, because we need three formations to cover that area for 60 minutes.

The target value V^{ω} can be used to reflect the significance of the targets. In the baseline case, all target values are considered equal to one. We also assume equal probabilities among all scenarios $\omega \in \Omega$. That is, $P^{\omega} = 1/15,\ V^{\omega} = 1,\ \forall \omega \in \Omega$.

3. Network reduction

The baseline test case has 6 origin locations, 15 destination (targets) points, and 24 FEZ and/or MEZ areas. So, the network has $|N| = 58$ nodes after the consolidation of 10 destinations into the corresponding FEZ or MEZ areas, and the separation of later location entities into two nodes each. Additionally, there are $|A| = 218$ arcs and $|\Omega| = 90$ scenarios. The optimization problem has 5,292 decision variables (72 binary, corresponding to first stage, x_{ijr}, variables, and 5,220 continuous in the second stage), and 26,175 constraints, as shown in Table 3. Also, we can see in that table the model size is mainly increased by the products of the number of scenarios and the number of interceptor types.

	1st stage	2nd stage
Decision Variables	|AI| x |R|	|N| x |Ω|
Constraints	|R| + (|R| x |AI|)	[|A| + (|R| x |AI|)] x |Ω|

Table 3. Number of decision variables and constraints, in both first and second stages.

We make a tactical assumption in order to decrease the computational effort: We consider air refueling is available for the attacker, so he can enter the defender's territory from any point, as needed, in order to reach the desired target. We implement this by connecting all the s^{ω} nodes to a super source node (with a zero-length arc), which represents the attackers departure point for every scenario $\omega \in \Omega$.

Additionally, in order to improve the formulation in (2.5) and further decrease the computational time, we tighten the Lagrangian multiplier λ_{ij} in constraints (2.5d) and (2.5e). In the discussion of formulation (1.3), we mentioned that $\lambda_{ij} = 1$ is a valid assumption, because we stated that the Lagrangian multiplier has to be greater than or equal to the network gains [6]. Now, having defined the p_{ij}, q_{ijr} values, we substitute them in equations (3.1) and (3.2) to determine the corrected networks gains $\hat{p}_{ij}, \hat{q}_{ijr}$. Finally, we define as:

$\lambda_{ij} = \max\left\{\hat{p}_{ij} : (i,j) \in AI\right\} \quad \forall (i,j) \in A$, in constraint (2.5d), and

$\lambda_{ij} = \max\left\{\hat{q}_{ijr} : (i,j) \in AI\right\} \quad \forall (i,j) \in AI, \ \forall r \in R$, in constraint (2.5e).

B. PERSISTENCE

Many managerial decisions are based on the solution to mathematical models. Often, small, last minute changes in some of the input data significantly alter the already calculated solutions—creating problems in many aspects. Brown, Dell, and Wood [21] address the problem by stating cases and solution approaches where a previously optimal solution may still be near-optimal, in a slightly changed scenario, and preferable to the fully updated, optimal one. The key question is how the optimization model will be used by the decision makers [21]. Pan et al. [6] address the persistence issue in the nuclear smuggling scenario by adding a penalty term $\delta \sum_{(i,j) \in AI} | x_{ij} - \tilde{x}_{ij} |$ whenever small changes in the number of available nuclear detectors evokes changes between the new and the already announced solutions $\tilde{x}_{ij}$.

In the IADS model, the optimization persistence feature is also reasonable from a tactical and operational point of view. Uncertainty, in terms of the available resources, is often present. Thus, in cases where many near optimal solutions exist, we wish to derive and implement "nested" plans. That is, we prefer to derive several plans for a wide range of budget values $b_r \ \forall r \in R$, so that the plan for *n* resources is "almost nested" into the plan for *n*+1 resources. Our objective is not to eliminate all relocations, because some of them are imperative as new resources become available [6], but to reduce the unnecessary ones.

In order to accomplish the above objective, we add the below persistence penalty term (3.3) to the minimization objective function (2.5a):

$$\delta \sum_{(i,j)\in AI} \sum_{r\in R|\tilde{x}_{ijr}=1} (1-x_{ijr}) \ , \tag{3.3}$$

where x_{ijr} are the defender's decision variables, $\tilde{x}_{ijr}$ are the current values resulting from the plan with one fewer unit of resource, and δ is a small, positive number. In (3.3), every change from an announced presence of an interceptor, $\tilde{x}_{ijr}=1$, to no such interceptor, $x_{ijr}=0$, penalizes the original objective function (2.5a) by adding a fixed cost δ.

C. NUMERICAL RESULTS

We have implemented the baseline case using General Algebraic Modeling System (GAMS) with CPLEX as solver [20], on a 2.53 GHz, Dell Intel Core TM laptop with 6 GB of memory. We also examine several excursions from that case, and present results and insights.

1. Output Display

For any interceptor resources, the solution report includes the optimal interceptor allocation (the first stage decisions x_{ijr}), as well as the optimal attacker's solution path, the fraction of the flow (strike package force) that arrives at the target, and the flight path ($s^{\omega} - t^{\omega}$) distance, for every scenario $\omega \in \Omega$. Table 4 presents a sample output that includes the optimal interceptor allocation and the relevant data for just one scenario (ω_6)

of the baseline case, and for a given budget (resource) vector $(b_{r1}, b_{r2}, b_{r3}) = (2,2,2)$ interceptors.

