NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OPTIMAL EMPLOYMENT OF PORT RADAR AND PICKET SHIPS TO DETECT ATTACKER SPEEDBOATS - A DEFENDER-ATTACKER OPTIMIZATION MODEL TO ENHANCE MARITIME DOMAIN AWARENESS

by

Ahmad M. Abdul-Ghaffar

June 2008

Thesis Advisor:	Gerald G. Brown
Second Reader:	Jeffrey E. Kline

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** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Optimal Employment of Port Radar and Picket Ships to Detect Attacker Speedboats - A Defender-Attacker Optimization Model to Enhance Maritime Domain Awareness		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Ahmad M. Abdul-Ghaffar			
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**	

13. ABSTRACT (maximum 200 words)

The U.S. Coast Guard has deployed several hundred port patrol vessels to protect U.S. Navy ships and other high-value assets in ports world-wide. Each vessel has an armed crew of four, is relatively fast, and features a simple surface search radar, radios, and a machine gun. These vessels coordinate surveillance patrols in groups of two or four, perhaps working with shore-based radar. We seek to advantageously position these vessels, and perhaps shore-based radar too, to minimize the probability that an intelligent adversary in one or more speed-boats will evade detection while mounting an attack. Attackers can use elevated obstructions to our radar detection in their attack paths, and ports feature many such restrictions to navigation and observation. We make a key, but realistic assumption that complicates planning: we assume the attackers will see or be told of our defensive positions and capabilities in advance of mounting their attack. We demonstrate our defender-attacker optimization with a fictitious port, and with Los Angeles-Long Beach, Hong Kong, U.S. Navy 5-th Fleet in Bahrain, and the Al Basra oil terminal. In cases we analyze, we can almost certainly detect any attack, even though the attacker, observing our pre-positions, plans clever, evasive attack tracks.

14. SUBJECT TERMS Maritime Domain Awareness, Defense-Attacker, Attacker Speedboats			**15. NUMBER OF PAGES** 85
			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

OPTIMAL EMPLOYMENT OF PORT RADAR AND PICKET SHIPS TO DETECT ATTACKER SPEEDBOATS - A DEFENDER-ATTACKER OPTIMIZATION MODEL TO ENHANCE MARITIME DOMAIN AWARENESS

Ahmad M. Abdul-Ghaffar
Captain, Royal Bahraini Navy
B.S., United States Naval Academy, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: Ahmad Abdul-Ghaffar

Approved by: Distinguished Professor Gerald G. Brown
Thesis Advisor

Captain Jeffrey E. Kline, USN (RET)
Second Reader

Professor James N. Eagle
Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The U.S. Coast Guard has deployed several hundred port patrol vessels to protect U.S. Navy ships and other high-value assets in ports world-wide. Each vessel has an armed crew of four, is relatively fast, and features a simple surface search radar, radios, and a machine gun. These vessels coordinate surveillance patrols in groups of two or four, perhaps working with shore-based radar. We seek to advantageously position these vessels, and perhaps shore-based radar too, to minimize the probability that an intelligent adversary in one or more speed-boats will evade detection while mounting an attack. Attackers can use elevated obstructions to our radar detection in their attack paths, and ports feature many such restrictions to navigation and observation. We make a key, but realistic assumption that complicates planning: we assume the attackers will see or be told of our defensive positions and capabilities in advance of mounting their attack. We demonstrate our defender-attacker optimization with a fictitious port, and with Los Angeles-Long Beach, Hong Kong, U.S. Navy 5-th Fleet in Bahrain, and the Al Basra oil terminal. In cases we analyze, we can almost certainly detect any attack, even though the attacker, observing our pre-positions, plans clever, evasive attack tracks.

THIS PAGE INTENTIONALLY LEFT BLANK

Table OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

We introduce a new planning tool for locating shore radar stations and mobile picket boats with radar to maximize the probability that one or more speedboat attackers will be discovered before reaching any of a set of defended assets, such as pier-side U.S. Navy ships or other high-value maritime assets at risk. The distinguishing contribution here is that our planning tool explicitly recognizes that the attackers can be expected to have prior knowledge of our defensive disposition, either through shore observers, satellite imagery, or on-board radar threat detectors: we assume the attackers will observe our defensive preparations, and respond accordingly. There is no other such decision support tool available today for maritime domain awareness.

Our motivation derives from the "Maritime Domain Awareness Concept" published by the Chief of Naval Operations on May 29, 2007, declaring the U.S. Navy's understanding and commitment to National Security Presidential Directive 41 "Maritime Security Policy," published on December 21, 2004. Maritime domain awareness is a worldwide problem, with shared responsibilities among allied governments and private enterprise.

We demonstrate how to position SAFE Defender Class picket ships optimally to protect high-value defended assets. We can also locate and fuse shore-based radar returns with those from our boats. We use standard radar equations for our detection predictions, but can accommodate any alternate means of assessing the probability of detection. Our model also represents any restriction to navigation, such as shoreline, islands, and breakwaters, with planner-specified fidelity; these obstructions may also obstruct our radars, so we use ray tracing to gauge whether or not an attacker can be detected from any defender position.

While detecting and alarming attacks is our primary goal, having a picket platform intercept a detected attack may or may not be possible, due to the relative speeds of the defending pickets and the attacker craft. In our scenario we use the SAFE Defender class boat which operates at a maximum speed of 46 knots. Speed matters, and an attacker with a significant speed advantage poses a vexing defense problem.

ACKNOWLEDGMENTS

A thesis is never a single person's work. It is usually a combined team effort to cultivate thoughts and ideas into a worthwhile academic exercise and final product. This thesis is no exception. First, I would like to thank my wife for her unequivocal support and sacrifice for the sake of this project. Furthermore, I also would like to express my deep appreciation and gratitude to Distinguished Professor Gerald Brown. His dauntless and untiring efforts were the main factor behind the success of this research. In addition, most certainly, Captain Jeffrey Kline USN, his inspiring idea and strong support planted the seed that grew into this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

1. What is the Problem?

Maritime port security is a newly-sharpened focus for the United States (U.S.) Congress, the Department of Homeland Security (DHS), and the U.S. Navy (USN). The U.S. deems maritime security a "vital national interest" (DHS, 2005, p. 1). Current maritime threats vary from the possible hijacking of a commercial vessel to ramming an explosive-packed small boat into a ship similar to the 2000 attack on the USS Cole (Carafano, 2007, p. 2).

Maritime ports are "sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks" (DHS, 2005, p. 9). Such ports are highly susceptible to enemies seeking multiple "high impact" objectives to attack. The Al-Qaida terrorist organization has demonstrated the desire and capability of carrying out such an attack (MI5, 2007).

A major maritime threat is exemplified by the Sea Tigers, a maritime detachment of the Liberation Tigers of Tamil Eelam (LTTE). The LTTE, a rebel organization in Sri Lanka, has fought for its independence since 1976. They demonstrate very sophisticated tactics in attacking Sri Lankan Naval and commercial ships (Murphy, 2006). Their first suicide boat attack was in 1990. In 1994, they managed to sink a Sri Lankan Navy warship. Their methods range from utilizing multiple boats (see Figures 1 and 2) simultaneously to the employment of distracting fire from shore to mount a coordinated attack. They continue to pose a significant threat and have carried out attacks as recently as May 2006 (Murphy, 2006).

Figure 1. Archival snapshot of a high-speed boat in a training video captured from the Liberation Tigers of Tamil Eelam (LTTE) (From: Murphy, 2006).

Figure 2. Archival snapshot of a high-speed boat in a training video captured from the Liberation Tigers of Tamil Eelam (LTTE) (From: Murphy, 2006).

We anticipate a determined adversary who plans to infiltrate a maritime port for an attack. We seek a systematic way to assign defensive pickets to detect and alarm such an attack, even though such defensive preparations will be visible to the attacker. Optimal placement of sensor platforms reduces the probability of a successful attack. For our purposes, a first, single successful enemy infiltration is the signal event we wish to alarm. Subsequent to such a first event, interdicted or not, we assume that defenses would qualitatively change.

B. MOTIVATION

1. Why is the Problem Important?

Figure 3. USS Cole after the deadly 2001 attack in Port of Yemen killing 17 Sailors (From: Murphy, 2006).

The world economy is dependent on maritime commerce, which accounts for approximately 80% of the world trade (DHS, 2005, p. 1). Today there are 30 mega-ports worldwide, which almost all cargo ships pass through in the intricate trade network (Caldwell, 2007, p. 1). A disruption in any one of these mega-ports, even for a short time, could have a devastating impact on the flow of goods and oil throughout the world.

In the aftermath of the September 11, 2001 attacks, Congress enacted two major bills specifically addressing maritime security. The Maritime Transportation Security Act

(MTSA) took effect in November 2002. It requires ports to develop security plans and to identify risk areas (Caldwell, 2007, p. 1). The Security and Accountability for Every Port Act (SAFE Port Act), passed in October 2006, is a MTSA amendment, addressing some security issues not previously covered. It also includes provisions that incorporate international ports as part of the overall security plan, recognizing that maritime security is not a one-nation concern, but rather part of a complex intertwined global network (Caldwell, p. 2).

National Security Presidential Directive (NSPD) 41 establishes policy and guidelines for all U.S. agencies and stakeholders in maritime security. At the same time it defines Maritime Domain Awareness (MDA) as the "effective understanding of anything associated with global maritime domain that could impact the security, safety, economy, or environment of the United States" (NSPD-41, 2004). Consequently, in May, the MDA Concept was published by the Chief of Naval Operations. The United States Navy (USN) reinforces NSPD-41 by declaring MDA is a world-wide problem, with shared responsibilities among allied governments and private enterprise. The MDA Concept also recognizes that simply adding more sensors and defensive assets does not suffice (NMDAC, 2007).

The economic impact of a single attack on one mega-port leading to degradation of throughput or even a complete port closure could be dire. For example, the ports of Los Angeles and Long Beach account for approximately 40% of all cargo container traffic entering the U.S. (The Caltrade Report, 2007). The longshoremen strike of 2002 lasted for just ten days, but has been estimated to have cost to the U.S. economy approximately $2 billion a day (Isidore, 2002).

Agencies responsible for maritime security include the U.S. Customs and Border Protection, the Transportation Security Administration, U.S. Coast Guard, and the U.S. Navy. DHS has funded a combined total of $3.8 billion for these activities from FY 2006 to FY 2008 alone (DHS, 2007, p. 19). Considerable investments are being made to develop new technologies to aid maritime security. These range from the Protector Unmanned Surface Vessels (USV) (JFS, 2008) to the Raytheon-developed Athena system that integrates existing sensors to provide decision makers with real-time

situational awareness (Weisman, 2005). USCG has also acquired approximately 700 SAFE Defender Class boats in order to fulfill the maritime security requirement mandated by the SAFE port act (Jane's, 2005). The USN has reestablished its riverine forces and equipped them with SAFE Small Unit Riverine Craft (SURC).

2. How Will the Problem be Solved without Our Involvement?

The burden of overall port security falls on the U.S. Coast Guard (USCG, 2005). The Coast Guard has established Area Maritime Security Committees (AMSC) involving all the different agencies and authorities at each port, and has created local operation centers to improve information sharing and coordination of assets (Caldwell, 2007, p. 5). At the same time, the U.S. Navy has expanded its operational focus from blue water to littoral waters as well. They are tasked with establishing ties with international allies to enhance MDA (NMDAC, 2008, p. 2).

The National Strategy for Maritime Security (NSMS) [2005] stipulates a layered security combining the capabilities of the different stakeholders of each port (DHS 2005, p. 20). This layered defense affords decision makers multiple points from which to react to any potential threat and perhaps serve as deterrence to any enemy. The physical protection of a port from land and sea is still the foundation, and divides a port into different enforcement zones and vessel movement control areas (DHS, 2005, p. 21).

The U.S. Coast Guard has employed a three-tiered Maritime Security (MARSEC) alert level that mimics the Homeland Security Advisory System (DHS, 2002) with Level 1 being the lowest and Level 3 the highest. The MARSEC addresses all aspects of maritime threats from ports to critical infrastructure located near sovereign waters. The Coast Guard sets preplanned responses for each level (USCG, 2007, p. 1).

Prior to September 11, 2001, the U.S. Coast Guard employed Port Security Units (PSU) comprised of mostly reserve personnel. They were not assigned to specific ports but could deploy within 24 hours and become fully-operational within 96 hours with a self-sustained capability of 30 days. Each unit had small boats that are easily deployable (USCG, 2004, p. 1).

Post 9/11 Port Security Units comprise the bulk of the USCG maritime defense teams. They operate in two postures depending on the threat level and manning: either with four boats on duty allowing two boats to be on station at all times, or with six boats on duty and four boats always on station. The two other boats not on station act as a standby or shuttle boat and a 24-hour maintenance boat (USCG, 2004, p. 4). Patrol times can vary from four to six hours. Disposition of boats is left to the judgment to the Tactical Action Officer (TAO) who is delegated by the Commanding Officer (CO) (USCG, 2004, p. 3). Employment and tactics depend heavily on the CO and TAO personal experience.

In accordance with the MTSA of 2002, Maritime Safety and Security Teams (MSST) have been created by the Coast Guard to fill the security gaps at major U.S. ports. The MSST are rapidly-deployable teams comprised of 75 active duty personnel trained in advanced tactical boat operations, anti-terrorism, and force protection. Currently, there are 14 teams based in some of the major U.S. ports (USCG, 2005).

Current security measures include patrol vessels, radars, container scanners, and patrol cars and trucks. Activities include land and water security patrols, boarding of suspected vessels and enforcement of fixed security zones. The intensity of the activities varies in accordance with MARSEC level (Caldwell, 2007, p. 11). Command and control of these operations are conducted from 35 sector inter-agency command centers covering the entire United States. These centers facilitate the gathering and dissemination of information to all agencies involved for a given port region. Twenty-four of these sectors need to upgrade their facilities at a cost of $260 million in order to meet the SAFE Port Act requirements, including new sensor networks that enable faster information sharing (Caldwell, 2007, p. 10).

The defense of ports has improved greatly in the past six years. However, disposition of assets is planned on a perceived threat basis. A lot of emphasis is placed on thwarting an attack through presence (i.e., assuming the potential attacker can observe our defensive preparations and may be dissuaded).

C. LITERATURE REVIEW

We will introduce a bi-level optimization model to position our radars and then predict how an intelligent attacker would respond, given these defensive positions are visible. This employs a bilevel mixed-integer linear program (MIP) to express a defender-attacker optimization.

Bard and Moore [1990] introduce techniques to solve a bilevel mixed integer linear programming problem. They develop an algorithm that can solve this bilevel MIP heuristically.

Wood [1993] develops a network interdiction model for an enemy who wants to maximize flow through a capacitated network; whereas a defender attempts to interdict this network and minimize flow with a limited number of defensive assets visible to the enemy. The model is applied to anti-drug smuggling operations where the main focus is the intercept of chemicals used in drug production.

Isreali and Wood [2002] describe a shortest-path network interdiction problem and formulate it using a bilevel MIP. They introduce efficient decomposition techniques to solve such a problem.

Brown et al. [2006] develop bilevel and trilevel optimization models for the defense of critical infrastructure. They apply these models to many real-world examples in order to highlight any vulnerabilities in such infrastructures. They show the benefits of such models in aiding decision makers make appropriate defensive plans.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SCENARIO DEVELOPMENT

We anticipate a determined intelligent attacker using speed boats to try to reach fixed high-value targets in the maritime domain. We are most interested in a port where, for instance, U.S. Navy ships might be anchored or pier-side. The attacker can employ several methods of attack, either ramming an explosive ridden boat into the target or getting close enough to employ weapons such as a rocket propelled grenade (RPG). The attacker's motivation is to cause maximum effect. That could entail serious damage to shipping or infrastructure, or merely as a psychological form of terrorism. Either way we consider a single successful initial undetected attack as a failure of the defender. We assume transparency in our model in that the enemy can view our defensive prepositioning and react accordingly to avoid detection.

The attacker utilizes a number of small speedboats similar to a 20 foot Baja Outlaw Class (Table 1). The defender employs SAFE Defender class patrol (see Table 2) boats along with shore radar instillations in order to detect the attacker.

Baja 20' Outlaw Class	
Length	20'4" - 6.2 m
Beam	7'10" - 2.39 m
Weight	2,900 lb - 1,315 kg
Weight w/ explosives	3,900 lb
Draft	34" - 86.36 cm
Fuel Capacity	50 gal - 170.3 L
Passenger Capacity	6
Max speed	54.2 knots
Attack Range w/RPG	200m

Table 1. 20' Baja Class Specifications (From: Baja Marine, 2008).

