PROTECT —
A Deployed Game-Theoretic System for Strategic Security Allocation for the United States Coast Guard

Bo An, Eric Shieh, Rong Yang, Milind Tambe,
Craig Baldwin, Joseph DiRenzo, Ben Maule, Garrett Meyer

■ *While three deployed applications of game theory for security have recently been reported, we as a community of agents and AI researchers remain in the early stages of these deployments; there is a continuing need to understand the core principles for innovative security applications of game theory. Toward that end, this article presents PROTECT, a game-theoretic system deployed by the United States Coast Guard (USCG) in the Port of Boston for scheduling its patrols. USCG has termed the deployment of PROTECT in Boston a success; PROTECT is currently being tested in the Port of New York, with the potential for nationwide deployment.*

PROTECT is premised on an attacker-defender Stackelberg game model and offers five key innovations. First, this system is a departure from the assumption of perfect adversary rationality noted in previous work, relying instead on a quantal response (QR) model of the adversary's behavior — to the best of our knowledge, this is the first real-world deployment of the QR model. Second, to improve PROTECT's efficiency, we generate a compact representation of the defender's strategy space, exploiting equivalence and dominance. Third, we show how to practically model a real maritime patrolling problem as a Stackelberg game. Fourth, our experimental results illustrate that PROTECT's QR model more robustly handles real-world uncertainties than a perfect rationality model. Finally, in evaluating PROTECT, this article for the first time provides real-world data: comparison of human-generated versus PROTECT security schedules, and results from an Adversarial Perspective Team's (human mock attackers) analysis.

The last several years have witnessed the successful application of game theory in allocating limited resources to protect critical infrastructures. The real-world deployed systems include ARMOR, used by the Los Angeles International Airport (Jain et al. 2010) to randomize checkpoints of roadways and canine patrols; IRIS, which helps the U.S. Federal Air Marshal Service (Jain et al. 2010) in scheduling air marshals on international flights; and GUARDS (Pita et al. 2011), which is under evaluation by the U.S. Transportation Security Administration to allocate the resources available for airport protection. Yet we as a community of agents and AI researchers remain in the early stages of these deployments, and must continue to develop core principles of applying game theory for security.

To this end, this article presents a new game-theoretic security application to aid the United States Coast Guard (USCG), called port tesilience operational/tactical enforcement to combat terrorism (PROTECT). The USCG's mission includes maritime security of the U.S. coasts, ports, and inland waterways; a security domain that faces increased risks in the context of threats such as terrorism and drug trafficking. Given a particular port and the variety of critical infrastructure that an adversary may attack within the port, USCG conducts patrols to protect this infrastructure; however, while the adversary has the opportunity to observe patrol patterns, limited security resources imply that USCG patrols cannot be at every location 24 hours a day, 7 days a week. To assist the USCG in allocating

Figure 1. USCG Boats Patrolling the Ports of Boston and New York.

its patrolling resources, similar to previous applications (Jain et al. 2010, Pita et al. 2011), PROTECT uses an attacker-defender Stackelberg game framework, with USCG as the defender against terrorist adversaries that conduct surveillance before potentially launching an attack. PROTECT's solution is to provide a mixed strategy, that is, randomized patrol patterns taking into account the importance of different targets, and the adversary's surveillance and anticipated reaction to USCG patrols.

While PROTECT builds on previous work, this article highlights five key innovations. The first and most important is PROTECT's departure from the assumption of perfect rationality (which was embedded in previous applications) on the part of the human adversaries. The assumption of perfect rationality is well recognized as a limitation of classical game theory, and a number of approaches have been proposed to model bounded rationality in behavioral game-theoretic approaches (Camerer 2003). Within this behavioral framework, quantal response equilibrium has emerged as a promising approach to model human bounded rationality (Camerer 2003; McKelvey and Palfrey 1995; Wright and Leyton-Brown 2010) including recent

results illustrating the benefits of the quantal response (QR) model in security games contexts (Yang et al. 2011). Therefore, PROTECT uses a novel algorithm called PASAQ (Yang, Tambe, and Ordóñez 2012) based on the QR model of a human adversary. To the best of our knowledge, this is the first time that the QR model has been used in a real-world security application.

Second, PROTECT improves PASAQ's efficiency through a compact representation of defender strategies exploiting dominance and equivalence analysis. Experimental results show the significant benefits of this compact representation. Third, PROTECT addresses practical concerns (such as grouping patrol points into areas) of modeling real-world maritime patrolling application in a Stackelberg framework. Fourth, this article presents a detailed simulation analysis of PROTECT's robustness to uncertainty that may arise in the real world. For various cases of added uncertainty, the article shows that PROTECT's quantal-response-based approach leads to significantly improved robustness when compared to an approach that assumes full attacker rationality.

PROTECT has been in use at the Port of Boston

since April 2011 and been evaluated by the USCG. This evaluation brings forth our final key contribution: for the first time, this article provides real-world data comparing human-generated and game-theoretic schedules. We also provide results from an Adversarial Perspective Team's (APT) analysis and comparison of patrols before and after the use of the PROTECT system from a viewpoint of an attacker. Given the success of PROTECT in Boston, PROTECT is currently being tested in the Port of New York (figure 1), and based on the outcome there, it may potentially be extended to other ports in the United States.

