A Defender-Attacker Optimization of Port Radar Surveillance

Gerald Brown, Matthew Carlyle, Ahmad Abdul-Ghaffar, Jeffrey Kline

Department of Operations Research, Naval Postgraduate School, Monterey, California 93943

Received 20 August 2008; revised 2 January 2010; accepted 3 June 2010
DOI 10.1002/nav.20423
Published online 16 March 2011 in Wiley Online Library (wileyonlinelibrary.com).

Abstract: The U.S. Coast Guard, Customs and Border Patrol, Marine Corps, and Navy have deployed several hundred port patrol vessels to protect waterways, 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 surface search radar, radios, and a machine gun. These vessels coordinate surveillance patrols in groups of two or four. We developed a mathematical model for advantageously positioning these vessels, and possibly shore-based radar too, to minimize the probability that an intelligent adversary in one or more speedboats will evade detection while mounting an attack. Attackers can use elevated obstructions to evade radar detection in their attack paths, and ports feature many such restrictions to navigation and observation. A key, but realistic assumption complicates planning: the attackers will be aware of defensive positions and capabilities in advance of mounting their attack. The defender-attacker optimization suggests plans here for a fictitious port, the port of Hong Kong, and the U.S. Navy Fifth Fleet Headquarters in Bahrain. In these cases, the defender can almost certainly detect any attack, even though the attacker, observing defender prepositioning, plans clever, and evasive attack tracks. Published 2011 Wiley Periodicals, Inc.[†] Naval Research Logistics 58: 223–235, 2011

Keywords: Port security; optimization; attacker-defender

"And thence discover how with most advantage
They may vex us with shot, or with assault."
Shakespeare, King Henry VI.

1. INTRODUCTION

We introduce a new planning tool for locating shore radars 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 high-value defended assets, such as anchored or pier-side U.S. Navy ships, commercial container ships, oil tankers, or liquefied natural gas carriers. The distinguishing contribution here is that this planning tool explicitly recognizes that the attackers can be expected to have prior knowledge of defensive disposition, either from shore observers, satellite imagery, or on-board radar threat detectors: the attackers will observe defensive preparations and plan their attacks accordingly. There is no other such decision-support tool available today for maritime domain awareness.

Standard radar equations provide detection predictions, but our model can accommodate any alternative means of assessing the probability of detection. Representation of restrictions to navigation, such as shoreline, islands, and breakwaters, follow planner-specified fidelity; these obstructions may also obscure defender radars, so line-of-sight precalculation determines whether an attacker can be detected from any defender position.

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" [1]. Current maritime threats vary from the possible hijacking of a commercial vessel to the ramming of an explosive-packed small boat into a ship, as happened with the USS Cole in the port of Yemen in 2000 [2] (see Fig. 1).

Protecting high-value assets in a port can be difficult. Maritime ports are "sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks" [1]. 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 [4].

One recent example of a major maritime threat was the Sea Tigers, a maritime detachment of the Liberation Tigers

Correspondence to: M. Carlyle (mcarlyle@nps.edu)

This article is dedicated in memory of our late colleague Richard E. Rosenthal.

Figure 1. USS Cole after the 2000 attack in Port of Yemen that killed 17 sailors [3].

of Tamil Eelam (LTTE). The LTTE, a rebel organization in Sri Lanka, has fought for its independence since 1976. Its members demonstrate very sophisticated tactics in attacking Sri Lankan Naval and commercial ships. 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 Fig. 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 [3].

We anticipate a determined adversary who plans to infiltrate a maritime port for an attack. We seek a systematic way to assign defensive radar-equipped ships "pickets," and possibly shore-based radar, to detect and alarm such an attack, even though such defensive preparations will be visible to the attacker. Optimal placement of sensor platforms will minimize the probability of a successful attack. For our purposes, a first, single successful enemy infiltration is the signal event to prevent. Subsequent to such a first event, interdicted or not, port defenses would change qualitatively (e.g., with more restrictive access rules, more patrol boats, etc.).

The world economy is dependent on maritime commerce, which is involved in $\sim$ 80% of world trade [1]. Today there are 30 mega-ports worldwide, which almost all cargo ships pass through in the intricate global trade network [5]. A disruption, called a Transportation Security Incident in our vernacular, 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. Standard protocol for responding to such an incident is an immediate shutdown of all port operations, followed by a systematic investigation of damage and any remaining threat to ensure restoration of safety and security, and finally gradual restoration of operations with heavy security oversight. Any transportation security incident at a port will disrupt port operations, perhaps for a long time.

National Security Presidential Directive 41 [6] establishes policy and guidelines for all U.S. agencies and stakeholders in maritime security, and it also defines the now-core [7] Navy mission of Maritime Domain Awareness as the "effective understanding of anything associated with global maritime domain that could impact the security, safety, economy, or environment of the United States."

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 $\sim$40% of all cargo container traffic entering the U.S. [8]. The longshoremen strike of 2002 lasted for just ten days, but cost the U.S. economy an estimated $20 billion [9].

Agencies responsible for maritime security include the U.S. Customs and Border Protection [10], 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 during fiscal years 2006–2008 alone [11]. The burden of overall port security falls on the U.S. Coast Guard [12], which is procuring up to 700 SAFE Boats' "Defender" class patrol boats (referred to hereafter as SAFE patrol boats) to provide maritime security [13]. At the same time, the U.S. Navy has expanded some operational focus from deep ocean to littoral (i.e., coastal) waters as well. The Navy has reestablished its riverine forces and equipped them with SAFE-like Small Unit Riverine Craft. Both agencies are extending ties with international allies to enhance global maritime domain awareness [31].

Coast Guard Port Security Units 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 boats not on station act as a standby pair or

Figure 2. Archival image of a high-speed boat from a training video captured from the Liberation Tigers of Tamil Eelam.

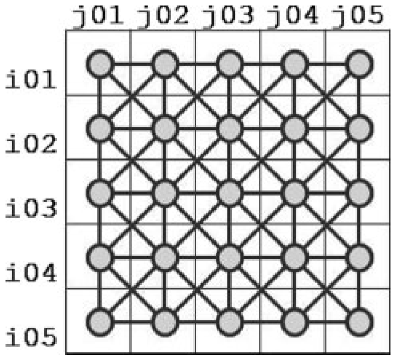


Figure 3. Sample network representation with square cells of constant width, each identified by a row and a column index. An attacker can traverse from any cell via an arc to any adjacent cell.

as a shuttle boat and a boat set aside for a 24-hour maintenance period. Patrol durations vary from 4 to 6 hours. The specific placement of boats is left to the judgment of the Tactical Action Officer, who reports to the Commanding Officer [14]. Employment and tactics depend heavily on the personal experience of these officers.

Defense of ports has improved substantively over the past 6 years. However, disposition of defenders is planned on a perceived-threat basis, and emphasis has been on thwarting an attack by assuming the potential attacker can observe the defensive patrol boats and may be dissuaded simply by their presence. These visible defensive positions can also be refined to gain maximal surveillance advantage.

1.1. Prior Literature

We apply bi-level mixed integer linear programming (MIP) to position our radar systems and then predict how an intelligent attacker would respond, given these defensive positions are visible. Bard and Moore [15] introduce a heuristic to solve a bi-level MIP. Wood [16] develops a defender-attacker maximum flow network interdiction model that maximally reduces the resulting network capacity using a limited number of defensive resources to eliminate arcs in a network, and which has applications to impeding drug trafficking networks. Israeli and Wood [17] describe an attacker-defender shortest-path network interdiction problem and formulate it using a bi-level MIP, introducing efficient decomposition techniques to solve such a problem. Brown et al. [18] develop attacker-defender, defender-attacker, and defender-attacker-defender (tri-level) optimization models for the defense of critical infrastructure. They apply these models to many real-world examples, such as the Strategic Petroleum Reserve, the U.S. Border Patrol at Yuma, AZ, and electrical transmission systems, in order to highlight vulnerabilities, and to advise the allocation of defensive resources.