SAFE Defender Class	
Length	25’ - 7.62 m
Beam	8’6” - 2.59 m
Draft	3’ – 0.91 m
Fuel Capacity	50 gal - 170.3 L
Crew	4
Max Capacity	10
Max speed	46 knots
Radar	Furuno 4 kW radar Range (36 NM)
Armament	Effective Range
One 12.7 mm machine gun	1500 m
Capabilities	Detect & Intercept

Table 2. SAFE Defender Class Patrol Boats (From: SAFE, 2003).

A. NETWORK REPRESENTATION

Because we are in the maritime domain, where there are no strict paths or routes, we represent our maritime environment using an mesh network. We break down the surface into square cells of a given width and generate a node in the middle of each. Each cell is connected by an arc to and from every adjacent node (horizontal, vertical, or diagonal) unless we specify an obstruction to navigation (see Figures 4 and 5). The attacker can traverse any arc between adjacent nodes to reach a goal cell. Each defender platform is assigned a cell (node) to occupy, from which he will surveil as much maritime domain as possible.

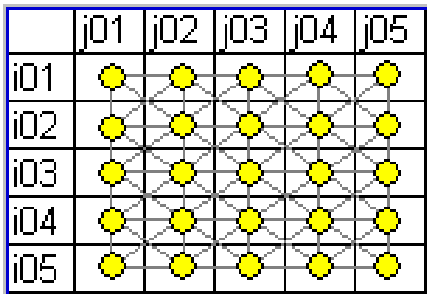

Figure 4. Sample network representation with square cells of constant width, each identified by a row and a column index. An attacker can traverse from any cell via an arc to any adjacent cell.

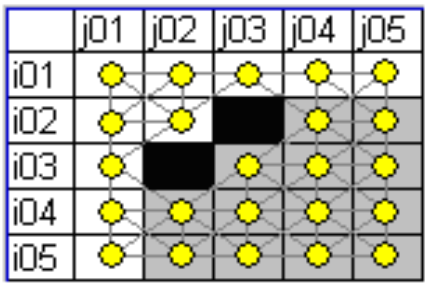

Figure 5. Sample network representation with cells and obstructions. Blackened cells are obstructions to navigation, as well as observation. Cells (i02, j02) and (i03, j03) are not adjacent. For instance, a defender in the North-West cell (i01, j01) cannot detect an attacker in the South-East cell (i05, j05) nor any of the grey cells (if any portion of a cell is obscured by an intermediate obstruction, we conservatively assume the entire cell is obscured).

B. PROBABILITY OF EVADING DETECTION

Equations (P1) through (P9) introduce our radar equations used to estimate the probability that a defender in one cell can detect an attacker in another one. The relative locations of defender and attacker are shown in (P1) and (P2). A defender in some given position may not be able to detect an attacker in some other position due to intervening obstructions. The following assumes positions with no such obstruction. To achieve the resolution we require we assign $cell\_width$ = 0.15 NM (P3). The maximum speed of a

Defender class boat is 46 nautical miles per hour (knots) and the cruise speed is 35 knots. Therefore, we assign $v = 35$ (P4). Each SAFE Defender boat is equipped with a Furuno 4 kW radar with a maximum range of 36 NM, therefore we assign $r_m = 36$ (P5). For our sweep rate in (P8) we assign $sr = 0.8$ (P6). The range between defender and attacker is expressed by (P7). The defender pays a penalty when travelling faster in the form of a decreased detection probability. The detection probability (P8) goes to zero once the distance between attacker and defender is greater then the maximum radar range.

We assume the intelligent attacker will want to maximize his probability of evasion by traversing a path with the maximum joint probability of evading detection while transiting each cell. In (P9), we compute this evasion probability. Assuming cell-to-cell independence, the joint probability that a path will evade detection is the product of the evasion probabilities of each cell traversed. We take the logarithm of this expression to render a linear summation of log likelihoods, and note that maximizing the sum of these logs is equivalent to maximizing the product of the probabilities. Our simple radar equation can be replaced by one with much higher fidelity, [e.g., Skolnik, 1990], but for purposes of our exposition this makes no difference at all.

(i_a, j_a)	attacker cell	(P1)
(i_d, j_d)	defender cell	(P2)
$cell\_width$	cell side distance	(P3)
v	defender velocity	(P4)
r_m	maximum radar range	(P5)
sr	searcher sweep rate	(P6)
$x = cell\_width * \sqrt{(i_a - i_d)^2 + (j_a - j_d)^2}$		(P7)
$P_d = 1 - \exp\left(-2sr \frac{\sqrt{r_m^2 - x^2}}{v}\right)$		(P8)
$P_e = \exp\left(-2sr \frac{\sqrt{r_m^2 - x^2}}{v}\right)$		(P9)

Table 3. Derivation of evasion probability by an attacker located at cell (i_a, j_a) from a defender at cell (i_d, j_d), assuming no intervening obstruction to observation.

C. RAY TRACING

We use ray tracing to determine if an obstacle between a searcher and an attacker obscures the attacker. We assume a ray from searcher *p* to target *a* intersects some intermediate obstacle *x*.

r_{px} distance from searcher *p* to obstacle *x* [meters]

r_{xa} distance from obstacle *x* to attacker *a* [meters]

h_p height above surface of searcher *p* [meters]

h_x height above surface of obstacle *x*

h_a height above surface of attacker *a*

In plane geometry, x can be observed if

$$h_x > h_p + \left(\frac{-h_p + h_a}{r_{px} + r_{xa}} \right) r_{px} .$$

In spherical geometry, we need to define:

r_{px}, r_{xa} great-circle distances [meters]

R radius of Earth [$\cong 6.371 \text{x} 10^6$ meters]

$\theta_{px} = r_{px} / R$ [radians]

$\theta_{xa} = r_{xa} / R$ [radians]

los_{pa} straight line of sight from searcher *p* to attacker *a* [meters]

$$los_{pa} = \sqrt{(R + h_p)^2 + (R + h_a)^2 - 2(R + h_p)(R + h_a)\cos(\theta_{px} + \theta_{xa})}$$

$$C = \sin^{-1}\left(\frac{R + h_a}{los_{pa}} \sin(\theta_{px} + \theta_{xa}) \right)$$

$$D = \pi - (C + \theta_{px})$$

$$h_x > (R + h_p) \frac{\sin(C)}{\sin(D)} - R .$$

D. MODEL FORMULATION

1. The Attacker

The attacker has a set of speedboats $a \in A$ that can each choose to enter a network at any of a number of entry cells $c \in E$, traverse a set of cell-to-cell arcs $d \in D$ to reach and exit the network at any of a number of goal cells $c \in G$ where defended assets are located. Each arc admits a limited number of speed boat traversals *arc_cap*. Traversing each arc carries a risk of detection the attacker cannot control, and the log likelihood that an attacker will evade detection while traversing arc d is $\widehat{evX}_d$. The attacker seeks attack paths that maximize the log likelihood of evading detection.

We express the attackers' planning problem with the model **AMAX($\widehat{\mathbf{evX}}$)**.

Indexes and index sets [~cardinality]

$a \in A$	attacker [~5]
$c \in C_{ij}$	cells with horizontal, vertical coordinates (alias c1, c2) [~1,000]
$c \in E \subseteq C$	cells where an attacker can enter the network [~100]
$c \in G \subseteq C$	goal cells with defended assets [~10]
$d \in D_{c1,c2} = D$	cell adjacencies, or traversal arcs [~8,000]

Data [units]

arc_cap	maximum attackers traversing any arc [attackers]
$\widehat{evX}_d$	log of probability that an attacker will evade detection traversing arc d [log likelihood]

Variables [units]

$ENTER_c$	number of attackers entering network at entry cell c [attackers]
Y_d	number of attackers traversing arc d [attackers]
$GOAL_c$	number of attackers exiting network at goal cell c [attackers]

Formulation [dual variables]

$$Z_{\max}(\widehat{evX}) = \max_{Y} \sum_{d \in D} \widehat{evX}_d Y_d \qquad (A0)$$

$$s.t. \quad \sum_{c \in E} ENTER_c \le +|A| \qquad [\alpha] \qquad (A1)$$

$$\sum_{d \in D_{c,c2}} Y_d - \sum_{d \in D_{c1,c}} Y_d - ENTER_c\big|_{c \in E} + GOAL_c\big|_{c \in G} \le 0 \;\forall c \in C \qquad [\beta_c] \qquad (A2)$$

$$-\sum_{c \in G} GOAL_c \le -|A| \qquad [\delta] \qquad (A3)$$

$$0 \le ENTER_c \qquad \forall c \in E \qquad (A4)$$

$$0 \le Y_d \le arc\_cap \qquad \forall d \in A \qquad [\gamma_d] \qquad (A5)$$

$$0 \le GOAL_c \qquad \forall c \in G \qquad (A6)$$

Discussion

The attackers' objective (A0) is to maximize the total expected log likelihood that attackers traversing arcs from entry cells on paths to goal cells will evade detection (or, equivalently, to maximize the joint probability that they evade detection over all the arcs they choose to traverse). Constraint (A1) limits the number of entries into the network via entry cells, each constraint (A2) forces conservation of flow at a cell in the network, and constraint (A3) limit the number of exits from the network via goal cells. Stipulations (A4-6) give bounds on the decision variables. If the data in (A1), (A3), and (A5) is integral, this linear program will produce an intrinsically integral solution Y^*.

2. The Defender

The defender controls a set of surveillance platforms (e.g., patrol boats, shore radar installations, etc.) $p \in P$ that may each be located at a set of cells $c \in S_p$ to surveil arcs in the network. The log likelihood that an attacker traversing arc d will evade detection by defender boat p located in cell c is $ev_{d,p,c}$. The defender seeks positions for his surveillance platforms to collectively minimize the total log likelihood of attackers evading his surveillance. We express the defender's problem as follows **DMIN($\hat{\mathbf{Y}}$)**.

New indices and index sets [~cardinality]

$p \in P$ defending platforms [~5]

$c \in S_p \subseteq C$ cells where a platform p can be located [~250]

New data [units]

$ev_{d,p,c}$ log likelihood that an attacker traversing arc d would evade detection by defender p in position c [log likelihood]

$\hat{Y}_d$ number of attackers traversing arc d [attackers]

Variables [units]

$X_{p,c}$ =1 if platform p located in cell c, 0 otherwise [binary]

Z total log likelihood of evading detection [log likelihood]

Formulation

$$Z_{\min}(\hat{Y}) = \min_{X,Z} Z \qquad \text{(D0)}$$

$$s.t. \quad Z \geq \sum_{\substack{d \in D, \\ p \in P, c \in S_p}} ev_{d,p,c} \hat{Y}_d X_{p,c} \qquad \text{(D1)}$$

$$s.t. \quad \sum_{c \in S_p} X_{p,c} \leq 1 \qquad \forall p \in P \qquad \text{(D2)}$$

$$\sum_{p \in P | c \in S_p} X_{p,c} \leq 1 \qquad \forall c \in S \qquad \text{(D3)}$$

$$X_{p,c} \in \{0,1\} \qquad \forall p \in P, c \in S_p \qquad \text{(D4)}$$

Discussion

(D0) introduces the objective, and constraint (D1) defines the objective variable as the minimum upper bound on total log likelihood of evasion. Each constraint (D2) requires a defender platform to be located in just one cell, each constraint (D3) allows any cell to be occupied by at most one defender, and (D4) stipulates a binary location decision for each defender.

3. Defender-Attacker Model

We now consider a realistic case, and a worrisome one. The defender wishes to optimize defensive pre-positioning of surveillance platforms *while assuming the attacker will observe these preparations and optimize attacks to exploit any weakness in these defenses*. The defender's objective is to minimize the maximum probability of evasion by attackers. We note that this model is a conservative one for the defender because he must protect against the worst possible set of attacks. Moreover, it is conservative for the attacker because he must plan against the best possible defense.

We state the opposing decision as model MINMAX:

$$Z^* = \min_{Z,X} \max_{Y} \sum_{\substack{d\in D,\\ p\in P, c\in S_p}} ev_{d,p,c} Y_d X_{p,c}$$

$$s.t. \quad (\mathrm{A1}) - (\mathrm{A6}) \text{ and } (\mathrm{D1}) - (\mathrm{D4})$$

We cannot solve MINMAX with conventional techniques, but if we temporarily fix variables Z and X, the result is a capacitated network flow linear program. Taking the dual of this linear program, and freeing Z and X, we achieve an integer linear program **SAFE-ILP** we can solve with conventional techniques.

$$\min_{\substack{\alpha,\beta,\gamma,\delta,\\ X}} \quad |A|\alpha - |A|\delta + \sum_{d\in D} arc\_cap\ \gamma_d \qquad \text{(T0)}$$

$$\alpha - \beta_c \geq 0 \qquad \forall c \in E \qquad \text{(T1)}$$

$$s.t. \quad -\beta_{c1} + \beta_{c2} - \gamma_d \geq \sum_{\substack{p\in P,\\ c\in S_p}} ev_{d,p,c} X_{p,c} \quad \forall d \in D_{c1,c2} \qquad \text{(T2)}$$

$$-\delta + \beta_c \geq 0 \qquad \forall c \in G \qquad \text{(T3)}$$

$$\sum_{c\in S_p} X_{p,c} \leq 1 \qquad \forall p \in P \qquad \text{(T4)}$$

$$\sum_{p\in P | c\in S_p} X_{p,c} \leq 1 \qquad \forall c \in S \qquad \text{(T5)}$$

$$\alpha \geq 0$$

$$\beta_c \geq 0 \qquad \forall c \in C$$

$$\gamma \geq 0$$

$$\delta_d \geq 0 \qquad \forall d \in D$$

$$X_{p,c} \in \{0,1\} \qquad \forall p \in P, c \in S_p \qquad \text{(T6)}$$

Discussion

This reformulation uses the variables introduced as duals for the constraints in AMAX.

The "defender-attacker" two-sided option solves **SAFE_ILP** to position seen defender platforms, recovering the corresponding attack plans by solving **AMAX($\widehat{\mathbf{evX}}$)** with variables X fixed at their optimal values, and $\widehat{\mathbf{evX}}_{d,p,c} = ev_{d,p,c} X_{p,c}$.

4. Decomposition

SAFE_ILP can be (very) hard to solve at large scale. Accordingly, we have decomposed the SAFE optimization as follows. We modify **DMIN($\hat{\mathbf{Y}}$)**, replacing equation (D1) with a set of constraints (D1D).

New index

$k \in K$ decomposition iteration

New Data

$\hat{Y}_k$ attacker plans for iteration k

DMIND($\hat{\mathbf{Y}}$) formulation

$$Z_{\min}(\hat{Y}) = \min_{Z,X} Z$$

$$s.t. \quad Z \geq \sum_{\substack{d \in D, \\ p \in P, c \in S_p}} ev_{d.p,c} \hat{Y}_d^k X_{p,c}, \quad k=1,\ldots,K \quad \text{(D1D)}$$

and constraints (D2)-(D4).

The complete decomposition algorithm is as follows:

Algorithm MINMAX

Input: Data for defense problem, optimality tolerance $\varepsilon \geq 0$;

Output: ε-optimal SAFE location plan $\mathbf{X}^*$, and responding attacker plan $\mathbf{Y}^*$;

1. Initialize best upper bound $Z_{UB} \leftarrow \infty$, best lower bound $Z_{LB} \leftarrow -\infty$, define the incumbent, null SAFE plan $\mathbf{X}^* \leftarrow \hat{\mathbf{X}}^1 \leftarrow \mathbf{0}$ as the best found so far, and set iteration counter $K \leftarrow 1$;

2. **Subproblem**: Using $\widehat{\mathbf{evX}}_{d,p,c} = ev_{d,p,c} X_{p,c}$, solve subproblem **AMAX($\widehat{\mathbf{evX}}$)** to determine the optimal attack plan $\hat{\mathbf{Y}}^K$ given $\hat{\mathbf{X}}^K$; the bound on the associated objective is $\overline{Z}_{\max}(\hat{\mathbf{X}}^K)$;

3. If ($Z_{UB} > \overline{Z}_{\max}(\hat{\mathbf{X}}^K)$) set $Z_{UB} \leftarrow \overline{Z}_{\max}(\hat{\mathbf{X}}^K)$ and record improved incumbent SAFE plan $\mathbf{X}^* \leftarrow \hat{\mathbf{X}}^K$, and responding attacker plan $\mathbf{Y}^* \leftarrow \hat{\mathbf{Y}}^K$;

4. If ($Z_{UB} - Z_{LB} \le \varepsilon$) go to **End**;

5. **Master Problem:** Given attack plans $\hat{\mathbf{Y}}^k$, k=1,…K, attempt to solve master problem **DMIN($\hat{\mathbf{Y}}$)** to determine an optimal defender plan $\hat{\mathbf{X}}^{K+1}$. The bound on the objective is $\underline{Z}_{\min}(\hat{\mathbf{Y}})$;

6. If $Z_{LB} < \underline{Z}_{\min}(\hat{\mathbf{Y}})$ set $Z_{LB} \leftarrow \underline{Z}_{\min}(\hat{\mathbf{Y}})$;

7. If ($Z_{UB} - Z_{LB} \le \varepsilon$) go to **End**;

8. Set $K \leftarrow K+1$ and go to step (2) (**Subproblem)**;

9. **End**: Print "$\mathbf{X}^*$ is an ε-optimal SAFE solution, and $\mathbf{Y}^*$ is the attacker response to that plan," and halt.