USCG and PROTECT's Goals

The USCG continues to face challenges from potential terrorists within the maritime environment, which includes both the Maritime Global Commons and the ports and waterways that make up the United States Maritime Transportation System. The former Director of National Intelligence, Dennis Blair noted in 2010 a persistent threat "from al-Qa'ida and potentially others who share its anti-Western ideology. A major terrorist attack may emanate from either outside or inside the United States" (Blair 2010). This threat was reinforced in May of 2011 following the raid on Osama Bin Laden's home, where a large trove of material was uncovered, including plans to attack an oil tanker. "There is an indication of intent, with operatives seeking the size and construction of tankers, and concluding it's best to blow them up from the inside because of the strength of their hulls" (Dozier 2011). These oil tankers transit the U.S. Maritime Transportation System. The USCG plays a key role in the security of this system and the protection of seaports to support the economy, environment, and way of life in the United States (Young and Orchard 2011).

Coupled with challenging economic times, USCG must operate as effectively as possible, achieving maximum benefit from every hour spent on patrol. To that end, the goal of PROTECT is to use game theory to assist the USCG in maximizing its effectiveness in the Ports, Waterways, and Coastal Security (PWCS) Mission. The PROTECT system, focused on the PWCS patrols, addresses how the USCG should optimally patrol critical infrastructure in a port to maximize protection, knowing that the adversary may conduct surveillance and then launch an attack.

PWCS patrols are focused on protecting critical infrastructure; without the resources to provide 100 percent on-scene presence at any, let alone all of the critical infrastructure, optimized use of security resources is critical. Toward that end, unpredictability creates situations of uncertainty for an enemy and can be enough to deem a target less

appealing. While randomizing patrol patterns is key, PROTECT also addresses the fact that the targets are of unequal value, understanding that the adversary will adapt to whatever patrol patterns USCG conducts. The output of PROTECT is a schedule of patrols that includes when the patrols are to begin, what critical infrastructure to visit for each patrol, and what activities to perform at each critical infrastructure. While initially pilot tested in the Port of Boston, the solution technique is intended to be generalizable and applicable to other ports.

Key Innovations in PROTECT

Stackelberg games have been well established in the literature (Conitzer and Sandholm 2006; Korzhyk, Conitzer, and Parr 2011; Fudenberg and Tirole 1991) and PROTECT models the PWCS patrol problem as a Stackelberg game with USCG as the leader (defender) and the terrorist adversaries in the role of the follower. The choice of this framework was also supported by prior successful applications of Stackelberg games (Jain et al. 2010, Paruchuri et al. 2008, Pita et al. 2011). (For those unfamiliar with Stackelberg games, the sidebar article provides an introduction.)

In this Stackelberg game framework, the defender commits to a mixed (randomized) strategy of patrols, which is known to the attacker. This is a reasonable approximation of the practice since the attacker conducts surveillance to learn the mixed strategies that the defender carries out, and responds with a pure strategy of an attack on a target. The optimization objective is to find the optimal mixed strategy for the defender.

In the rest of this section, we begin by discussing how to practically cast this real-world maritime patrolling problem of PWCS patrols as a Stackelberg game. We also show how to reduce the number of defender strategies before addressing the most important innovation in PROTECT: its use of the quantal response model.

Game Modeling

To model the USCG patrolling domain as a Stackelberg game, we need to define the set of attacker strategies, the set of defender strategies, and the payoff function. These strategies and payoffs center on the targets in a port — ports, such as the Port of Boston, have a significant number of potential targets (critical infrastructure). As discussed above, our Stackelberg game formulation assumes that the attacker learns the defender's strategy through conducting surveillance, and can then launch an attack. Thus, the attacks an attacker can launch on different possible targets are considered as his pure strategies.

However, the definition of defender strategies is not as straightforward. Patrols last for some fixed duration during the day as specified by USCG, for example, 4 hours. Our first attempt was to model each target as a node in a graph and allow patrol paths to go from each individual target to (almost all) other targets in the port, generating an almost complete graph on the targets. This method yields the most flexible set of patrol routes that would fit within the maximum duration, covering any permutation of targets within a single patrol. This method unfortunately faced significant challenges: it required determining the travel time for a patrol boat for each pair of targets, a daunting knowledge acquisition task given the hundreds of pairs of targets; it did not maximize the use of port geography whereby boat crews could observe multiple targets at once and it was perceived as micromanaging the activities of the USCG boat crews, which was undesirable.

Our improved approach to generating defender strategies therefore grouped nearby targets into patrol areas (in real-world scenarios such as the Port of Boston, some targets are very close to each other and it is thus natural to group targets together according to their geographic locations). The presence of patrol areas led the USCG to redefine the set of defensive activities to be performed on patrol areas to provide a more accurate and expressive model of the patrols. Activities that take a longer time provide the defender a higher payoff compared to activities that take a shorter time to complete. This affects the final patrol schedule as one patrol may visit fewer areas but conduct longer duration defensive activities at the areas, while another patrol may have more areas with shorter duration activities.