Optimal interceptor allocation
Node B1 to Node B1a installed resource r1
Node B2 to Node T1 installed resource r3
Node C2 to Node T7 installed resource r3
Node C3 to Node C3a installed resource r2
Node C4 to Node C4a installed resource r2
Node D4 to Node T10 installed resource r1
Attacker's Flight Path for scenario ω6
Node S1 to Node A1 flow = 1.0000
Node A1 to Node A1a flow = 0.9967
Node A1a to Node B1 flow = 0.9770
Node B1 to Node B1a flow = 0.9770 (intercepted with resource r1)
Node B1a to Node C1 flow = 0.5668
Node C1 to Node T6 flow = 0.5668
Node T6 to Node T6a flow = 0.5556
Final force on target = 0.5556%
Flight path distance = 190.00 nautical miles

Table 4. The output displays the optimal interceptor allocation, as well as the attacker's flight path, the final attacking force on target and the distance $s^{\omega} - t^{\omega}$ for scenario ω_6. Budget vector is $(b_{r1}, b_{r2}, b_{r3}) = (2,2,2)$ interceptors.

2. Changing the Amount of Interceptors

We solve the stochastic IADS model starting with budget vector $(b_{r1}, b_{r2}, b_{r3}) = (1,1,1)$ and iteratively increase the available resources to $(b_{r1}, b_{r2}, b_{r3}) = (8,8,8)$. Table 5 shows the computational effort (in seconds), and the optimal solution (the attacker's probability of evasion) as the defender's resources increase.

Budget (b_{r1}, b_{r2}, b_{r3})	Computational time (seconds)	Optimal value
(1,1,1)	1	0.857842
(2,1 1)	5.9	0.828381
(2,2,1)	6.7	0.792637
(2,2,2)	13.8	0.759867
(3,2,2)	18.3	0.712325
(3,3,2)	34.2	0.682133
(3,3,3)	45.3	0.636128
(4,3,3)	94.3	0.605176
(4,4,3)	105.6	0.596484
(4,4,4)	133.4	0.560683
(5,4,4)	202.1	0.534955
(5,5,4)	225.1	0.517078
(5,5,5)	371.2	0.489927
(6,5,5)	385.8	0.452058
(6,6,5)	357.3	0.444301
(6,6,6)	227.8	0.404100
(7,6,6)	373.7	0.396269
(7,7,6)	444.3	0.378298
(7,7,7)	463.5	0.360124
(8,7,7)	436.3	0.344073
(8,8,7)	457.3	0.340977
(8,8,8)	476.5	0.327881

Table 5. Numerical results testing the baseline case, including computational time in seconds, and the optimal solution (attacker's probability of evasion), as the available defender's budget (b_{r1}, b_{r2}, b_{r3}) is sequentially increased from (1,1,1) to (8,8,8)

3. Changing the Number of Interceptor Types

The degradation of the computational efficiency for larger values of resources prompts us to examine the influence of each interceptor type on the problem complexity. To do this, we modify the baseline case and assess the effect of the number of types of interceptors.

Specifically, we compare three cases where the defender uses one, two, and three types of interceptors, given that the total number of interceptor units is the same. Figure 5

presents the results. These reveal that as the number of total available resources is increased, the more interceptor types we model, the more computational effort is required.

Also of note, in the single-interceptor type case, the computational time is not affected by the total number of interceptors.

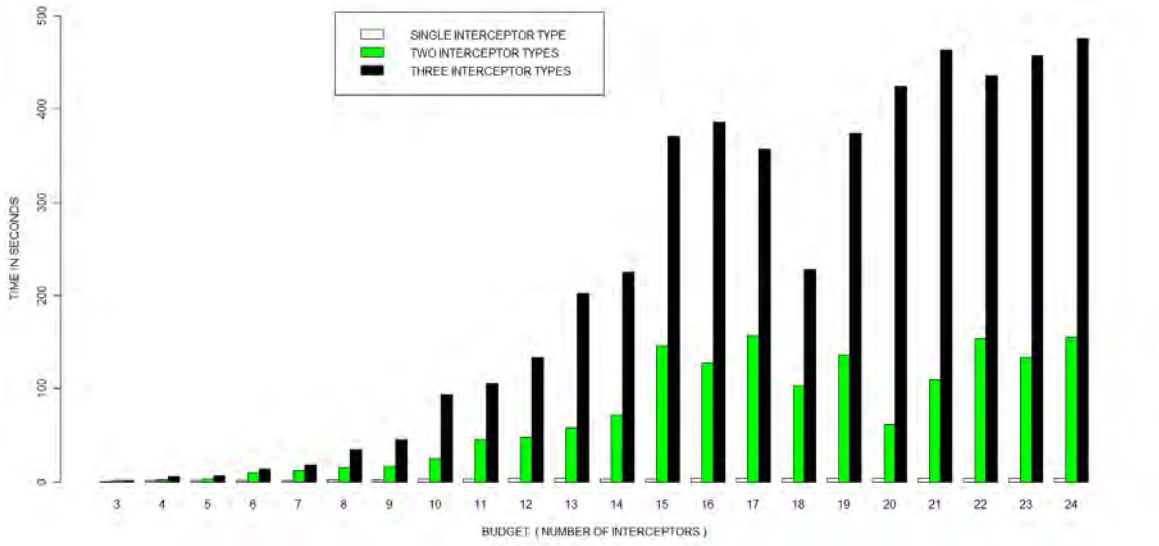

Figure 5. Comparison of the computational effort among three instances of the baseline case, with equal number of resources, but with one, two, and three types of interceptors. The horizontal axis represents the budget range b_r for one interceptor type. The respective budget range for two types is $(b_{r1}, b_{r2}) = \{(2,1),(2,2),(3.2),...,(12,12)\}$, and for three types is $(b_{r1}, b_{r2}, b_{r3}) = \{(1,1,1),(2,1,1),(2,2,1),...,(8,8,8)\}$. The more interceptor types we model, the more the computational time is needed for the same total number of interceptors.