1.2. Our Problem

We anticipate a determined, intelligent attacker will try to reach fixed high-value targets in a large port where U.S. Navy ships or other high-value ships are anchored or pier-side. We consider a single successful undetected attack as a failure for the defender. We assume transparency in our model in that the enemy can view our defensive prepositioning and react accordingly to avoid detection.

In our scenarios the attacker utilizes a number of small speedboats similar to a 20-foot Baja Outlaw Class, which can hold up to six people, and can travel at up to about 54 knots (nm/hr) [19]. The defender employs SAFE patrol boats, which have a crew of four, can carry up to 10 people, and travel at up to 46 kts. SAFE patrol boats can be equipped with a 12.7 mm machine gun with an effective range of 1500 meters [20]. The defender also has shore radar installations that help detect any attacker.

There are no strict paths or routes over water, so we represent our maritime environment using a mesh network. We break down the surface into square cells of a given width. Each cell is connected by an arc to and from every adjacent cell (horizontal, vertical, or diagonal) unless we specify an obstruction to navigation (see Figs. 3 and 4). The attacker can traverse any arc between adjacent cells 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.

Table 1 shows how we estimate the probability of evasion, $P_e(s,t)$, as defined in (P9), for an attacker transiting a given cell, t, and a defender searching from another given cell, s,

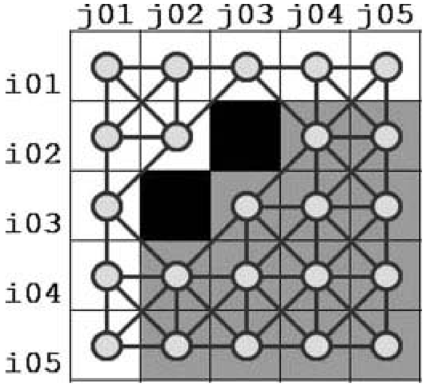


Figure 4. Sample network representation with cells and obstructions. Black cells represent obstructions to navigation. Cells (i02, j02) and (i03, j03) are not adjacent. Assuming these black cells not only block navigation but also contain obstacles whose height above the water is sufficient to obstruct observation, then a defender in the North-West cell (iOl, jOl), for instance, 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).

Table 1. Derivation of evasion probability by an attacker located at cell $t = (i_t, j_t)$ from a defender at $s = (i_s, j_s)$, assuming no intervening obstruction to observation. The coordinates in (PI) and (P2) are expressed in the same terms as those in Figures 3 and 4.

$s = (i_s, j_s)$	Defender cell	(P1)
$t = (i_t, j_t)$	Attacker cell	(P2)
cell_width	Cell side distance	(P3)
v	Defender velocity	(P4)
r_m	Maximum radar range	(P5)
sr	Searcher sweep rate	(P6)
$x = \text{cell\_width}^* \sqrt{(i_t - i_s)^2 + (j_t - j_s)^2}$		(P7)
$P_d(s,t) = 1 - \exp\left(-2sr\frac{r_m^2 - x^2}{v}\right)$		(P8)
$P_e(s,t) = \exp\left(-2sr\frac{r_m^2 - x^2}{v}\right)$		(P9)

assuming there is no intervening obstruction to observation. The defender pays a penalty for travelling faster in the form of a decreased detection probability. The function in (P8) models area search (see, e.g., Ref. 21, p.173).

We assume the intelligent attacker will want to maximize his probability of evasion by traversing a path, PATH, of contiguous cells $t \in$ PATH, that has the maximum joint probability of evading detection while transiting all of the cells in the path. This is a conservative estimate of his capabilities to observe our defensive positions and navigate to avoid them. Assuming that multiple defenders will detect an attacker independently of each other, the overall probability of the attacker evading detection in any cell t is the product of the evasion probabilities, $\prod_s P_e(s,t)$, where the product is taken over all cells s occupied by defenders. Assuming cell-to-cell independence, (specifically, that failure to detect an attacker early on does not influence the probability of detection later in the attacker's path), the overall joint probability that the attacker will evade detection on his path is then the product of the evasion probabilities of each cell traversed, $P_e = \prod_{t \in \text{PATH}} \prod_s P_e(s,t)$. We take the logarithm of this expression to render a summation of logs of probabilities, and note that maximizing the sum of these logs is equivalent to maximizing the product of the probabilities. In our models we will allow for defenders of varying capabilities (i.e., sweep widths, maximum range), and we will derive the appropriate log-probabilities as coefficients for linear objective functions. Our simple radar equation can be replaced by one with much higher fidelity, [e.g., [22]], but for purposes of our exposition this only changes exogenous data, and makes no difference to the structure or complexity of the mathematical optimization models.

For each pair of cells s and t in the operating region, we determine which cells are encountered along a straight line-of-sight between s and t. If any such intervening cell contains an obstacle that is high enough above the waterline (taking into account whether the object floats, the current tide height, and curvature of the earth) to obscure that line of sight, a ship in cell t cannot be observed by a ship in cell s.

2. MODEL FORMULATION

2.1. 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 speedboat traversals arc_cap. Traversing each arc carries a risk of detection the attacker cannot control, based on the (fixed) positions of searchers. We refer to the fixed searcher positions by the exogenous data vector $\hat{X}$, where $\hat{X}_s = 1$ if cell s is occupied by a searcher, and is zero otherwise. For an arc d that emanates from cell c_1 and terminates at cell c_2, we could calculate the log probability of evasion on that arc to be the same as the log probability of evasion in cell c_1. The overall path log probability of evasion would then be the sum of the cell log probabilities of evasion along the path, omitting the term for the final cell. We choose a slightly different approach, in which we calculate each arc log probability of evasion based on the probabilities of evasion in both the start cell *and* end cell of the arc. The log probability that an attacker will evade detection while traversing arc d is then:

$$\widehat{evX}_d \equiv 1/2 \log\left(\prod_{s:\hat{X}_s=1} P_e(s,c_1)\right) + 1/2 \log\left(\prod_{s:\hat{X}_s=1} P_e(s,c_2)\right), \quad \text{(P10)}$$

where we assume the attacker spends half of his time on arc d in each of those adjacent cells. This formula, when used to calculate the log probability of evasion for the entire path, assumes the attacker starts in the middle of his entry cell and ends his path at the center of his goal cell. Each intermediate cell on the path appears twice, once for the inbound arc, and once for the outbound arc, hence the 1/2 coefficients in (P10). The attacker seeks one attack path per speedboat that maximizes the sum of the log probabilities of evading detection along that path.

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

2.1.1. *Indexes and index sets [∼cardinality]*

$a \in A$	attacker [∼5]
$i \in I$	horizontal discrete cell coordinate [∼30]
$j \in J$	vertical cell coordinate [∼30]

$c \in C$ cells, each with horizontal coordinate i_c, and vertical coordinate j_c (alias $c1$, $c2$) [~1000]

$c \in E \subseteq C$ 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 (e.g., given cell c, $d \in D_{c,c2}$ includes every out-arc from cell c to an adjacent cell $c2$) [~8000]

2.1.2. *Data [units]*

arc_cap maximum attackers allowed to traverse any arc [attackers]

$\widehat{evX_d}$ log of probability that an attacker will evade detection traversing arc d [log likelihood]

2.1.3. *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]

2.1.4. *Formulation [dual variables]*

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

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

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

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

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

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

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

2.1.5. *Discussion*

The attacker's objective (A0) is to maximize the total joint probability that attacker boats evade detection over all the arcs they choose to traverse, through maximizing the sum of the logs of individual successful arc traversal probabilities. 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) limits the number of exits from the network via goal cells. Stipulations (A4–A6) bound the decision variables. (A5) limits the number of attackers transiting any cell, a limit that can be used to force attack path diversity. If the data in (A1), (A3), and (A5) are integral, this linear program is equivalent to a shortest path problem in a network, and will therefore produce an intrinsically integral solution Y^*, ENTER*, and GOAL*. For simplicity, we refer to such a solution in the following as simply Y^*.