To generate all the permutations of patrol schedules, a graph $G = (\mathcal{V}, \mathcal{E})$ is created with the patrol areas as vertices $\mathcal{V}$ and adjacent patrol areas as edges $\mathcal{E}$. Using the graph of patrol areas, PROTECT generates all possible patrol schedules, each of which is a closed walk of G that starts and ends at the patrol area $b \in \mathcal{V}$, the base patrol area for the USCG. Each patrol schedule is a sequence of patrol areas and associated defensive activities at each patrol area in the sequence, and schedules are constrained by a maximum patrol time τ. (Note that even when the defender just passes by a patrol area, this is treated as an activity.) The defender may visit a patrol area multiple times in a schedule due to geographic constraints and the fact that each patrol is a closed walk. For instance, the defender in each patrol should visit the base patrol area at least twice since she needs to start the patrol from the base and finally come back to the base to finish the patrol.

The graph G along with the constraints b and τ are used to generate the defender strategies (patrol

Stackelberg Game

A generic Stackelberg game has two players, a leader, and a follower (Fudenberg and Tirole 1991). A leader commits to a strategy first, and then a follower optimizes her reward, considering the action chosen by the leader (von Stengel and Zamir 2004). The two players in a Stackelberg game need not represent individuals, but could also be groups that cooperate to execute a joint strategy, such as a police force or a terrorist organization. Each player has a set of possible pure strategies, or the actions that they can execute. A mixed strategy allows a player to play a probability distribution over pure strategies. Payoffs for each player are defined over all possible pure-strategy outcomes for both the players. The payoff functions are extended to mixed strategies by taking the expectation over pure-strategy outcomes. The follower can observe the leader's strategy, and then act in a way to optimize his own payoffs.

To see the advantage of being the leader in a Stackelberg game, consider the game with the payoff as shown in the sidebar table. The leader is the row player and the follower is the column player. The only pure-strategy Nash equilibrium for this game is when the leader plays *a* and the follower plays *c*, which gives the leader a payoff of 3; in fact, for the leader, playing *b* is strictly dominated.

However, in the simultaneous game if the leader can commit to playing *b* before the follower chooses his strategy, then the leader will obtain a payoff of 4, since the follower would then play *d* to ensure a higher payoff for himself. If the leader commits to a mixed strategy of playing *a* and *b* with equal (0.5) probability, then the follower will play *d*, leading to a higher expected payoff for the leader of 4.5. As we can see from this example, the equilibrium strategy in the Stackelberg game can be in fact different from the Nash equilibria.

Stackelberg games are used to model the attacker-defender strategic interaction in security domains and this class of Stackelberg games (with certain restrictions on payoffs [Yin et al. 2010]) is called Stackelberg security games. In the Stackelberg security game framework, the security force (defender) is modeled as the leader and the terrorist adversary (attacker) is in the role of the follower. The defender commits to a mixed (randomized) strategy, whereas the attacker conducts surveillance of these mixed strategies and responds with a pure strategy of an attack on a target. Thus, the Stackelberg game framework is a natural approximation of the real-world security scenarios. In contrast, the surveillance activity of the attacker cannot be modeled in the simultaneous move games with the Nash equilibrium solution concept. The objective is to find the optimal mixed strategy for the defender. See Tambe (2011) for a more detailed introduction to research on Stackelberg security games.

	c	d
a	3, 1	5, 0
b	2, 0	4, 2

Payoff Table for Example Stackelberg Game.

Patrol Schedule	Target 1	Target 2	Target 3	Target 4
$(1:k_1), (2:k_1), (1:k_1)$	50, –50	...	15, –15	...
$(1:k_2), (2:k_1), (1:k_1)$	...	60,-60	...	...
$(1:k_1), (2:k_1), (1:k_2)$	...	...	...	-20, 20
$(1:k_1), (3:k_1), (2:k_1), (1:k_1)$	50, –50	...	...	...
$(1:k_1), (2:k_1), (3:k_1), (1:k_1)$	...	...	15, –15	...

Table 1. Portion of a Simplified Example of a Game Matrix.

schedules). Given each patrol schedule, the total patrol schedule time is calculated (this also includes traversal time between areas, but we ignore it in the following for expository purposes); we then verify that the total time is less than or equal to the maximum patrol time τ. After generating all possible patrol schedules, a game is formed where the set of defender strategies is composed of patrol schedules and the set of attacker strategies is the set of targets. The attacker's strategy was based on targets instead of patrol areas because an attacker will choose to attack a single target.