4. Changing the Number of Scenarios

We examine the effect of the number of scenarios on: (i) the overall probability of evasion, and (ii) the computational effort. We carry out the comparison by considering two budget resources, (4,4,4) and (6,6,6), and running the model from |Ω|=1 to |Ω|=15 scenarios, with equal probabilities (1/|Ω|) for the defined scenarios $\omega \in \Omega$. Figure 6 indicates the results for probability of evasion which, as anticipated, is roughly

proportional to the number of scenarios: The more attacker's scenarios for which the defender needs to plan, the less effective the defensive strategy results

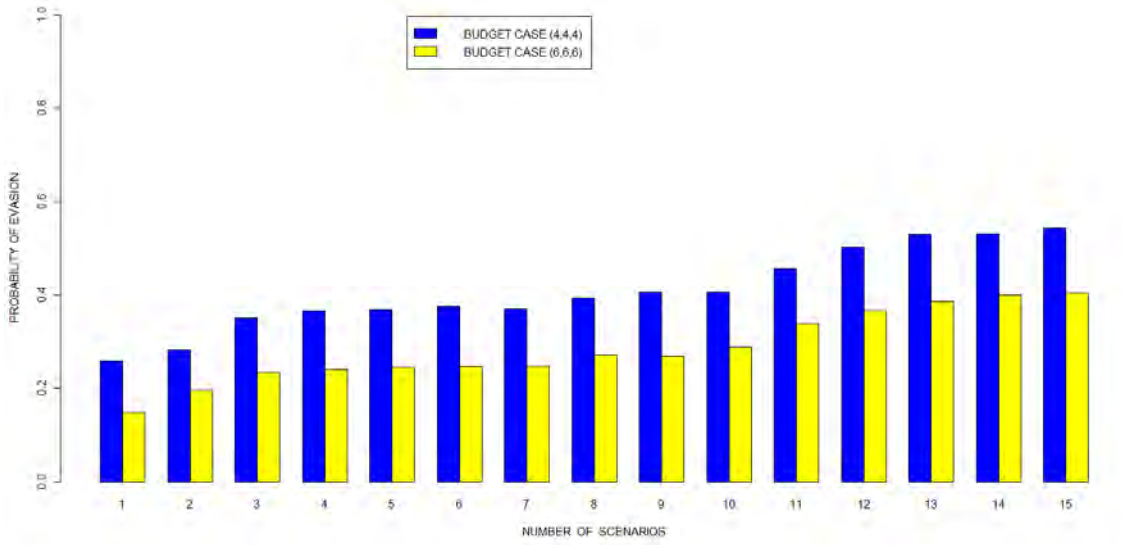

Figure 6. For select budget cases, that the probability of attacker's evasion is increased as the number of scenarios $|\Omega|$ is increases.

Figure 7 depicts computational time, which is not necessarily increasing on the number of scenarios.

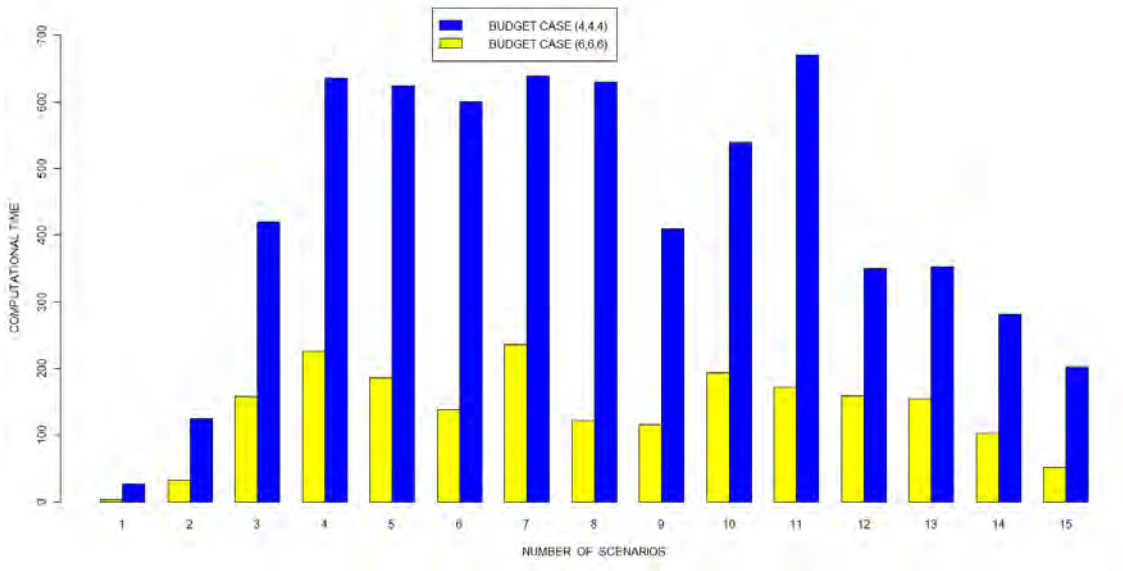

Figure 7. For select budget cases, the computational effort is not increasing in $|\Omega|$.