2.2. 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 $s \in C_p$ to surveil arcs in the network. The log probability that an attacker traversing arc d will evade detection by defender boat p located in cell s is $ev_{d,p,s}$. The defender seeks positions for his surveillance platforms collectively to minimize the sum of the log probabilities of attackers evading his surveillance. We express the defender's problem **DMIN($\hat{\mathbf{Y}}$)** as follows:

2.2.1. *New indices and index sets [~cardinality]*

$p \in P$ defending platforms [~4]

$s \in C_p \subseteq C$ cells where a defending platform p can be located [~250]

2.2.2. *New data [units]*

$ev_{d,p,s}$ log probability that an attacker traversing arc $d = (c_1, c_2)$ would evade detection by defender p in position s [log probability]

$$ev_{d,p,s} \equiv 1/2 \log(P_e(s, c_1)) + 1/2 \log(P_e(s, c_2)) \hat{Y}_d$$

number of attackers traversing arc d [attackers]

2.2.3. *Variables [units]*

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

Z total log likelihood of evading detection [log probability]

2.2.4. *Formulation*

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

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

$$\sum_{s \in C_p} X_{p,s} \le 1 \qquad \forall p \in P \qquad \text{(D2)}$$

$$\sum_{p\in P|s\in C_p} X_{p,s} \leq 1 \quad \forall s \in C \qquad \text{(D3)}$$

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

2.2.5. *Discussion*

Together, (D0) and (D1) define an objective function that is the minimum upper bound on the sum of the log probabilities 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. We formulate (D0) and (D1) in this way to set up our decomposition algorithm, which follows.

2.3. 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, and it therefore yields a sequential decision problem in which the defender must place ships or other sensors before the attacker chooses his minimum-risk path.

This is a zero-sum Stackelberg game [23] (i.e., a sequential-play game with perfect information). Using notation already defined, an optimization formulation of this monolith follows.

$$\min_{X} Z = \left[\begin{array}{lllll}
\max\limits_{Y,\,\text{ENTER},\,\text{GOAL}} & \sum\limits_{\substack{d\in D,\\ p\in P, s\in C_{\mathrm{p}}}} ev_{\mathrm{d,p,s}}\hat{X}_{\mathrm{p,s}}Y_{\mathrm{d}} & & & \text{(AD0)}\\
\text{s.t.} & \sum\limits_{c\in E} ENTER_{\mathrm{c}} \leq \ +|A| & & [\alpha] & \text{(A1)}\\
& \sum\limits_{d\in D_{\mathrm{c},c2}} Y_d - \sum\limits_{d\in D_{c1,c}} Y_d & & & \\
& \quad -ENTER_c|_{c\in E} + GOAL_c|_{c\in G} \leq 0 & \forall c \in C & [\beta_c] & \text{(A2)}\\
& \quad -\sum\limits_{c\in G} GOAL_c \leq -|A| & & [\delta] & \text{(A3)}\\
& 0 \leq ENTER_c & \forall c \in E & & \text{(A4)}\\
& 0 \leq Y_{\mathrm{d}} \leq arc\_cap & \forall d \in A & [\gamma_d] & \text{(A5)}\\
& 0 \leq GOAL_c & \forall c \in G & & \text{(A6)}
\end{array}\right]_{\hat{X}=X}$$

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

$$\sum_{p\in P|s\in C_p} X_{p,s} \leq 1 \qquad \forall s \in C \qquad \text{(D3)}$$

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

The opponents share the objective (AD0), while the constraints (D2–D4) govern defender preparations, and (A2–A6) limit the attacker courses of action. The objective coefficient $ev_{\mathrm{d,p,s}}$ is the logarithm of the probability of evasion given cell d is traversed by an attacker when defender platform p is located in cell s. The square brackets emphasize the sequential nature of these decisions: first, the defender (the leader) decides where to place observers, next the attacker (follower), observing these placements, decides how to attack to minimize the probability of detection. The attacker problem inside the square brackets is a linear program when X is fixed, and the Greek notation defines dual variables for the constraints.

We state this sequential decision problem more compactly as model MINMAX:

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

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

We cannot solve MINMAX with conventional techniques, but if we temporarily fix variables Z and X, the result is a capacitated minimum cost network flow problem. Taking the dual of this linear program, and freeing Z and X, (See [16] for a proof of the correctness of this basic reformulation technique) we achieve an integer linear program **SAFE-ILP** we can solve with conventional techniques:

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

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

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

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

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

$$\sum_{p\in P | s\in C_p} X_{p,s} \leq 1 \qquad \forall s \in C \qquad \text{(T5)}$$

$$\alpha \geq 0$$

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

$$\gamma \geq 0$$

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

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

2.3.1. Discussion

This reformulation uses the variables introduced as duals for the constraints in $\mathbf{AMAX}(\widehat{\mathbf{evX}})$.

The optimal solution to the defender-attacker model **SAFE_ILP** positions seen defender platforms, recovering the corresponding attack plans by solving $\mathbf{AMAX}(\widehat{\mathbf{evX}})$ with variables X fixed at their optimal values $\hat{X}$, and $\widehat{evX}_{d,p,s} = ev_{d,p,s}\hat{X}_{p,s}$.

2.4. Decomposition

SAFE_ILP can be (very) hard to solve at large scale. Accordingly, we have decomposed the SAFE optimization as follows [24]. We modify $\mathbf{DMIN}(\hat{\mathbf{Y}})$, replacing equation (D1) with a set of constraints (D1D).

2.4.1. New index

$k \in K$ decomposition iteration

2.4.2. New Data

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

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

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

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

and constraints (D2)–(D4).

The complete decomposition algorithm is as follows:

2.5. 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 $Z_{\mathrm{UB}} \leftarrow \infty$, best lower bound $Z_{\mathrm{LB}} \leftarrow -\infty$, 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 $\widehat{evX}_{\mathrm{d,p,s}} = ev_{\mathrm{d,p,s}}\hat{X}^k_{\mathrm{p,s}}$, solve subproblem $\mathbf{AMAX}(\widehat{\mathbf{evX}})$ to determine the optimal attack plan $\hat{\mathbf{Y}}^K$ given $\hat{\mathbf{X}}^K$; the bound on the associated objective is $Z_{\max}(\hat{\mathbf{X}}^K)$;
3. If $K = 1$ and $\hat{\mathbf{Y}}^K$ is not an admissible solution, Goto step (6) (**Master Problem)**
4. If $(Z_{\mathrm{UB}} > Z_{\max}(\hat{\mathbf{X}}^K))$ set $Z_{\mathrm{UB}} \leftarrow Z_{\max}(\hat{\mathbf{X}}^K)$ and record improved incumbent SAFE plan $\mathbf{X}^* \leftarrow \hat{\mathbf{X}}^K$, and responding attacker plan $\mathbf{Y}^* \leftarrow \hat{\mathbf{Y}}^K$;
5. If $(Z_{\mathrm{UB}} - Z_{\mathrm{LB}} \leq \varepsilon)$ go to **End**;
6. **Master Problem:** Given attack plans $\hat{\mathbf{Y}}^k$, $k = 1,\ldots K$, attempt to solve master problem $\mathbf{DMIN}(\hat{\mathbf{Y}})$ to determine an optimal defender plan $\hat{\mathbf{X}}^{K+1}$. The bound on the objective is $Z_{\min}(\hat{\mathbf{Y}})$;
7. If $Z_{\mathrm{LB}} < Z_{\min}(\hat{\mathbf{Y}})$ set $Z_{\mathrm{LB}} \leftarrow Z_{\min}(\hat{\mathbf{Y}})$;
8. If $(Z_{\mathrm{UB}} - Z_{\mathrm{LB}} \leq \varepsilon)$ go to **End**;
9. Set $K \leftarrow K + 1$ and go to step (2) (**Subproblem**);
10. **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 4. These can be recovered after-the-fact by computing $\widehat{\mathbf{evX}}_{d,p,s} = ev_{d,p,s}X^*_{p,s}$ and solving $\mathbf{AMAX}(\widehat{\mathbf{evX}})$.