Table 1 gives an example, where the rows correspond to the defender's strategies and the columns correspond to the attacker's strategies. In this example, there are two possible defensive activities, activity k_1 and k_2, where k_2 provides more effective protection (also takes more time) for the defender than k_1. Suppose that the time bound disallows more than two k_2 activities (given the time required for k_2) within a patrol. Patrol area 1 has two targets (target 1 and 2) while patrol areas 2 and 3 each have one target (target 3 and 4 respectively). In the table, a patrol schedule is composed of a sequence of patrol areas and a defensive activity in each area. The patrol schedules are ordered so that the first patrol area in the schedule denotes which patrol area the defender needs to visit first. In this example, patrol area 1 is the base patrol area, and all of the patrol schedules begin and end at patrol area 1. For example, the patrol schedule in row 2 first visits patrol area 1 with activity k_2, then travels to patrol area 2 with activity k_1, and returns back to patrol area 1 with activity k_1. For the payoffs, if a target i is the attacker's choice and the attack fails, then the defender would gain a reward R_i^d while the attacker would receive a penalty P_i^a, else the defender would receive a penalty P_i^d and the attacker would gain a reward R_i^a. Furthermore, let G_{ij}^d be the payoff for the defender if the defender chooses patrol j and the attacker chooses to attack target i. G_{ij}^d can be represented as a linear combination of the defender reward/penalty on

target i and A_{ij}, the effectiveness probability of the defensive activity performed on target i for patrol j, as described by equation 1. A_{ij} depends on the most effective activity on target i in patrol j. The value of A_{ij} is 0 if target i is not in patrol j. If patrol j only includes one activity in a patrol area that covers target i, then we determine its payoff using the following equation (any additional activity may provide an additional incremental benefit in that area and we discuss this in the following section).

$$G_{ij}^d = A_{ij}R_i^d + (1 - A_{ij})P_i^d \tag{1}$$

For instance, suppose target 1 is covered using k_1 in strategy 5, and the value of A_{15} is 0.5. If $R_i^d = 150$ and $P_1^d = -50$, then $G_{15}^d = 0.5(150) + (1 - 0.5)(-50) = 50$. G_{ij}^a would be computed in a similar fashion.

In the USCG problem, rewards and penalties are based on an analysis completed by a contracted company of risk analysts that looked at the targets in the Port of Boston and assigned corresponding values for each one. The types of factors taken into consideration for generating these values include economic damage and injury/loss of life. Meanwhile, the effectiveness probability, A_{ij}, for different defensive activities are decided based on the duration of the activities. Longer activities lead to a higher possibility of capturing the attackers.

While loss of life and property helps in assessing damage in case of a successful attack, assessing payoffs requires that we determine whether the loss is viewed symmetrically by the defender and attacker. Similarly, whether the payoffs are viewed symmetrically for the attacker and defender also holds for the scenario when there is a failed attack. These questions to go the heart of determining whether security games should be modeled as zero-sum games (Tambe 2011).

Past work in security games (for example, ARMOR [Jain et al. 2010], IRIS [Jain et al. 2010], GUARDS [Pita et al. 2011]) has used nonzero-sum game models; for example, one assumption made is that the attacker might view publicity of a failed attack as a positive outcome. However, nonzero-sum games require further knowledge acquisition efforts to model the asymmetry in payoffs. For simplicity, as the first step PROTECT starts with the assumption of a zero-sum game. However, the algorithm used in PROTECT is not restricted to zero-sum games, as in the future, USCG proposes to relax this assumption. It is also important to note that while table 1 shows point estimates of payoffs, we recognize that estimates may not be accurate. To that end, in the experimental results section, we evaluated the robustness of our approach when there is payoff noise, observation noise, and execution error.

Compact Representation

In our game, the number of defender strategies, that is, patrol schedules, grows combinatorially, generating a scale-up challenge. To achieve scale-up, PROTECT uses a compact representation of the patrol schedules using two ideas: combining equivalent patrol schedules and removal of dominated patrol schedules.

With respect to equivalence, different permutations of patrol schedules provide identical payoff results. Furthermore, if an area is visited multiple times with different activities in a schedule, we only consider the activity that provides the defender the highest payoff, not the incremental benefit due to additional activities. This decision is made in consideration of the trade-off between modeling accuracy and efficiency. On the one hand, the additional value of more activities is small. Currently, the patrol time of each schedule is relatively short (for example, 1 hour) and the defender may visit a patrol area more than once within the short period and will conduct an activity each time. For instance, the defender may pass by a patrol area 10 minutes after conducting a more effective activity at the same patrol area. The additional value of the pass by activity given the more effective activity is therefore very small. On the other hand, it leads to significant computational benefits, which are described in this section, if we just consider the most effective activity in each patrol.

Therefore, many patrol schedules are equivalent if the set of patrol areas visited and the most effective defensive activities in each patrol area in the schedules are the same even if their order differs. Such equivalent patrol schedules are combined into a single compact defender strategy, represented as a set of patrol areas and defensive activities (and minus any ordering information). The idea of combining equivalent actions is similar to action abstraction for solving large-scale dynamic games (Gilpin 2009). Table 2 presents a compact version of table 1, which shows how the game matrix is simplified by using equivalence to form compact defender strategies, for example, the patrol schedules in rows 2 and 3 from table 1 are represented as a compact strategy $\Gamma_2 = \{(1, k_2), (2, k_1)\}$ in table 2.