5. Considering High-Value Targets

We examine the effect of the target value (parameter V^{ω}) in the model. We modify the baseline case by assuming a higher value for five of the fifteen targets: T3, T7, T12, T13 and T14. In this case, the optimal objective function value does not represent the expected probability of evasion because for some destinations the corresponding probability is multiplied by the assigned value. That is, the objective function now represents the expected target value collected by the attacker. The computational effort, on average, is slightly increased for the same level of interceptor budget (see Figure 8).

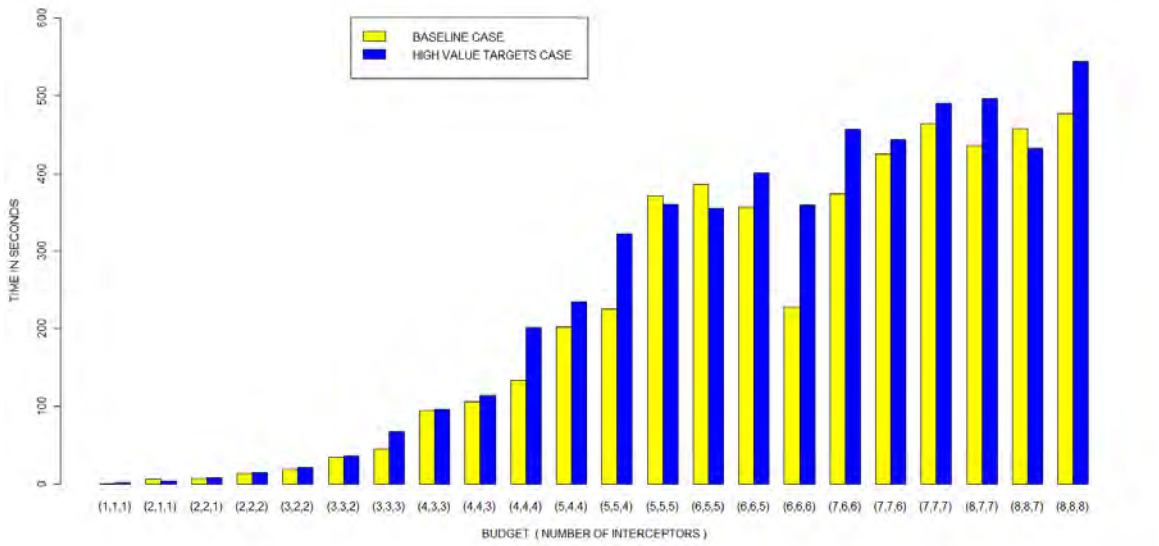

Figure 8. The graph compares the computational effort in seconds, between the baseline case (with equal-value targets) and a case that involves five higher-value targets (out of 15), as a function of interceptor budget (b_{r1}, b_{r2}, b_{r3}). The computational time, on average, is slightly increased in the high-value target case.

By modifying target values, interceptors are reallocated to focus on the protection of high-value assets. The refinement of targets into value categories provides more realistic and effective defensive plans, because the defender can address the significance of the targets. For example, for a budget $(b_{r1}, b_{r1}, b_{r3}) = (4,4,4)$, Figure 9 depicts the allocation of defensive assets under the assumption that all targets have value equal to

one. In Figure 10 we observe a different interceptor allocation when the targets T3, T7, T12, T13, and T14 are assigned a value equal to two.