The advantage here is that the decomposition isolates a large sub-problem that is a minimum cost network flow problem 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., [25]), and the latter can be solved with a local search heuristic. This offers the opportunity to write a customized solver in any available programming

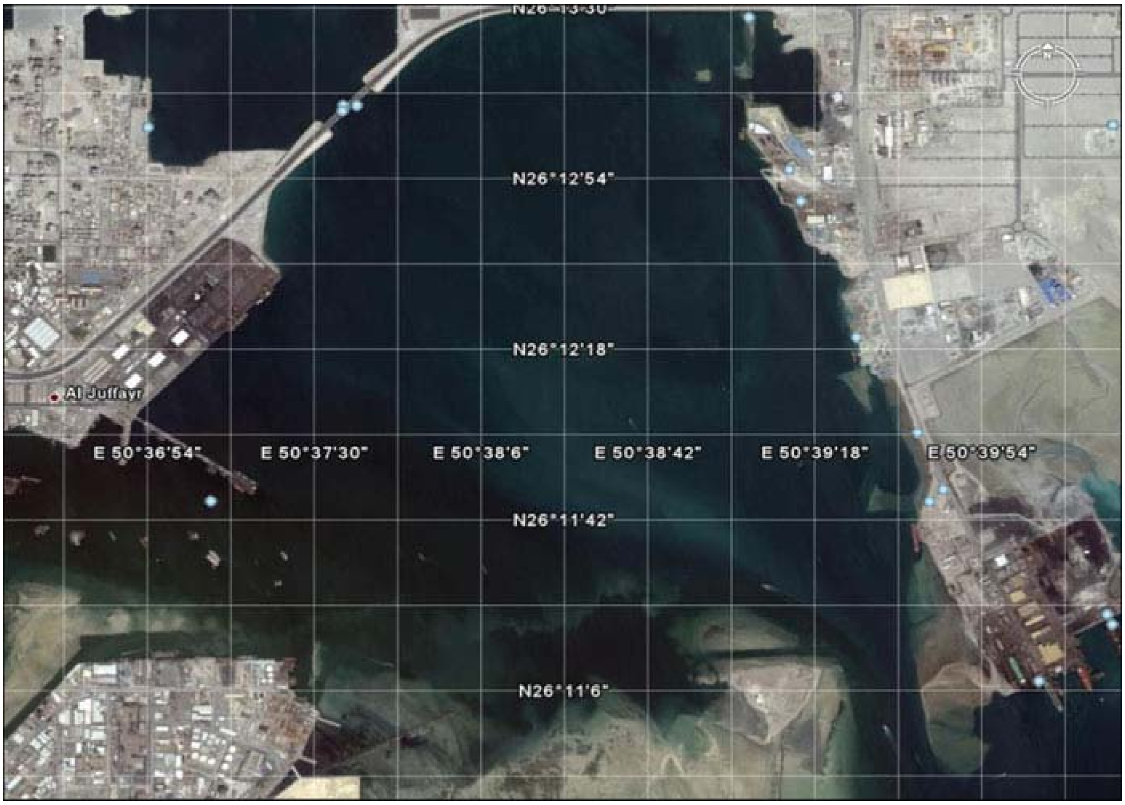


Figure 5. Aerial image of Mina Salman - Bahrain US 5th Fleet Headquarters [27] which oversees defense of the freedom of sea commerce in the Persian Gulf. The horizontal latitude parallels are separated by 18 arc seconds, or about 0.3 NM (556 meters).

language without need for procuring a licensed mathematical modeling language or commercial optimization solver.

3. SAMPLE PLANNING PROBLEMS

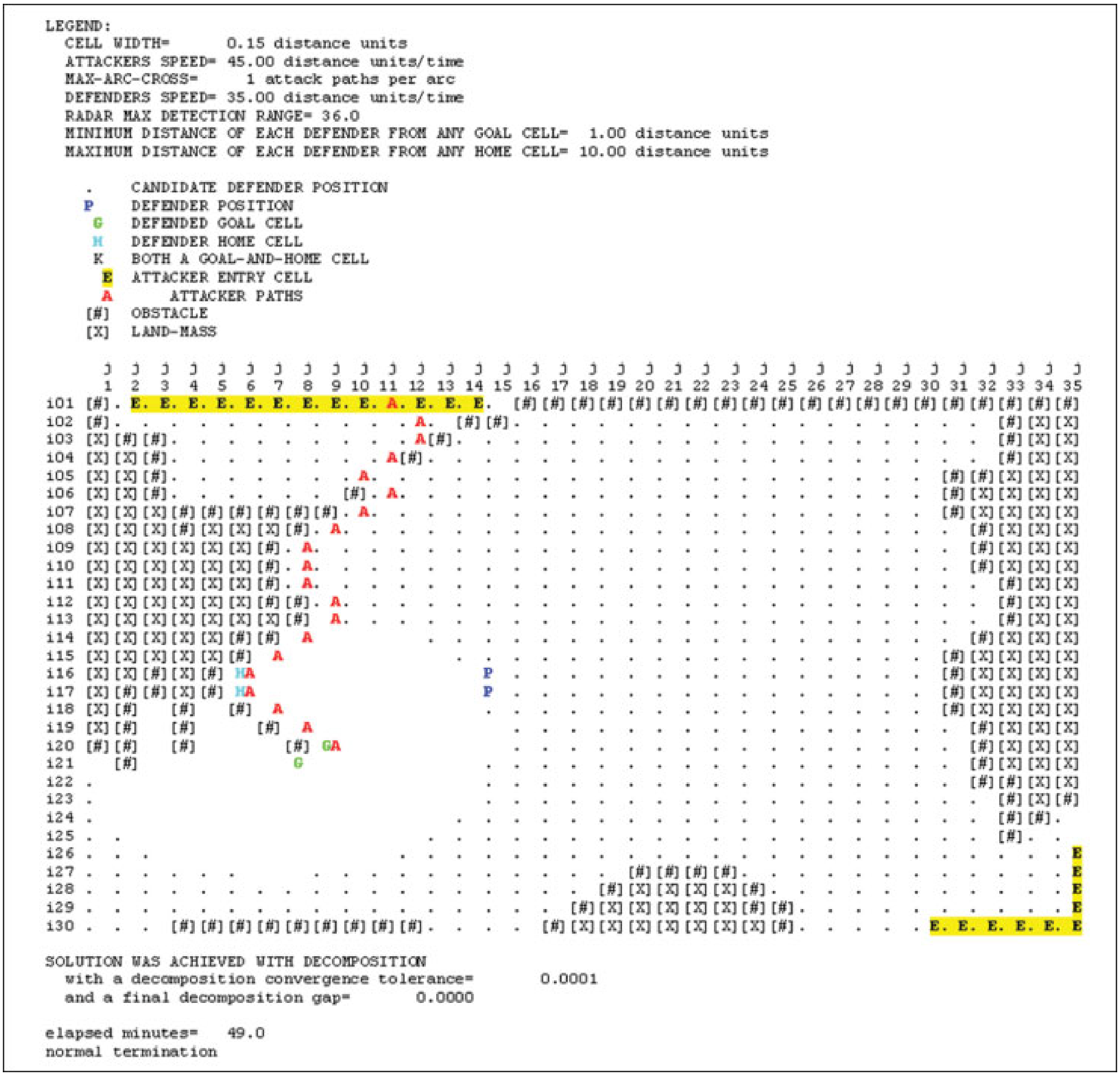
We illustrate with the U.S. Fifth Fleet Headquarters, Bahrain, a generic test problem for experimentation, and the Port of Hong Kong.