For the sake of efficiency, one need not store incumbent attacker plans $\mathbf{Y}^*$ in step 3. These can be recovered after-the-fact by computing $\widehat{\mathbf{evX}}_{d,p,c} = ev_{d,p,c} X^*_{p,c}$ and solving **AMAX($\widehat{\mathbf{evX}}$)**.

The advantage here is that the decomposition isolates a large subproblem that is a capacitated maximum-flow linear program from the much smaller, and simpler integer linear program master problem to locate platforms. The former problem can be solved very quickly with a specialized network simplex algorithm (e.g., Bradley, et al. 1977), and the latter can be solved with a local search heuristic. This offers the opportunity to write a customized solver in a programming language without need for licensed mathematical modeling language or commercial optimization solver, thus reducing the cost per seat from about $8,000 to zero.

E. INSTANCES

We produce several instances that include a generic situation for sensitivity tests as well as several real-world ports and maritime assets. Our real-world examples include the Port of Los Angeles and Long Beach, Port of Hong Kong, USN Fifth Fleet headquarters in Bahrain, and Al Basra Oil Terminal (ABOT) in Iraq. The first two are considered mega-ports both of which are an integral part of the international commerce network. An attack on either one could critically disrupt international trade causing massive delays and ultimately losses of millions of dollars. Bahrain holds strategic importance for the United States. The Fifth Fleet includes all naval assets from the Suez Canal to the Indian Ocean. ABOT is considered the lifeline of the Iraqi economy. It currently accounts for 97% of the Iraqi crude oil exports to the world (United States Embassy – Iraq, 2006). As the only major source of funding to the Iraqi government, any disruption of operations will hinder rebuilding operations and will be another factor of instability in that country.

III. RESULTS AND ANALYSIS

We demonstrate planning methods with our sample of defense surveillance problems using different numbers of defenders and numbers of attackers. Each SAFE Defender class boat normally operates within ten nautical miles of its home base location (USCG, 2004, p. 4ff).

For each defense planning problem, we evaluate a combination of one-to-four attacker boats versus two and four defender boats. We include obstruction masking of defender radars, with ray tracing to determine exactly which cells can be seen by a defender boat in any particular picket position. The obstruction masking ray tracing is very computationally expensive in our mathematical modeling language, but trivial, and fast, in a procedural programming language. We have programmed the ray tracing and obstruction geometry separately from the model generation language, thus achieving two orders of magnitude speed-up of computation (e.g., ray tracing for a single scenario has been reduced from almost two hours to less than a minute). The obstruction masking elicits real-world terrorist behavior to hide and evade detection.

Our model achieves nearly 100% probability of detection for every surveillance problem.

We are dealing with small, fast attack boats, and we want a high-resolution maneuver network. We assign cell width to be 0.15 NM. The surveillance problems we state fit within a 30 vertical by 35 horizontal cell matrix. The marine domains are about 4.5 NM by 5.3 NM, or a total surveillance area of about 24 NM^2.

The GAMS modeling language and CPLEX solver (GAMS, 2008) respectively generate a problem instance in about a two hours (with almost all of this time spend ray tracing for cell-to-cell radar visibility), and a few minutes in CPLEX. Exporting the ray tracing reduces the GAMS execution time to less than a minute.

CPLEX cannot solve some instances, issuing obscure diagnostics that turn out to be due to insufficient random access computer memory. For example, our Los Angeles-Long Beach DUAL-ILP has (6,799 rows, 3,862 columns, and 18,210,510 nonzero elements), overflowing two gigabytes of memory.

We have employed the Benders Decomposition. Each Benders decomposition subproblem has only 838 rows, 6,016 continuous variables, and 12,032 nonzero elements; and each master problem 761 rows, 3,025 binary variables, and 9,073 non-zero elements. The decomposition converges to zero decomposition gap in 13 iterations (just a few seconds of compute time).

A. GENERIC SURVEILLANCE PLANNING PROBLEM

In our generic instance we pose a maritime environment where there are islands and obstacles between the attacker and the goal target cells. Table 4 shows the suggested positions of each of two defender platforms, and Table 5 for four defenders. We solve these instances using decomposition and achieve, at once, a decomposition gap of 0% and approximately 100% probability of detection for each instance.

	Defender 1 Position	**Defender 2 Position**
One Attacker	i01 j27	i27 j01
Two Attackers	i01 j27	i27 j01
Three Attackers	i30 j09	i02 j25
Four Attackers	i30 j09	i02 j25

Table 4. Generic instance positioning two defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning and radar capabilities.

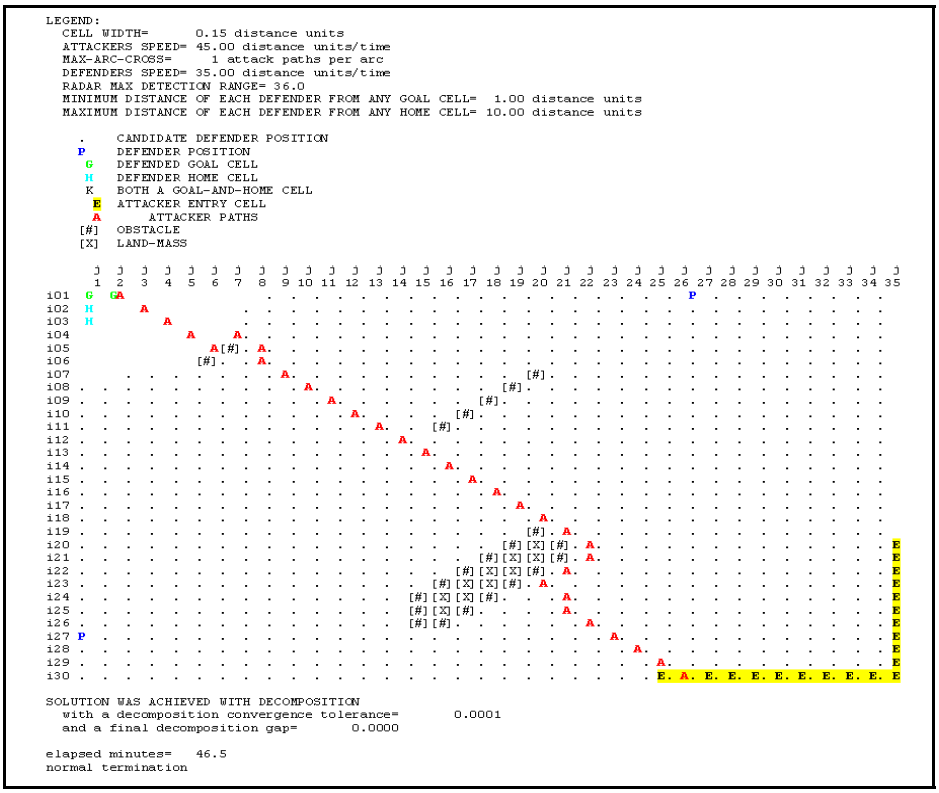

Figure 6. Generic instance with a single attacker and two SAFE Defender boats. The defended goal cells "G" are (i01,j1) and (i01,j02). The SAFE defender boats are based at cells "H" (i02,j01) and (i03,j01). Obstacle boundaries are shown with "[#]". The attacker can enter via any cell on the threat axis labeled "E" (the southeast border). Defender boats cannot locate too close to goal cells, or their alarm would be of little use, and "." indicates just how close (or where else) they can locate. Here, the defenders are located at (i27,j01) and (i01,j26). The lone attacker enters at (i30,j26), and, knowing defender positions, uses obstacles as best able to maximize probability of evasion, then plans a nearly-direct run at goal cell (i01,j02). The attacker probability of evasion is near zero.

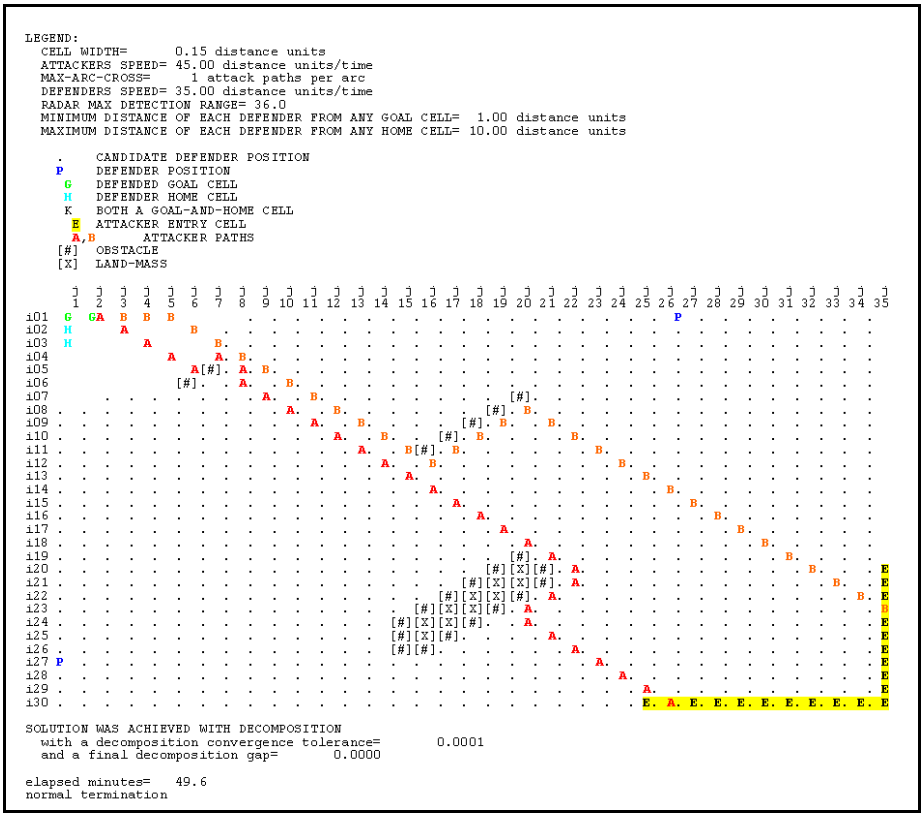

Figure 7. Generic instance with two attackers and two SAFE Defender boats. As with just one attacker, the defenders still position at (i27,j01) and (i01,j26), and the two attackers spread out to use obstructions to influence and weaken defender sensing. Recall, our defender positioning is in anticipation of a raid of two, and the two attackers know where we are pre-positioned. Note how the defender positions maximize the coverage of attacker transit cells, and minimize obscuration by obstructions.

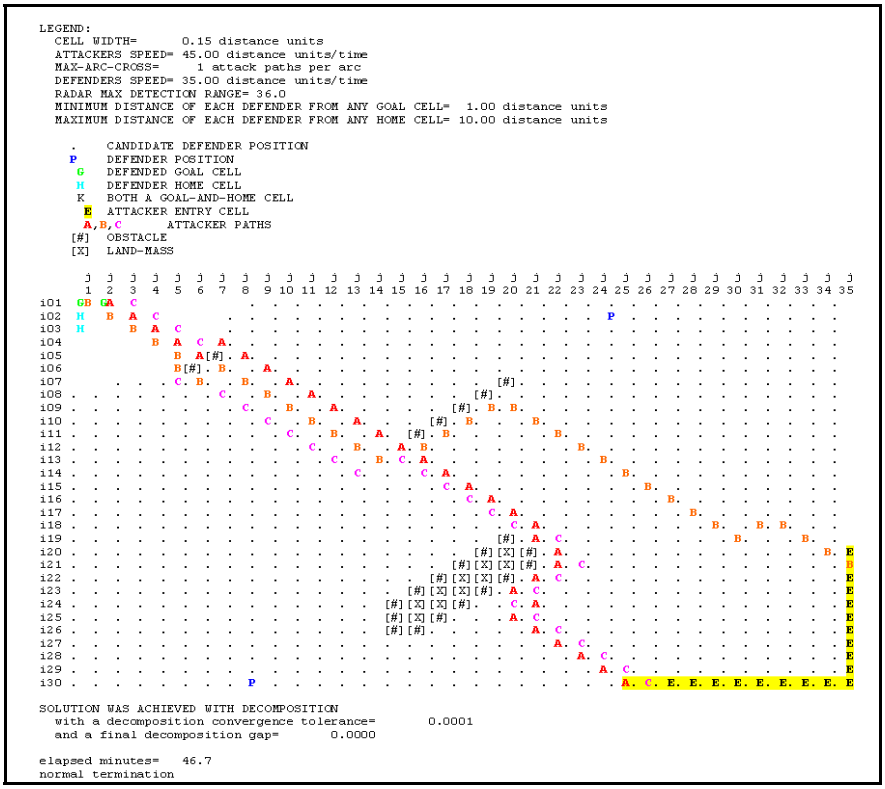

Figure 8. Generic instance with three attackers and two SAFE Defender boats. Defenders position at (i30,j08) and (i02,j24), the better to observe three independent attackers. Compare with the one- and two-attacker cases, and you see the defenders adapt to the attackers' increased degrees of freedom to use obstructions. The defenders are positioned to thwart the worst-case attack tracks shown, as well as all lesser attack plans not shown.

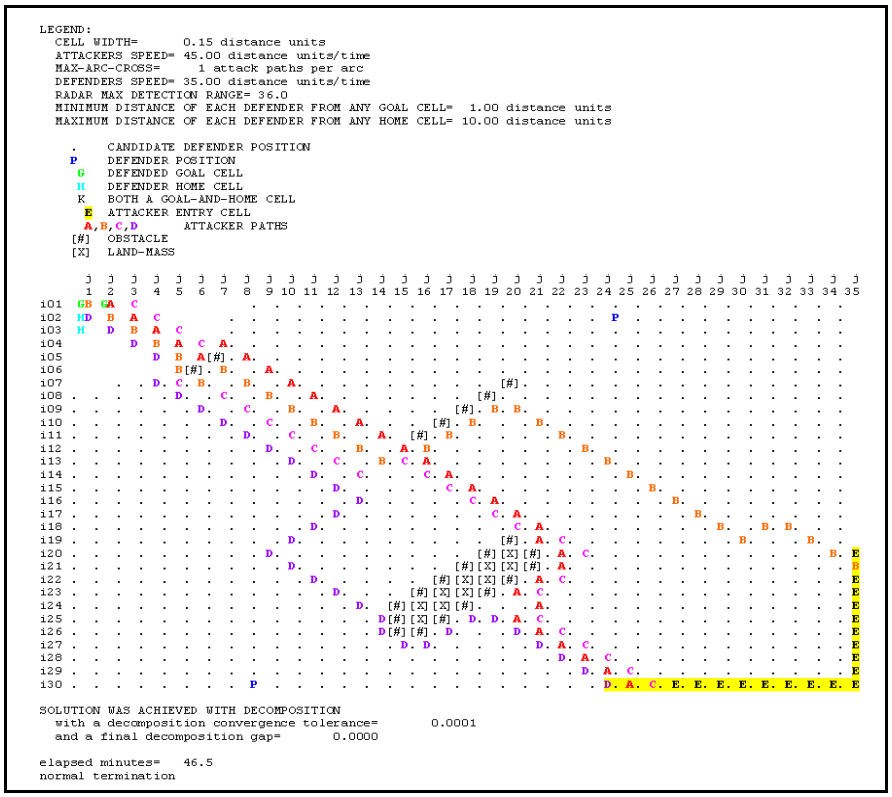

Figure 9. Generic instance with four attackers and two SAFE Defender boats. Optimal defender positions are the same picket locations as for the three-attacker case.

	Defender 1	Defender 2	Defender 3	Defender 4
One Attacker	i30 j06	i30 j09	i05 j22	i01 j27
Two Attackers	i27 j01	i30 j09	i05 j22	i01 j27
Three Attackers	i21 j08	i30 j21	i24 j08	i01 j27
Four Attackers	i28 j17	i30 j21	i22 j07	i02 j25

Table 5. Generic instance four Defender boats optimal positioning against one-to-four attacker boats.