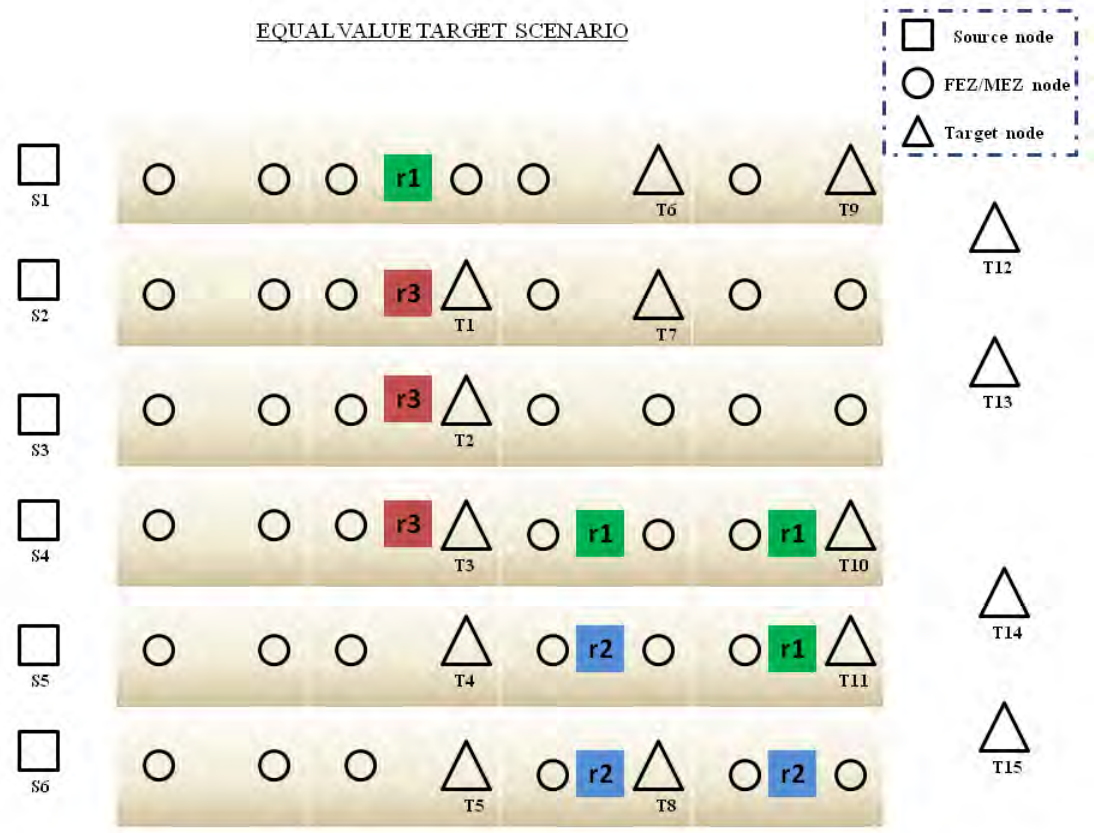

Figure 9. Interceptor optimal allocation for the baseline case, considering all targets have value one, and the available budget is $(b_{r1}, b_{r1}, b_{r3}) = (4,4,4)$.

Note: Recall that the interceptors that appear in Figures 9 and 10 are fewer than available, (4,4,4), because we need more than one aircraft formation to cover some areas for one hour. That is, the model computes one hour duration defensive plans, and we need 12 interceptors to implement these two specific plans.

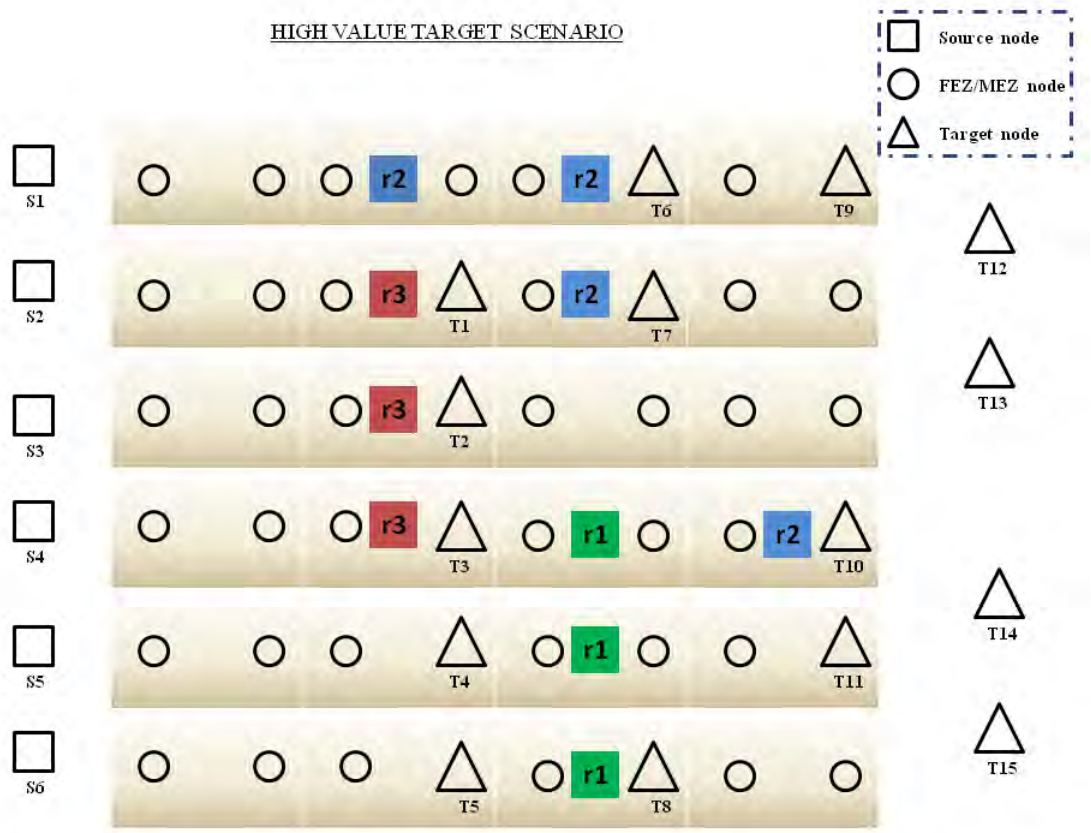

Figure 10. We modify the baseline case by assuming targets T3, T7, T12, T13, T14 are high-valued. The available budget is $(b_{r1}, b_{r1}, b_{r3}) = (4,4,4)$. The new optimal interceptor allocation is influenced by those targets.

6. Persistence

We add the penalty term introduced in equation (3.3) to the formulation of the objective function (2.5a) in order to seek solution persistence in our baseline case. We solve the problem iteratively for budget vectors $(b_{r1}, b_{r2}, b_{r3}) = (1,1,1)$ to $(8,8,8)$, and for three penalty factor values: δ = 0.000, 0.001, and 0.003. Note our model is susceptible to interceptor exchanges in the same area. That is, we want to find a near-optimal solution, which is not only persistent with the suggested interdicted areas, but also with the selected interceptor types.

The persistent version of the model computes the near optimal solutions slightly faster than the original one computes the optimal solutions, as expected (see, e.g., [21],

[6]). In Figure 11 we show the total time required to solve 22 instances of the baseline case iteratively for budget values (b_{r1}, b_{r2}, b_{r3}) ranging from (1,1,1) to (8,8,8), and for the aforementioned penalty values.