Next, the idea of dominance is illustrated using table 2 and noting the difference between Γ_1 and Γ_2 is the defensive activity on patrol area 1. Since activity k_2 gives the defender a higher payoff than k_1, Γ_1 can be removed from the set of defender strategies because Γ_2 covers the same patrol areas while giving a higher payoff for patrol area 1. To generate the set of compact defender strategies, a naive approach would be first to generate the full set of patrol schedules and then prune the dominated and equivalent schedules. Instead, PROTECT generates compact strategies in the following man-

Compact Strategy	Target 1	Target 2	Target 3	Target 4
$\Gamma1 = \{(1: k_1), (2: k_1)\}$	50, –50	30, –30	15, –15	–20, 20
$\Gamma2 = \{(1: k_2), (2: k_1)\}$	100, –100	60, –60	15, –15	–20, 20
$\Gamma3 = \{(1: k_1), (2: k_1), (3: k_1)\}$	50, –50	30, –30	15, –15	10, –10

Table 2. Example Compact Atrategies and Fame Matrix.

ner: we start with patrols that visit the most patrol areas with the least effective activities within the patrol time limit; these activities take a shorter amount of time but we can cover more areas within the given time limit. Then we gradually consider patrols visiting less patrol areas but with increasingly effective activities. This process will stop when we have considered all patrols in which all patrol areas are covered with the most effective activities and cannot include any additional patrol area.

Figure 2 shows a high level view of the steps of the algorithm using the compact representation. The compact strategies are used instead of full patrol schedules to generate the game matrix. Once the optimal probability distribution is calculated for the compact strategies, the strategies with a probability greater than 0 are expanded to a complete set of patrol schedules.

In this expansion from a compact strategy to a full set of patrol schedules, we need to determine the probability of choosing each patrol schedule, since a compact strategy may correspond to multiple patrol schedules. The focus here is to increase the difficulty for the attacker to conduct surveillance by increasing unpredictability,[1] which we achieve by randomizing uniformly over all expansions of the compact defender strategies. The uniform distribution provides the maximum entropy (greatest unpredictability). Thus, all the patrol schedules generated from a single compact strategy are assigned a probability of v_i / w_i where v_i is the probability of choosing a compact strategy Γ_i and w_i is the total number of expanded patrol schedules for Γ_i. The complete set of patrol schedules and the associated probabilities are then sampled and provided to the USCG, along with the start time of the patrol generated through uniform random sampling.

Human Adversary Modeling

While previous game-theoretic security applications have assumed a perfectly rational attacker, PROTECT takes a step forward by addressing this limitation of classical game theory. Instead, PROTECT uses a model of a boundedly rational adversary by using a quantal response (QR) model of an adversary, which has shown to be a promising
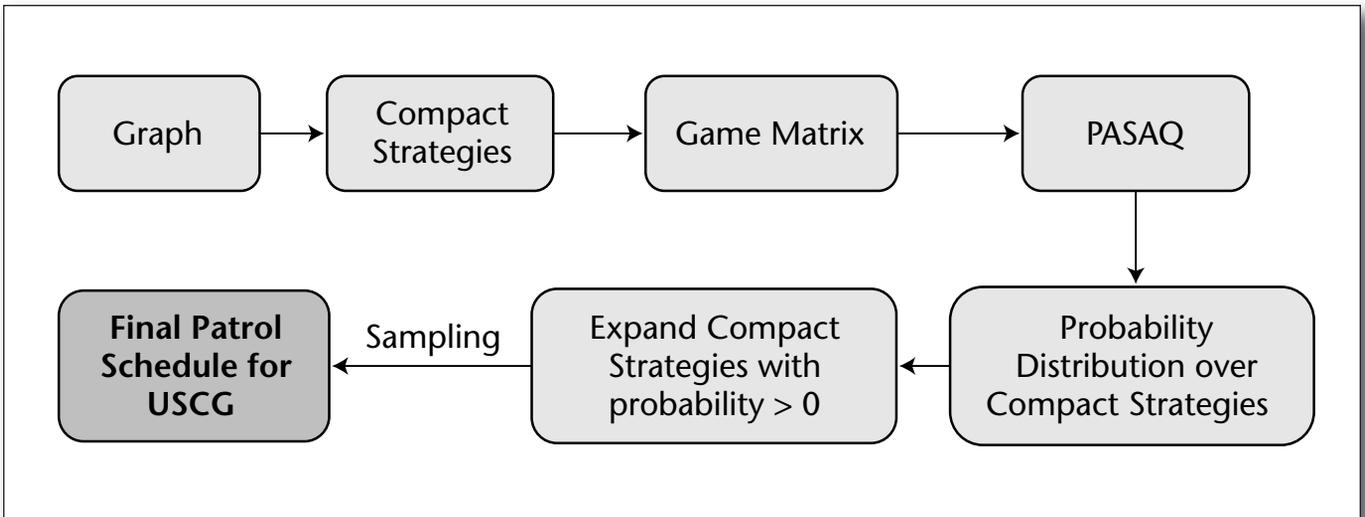
Figure 2. Flow Chart of the PROTECT System.