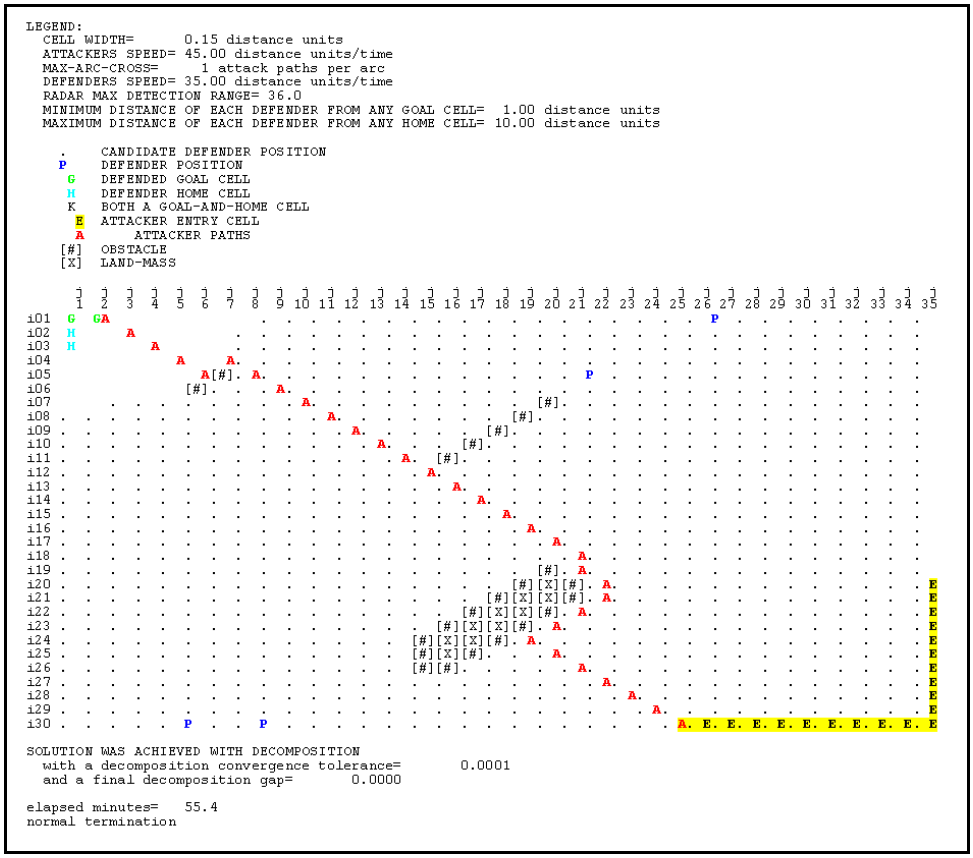

Figure 10. Generic instance with a single attacker and four SAFE Defender boats. Optimal defender locations are (i30,j5), (i30,j8), (i05,j21) and (i01,j26). Once you see this defensive plan, you can intuit why it dominates all others, given the attacker can see it too. However, without optimal advice such as this, you may not have discovered a plan nearly as effective at minimizing the maximum probability the attackers evade our surveillance.

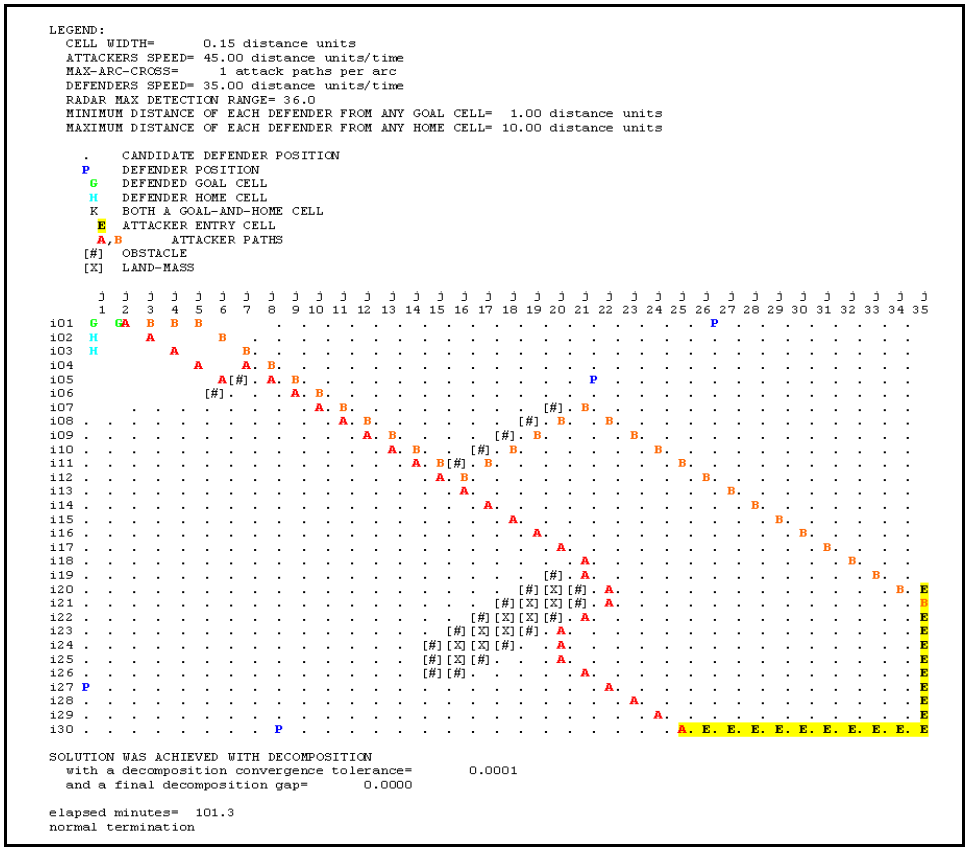

Figure 11. Generic instance with two attackers and four SAFE Defender boats. Optimal defender locations are (i27,j01), (i30,j09), (i05,j22) and (i01,j27). The defenders positions remains the same as the one-attacker case with exception that Defender 1 moves slightly north and west (i30,j06) to (j27, j02).

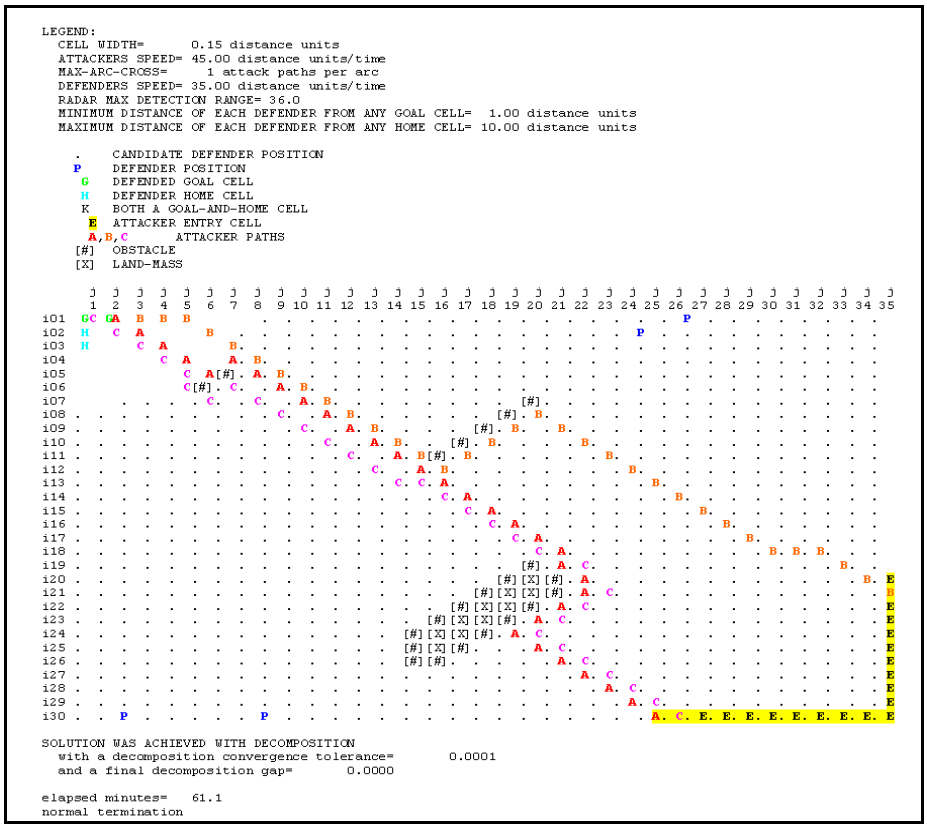

Figure 12. Generic instance with three attackers and four SAFE Defender boats. Optimal defender locations are (i30,j03), (i30,j09), (i02,j25) and (i01,j27). With the increase of attackers to three, we see the defenders one and three slightly reposition themselves for optimal detection.

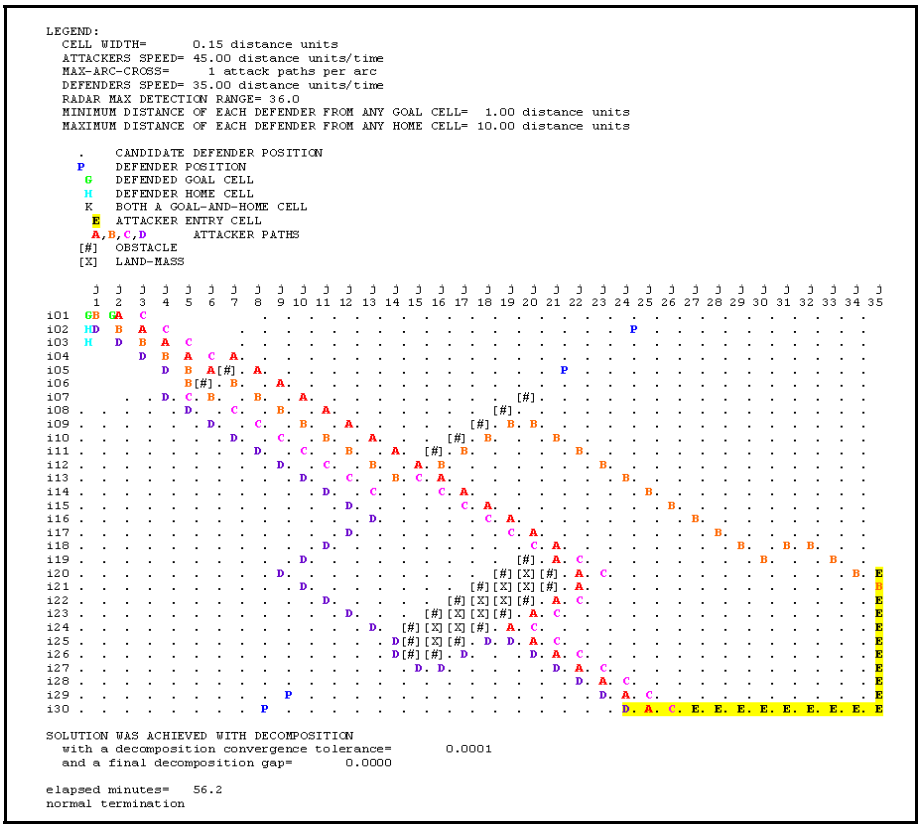

Figure 13. Generic instance with four attackers and four SAFE Defender boats. Optimal defender locations are (i29,j10), (i30,j09), (i05,j22) and (i02,j25). In this case we see all the defenders reposition themselves with the exception of Defender 2, who remains in the same position for all cases. Defenders 1 and 3 exhibit the most drastic repositioning to achieve optimal detection. Again, their actions prove not to be intuitive at all.

B. PORT OF LOS ANGLES

Figure 14. Satellite image of Port of Los Angeles (From: Google Earth).

For the Port of Los Angeles, we demonstrate our model using decomposition with either two defenders or four defenders. Subsequently, we try each combination against a single attacker and up to four. We can achieve an optimal probability of detection of 1.0 with all combinations. Optimal placement of the defenders is shown in Table 6 against a single attacker and up to four. Figures 15 through 18 illustrate the position of the defender boats for each scenario along with the responding optimal attacker paths. We observe that when the number of attackers increases to more then two, optimal boat positioning drastically changes from a close grouping inside the breakwater to one boat inside the breakwater and one at the mouth of the breakwater.

	Defender 1 Position	Defender 2 Position
One Attacker	i18 j08	i25 j08
Two Attackers	i19 j08	i24 j08
Three Attackers	i21 j08	i30 j19
Four Attackers	i23 j08	i30 j20

Table 6. Port of Los Angeles — Two Defender boats optimal positioning against one to four attacker boats.

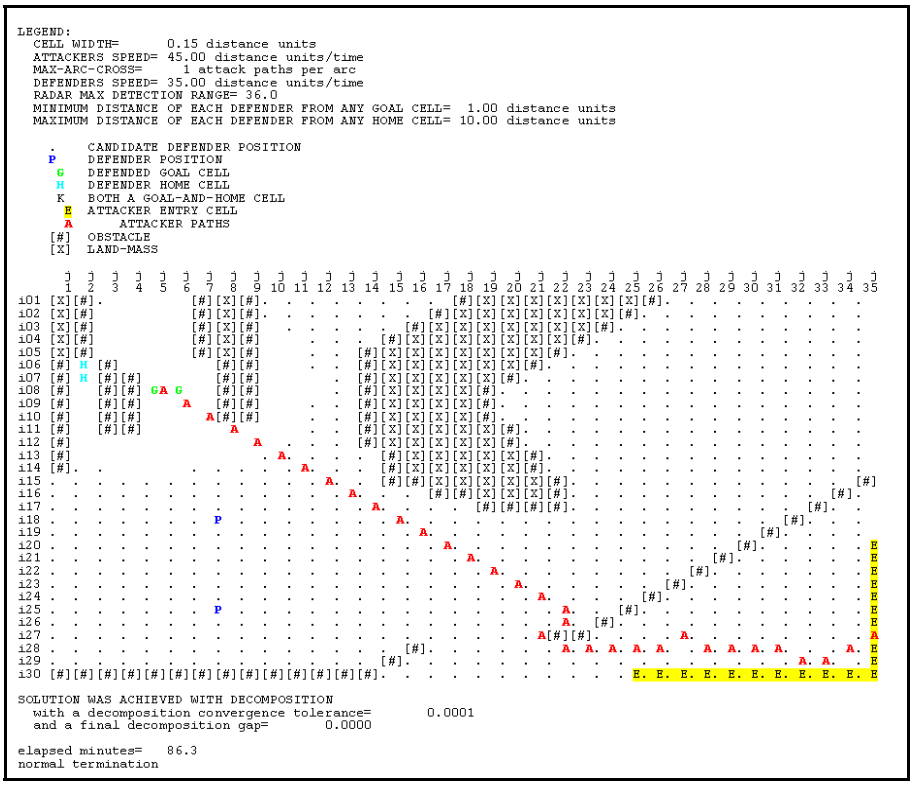

Figure 15. Port of Los Angeles instance with a single attacker and two SAFE Defender boats. The defended goal cells are (i08,j05) and (i08,j6). The SAFE defender boats are based at cells "H" (i06,j02) and (i07,j02). Obstacle boundaries are shown with "[#]", and land-mass with "[X]". The attacker can enter via any cell on the threat axis labeled "E" at the southeast border. Defender boats cannot locate too close to goal cells, or their alarm would be of little use, and "." indicates where defender boats can be located here, no closer than 1 NM to any goal cell. In this instance, the defenders are located at (i25,j08) and (i18,j08). The single attacker enters at (i27,j35), and while knowing defender preparations still decides to directly attack the goal cell (i08,j05). The attacker probability of evasion is near zero.