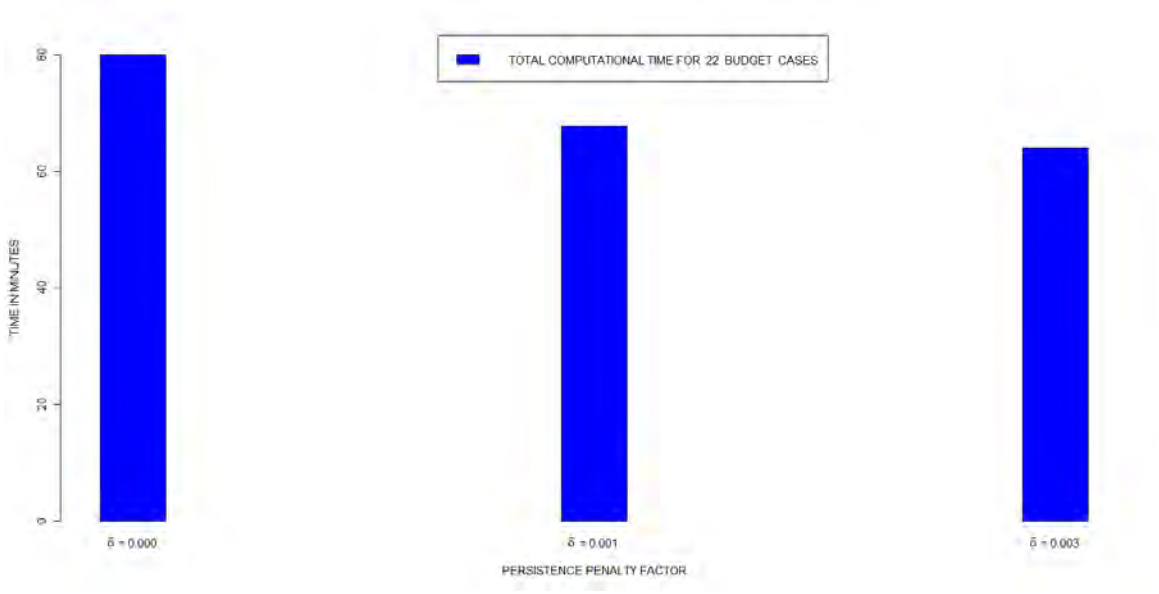

Figure 11. The graph compares the total computational time, in minutes, for 22 sequential runs of the program, with budget values ranging from (1,1,1) to (8,8,8), and persistence penalty factors δ = 0.000, 0.001, and 0.003. The "persistent" solutions require less computational effort.

We also demonstrate the persistence characteristic of the model, enumerating the number of interceptor relocations (both area and type exchanges), as the defender's interceptor budget gradually increases, and comparing the results for the three penalty factors. For each δ, we compare every budget optimal solution to the next, with one additional resource, counting any area and/or interceptor type change. Figure 12 shows the number of interceptor relocations for the above δ factors as a function of the available budget resources. When δ = 0.000 we attain optimal but not persistent solutions, totaling 92 relocations for 21 program runs (at different budget levels). A penalty factor δ = 0.003 induces only 39 interceptor relocations in the same runs.

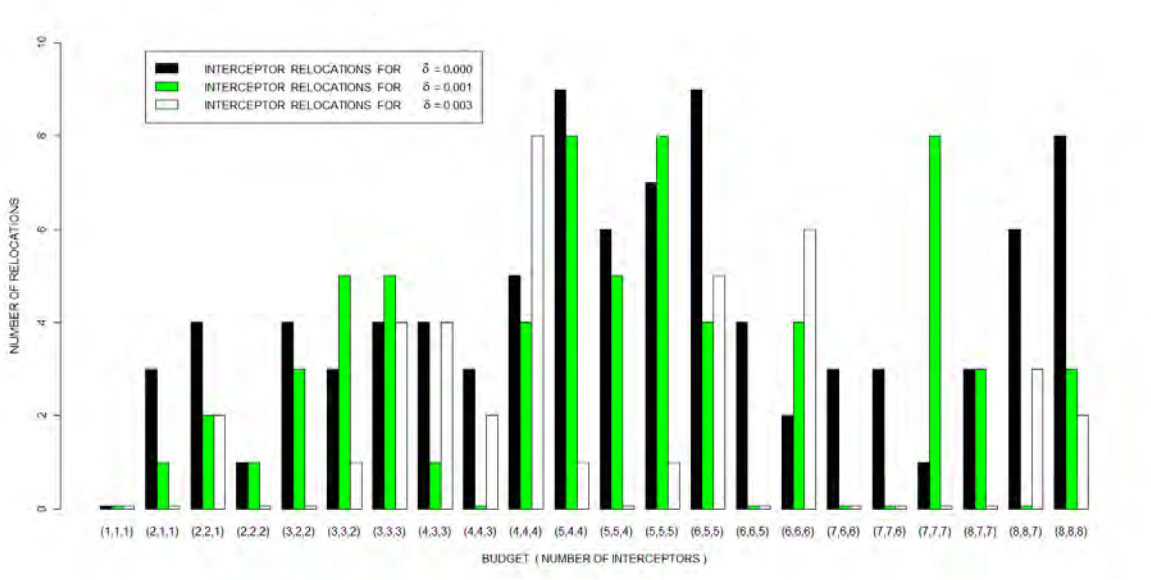

Figure 12. The graph compares the number of interceptor relocations, among three persistence penalty factor cases. For each case $\delta = 0.000$, 0.001, and 0.003, respectively, we enumerate the interceptor relocations, for different budget levels, where each optimal solution is compared to the next budget level for persistence. $\delta = 0.000$ provides optimal but not persistent solutions. $\delta = 0.003$ induces significantly fewer interceptor relocations.