t_i	Target i
$R^d{}_i$	Defender reward on covering t_i if it's attacked
$P^d{}_i$	Defender penalty on not covering t_i if it's attack
$R^a{}_i$	Attacker reward on attacking t_i if it's not covered
$P^a{}_i$	Attacker penalty on attacking t_i if it's covered
A_{ij}	Effectiveness probability of compact strategy Γ_j on t_i
a_j	Probability of choosing compact strategy Γ_j
J	Total number of compact strategies
x_i	Marginal coverage on t_i

Table 3. PASAQ Notation as Applied to PROTECT.

model of human decision making (McKelvey and Palfrey 1995; Rogers, Palfrey, and Camerer 2009; Yang et al. 2011). A recent study demonstrated the use of QR as an effective prediction model of humans (Wright and Leyton-Brown 2010). An even more relevant study of the QR model was conducted by Yang et al. (Yang et al. 2011) in the context of security games where this model was shown to outperform competitors in modeling human subjects. Based on this evidence, PROTECT uses a QR model of a human adversary, that is, in the Stackelberg game model, the attacker best-responds according to a QR model and the defender computes her optimal mixed patrolling strategy with this knowledge.

To apply the QR model in a Stackelberg framework, PROTECT employs an algorithm known as PASAQ (Yang, Tambe, and Ordóñez 2012). PASAQ computes the optimal defender strategy (within a guaranteed error bound) given a QR model of the

adversary by solving the following nonlinear and nonconvex optimization problem *P*, with table 3 listing the notation.

$$
\text{P}: \begin{cases}
\max_a \displaystyle\sum_{i=1}^{T} QR(i\,|\,\lambda)((R_i^d - P_i^d)x_i + P_i^d) \\[2ex]
x_i = \displaystyle\sum_{j=1}^{J} a_j A_{ij}, \forall i \\[2ex]
\displaystyle\sum_{j=1}^{J} a_j = 1 \\[2ex]
0 \le a_j \le 1, \forall j
\end{cases}
$$

The first line of the problem corresponds to the computation of the defender's expected utility resulting from a combination of equations 1 and 2 (in the sidebar). $QR(i|\lambda)$ is the probability that the attacker using the QR model will attack target *i*. Unlike in previous applications (Jain et al. 2010; Kiekintveld, Marecki, and Tambe 2011; Paruchuri et al. 2008), x_i in this case summarizes not just presence or absence on a target, but also the effectiveness probability A_{ij} on the target as well. That is, the second line computes the marginal coverage on the targets based on the effectiveness factor A_{ij} and the probability of choosing compact strategy Γ_j, denoted as a_j.

As with all QR models, a value for λ is needed to represent the noise in the attacker's strategy. Clearly, a λ value of 0 (uniform random) and ∞ (fully rational) are not reasonable. Given the payoff data for Boston, an attacker's strategy with λ = 4 starts approaching a fully rational attacker — the probability of attack focuses on a single target. In addition, an attacker's strategy with λ = 0.5 is similar to a fully random strategy that uniformly chooses a

target to attack. USCG experts (with expertise in terrorist behavior modeling) suggested that we could use a broad range for representing possible λ values used by the attacker. Combining the above observations, it was determined that the attacker's strategy is best modeled with a λ value that is in the range [0.5, 4], rather than a single point estimate. A discrete sampling approach was used to determine a λ value that gives the highest average defender expected utility across attacker strategies within this range to get λ = 1.5. Specifically, the defender considers different assumptions of the attacker's λ value and for each assumption about the λ value, the defender computes her expected utility against the attacker with different λ values within the range [0.5, 4]. We find that when the defender assumes the attacker is using the QR model with λ = 1.5, the defender's strategy leads to the highest defender expected utility when the attacker follows the QR model with a λ value uniformly randomly chosen from the range of [0.5, 4]. Selecting an appropriate value for λ remains a complex issue however, and it is a key agenda item for future work.

Evaluation

This section presents evaluations based on experiments completed through simulations and real-world patrol data along with USCG analysis. All scenarios and experiments, including the payoff values and graph (composed of nine patrol areas), were based off the Port of Boston. The defender's payoff values have a range of [–10,5] while the attacker's payoff values have a range of [–5,10]. The game was modeled as a zero-sum game in which the attacker's loss or gain is balanced precisely by the defender's gain or loss. For PASAQ, the defender's strategy is computed assuming that the attacker follows the QR model with λ = 1.5 as justified in the previous section. All experiments are run on a machine with an Intel Dual Core 1.4 GHz processor and 2 GB of RAM.

Memory and Run-Time Analysis

This section presents the results based on simulation to show the efficiency in memory and run time of the compact representation versus the full representation. In figure 3a, the *x*-axis is the maximum patrol time allowed and the *y*-axis is the memory needed to run PROTECT. In figure 3b, the *x*-axis is the maximum patrol time allowed and the *y*-axis is the run time of PROTECT. The maximum patrol time allowed determines the number of combinations of patrol areas that can be visited — so the *x*-axis indicates a scale-up in the number of defender strategies. When the maximum patrol time is set to 90 minutes, the full representation takes 30 seconds and uses 540 MB of memory

Quantal Response

Quantal response equilibrium is an important model in behavior game theory that has received widespread support in the literature in terms of its superior ability to model human behavior in simultaneous-move games (McKelvey and Palfrey 1995) and is the baseline model of many studies (Wright and Leyton-Brown 2010). It suggests that instead of strictly maximizing utility, individuals respond stochastically in games: the chance of selecting a nonoptimal strategy increases as the cost of such an error decreases. However, the applicability of these models to Stackelberg security games had not been explored previously. In Stackelberg security games, we assume that the attacker acts with bounded rationality; the defender is assisted by software and thus we compute the defender's optimal rational strategy (Yang et al. 2011).