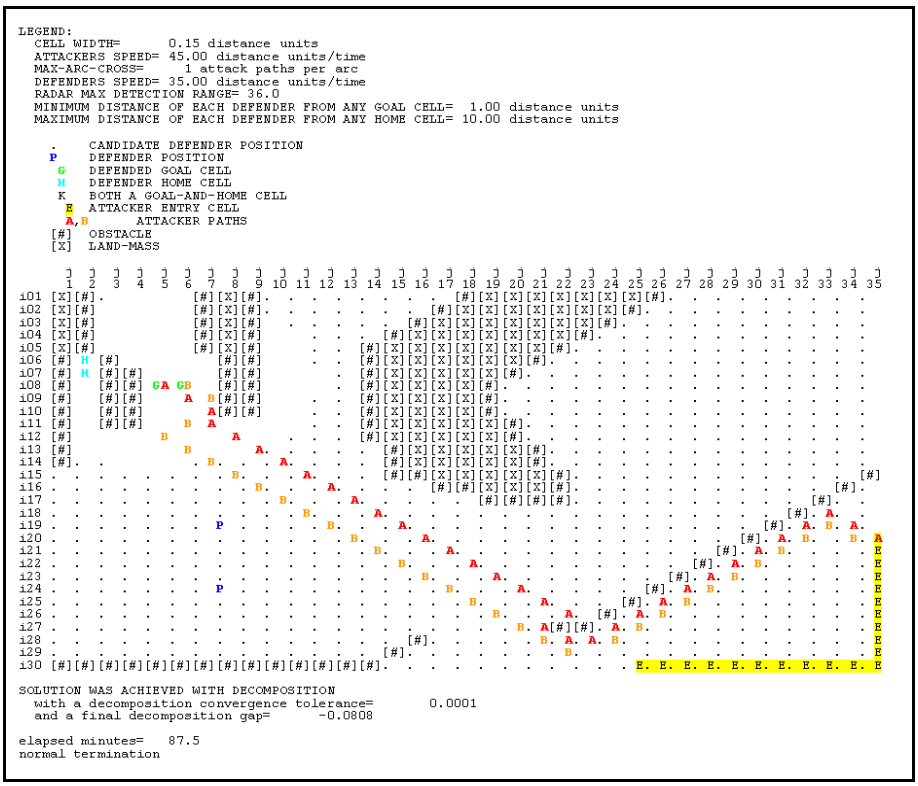

Figure 16. Port of Los Angles instance with two attackers and two SAFE Defender boats. Optimal defender locations are cells (i19,j08) and (i24,j08). The defenders move one cell toward each other in order to detect the two attacking boats.

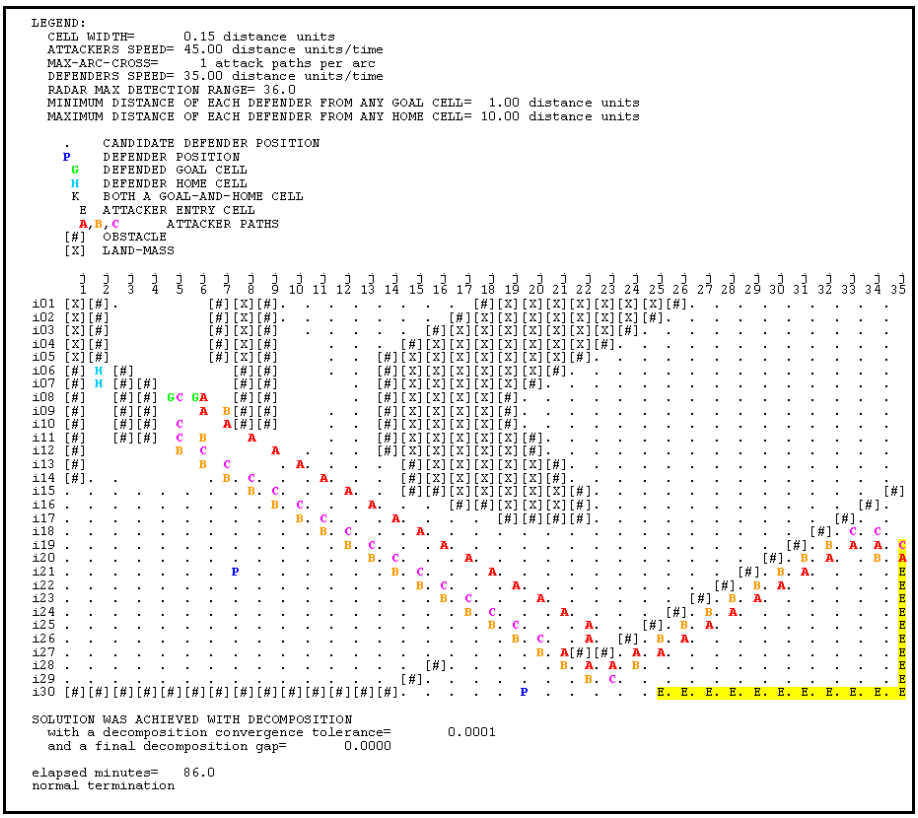

Figure 17. Port of Los Angeles instance with three attackers and two SAFE Defender boats. Optimal defender locations are cells (i21,j08) and (i30,j19). With the increase of the attacker from two to three, defender 1 slightly moves two cells south (0.3 NM) while defender 2 is repositioned dramatically to the mouth of the breakwater at cell (i30,j19).

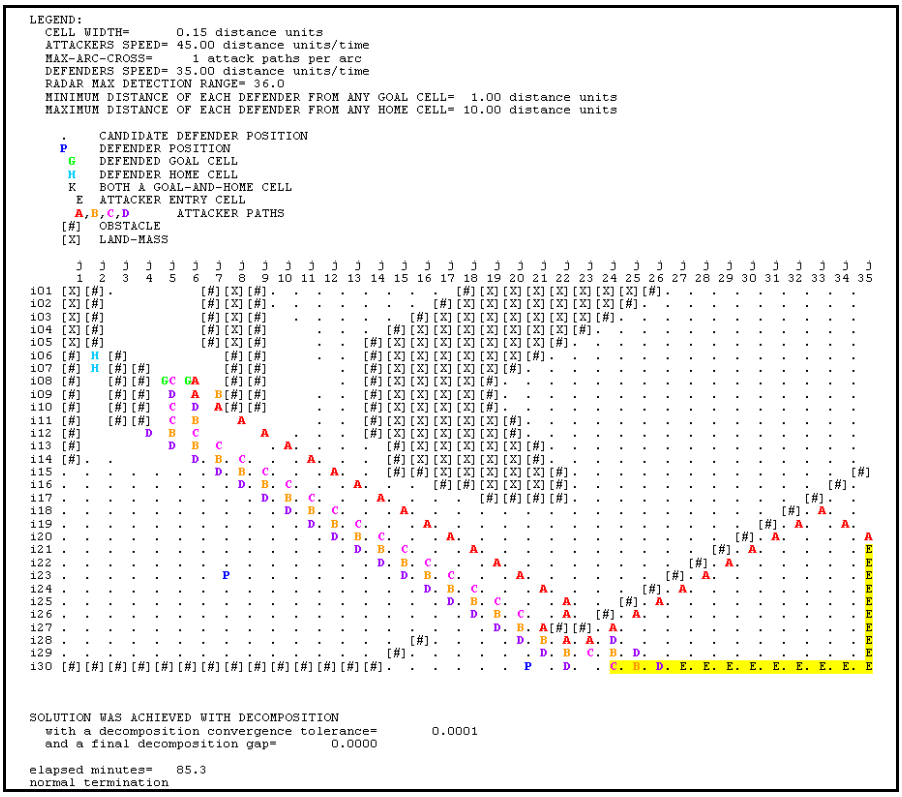

Figure 18. Port of Los Angeles instance with four attackers and two SAFE Defender boats. Optimal defender locations are cells (i23,j08) and (i30,j20). The defender boats only slightly reposition from the case of three attackers to maintain a probability of evasion by the enemy at nearly zero.

When running the Los Angeles instance with four defenders, optimal positioning is slightly different with respect to the number of attackers. Table 7 lists the optimal positions of the four defender boats against the one-to-four attackers. Against one attacker, the defender assignments are all within the breakwater of the port. As the number of attackers increases to two and three, one defender is positioned at the entrance of the port while the others remain inside (see Figures 20 and 21). With four attackers, we can see a split of two at the entry of the breakwater and two within the port waters (see Figure 22).

	Defender 1	Defender 2	Defender 3	Defender 4
One Attacker	i17 j08	i18 j08	i19 j08	i25 j08
Two Attackers	i22 j07	i23 j08	i24 j08	i29 j22
Three Attackers	i21 j08	i24 j07	i24 j08	i30 j21
Four Attackers	i22 j07	i23 j08	i28 j17	i30 j21

Table 7. Port of Los Angles instance – positioning four defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

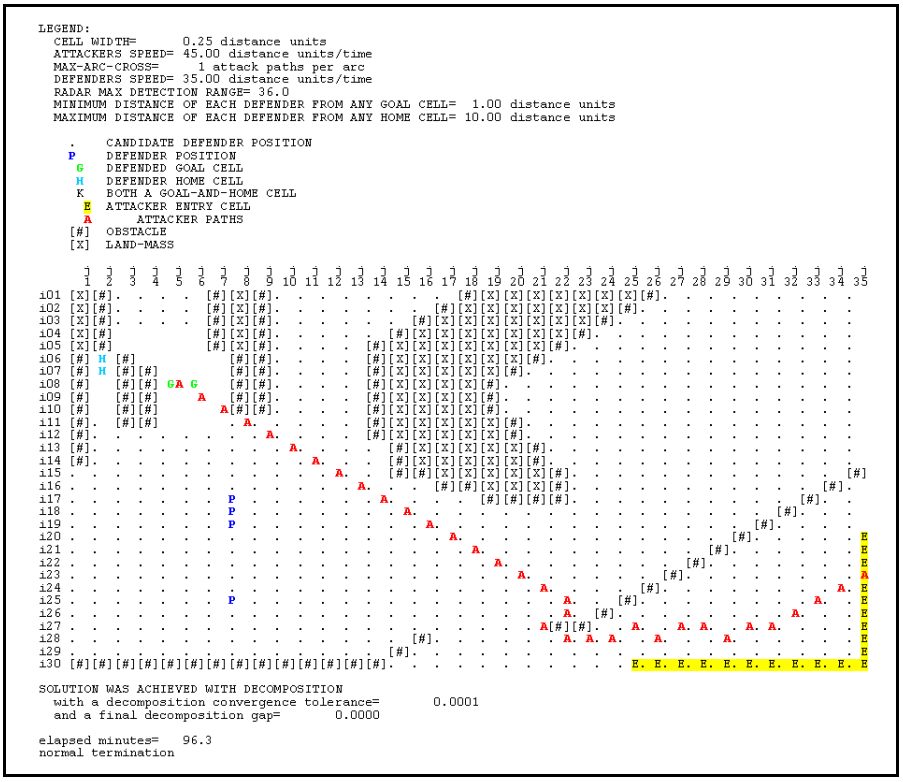

Figure 19. Port of Los Angeles instance with one attacker and four SAFE Defender boats. Optimal defender locations are cells (i17,j08), (i18,j08), (i19,j08), and (i25,j08). The defenders are positioned in a straight line, with defender 4 six cells (0.9NM) further from the rest.

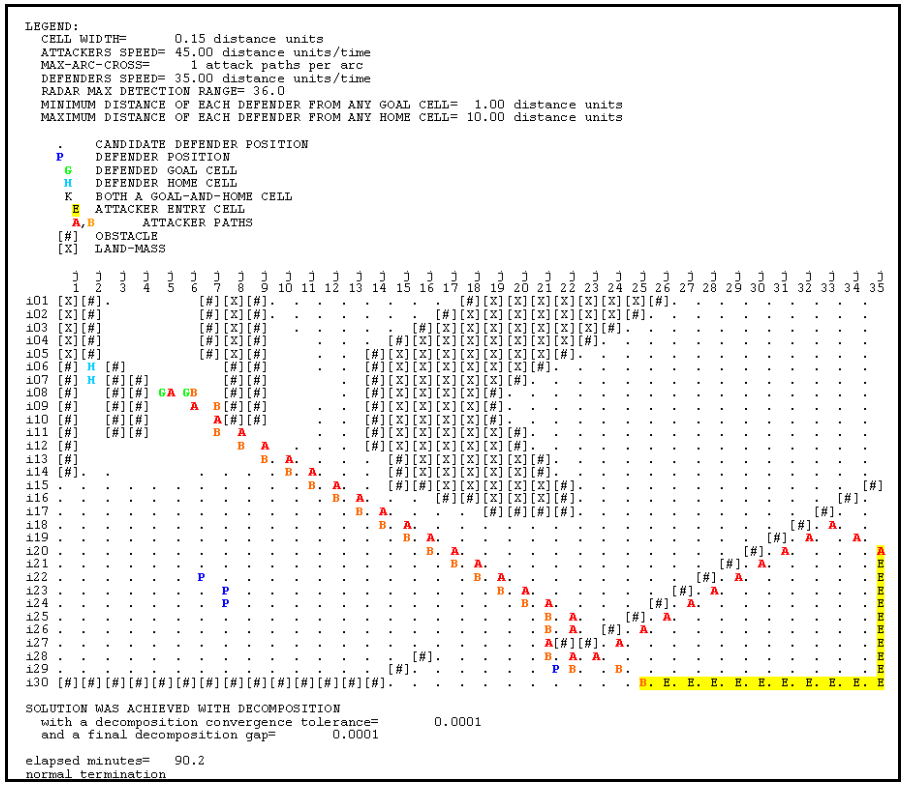

Figure 20. Port of Los Angeles instance with two attackers and four SAFE Defender boats. Optimal defender locations are cells (i22,j07), (i23,j08), (i24,j08), and (i29,j22). An increase of only one attacker invokes a remarkable change in defensive positioning. The first three defenders break their line, but nonetheless maintain a tight grouping, and the fourth defender is placed at the mouth of the breakwater.

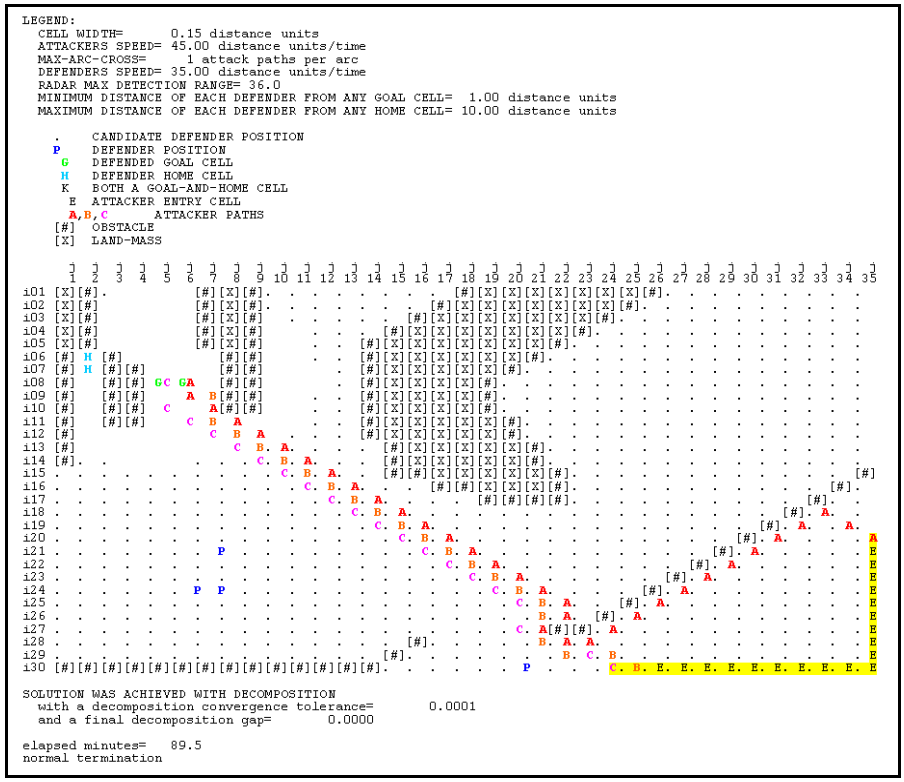

Figure 21. Port of Los Angeles instance with three attackers and four SAFE Defender boats. Optimal defender locations are cells (i21,j08), (i24,j07), (i24,j08), and (i30,j21). The defensive positioning barely changes from the two attacker instance.