In Figure 13 we present the reduction of the attacker's probability of evasion, for different persistence penalties, as a function of available interceptor resources. By adopting small positive values for the persistence penalty δ, we accept a near-optimal solution (instead of the optimal one for $\delta = 0.000$), but also save computational time and attain persistence, which is convenient for the abovementioned reasons. We estimate δ=0.003 as an adequate persistence penalty factor in our IADS test case, providing the best tradeoff between increased probability of evasion (almost negligible) and increased persistence.

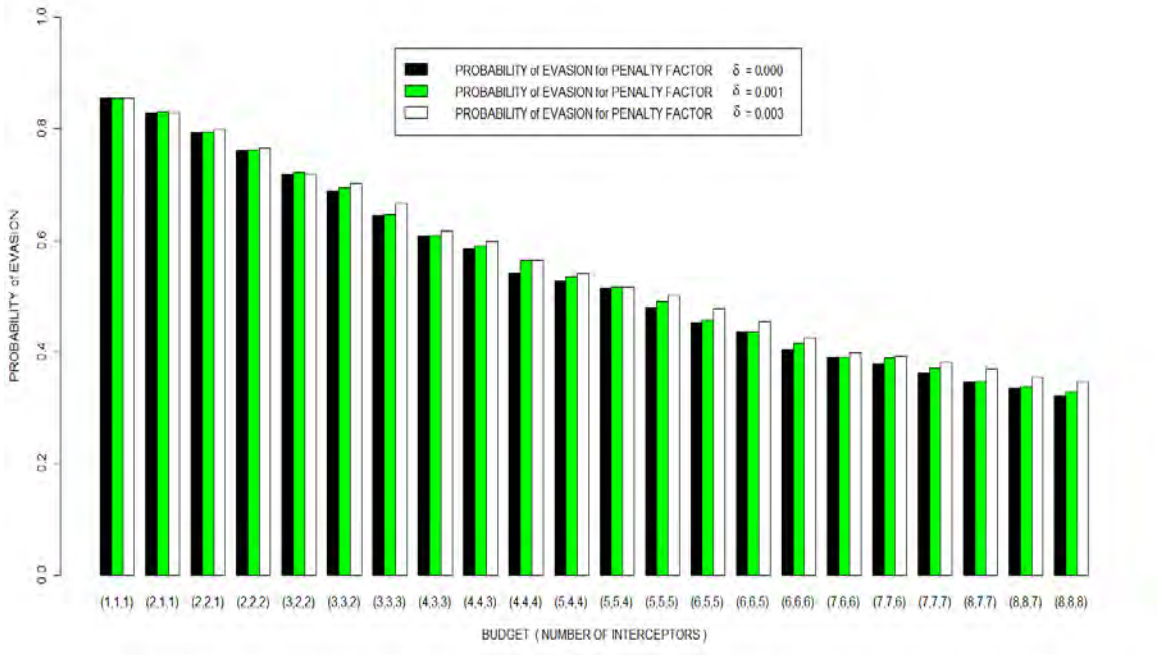

Figure 13. The graph compares the probability of the attacker's evasion among three cases with persistence penalty factors δ = 0.000, 0.001, and 0.003 respectively, as a function of the available interceptor resources. δ=0.001 and 0.003 cause a negligible increase in the probability of evasion, compared to the benefit of providing persistent solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSIONS AND FUTURE DEVELOPMENT

A. CONCLUSIONS

This thesis has modeled a layered IADS structure, which consists of FEZ and MEZ areas, in order to propose a decision support aid for DCA operations planning. We have extended the stochastic network interdiction program of Pan et al. [6] to handle multiple types of interdictors, and have constrained the second-stage attacker's shortest-path problem on a mission resource, a realistic constraint.

We have extended previous stochastic network interdiction models to handle multiple types of interdiction assets, add an additional distance constraint, and adapt the resulting mathematical program to model the airspace covered by an IADS consisting of FEZ and MEZ of multiple weapons systems.

The program output includes the optimal defender's multi-type interceptor allocation, and the attacker's optimal routing through the interdicted network for every defined scenario (origin-destination pair). The suggested defensive plans can be made consistent to small, last minute input data variations, by adding a small persistence penalty to the formulation.

We have used a heuristic restriction for the second-stage problem, in order to handle the attacker's flight paths on a maximum traveled distance limit. This entails modifying the arcs gains to reflect dependence with the arcs distance. Using the concept of the Lagrangian multiplier, the formulation is flexible, allowing the addition of other constraints without deteriorating the model complexity.

Additionally, the formulation allows various input parameters to realistically model the air-defense problem. The arcs' gains reflect the deployed interceptor efficiency, while the arcs' cost depends on the vicinity to the nearest refueling area, and thus, they are related to the duration of continuous coverage the air interceptors can provide. The target categorization in a value scale, and the ability to assign probabilities to the potential scenarios, enables the planner to prioritize the different elements in the

problem, for example, to minimize either the expected probability of evasion or the expected target value collected by the evader.

Specifically, we have solved a hypothetical instance of the problem assuming the relevant airspace over an area of 360-by-360 nautical miles, and presented computational results and insights, including the assessment of factors that affect the computational effort of this NP-hard problem.