Given the strategy of the defender, the quantal best response of the attacker is defined as

$$q_i = \frac{e^{\lambda G_i^a(x_i)}}{\sum_{j=1}^{T} e^{\lambda G_j^a(x_i)}} \tag{2}$$

The parameter λ represents the amount of noise in the attacker's strategy. λ can range from 0 to ∞ with a value of 0 representing a uniform random probability over attacker strategies and with a value of ∞ representing a perfectly rational attacker. q_i corresponds to the probability that the attacker chooses a target *i*; $G_i^a(x_i)$ corresponds to the attacker's expected utility of attacking target *i* given x_i, the probability that the defender covers target *i*; and *T* is the total number of targets.

Consider the Stackelberg game with the payoffs shown in table 4. Assume that the leader commits to playing *b*. The follower obtains a payoff of 0 by playing *c* and obtains a payoff of 2 by playing *d*. A rational attacker will play *d* to maximize his payoff. However, the quantal best response of the attacker would be playing *c* with probability

$$\frac{e^0}{e^0 + e^{2\lambda}}$$

and playing *d* with probability

$$\frac{e^{2\lambda}}{e^0 + e^{2\lambda}} .$$

while the compact representation takes 11 seconds to run and requires 20 MB of memory. Due to the exponential increase in the memory and run time that is needed for the full representation, it cannot be scaled up beyond 90 minutes.
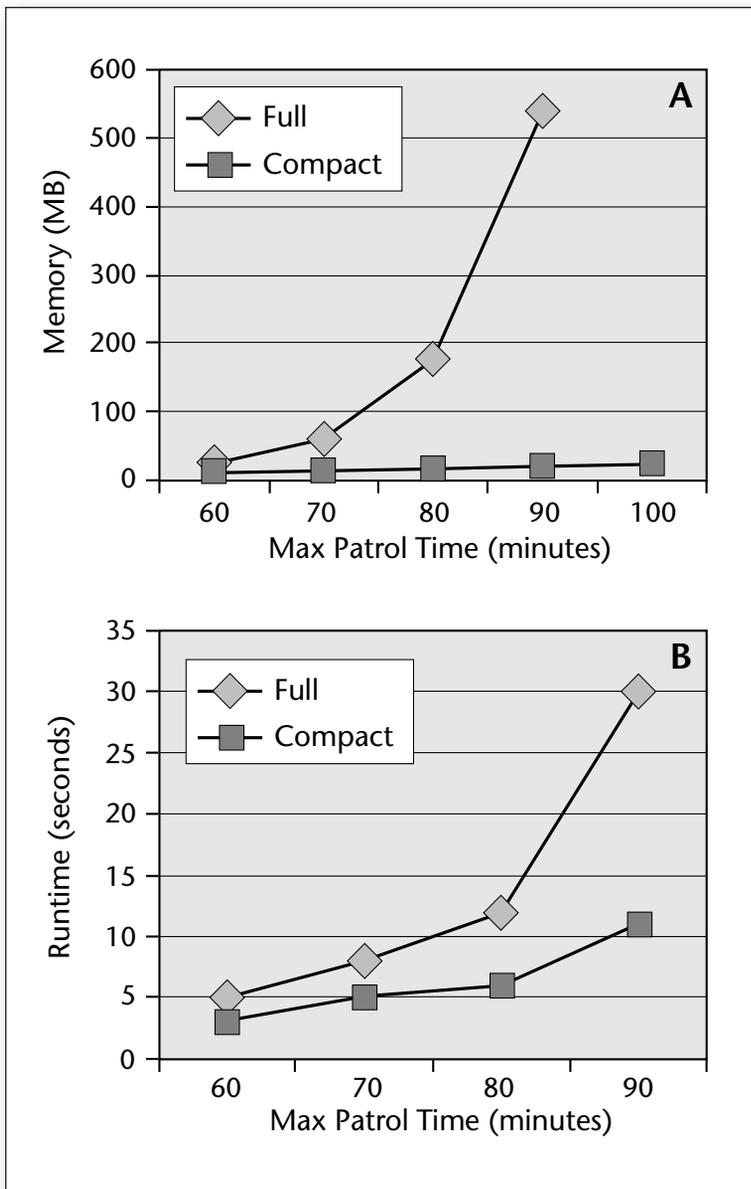
Figure 3. Comparison of Full Versus Compact Representation.