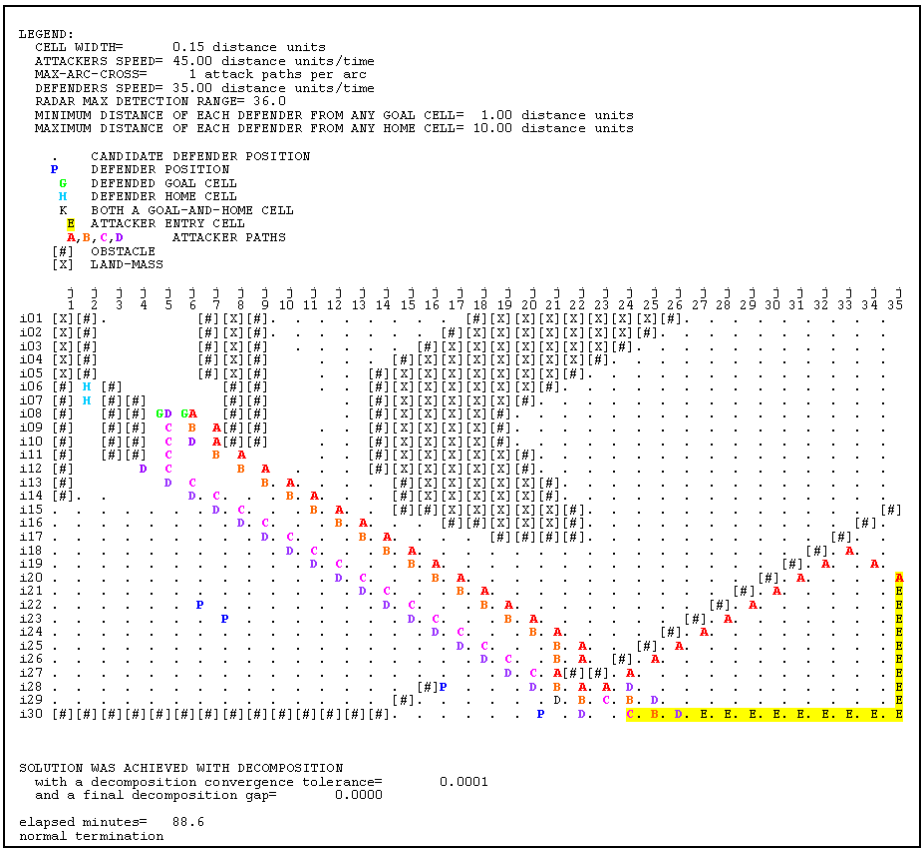

Figure 22. Port of Los Angeles instance with four attackers and four SAFE Defender boats. Optimal defender locations are cells (i22,j07), (i23,j08), (i28,j17), and (i30,j21). We observe that as the attackers increase to four, two boats are positioned at the mouth of the breakwater and two remain within the confines of the port's waters.

C. PORT OF HONG KONG

Figure 23. Satellite image of the port of Hong Kong (From: Google Earth).

The port of Hong Kong is one of the busiest in the world and traffic density presents a challenge to defenders. Allowing threat entry cells from the east and west, we invoke an unexpected optimal defender positioning. We demonstrate planning using Benders decomposition for one-to-four attackers and two or four picket boats.

	Defender 1 Position	Defender 2 Position
One Attacker	i17 j05	i18 j05
Two Attackers	i25 j05	i26 j05
Three Attackers	i25 j05	i26 j05
Four Attackers	i25 j05	i26 j05

Table 8. Port of Hong Kong – positioning two Defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

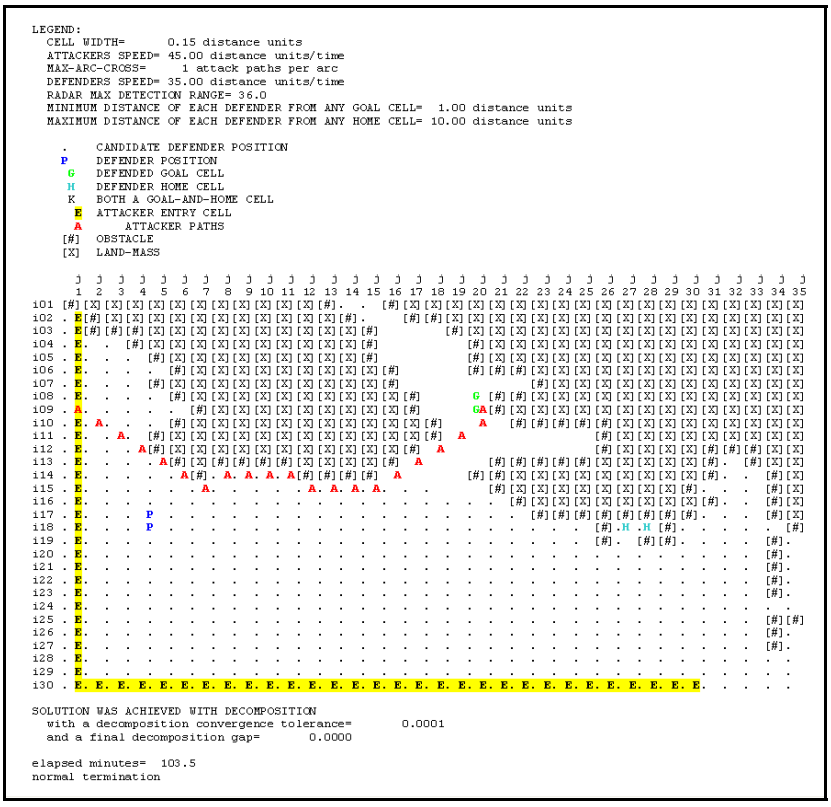

Figure 24. Port of Hong Kong instance with a single attacker and two SAFE Defender boats. The defended goal cells are (i08,j20) and (i09,j20). The SAFE defender boats are based at cells "H" (i18,j27) and (i18,j28). Obstacle boundaries are shown with "[#]", and land-mass with "[X]". The attacker can enter via any cell on the threat axis labeled "E". Defender boats cannot locate too close to goal cells, or their alarm would be of little use, and "." indicates possible defender boats can be locations. The two defenders are positioned in cells (i17,j05) and (i18,j05) which forces the single attacker to enter at cell (i09,j01) to attack the goal cells. However, probability of evasion is reduced to near zero.

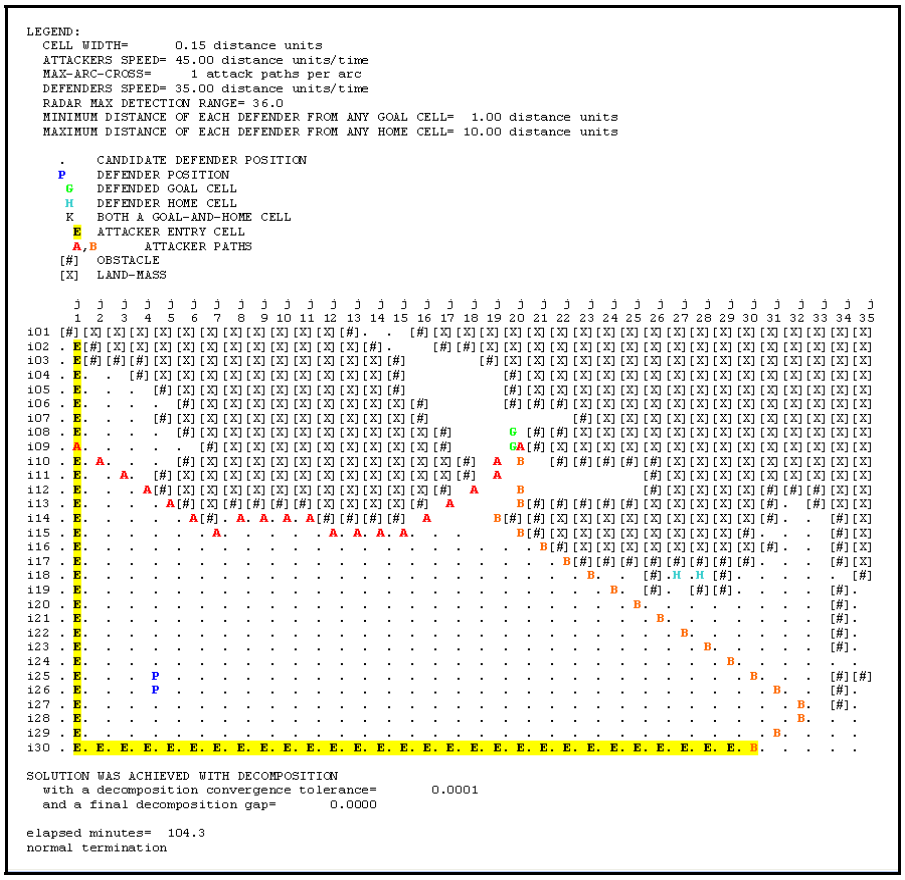

Figure 25. Port of Hong Kong instance with two attackers and two SAFE Defender boats. Optimal positioning of defenders are in cells (i25,j05) and (i26,j05). The two defenders shift down eight cells (1.2 NM) as the attackers increase from one to two. One optimal attacker enters from the north-west, and the other from the south-east.

	Defender 1	Defender 2	Defender 3	Defender 4
One attacker	i18 j04	i17 j05	i18 j05	i19 j05
Two attackers	i26 j04	i25 j05	i26 j05	i26 j05
Three attackers	i26 j04	i25 j05	i26 j05	i26 j05
Four attackers	i26 j04	i25 j05	i26 j05	i26 j05

Table 9. Port of Hong Kong instance – positioning four defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

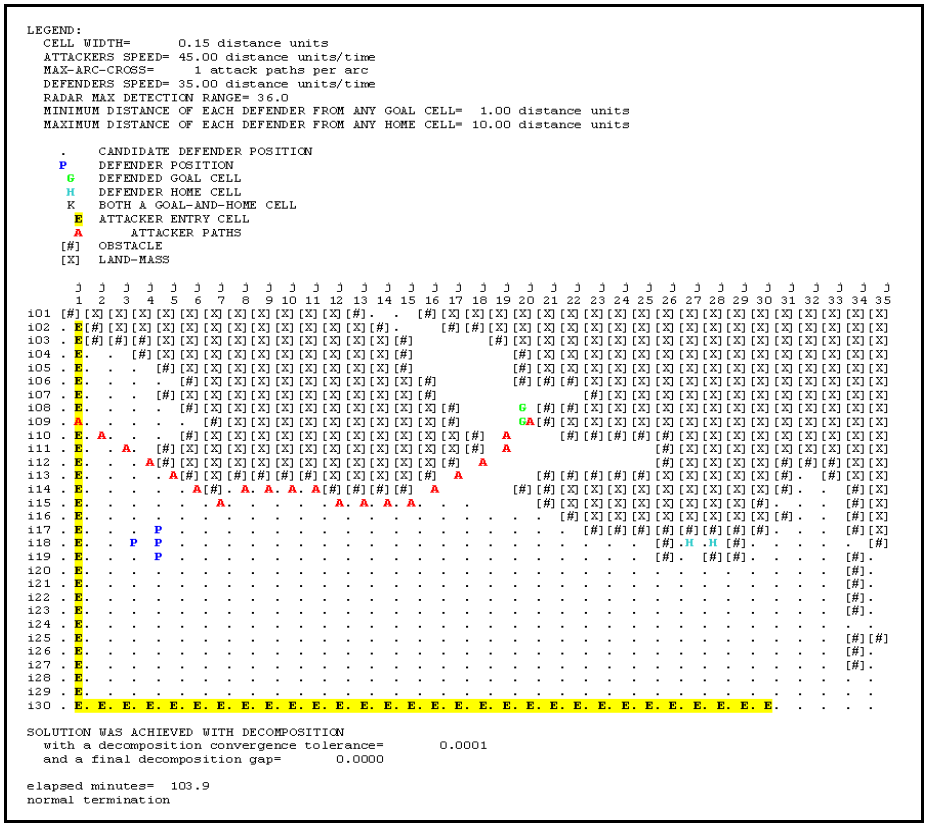

Figure 26. Port of Hong Kong instance with a single attacker and four SAFE Defender boats. Optimal positioning of defenders are in cells (i18,j04), (i17,j05), (i18,j05), and (i19,j05). The defenders maintain a tight grouping even as the number of defenders is increased to four.

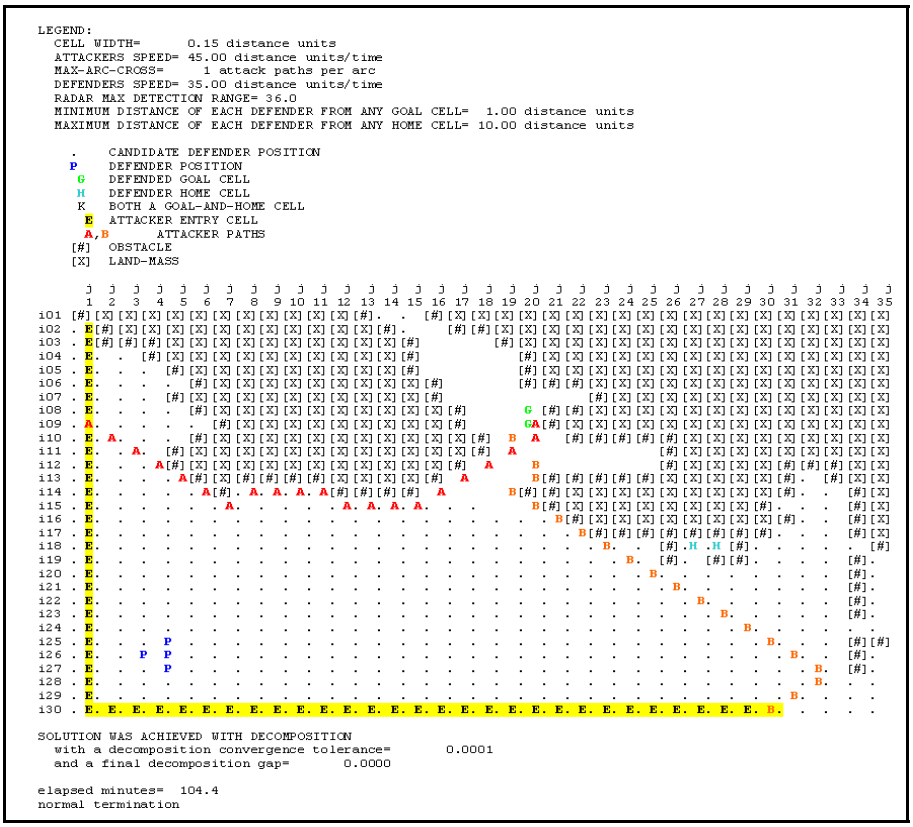

Figure 27. Port of Hong Kong instance with two attackers and four SAFE Defender boats. Optimal positioning of defenders are in cells (i26,j04), (i25,j05), (i26,j05), and (i27,j05). The defenders maintain the same tight grouping.

In the two-defender scenarios the optimal positioning of defensive assets exhibit little to no change as the number of attackers increases from two to four attackers. Similarly, with the four-defender situations, the positioning of defenders does not change. In essence, whether two or four defenders are available, if we anticipate two or more attackers, or defensive positioning should remain the same.

D. AL BASRA OIL TERMINAL (ABOT)

Figure 28. Oil tankers taking on fuel at Al Basra Oil Terminal (from: Royal Navy, 2006).

The Al Basra Oil Terminal proves the hardest to defend, because it has no geographical obstruction between any of the threat entry cells and the goal cells. The goal cells on all sides of the terminal mimic the fragile reality of such an offshore structure. Even without obstructions between the entry cells and the goal cells, the optimal defender-attacker solutions is surprising; we can still optimally position pickets and achieve a near 1.0 probability of detection.

Optimal positioning of two defenders for the ABOT instance is not significantly altered whether facing a single attacker or four. Similarly, with four defenders their positioning remains relatively the same. However, what proves to be interesting is the attacker's behavior as his number of boats increases. Attackers always enter at the cells nearest to the terminal. Against two defenders, the attackers enter from the north first and as their numbers increase they enter from both the north and the south. They use the target as an obstruction before preceded with a final, direct attack.