We are dealing with small, fast attack boats, and we want a high-resolution network to represent their maneuvers. We use a cell width of 0.15 nautical miles (NM) (about 278 meters). The surveillance problems we state fit within a 30 vertical by 35 horizontal cell array, or maritime domains about 4.5 NM by 5.3 NM, for a total surveillance area of about 24 NM^2. The SAFE defenders cruise at 35 knots, the radar sweep rate is 0.8 revolutions per minute with a maximum range of 36 NM, and the SAFE boats cannot locate closer than one nautical mile away from any defended asset, and do not customarily venture more than 10 NM from their home base.

We include obstruction masking of defender radars, with line-of-sight calculations to determine exactly which cells can be seen by a defender boat in any particular defensive position. To develop experiments completely reproducible from this paper alone, we have endowed every obstruction here with sufficient elevation to obscure any incident ray. In reality, there may be many low obstructions that limit observability only for certain tide heights. The obstruction masking elicits real-world terrorist behavior to hide and evade detection. Our custom FORTRAN ray tracing routine to perform these line-of-sight calculations is only invoked when some change to obstructions is sensed, and takes a couple of minutes to revise tables of cell-to-cell observability using formula (H1) or (H2), as appropriate.

For each planning problem, we have evaluated all combination of from one to four attacker boats versus either two or four defender boats.

In our experience, the GAMS modeling language and CPLEX 11 solver [26] generate and solve a problem instance via decomposition in about a minute. Some instances of **SAFE-ILP** cannot be solved as a single monolithic model, but the decomposition converges to a zero optimality tolerance (i.e., solves the problem optimally) in somewhere between 5 and 15 iterations. Even for cases where the ILP monolith is directly solvable, the decomposition is much faster to generate and solve.



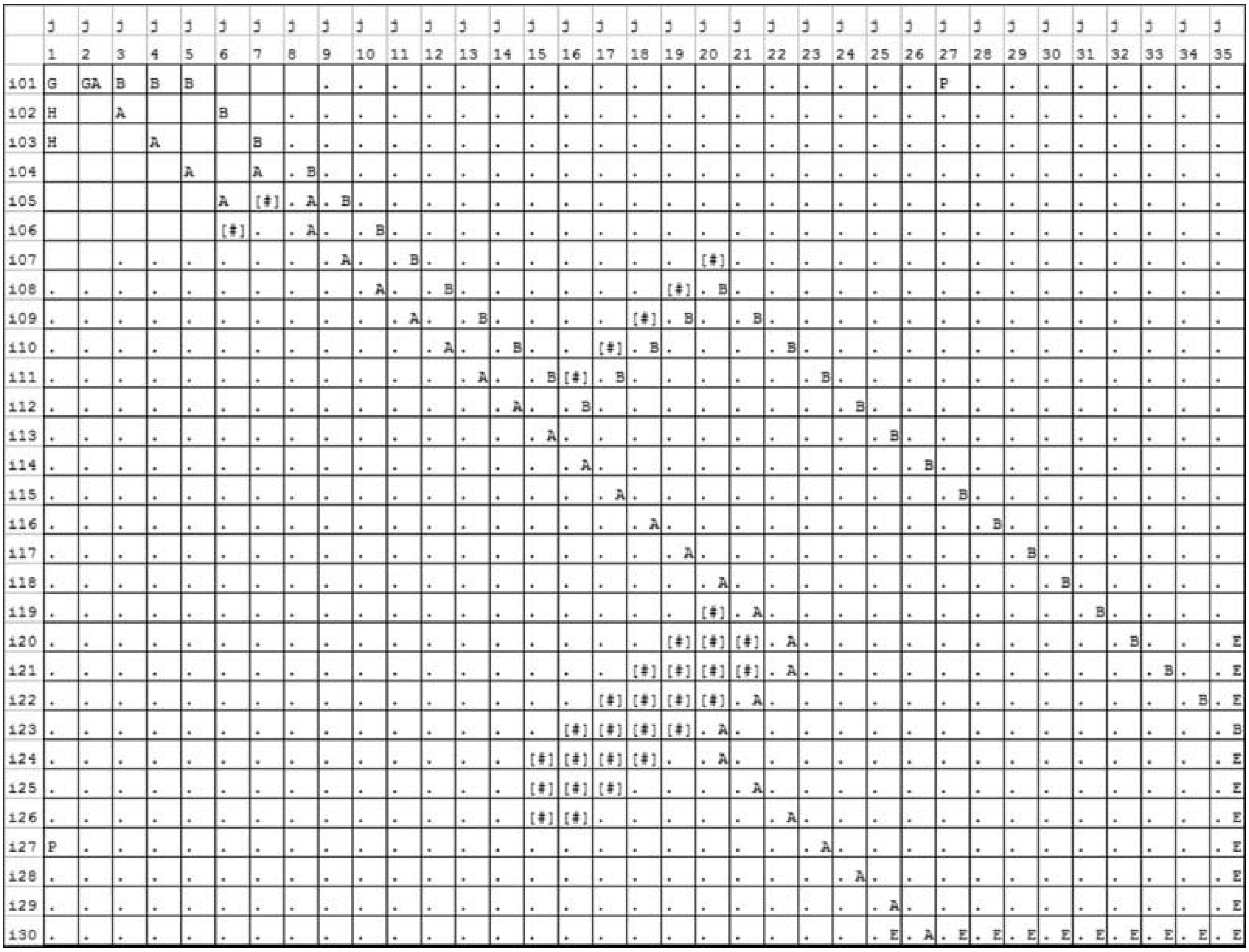
```
LEGEND:
  CELL WIDTH=      0.15 distance units
  ATTACKERS SPEED= 45.00 distance units/time
  MAX-ARC-CROSS=     1 attack paths per arc
  DEFENDERS SPEED= 35.00 distance units/time
  RADAR MAX DETECTION RANGE= 36.0
  MINIMUM DISTANCE OF EACH DEFENDER FROM ANY GOAL CELL=  1.00 distance units
  MAXIMUM DISTANCE OF EACH DEFENDER FROM ANY HOME CELL= 10.00 distance units

      .  CANDIDATE DEFENDER POSITION
      P  DEFENDER POSITION
      G  DEFENDED GOAL CELL
      H  DEFENDER HOME CELL
      K  BOTH A GOAL-AND-HOME CELL
      E  ATTACKER ENTRY CELL
      A      ATTACKER PATHS
    [#]  OBSTACLE
    [X]  LAND-MASS

      J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J  J
      1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
i01 [#]. E. E. E. E. E. E. E. E. E. A. E. E. E.  [#][#][#][#][#][#][#][#][#][#][#][#][#][#][#][#][#][#][#][#]
i02 [#].  .  .  .  .  .  .  .  .  .  . A.  [#][#].  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i03 [X][#][#].  .  .  .  .  .  .  .  . A[#].  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i04 [X][X][#].  .  .  .  .  .  .  . A[#].  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i05 [X][X][#].  .  .  .  .  .  . A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][#][X][X][X]
i06 [X][X][#].  .  .  .  .  .  [#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i07 [X][X][X][#][#][#][#][#][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i08 [X][X][X][#][X][X][X][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i09 [X][X][X][X][X][X][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i10 [X][X][X][X][X][X][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i11 [X][X][X][X][X][X][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i12 [X][X][X][X][X][X][#][#]. A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i13 [X][X][X][X][X][X][X][#]  A.  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X]
i14 [X][X][X][X][X][#][#]  A            .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i15 [X][X][X][X][X][#]  A                  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i16 [X][X][#][X][#] HA                        P  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i17 [X][#][#][X][#] HA                        P  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i18 [X][#]   [#]   [#]  A                     .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X]
i19 [X][#]   [#]      [#]  A                     .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i20 [#][#]   [#]         [#] GA                  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i21    [#]                G                   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X]
i22 .                                         .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][#][X][X]
i23 .                                         .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][#]
i24 .                                      .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][#].
i25 .  .                                .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#].  .
i26 .  .  .                          .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  . E
i27 .  .  .  .  .  .        .  .  .  .  .  .  .  .  .  .  .  [#][#][#][#].  .  .  .  .  .  .  .  .  .  . E
i28 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X][#].  .  .  .  .  .  .  .  .  . E
i29 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  [#][X][X][X][X][X][#][#].  .  .  .  .  .  .  .  . E
i30 .  .  .  [#][#][#][#][#][#][#][#][#].  .  .  .  [#][X][X][X][X][X][X][X][#].  .  .  .  . E. E. E. E. E. E

SOLUTION WAS ACHIEVED WITH DECOMPOSITION
  with a decomposition convergence tolerance=       0.0001
  and a final decomposition gap=       0.0000

elapsed minutes=   49.0
normal termination
```