The computational time is increased as the number of interceptor types is increased, for the same number of total resources. We also show that the computational time is not necessarily increasing with the number of scenarios, whereas the probability of attacker's evasion does. Other factors that affect the computational effort are the number of interdictable arcs, and the number of interceptor resources. Cases that involve larger-size networks (over 100 nodes and a few hundred arcs) with a combination of large values of the above parameters may make the problem intractable for tactical use, requiring several hours to solve.

Realistic air-defense problems can be modeled using networks of the size and characteristics similar to the one analyzed in this thesis because, for example, a FEZ or MEZ (representing an interdictable arc) covers a 60-by-80 nautical miles area, whereas an interceptor unit represents four to eight fighters or a SAM system battery. Thus, the stochastic IADS model presented in this work can contribute to the preparation phase of the DCA operations and both the operational and tactical levels of the air-war campaign.

B. FUTURE DEVELOPMENT

The IADS model addresses the DCA operations planning problem for a single strike package. The first intuitive model reformulation would focus on a multiple attackers, with sub-cases to either attack the same target or not.

Another reformulation would revise the independence assumption for the probabilities of interdiction, among the successive arcs in an evader's path. In the DCA operations, the layered IADS structure will increase the probability that the attacker is intercepted, if he has already been intercepted at the preceding arcs. The dependence

assumption will further minimize the optimal solution (probability of evasion value) more realistically for the defender.

Future development, with minimal effort, can generalize the interceptor deconfliction issue by modeling multiple interceptors in a single (joint engagement zone) area, or adding point defense assets to every target in the network. Additionally, further studies may explore the ability to model the MEZ as concentric circles (and not only as rectangular areas), integrating air and missile interceptors in a different way.

Finally, we propose further algorithmic development so that the IADS model may be used to solve other relevant, larger-scale problems faster, for tactical use in the air-campaign.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Royal Air Force, Air Warfare Centre, "Air and Space Warfare," *AP 3002,* UK, Waddington, 2009.

[2] US Air Force, "Counter Air Operations," *Air Force Doctrine Document 2-1.1*, 2002.

[3] Joint Chiefs of Staff, "Joint Doctrine for Countering Air and missile Threats," *Joint Publication 3-01*, 2007.

[4] S. Bungay, *The most dangerous enemy: a history of the Battle of Britain*. London, UK: Aurum, 2000, pp. 62–64.

[5] Joint Chiefs of Staff, "Joint Airspace Control," *Joint Publication 3–52*, 2010.

[6] F. Pan, W. Charlton and D. Morton, "A stochastic program for interdicting smuggled nuclear material," in D.L. Woodruff, ed., *Network Interdiction and Stochastic Integer Programming*, Kluwer Academic Publishers, 2003, pp. 1–20.

[7] A. McMasters and T. Mustin, "Optimal interdiction of a supply network," *Naval Research Logistics Quarterly*, vol. 17, pp.261–268, 1970.

[8] A. Washburn, and K. Wood, "Two-Person Zero-Sum Games for Network Interdiction," *Operations Research*, vol. 43, pp. 243–251, 1994.

[9] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending Critical Infrastructure," *Interfaces*, vol. 36, pp. 530–544, 2006.

[10] K. Cormican, D. Morton, and K. Wood, "Stochastic network interdiction," *Operations Research*, vol. 46, pp. 184–197, 1998.

[11] E. Israeli and K. Wood, "Shortest-path network interdiction," *Networks*, vol. 40, pp. 97–111, 2002.

[12] U. Janjarassuk and J. Linderoth, "Reformulation and sampling to solve a stochastic network interdiction problem," *Networks*, vol. 52, pp. 120–132, 2006.

[13] K. Wood, "Deterministic network interdiction," *Mathematical and Computer Modeling*, vol-17, pp 1–18, 1993.

[14] M. Simaan, and J. Cruz, "On the Stackelberg strategy in nonzero-sum games," *Journal of Optimization Theory and Applications*, vol. 11, pp. 533–555, 1973.

[15] J. Royset, M. Carlyle and K. Wood, "Routing military aircraft with a constrained shortest-path algorithm," *Military Operations Research*, vol. 14, No. 3, pp.31–52, 2009.

[16] J. Birge and F. Louveaux, "Uncertainty and Modeling Issues, Basic Properties and Theory," in *Introduction to Stochastic Programming.* New York, NY: Springer - Verlag, 1997, pp. 49–122.

[17] A. Shapiro, D. Dentcheva and A. Ruszczynski, *Lectures on Stochastic Programming Modeling and Theory*, Philadelphia, PA: Mathematical Programming Society, Society for Industrial and Applied Mathematics, series on optimization, 2009, pp. 1–60.

[18] A. Ruszczynski and A. Shapiro, "Stochastic Programming," in *Handbooks in Operations Research and Management Science*, B.V., Elsevier science, vol. 10, 2003.

[19] D. Bertsekas, "Network Problems with integer Constraints, Nonlinear Network Optimization," in *Network optimization continuous and discrete models*. Belmont, MA: Athena Scientific, 1998.

[20] General Algebraic Modeling System, CPLEX (2009) [Online]. Available: http://www.gams.com/dd/docs/solvers/cplex, (accessed 28 July 2011)

[21] G. Brown, R. Dell and K. Wood, "Optimization and persistence," *Interfaces*, vol. 27, pp. 15–37, 1997.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Javier Salmeron
   Naval Postgraduate School
   Monterey, California

4. Professor Johannes O. Royset
   Naval Postgraduate School
   Monterey, California

5. Charalampos I. Tsamtsaridis
   Larissa, Greece