	Defender 1 Position	Defender 2 Position
One attacker	i16 j33	i18 j35
Two attackers	i16 j33	i18 j35
Three attackers	i16 j33	i18 j35
Four attackers	i16 j33	i18 j35

Table 10. ABOT instance positioning two defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

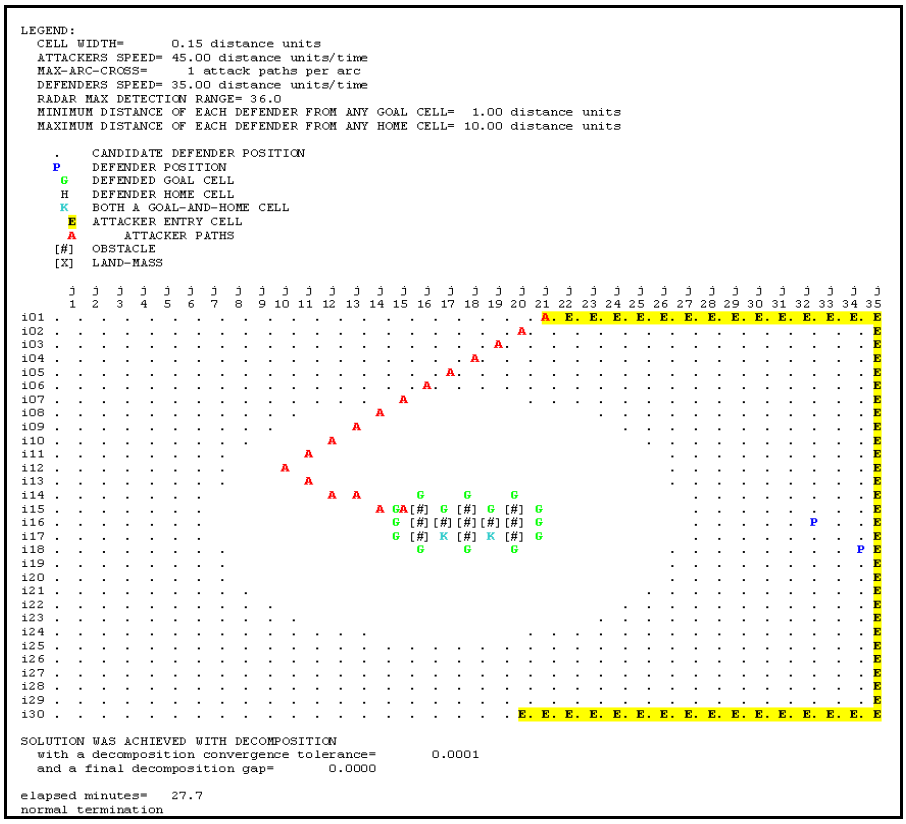

Figure 29. ABOT instance with a single attacker and two SAFE Defender boats. The defended goal cells are all sides of the terminal and marked with "G". The SAFE defender boats are based at cells "K", both a home and goal cells at (i17,j17) and (i17,j19). Obstacle boundaries are shown with "[#]". The attacker can enter via any cell on the threat axis labeled "E". Defender boats cannot locate too close to goal cells, or their alarm would be of little use, and "." indicates possible defender boat locations. The two defenders are positioned in cells (i16,j33) and (i18,j35) which forces the single attacker to enter at cell (i01,j21) to attack the goal cells via an indirect path using the target as an obstruction before turning inbound for a direct final attack run. Probability of evasion is near zero.

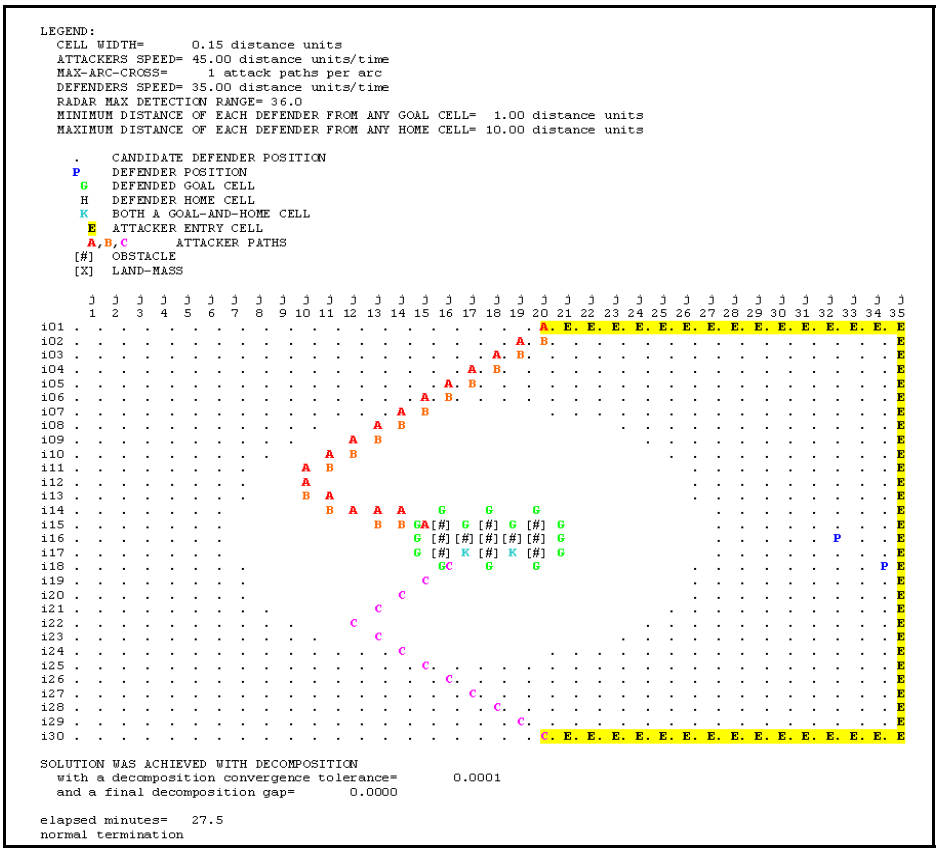

Figure 30. ABOT instance with three attackers and two SAFE Defender boats. The two defenders are positioned in cells (i16,j33) and (i18,j33). The defenders do not change their positions from the one-attacker plan.

	Defender 1	Defender 2	Defender 3	Defender 4
One attacker	i15 j33	i16 j33	i18 j31	i18 j32
Two attackers	i15 j33	i16 j33	i18 j31	i18 j32
Three attackers	i15 j33	i16 j33	i18 j32	i18 j33
Four attackers	i15 j33	i16 j33	i18 j32	i18 j34

Table 11. ABOT instance positioning four defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

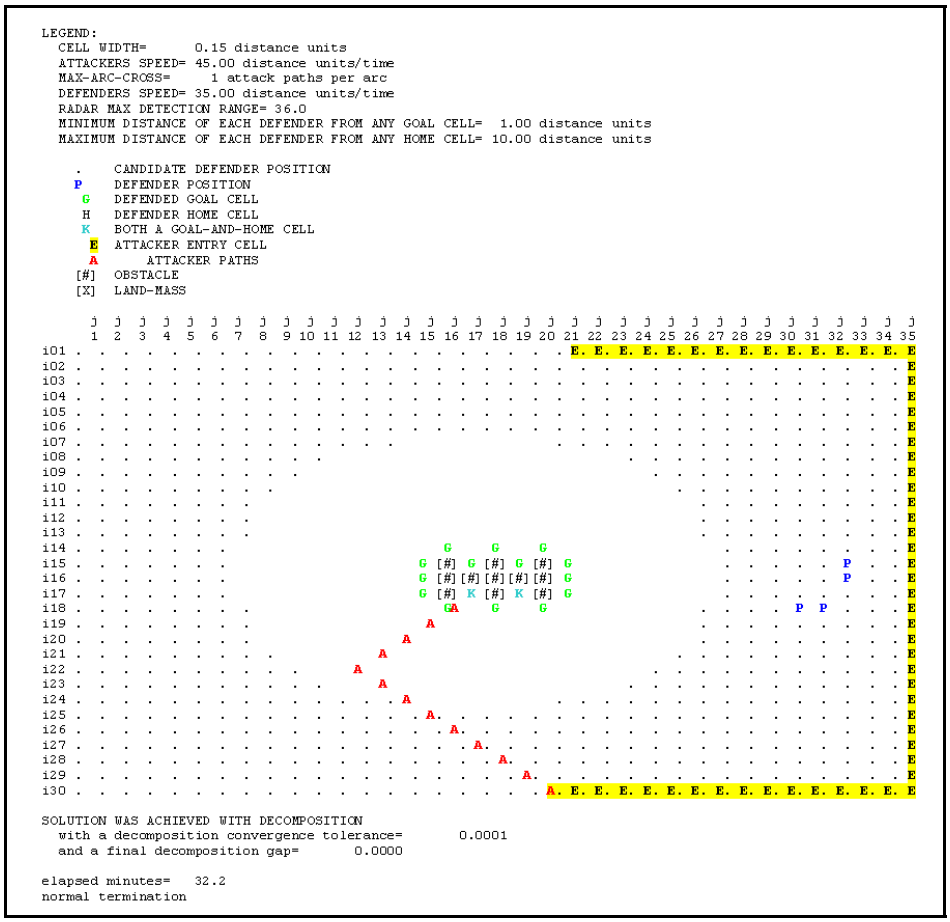

Figure 31. ABOT instance with a single attacker and four SAFE Defender boats. The four defenders are positioned in cells (i15,j33), (i16,j33), (i18,j31), and (i18,j32). The defenders can reduce the probability of evasion to almost zero.

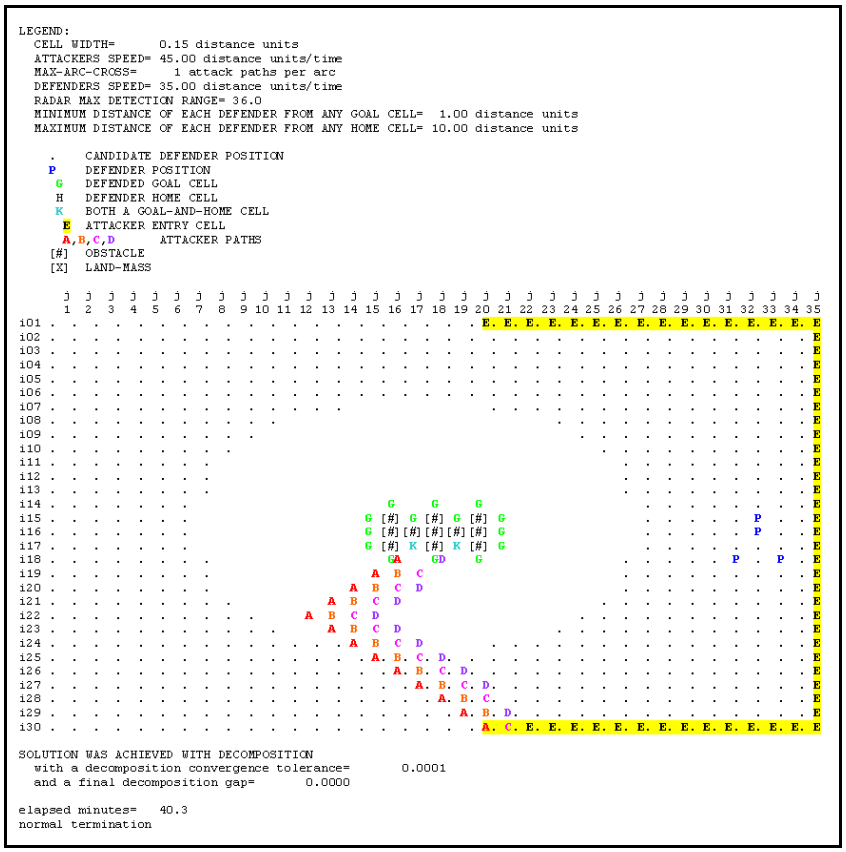

Figure 32. ABOT instance with four attackers and four SAFE Defender boats. The four defenders are positioned in cells (i15,j33), (i16,j33), (i18,j32), and (i18,j34). Only defender 4 moves one cell to the right to maintain optimality.

E. U.S. NAVCENT 5TH FLEET – BAHRAIN

Figure 33. Aerial image of Mina Salman – Bahrain US 5th Fleet Headquarters (from: Google Earth).

Mina Salman's approaches in Bahrain are very constrained, with only one main channel for commercial shipping entering from the south east. However, there are two other approaches that small boats can use to enter the port area. In this instance, we allow entry cells in both directions to gain insight into the defenders behaviors when faced with such a situation. Optimal defenders positions are achievable for all the combinations of attackers and defenders with a probability of detection in the neighborhood of 1.0.

	Defender 1 Position	Defender 2 Position
One attacker	i16 j15	i17 j15
Two attackers	i16 j15	i17 j15
Three attackers	i16 j15	i16 j18
Four attackers	i16 j15	i17 j15

Table 12. Four attacker boats that attack with prior knowledge of defender positioning.

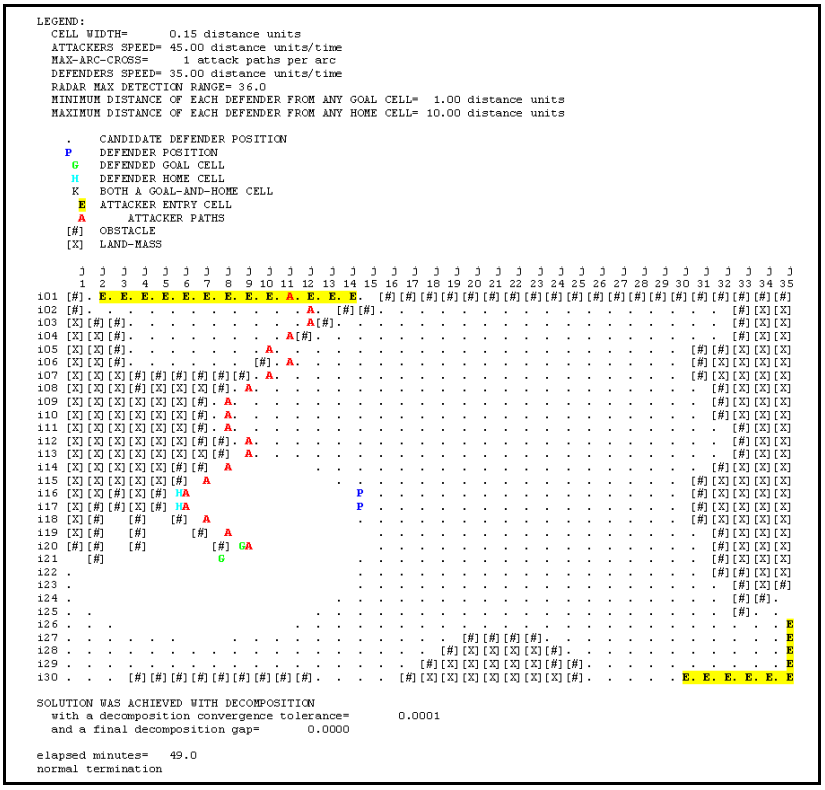

Figure 34. Bahrain instance with a single attacker and two SAFE Defender boats. The defended goal cells "G" are (i20,j09) and (i21,j08). The SAFE defender boats are based at cells "H" at cells (i16,j06) and (i17,j07). Obstacle boundaries are shown with "[#]", and land-mass with "[X]". The attacker can enter via any cell on the threat axis labeled "E" at the northwest and southeast corners. Defender boats cannot locate too close to goal cells, or their alarm would be of little use, and "." indicates where they can locate. Here, the defenders are located at (i16,j15) and (i17,j15). The lone attacker enters at (i01,j11) and, while knowing defender positions, uses the coast to maximize probability of evasion to attack goal cell (i20,j09). The attacker probability of evasion is near zero.

	Defender 1	Defender 2	Defender 3	Defender 4
One attacker	i16 j15	i16 j16	i17 j15	i18 j15
Two attackers	i16 j15	i16 j16	i16 j18	i17 j15
Three attackers	i10 j12	i16 j15	i16 j17	i09 j21
Four attackers	i05 j11	i12 j12	i16 j18	i16 j30

Table 13. Bahrain instance – positioning four defender boats against one-to-four attacker boats that attack with prior knowledge of defender positioning.

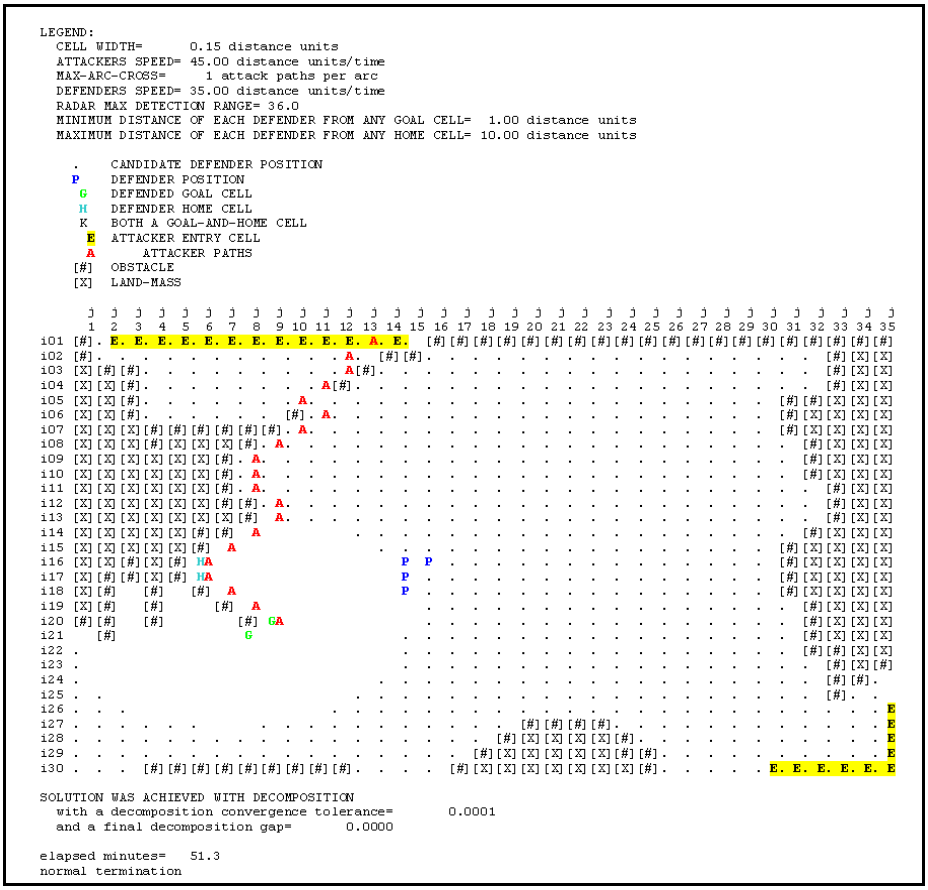

Figure 35. Bahrain instance with a single attacker and four SAFE Defender boats. The defenders are optimally located at (i16,j15), (i16,j16), (i17,j15), and (i18, j15). They are tightly grouped and achieve an almost zero probability of attack evasion.