Figure 6. 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 (il6,j06) and (il7,j06). 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 within one nautical mile of any goal cell, 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). These positions offer advantaged unobstructed surveillance of both north-west and south-east threat axes, as well as the defended goal cells. The lone attacker enters at (i01,j11) and, while knowing defender positions, hugs the shoreline to maximize probability of evasion to attack goal cell (i20,j09). The attacker probability of evasion is near zero.

4. U.S. NAVCENT FIFTH FLEET – BAHRAIN

Bahrain's port Mina Salman is strategically positioned in the Persian Gulf, and hosts US Fifth Fleet Headquarters, but its approaches are very constrained for deep-draft vessels, with only one main channel for commercial shipping entering from the southeast. See Fig. 5 for satellite imagery of the port. However, there are two other approaches that small boats can use to enter the port area.

We took this image of Mina Salman and manually discretized it into square regions by graphically overlaying a grid, and then using our own judgment as to whether each cell in this grid was navigable, or was an obstruction. We then chose goal cells as locations for a hypothetical target,



	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
i01	G	GA	B	B	B				.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	P	.	.	.	.	.	.	.	.
i02	H		A			B		.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i03	H			A			B	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i04					A		A	. B	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i05						A	[#]	. A	. B	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i06						[#]	.	. A	.	. B	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i07			.	.	.	.	.	.	. A	.	. B	.	.	.	.	.	.	.	.	[#]	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i08	.	.	.	.	.	.	.	.	.	. A	.	. B	.	.	.	.	.	.	[#]	. B	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i09	.	.	.	.	.	.	.	.	.	.	. A	.	. B	.	.	.	.	[#]	. B	.	. B	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i10	.	.	.	.	.	.	.	.	.	.	.	. A	.	. B	.	.	[#]	. B	.	.	.	. B	.	.	.	.	.	.	.	.	.	.	.	.	.
i11	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	. B	[#]	. B	.	.	.	.	.	. B	.	.	.	.	.	.	.	.	.	.	.	.
i12	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	. B	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	.	.	.	.
i13	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	.	.	.
i14	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	.	.
i15	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	.
i16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.
i17	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.
i18	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.
i19	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	. A	.	.	.	.	.	.	.	.	.	. B	.	.	.	.
i20	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	. A	.	.	.	.	.	.	.	.	.	. B	.	.	. E
i21	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	[#]	. A	.	.	.	.	.	.	.	.	.	.	. B	.	. E
i22	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	[#]	. A	.	.	.	.	.	.	.	.	.	.	.	.	. B	. E
i23	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	[#]	. A	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B
i24	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	[#]	.	. A	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. E
i25	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	[#]	.	.	.	. A	.	.	.	.	.	.	.	.	.	.	.	.	.	. E
i26	.	.	.	.	.	.	.	.	.	.	.	.	.	.	[#]	[#]	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	.	.	.	. E
i27	P	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	.	.	. E
i28	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	.	. E
i29	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. A	.	.	.	.	.	.	.	.	.	. E
i30	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. E	. A	. E	. E	. E	. E	. E	. E	. E	. E	. E

Figure 7. Generic instance with two SAFE Defender boats and two attackers that can enter from any cell "E" from the southeast. The defended assets are located at northwest goal cells "G" (i01,j01) and (i02,j02), and defender boats must locate at least one nautical mile from these in candidate positions labeled ".". Defender boats, denoted by "P," must also be located within 10 NM of their home cells, marked "H," but this restriction is vacuous in this scenario. The defenders position at (i27,j01) and (i01,j26), and the two attackers "A" and "B," knowing where we are pre-positioned, spread out to use obstructions "[#]" to evade detection. Note how the defender positions maximize the coverage of attacker transit cells, and minimize obscuration by obstructions.

and specified entry cells on the left side of the top boundary and along the edges of the bottom-right corner. We used equations (P1)–(P9) to determine probabilities of evasion concerning each pair of navigable locations on this map, and then formulated and solved the max–min formulation using Benders decomposition, implemented in GAMS, using CPLEX as the solver. In Fig. 6 we provide some of the output generated by our solver for this specific instance, including an ASCII map of the scenario displaying all relevant features, including the optimal placement of the defender boats and the resulting attacker's optimal path. We have added color to this display to clarify some of the output. At the bottom of this display, we can see that our decomposition algorithm converged to a provable optimal solution, with no gap between the upper and lower bounds.

5. GENERIC SURVEILLANCE PLANNING PROBLEM

In order to appreciate the size of the optimization problems we are solving, we provide a generic instance in which we posit a geographically simple maritime port (see Fig. 7) with three islands (obstacles) between the attacker entry cells (along the bottom-right corner) and the goal target cells (in the top-left corner). For two attackers and two defenders, SAFE-ILP has 8640 constraints, 10,611 variables (1952 binary) and 14,943,881 nonzero coefficients. CPLEX 11 cannot solve this; the enumeration tree runs out of space even with 2GB of random access memory available. Using Benders decomposition, each sub-problem has 1021 constraints, 7662 variables, and 22,961 coefficients, while the last (14th) restricted master

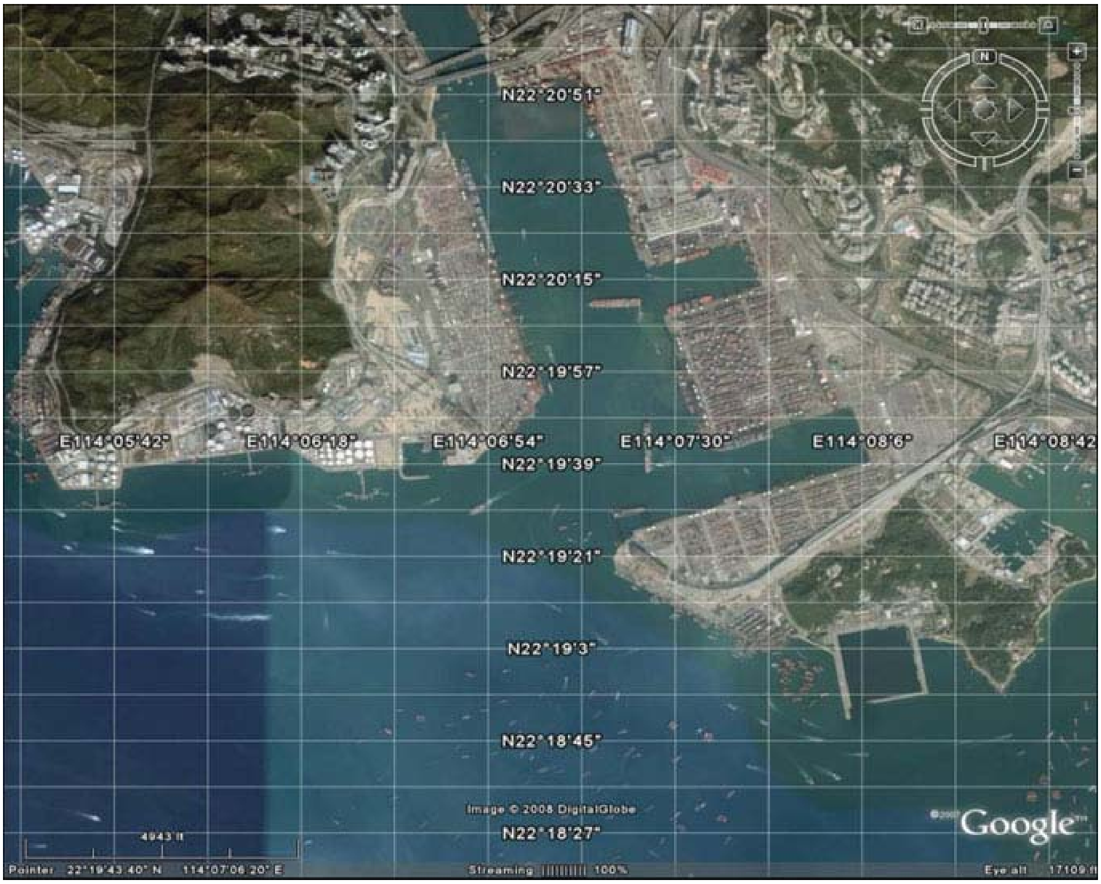


Figure 8. Satellite image of the port of Hong Kong [27]; Hong Kong is one of the three largest ports in the world, handling in 2008 about 22 million 20-foot Equivalent Units (TEUs) of container cargo worth ~\$24 thousand each, or about a half trillion dollars [29, 30]. The horizontal lines are latitude parallels, separated by eight arc seconds, which is ~0.133 NM, or just under 250 meters.

problem has 992 constraints, 1953 variables (1952 binary), and 31,246 coefficients. We satisfy an optimality tolerance of zero and achieve essentially a 100% probability of detection over any inbound attacker path in about a minute.

6. PORT OF HONG KONG

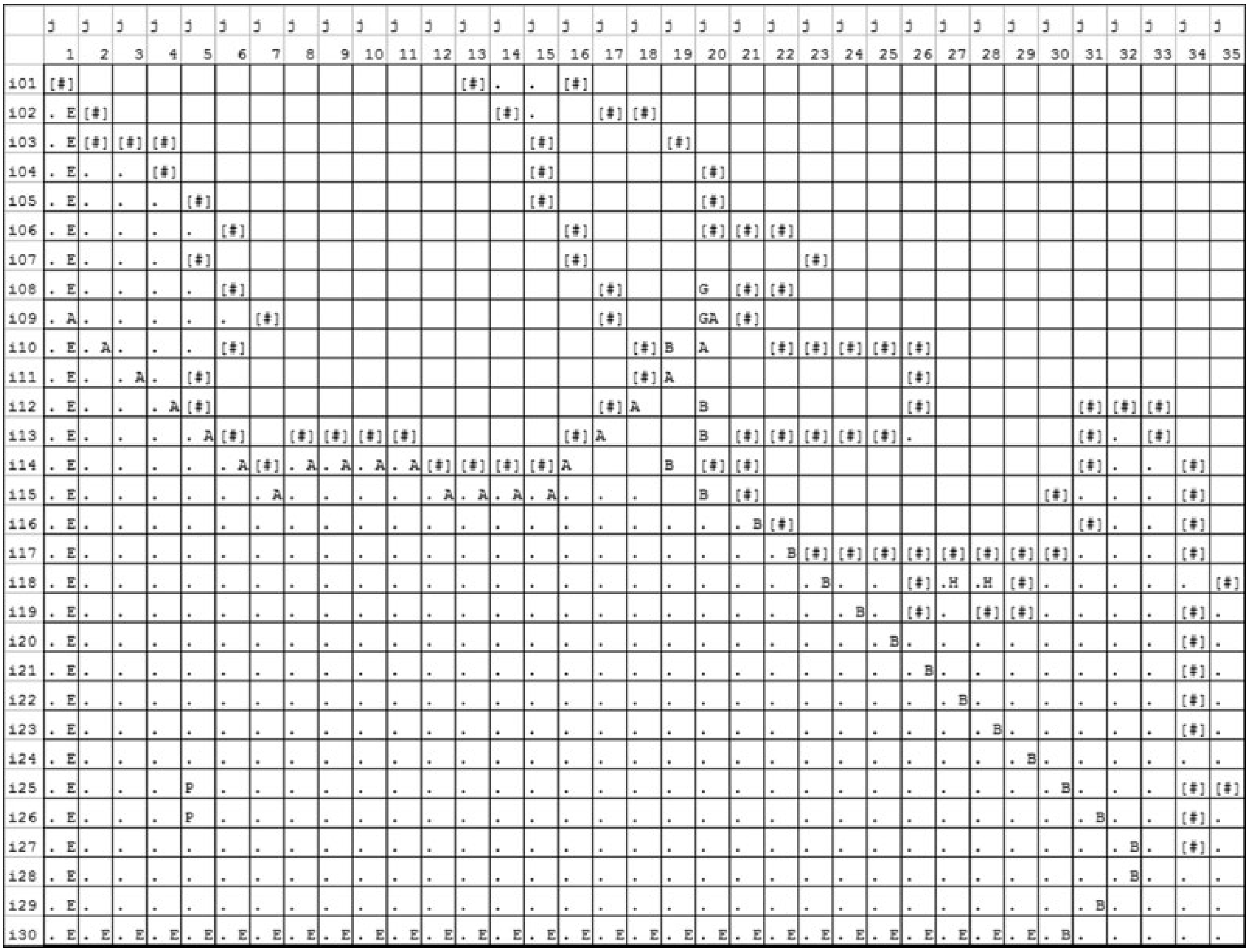
The port of Hong Kong is one of the busiest in the world. We anticipate attacker entries from anywhere west-to-south. See Fig. 8. In the decomposition, each sub-problem has 952 constraints, 6651 variables, and 19,984 coefficients, while the last (fifth) restricted master problem has 834 constraints, 1657 variables (1656 binary), and 9940 coefficients. See Fig. 9. In the optimal solution, the two defenders are positioned in adjacent cells, each of which has visibility of almost every cell along any reasonable path approaching the goal. Other potential defender cells are either not able to "see" the approach from the west, [roughly, cells (i01,j01) to (i12,j03)], or lose visibility of the goal cells themselves.

7. CONCLUSION

We introduce a bi-level defender-attacker integer linear program to advise optimal prepositioning of defender surveillance pickets in a maritime domain to minimize the maximum probability that intelligent attackers, observing our surveillance positions, can evade us with multiple attacking boats and reach any one of a set of a high-value targets.

In every instance we examine, alert defenders with existing radar can detect attacker raids with near 100% probability using optimal prepositioning. 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.