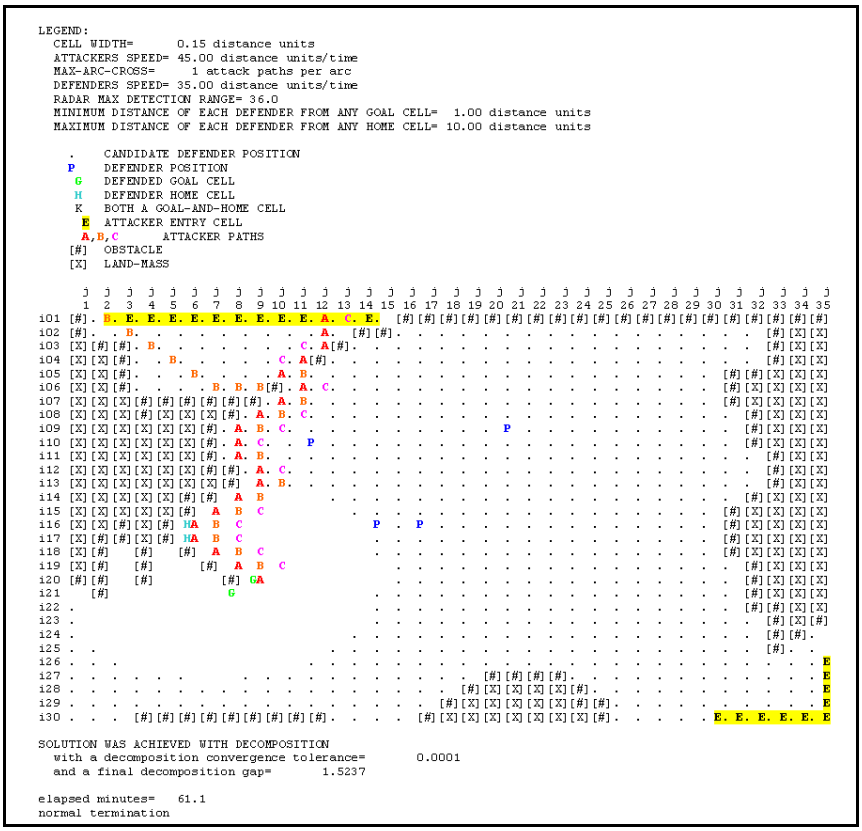

Figure 36. Bahrain instance with three attackers and four SAFE Defender boats. The defenders are located at (i10,j12), (i16,j15), (i16,j17), and (i09,j21). As the number of attackers increases to three, we see an interesting optimal positioning of defenders. The defenders are more spread out and one defender is close to the bridge that the attackers favor for their approach.

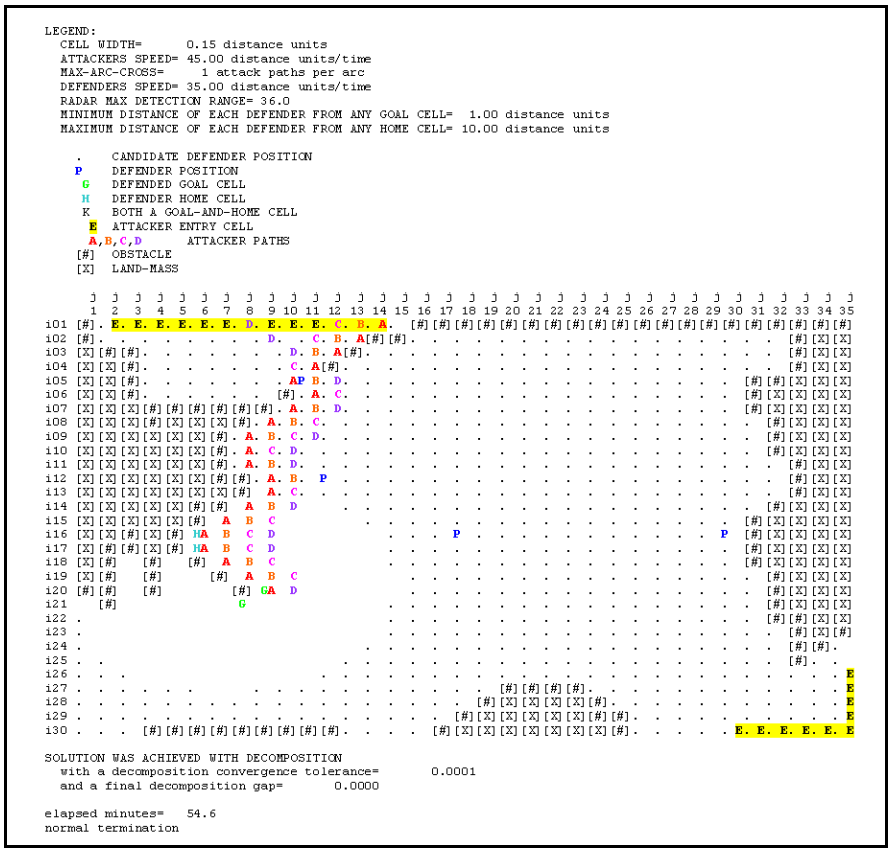

Figure 37. Bahrain instance with four attackers and four SAFE Defender boats. The defenders are located at (i05,j11), (i12,j12), (i16,j18), and (i16,j30). When expecting four attackers the defenders spread out even more to defend against both possible threat axes. The first defender locates right under the bridge in order to bring the probability of detection to almost 1.0.

F. GENERIC SURVEILLANCE PLANNING PROBLEM -- POSITIONING A SHORE RADAR, PICKET BOATS, AND CONSIDERING ELEVATION OF OBSTACLES.

In our generic instance, we examine the optimal placement of defender boats working in conjunction with a shore radar. We seek to optimally place a shore radar given several candidate locations. We also assign elevation to the shore search radar as well as to each obstruction. Also, we increment boat elevations by the tide level. This is to account for any elevated obstructions, as well as to asses the benefit of elevating a sensor over a low-lying one.

The behavior observed is very different from our previous instances: the defender platforms are optimally placed on the opposite side of the fixed shore radar (see Figure 38). Also, the attackers are clearly more concerned with detection by the more powerful shore radar than the less capable defender boats.

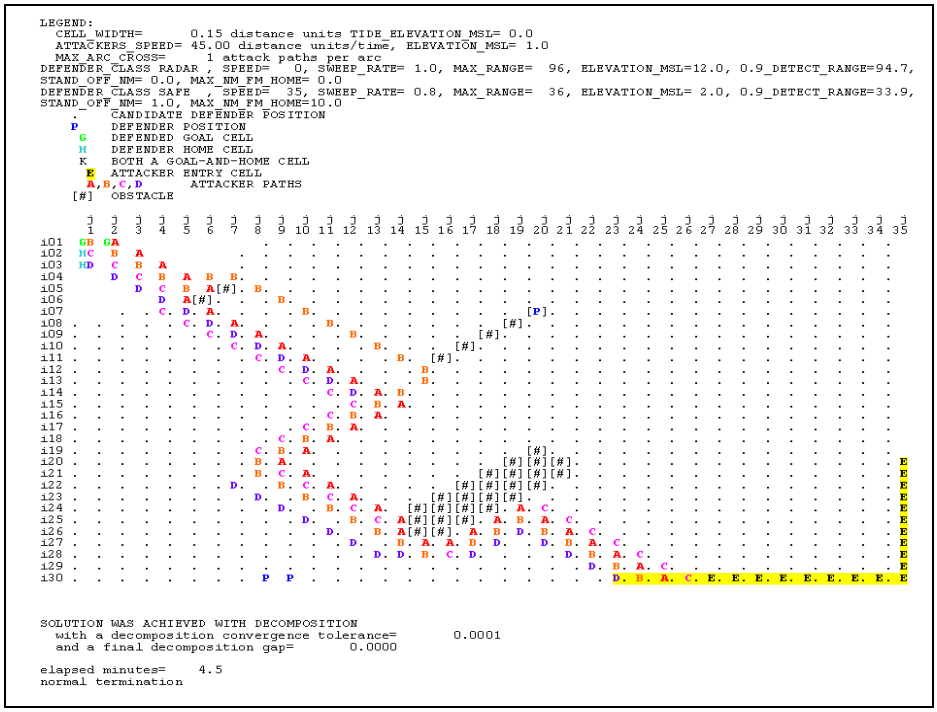

Figure 38. Generic instance with four attackers two SAFE Defender boats, and one shore based-radar. The defenders are located at (i30,j09) and (i30,j10). The shore radar is optimally placed in position (i07, j20). When expecting four attackers the defenders place the shore radar and the defender boats on the opposite sides from each other. The shore radar is placed in the north east possible location, while the defender boats are placed in the south east. The attackers choose paths to avoid altogether the side of the more powerful shore radar. In all cases, the probability of detection is increased to almost 1.0.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

We introduce a bi-level "defender-attacker" integer linear program to advise optimal pre-positioning of defender surveillance pickets to minimize the maximum probability that intelligent attackers, observing our surveillance positions, can evade us.

In every instance we examine, alert defenders with existing radar can detect attacker raids with near 100% probability via their optimal pre-positioning. This is due, in part, to the restricted navigational access channels to ports: These are bottlenecks that offer effective defense postures against attacker speedboats. Still, our optimization sometimes suggests surveillance positions far from the bottlenecks, the better to detect stealthy, evading attackers.

In the real world, exceptional conditions such as stormy sea state may complicate our planning, and (fortunately) that of our adversary. Suffice to say, if we can evaluate the probability that any surveillance platform, in any environmental state, can detect an attacking one, we can optimize our pre-positioning as well or better than anyone with less knowledge.

While detection is desirable, early detection is preferable. We can easily weight our objective function to move our surveillance forward to press for early detection, perhaps at the expense of overall detection.

Although we are merely planning for a detection and alert, we would prefer to also be able to not just contribute to, but to also participate in interdiction. This poses a bi-criterion optimization to detect and interdict. While, in theory, we can pose and solve such problems, in reality the attacker speeds exceed those of our defenders, complicating both the analysis of and the reality of interdiction. We have opted conservatively to detect, and alert shore and defended asset point defenses as best we can. We admire the combined detect-interdict problem, but leave it to our successors to solve.

The interested reader can reproduce all of our experiments from the data shown in this document.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Baja Marine. (2008). Baja 20' Outlaw Specifications. Retrieved February 22, 2008 from http://www.bajamarine.com/index.asp?display=brochure&tab=0&modelid=104525.

Bard. J. and Moore, J. (1990). The Mixed Integer Linear Bi-level Programming Problem, *Operations Research*, 38(5), pp. 911-921.

Bradley, G.H., Brown, G.G., and Graves, G.W. (1977). Design and Implementation of Large-Scale Primal Transshipment Algorithms, *Management Science,* 24(1), pp. 1-34.

Brown, G., Carlyle, M., Salmerón, J. and Wood, K. (2006). "Defending Critical Infrastructure," *Interfaces*, 36, pp. 530-544.

Caldwell, S. (2007). Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. *Testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate*. Retrieved December 7, 2007 from https://www.hsdl.org/homesec/docs/gao/nps33-103007-04.pdf&code=817fa80b0a833c93a10515ee3560896d.

Carafano, J. (2007). Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea. *Backgrounder*. Retrieved December 5, 2007 from http://www.heritage.org/Research/HomelandDefense/upload/bg_2041.pdf.

Department of Homeland Security (DHS). (2002). *Homeland Security Advisory System – Guidance for Federal Departments and Agencies*. Retrieved December 4, 2007 from http://www.dhs.gov/xnews/releases/press_release_0046.shtm.

Department of Homeland Security (DHS). (2005). The National Strategy for Maritime Security. Retrieved December 4, 2007 from http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf.

Department of Homeland Security (DHS). (2007). Budget-in-Brief: Fiscal Year 2008. http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf. (Retrieved December 16, 2007).

Department of the Navy (DON). (2007). Navy Maritime Domain Awareness Concept. Retrieved April 30, 2008 from http://www.dhs.gov/xnews/releases/press_release_0046.shtm.

General Algebraic Modeling System (GAMS). (2008). CPLEX Solver Guide. Retrieved June 2, 2008 from http://www.gams.com/solvers/cplex.pdf.

Google Earth. (2008). Retrieved June 10, 2008 from http://earth.google.com/.

Isidore, C. (2002). *Hope in West Coast Port Talks*. CNN. Retrieved December 5, 2007 from http://money.cnn.com/2002/10/02/news/economy/ports/index.htm.

Isreali and Wood. (2002). Shortest Path Network Interdiction. *2002 Networks*, Vol. 40(2), pp. 97–111.

Jane's Information Group. (2005). *SAFE Boats International*. Retrieved January 20, 2008 from http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/binder/jnc/jnc_9537.htm@current&pageSelected=janesReference&keyword=SAFE%20boats&backPath=http://search.janes.com/Search&Prod_Name=JNC&.

MI 5 Security Service. (2007). *Al Qaida*. Retrieved December 4, 2007 from http://www.mi5.gov.uk/print/Page33.html.

Murphy, M. (2006). *Maritime threat: tactics and technology of the Sea Tigers*. Jane's Intelligence Review. Retrieved February 19, 2008 from http://www8.janes.com/Search/documentView.do?docId=/content1/janesdata/mags/jir/history/jir2006/jir01489.htm@current&pageSelected=allJanes&keyword=maritime%20threat&backPath=http://search.janes.com/Search&Prod_Name=JIR&.

National Security Presidential Directive NSPD-41. (2004). Maritime Security Policy. *The White House*, Washington, DC.

Royal Navy. (2006). Combined Task Force 158 (CTF 158). Retrieved May 16, 2008 from http://www.royalnavy.mod.uk/server?show=nav.00h00400100500700e002&outputFormat=print

SAFE. (2003). Defender Class Operator's Handbook. Retrieved March 20, 2008 from http://www.defenderclass.com/pages/nigerian%20navy/training/DefenderClassOPS_small.pdf.

Skolnik, M.I. (1990). RADAR Handbook (2nd Edition), *McGraw-Hill*, New York, New York.

The Caltrade Report (2007). *Strike Looms at Ports of Los Angeles, Long Beach.* Retrieved December 5, 2007 from http://www.caltradereport.com/eWebPages/front-page-1184673116.html

United States Coast Guard (USCG). (2004). *Port Security Units Organization Manual*. Retrieved March 20, 2008 from https://www.hsdl.org/homesec/docs/dod/nps37-121707-07.pdf&code=817fa80b0a833c93a10515ee3560896d.

United States Coast Guard (USCG). (2005). *Fact File - Maritime Safety and Security Teams*. Retrieved December 8, 2007 from http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/MSST.htm.

United States Coast Guard (USCG). (2007a). *MARSEC Levels*. Retrieved December 8, 2007. http://www.uscg.mil/safetylevels/whatismarsec.asp.

United States Coast Guard (USCG). (2007b.*) Fact File - Port Security Units*. Retrieved December 8, 2007. http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/PSUs.html.

United States Embassy - Iraq. (2006, December 23). *Press Release*. Retrieved May 20, 2008 from http://iraq.usembassy.gov/iraq/20061224_basra_oil_termina.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Distinguished Professor Gerald Brown
   Naval Postgraduate School
   Monterey, California

4. Senior Lecturer Jeffrey Kline, CAPT, USN (ret)
   Naval Postgraduate School
   Monterey, California