These models advise optimal defender positions (i.e, "cells"), but do not dictate that each defender must maintain a fixed position at all times. The prescriptions are for maximally-advantaged positions, and the models can be used



	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j	j
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
i01	[#]												[#]	.	.	[#]																			
i02	. E	[#]												[#]	.		[#]	[#]																	
i03	. E	[#]	[#]	[#]											[#]				[#]																
i04	. E	.	.	[#]											[#]					[#]															
i05	. E	.	.	.	[#]										[#]					[#]															
i06	. E	.	.	.	.	[#]										[#]				[#]	[#]	[#]													
i07	. E	.	.	.	[#]											[#]							[#]												
i08	. E	.	.	.	.	[#]											[#]			G	[#]	[#]													
i09	. A	.	.	.	.	.	[#]										[#]			GA	[#]														
i10	. E	. A	.	.	.	[#]												[#]	B	A		[#]	[#]	[#]	[#]	[#]									
i11	. E	.	. A	.	[#]													[#]	A							[#]									
i12	. E	.	.	. A	[#]												[#]	A		B						[#]					[#]	[#]	[#]		
i13	. E	.	.	.	. A	[#]		[#]	[#]	[#]	[#]					[#]	A			B	[#]	[#]	[#]	[#]	[#]	.					[#]	.	[#]		
i14	. E	.	.	.	.	. A	[#]	. A	. A	. A	. A	[#]	[#]	[#]	[#]	A			B	[#]	[#]										[#]	.	.	[#]	
i15	. E	.	.	.	.	.	. A	.	.	.	.	. A	. A	. A	. A	.	.	.		B	[#]									[#]	.	.	.	[#]	
i16	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	[#]									[#]	.	.	[#]	
i17	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	[#]	[#]	[#]	[#]	[#]	[#]	[#]	[#]	.	.	.	[#]	
i18	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	[#]	.H	.H	[#]	.	.	.	.	.	[#]
i19	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	[#]	.	[#]	[#]	.	.	.	.	[#]	.
i20	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	.	[#]	.
i21	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	.	[#]	.
i22	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.	[#]	.
i23	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	[#]	.
i24	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.	.	.
i25	. E	.	.	.	P	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	[#]	[#]
i26	. E	.	.	.	P	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	[#]	.
i27	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	[#]	.
i28	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.
i29	. E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. B	.	.	.	.
i30	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. E	. B	.	.	.	.	.

Figure 9. Port of Hong Kong instance with two SAFE Defender boats and two attackers. Attackers can enter from any cell "E" west or south. Defended asset goal cells "G" are (i08,j20) and (i09,j20). Optimal positions for defenders "P" are cells (i25,j05) and (i26,j05). One optimal attacker "A" enters from the northwest, and the other "B" from the southeast. It turns out these two cells offer superior surveillance of the entire port, including restricted passages.

to evaluate the returns from alternative positions. And, for instance, obstacle heights and tides (complicating details accommodated here, but not used in our simplified numerical examples) make a difference.

Abduhl-Ghaffar [28] includes more instances for these cases, as well as for the Port of Los Angeles and the Al Basra Oil Terminal (ABOT) in Iraq. He considers cases with one to four attackers and either two or four defenders and also considers coordination of more powerful shore-based radars in tandem with the SAFE boats afloat.

In the real world, exceptional conditions such as stormy sea state may complicate our planning, and (fortunately) that of our adversary. Suffice it 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. For example, if we multiply each $ev_{d,p,s}$ by $(1 + dg_s\theta)$, where dg_s is the distance, in nm, from cell s to the nearest goal cell, and $\theta \geq 0$ is a single scalar controlling our defensive posture, then setting $\theta = 1$ in our test scenario moves the defenders forward, to cells (i30, j08) and (i01, j26), respectively.

The interested reader can reproduce each of our experiments from the data shown in this paper.

REFERENCES

[1] Department of Homeland Security (DHS), The national strategy for maritime security, Accessed 4 December 2007, Available at http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf, 2005.

[2] J. Carafano, Small boats, big worries: Thwarting terrorist attacks from the sea, Backgrounder, Accessed 5 December 2007, Available at http://www.heritage.org/Research/HomelandDefense/upload/bg_2041.pdf, 2007.

[3] M. Murphy, Maritime threat: Tactics and technology of the sea tigers, Jane's Intelligence Review, Accessed 19 February 2008, Available at 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&, 2006.

[4] MI5 Security Service Al Qaida, Accessed 4 December 2007, Available at http://www.mi5.gov.uk/print/Page33.html, 2007.

[5] S. Caldwell, 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, Accessed 7 December 2007, Available at https://www.hsdl.org/homesec/docs/gao/nps33-103007-04.pdf&code=817fa80b0a833c93a10515ee3560896d, 2007.

[6] Maritime security policy, The White House, Washington, DC, 2004.

[7] "Maritime domain awareness concept," Chief of Naval Operations, Washington, D.C., 2007.

[8] Caltrade Report, Strike looms at ports of Los Angeles, long beach, Accessed 5 December 2007, Available at http://www.caltradereport.com/eWebPages/front-page-1184673116.html, 2007.

[9] C. Isidore, Hope in west coast port talks, CNN, Accessed 5 December 2007, Available at http://money.cnn.com/2002/10/02/news/economy/ports/index.htm, 2002.

[10] United States Customs and Border Protection (CBP), Accessed 29 July 2008, Available at http://www.cbp.gov/xp/cgov/border_security/air_marine/marine/marine_asset/safe_boat.xml, 2008.

[11] Department of Homeland Security (DHS), Budget-in-brief: Fiscal year 2008, Accessed 16 December 2007, Available at http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf, 2007.

[12] United States Coast Guard (USCG), Fact file — Maritime safety and security teams, Accessed 8 December 2007, Available at http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/MSST.htm, 2005.

[13] Jane's Information Group, SAFE Boats International, Accessed 20 January 2008, Available at 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&, 2005.

[14] United States Coast Guard (USCG), Port security units organization manual, Accessed 20 March 2008, Available at https://www.hsdl.org/homesec/docs/dod/nps37-121707-07.pdf&code=817fa80b0a833c93a10515ee3560896d, 2004.

[15] J. Bard and J. Moore, The Mixed Integer Linear Bi-level Programming Problem, Oper Res 38 (1990), 911–921.

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

[17] I. Israeli and K. Wood, Shortest path network interdiction, Networks 40 (2002), 97–111.

[18] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, Defending critical infrastructure, Interfaces 36 (2006), 530–544.

[19] Baja Marine, Baja 20 Outlaw Specifications, Accessed 22 February 2008, Available at http://www.bajamarine.com/index.asp?display=brochure&tab=0&modelid=104525, 2008.

[20] SAFE, Defender class operator's handbook, Accessed 20 March 2008, Available at http://www.defenderclass.com/pages/nigerian%20navy/training/DefenderClassOPS_small.pdf, 2003.

[21] D.H. Wagner, W.C. Mylander, and T.J. Sanders, Naval operations analysis, 3rd Ed., Naval Institute Press, Annapolis, MD, 1999.

[22] M. Skolnik, RADAR handbook, 2nd ed., McGraw-Hill, New York, 1990.

[23] H. von Stackelberg, The theory of the market economy, William Hodge, London, UK, 1952.

[24] J. Benders, Partitioning procedures for solving mixed variables programming problems, Numerische Mathematik 4 (1962), 238–252.

[25] G. Bradley, G. Brown, and G. Graves, Design and implementation of large-scale primal trans-shipment algorithms, Manage Sci 24 (1977), 1–34.

[26] General Algebraic Modeling System (GAMS), CPLEX solver guide, Accessed 2 June 2008, Available at http://www.gams.com/solvers/cplex.pdf, 2008.

[27] Google Earth, Accessed 10 June 2008, Available at http://earth.google.com/, 2008.

[28] A.M. Abdul-Ghaffar, Optimal employment of port radar and picket ships to detect attacker speedboats — A defender-attacker optimization model to enhance maritime domain awareness, M.S. thesis—, Naval Postgraduate School, Monterey, 2008.

[29] American Association of Port Authorities, World Port Rankings, Accessed 5 April 2009, Available at http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=900, 2007.

[30] J.J. Wang, D. Oliver, T. Notteboom, and B. Slack, Ports, cities, and global supply chains, Ashgate Publishing, Surrey, United Kingdom, 2007.

[31] Department of the Navy (DON), Navy maritime domain awareness concept, Accessed 30 April 2008, Available at http://www.dhs.gov/xnews/releases/press_release_0046.shtm, 2007.