Utility Analysis

It is useful to understand whether PROTECT using PASAQ with $\lambda = 1.5$ provides an advantage when compared to: (1) a uniform random defender's strategy; (2) a mixed strategy with the assumption of the attacker attacking any target uniformly at random ($\lambda = 0$) or; (3) a mixed strategy assuming a fully rational attacker ($\lambda = \infty$). The previously existing DOBSS algorithm was used for $\lambda = \infty$ (Paruchuri et al. 2008). Additionally, comparison with the $\lambda = \infty$ approach is important because of the extensive

use of this assumption in previous applications (for our zero-sum case, DOBSS is equivalent to minimax but the utility does not change). Typically, we may not have an estimate of the exact value of the attacker's λ value, only a possible range. Therefore, ideally we would wish to show that PROTECT (using $\lambda = 1.5$ in computing the optimal defender strategy) provides an advantage over a range of λ values assumed for the attacker (not just over a point estimate) in his best response, justifying our use of the PASAQ algorithm. In other words, we are distinguishing between (1) the actual λ value employed by the attacker in best-responding, and (2) the λ assumed by PASAQ in computing the defender's optimal mixed strategy. The point is to see how sensitive the choice of (2) is, with respect to prevailing uncertainty about (1).

To achieve this, we compute the average defender utility of the four approaches above as the λ value of the attacker's strategy changes from [0, 6], which subsumes the range [0.5, 4] of reasonable attacker strategies. In figure 4, the *y*-axis represents the defender's expected utility and the *x*-axis is the λ value that is used for the attacker's strategy. Both uniform random strategies perform well when the attacker's strategy is based on $\lambda = 0$. However, as λ increases, both strategies quickly drop to a very low defender expected utility. In contrast, the PASAQ strategy with $\lambda = 1.5$ provides a higher expected utility than that assuming a fully rational attacker over a range of attacker λ values (and indeed over the range of interest), not just at $\lambda = 1.5$.

Robustness Analysis

In the real world, observation, execution, and payoffs are not always perfect due to the following: noise in the attacker's surveillance of the defender's patrols, the many tasks and responsibilities of the USCG where the crew may be pulled off a patrol, and limited knowledge of the attacker's payoff values. Our hypothesis is that PASAQ with $\lambda = 1.5$ is more robust to such noise than a defender strategy that assumes full rationality of the attacker such as DOBSS (Paruchuri et al. 2008), that is, PASAQ's expected defender utility will not degrade as much as DOBSS over the range of attacker λ of interest. This is illustrated by comparing both PASAQ and DOBSS against observation, execution, and payoff noise (Kiekintveld, Marecki, and Tambe 2011; Korzhyk, Conitzer, and Parr 2011; Yin et al. 2011). Intuitively, the QR model is more robust than models assuming perfect rationality since the QR model assumes that the attacker may attack multiple targets with positive probabilities, rather than attacking a single target in the model assuming perfect rationality of the adversaries. Such intuition has been verified in other contexts (Rogers, Palfrey, and Camerer 2009). All

experiments were run generating 200 samples with added noise and averaging over all the samples.

Figure 5 shows the performance of different strategies while considering execution noise. The y-axis represents the defender's expected utility and the x-axis is the attacker's λ value. If the defender covered a target with probability p, this probability now changes to be in $[p - x, p + x]$ where x is the noise. The low execution error corresponds to $x = 0.1$ whereas high error corresponds to $x = 0.2$. In the experiments, the attacker best-responds to the mixed strategy with added noise. The key takeaway here is that execution error leads to PASAQ dominating DOBSS over all tested values of λ, further strengthening the reason to use PASAQ rather than a full-rationality model. For both algorithms, the defender's expected utility decreases as more execution error is added because the defender's strategy is affected by the additional error. When execution error is added, PASAQ dominates DOBSS because the latter seeks to maximize the minimum defender's expected utility so multiple targets will have the same minimum defender utility. For DOBSS, when execution error is added, there is a greater probability that one of these targets will have less coverage, resulting in a lower defender's expected utility. For PASAQ, typically only one target has the minimum defender expected utility. As a result changes in coverage do not affect it as much as DOBSS. As execution error increases, the advantage in the defender's expected utility of PASAQ over DOBSS increases even more. This section only shows the execution noise results; the details of the observation and payoff noise results can be found in Shieh et al. (2012).

USCG Real-World Evaluation

In addition to the data made available from simulations, the USCG conducted its own real-world evaluation of PROTECT. With permission, some aspects of the evaluation are presented in this article.

Real-World Scheduling Data

Unlike prior publications of real-world applications of game theory for security, a key novelty of this article is the inclusion of actual data from USCG patrols before and after the deployment of PROTECT at the Port of Boston. Figure 6 and figure 7 show the frequency of visits by USCG to different patrol areas over a number of weeks. Figure 6 shows pre-PROTECT patrol visits per day by area and figure 7 shows post-PROTECT patrol visits per day by area. The x-axis is the day of the week, and the y-axis is the number of times a patrol area is visited for a given day of the week. The y-axis is intentionally blurred for security reasons as this is real data from Boston. There are more lines in figure 6 than in figure 7 because during the implementation of PROTECT, new patrol areas were
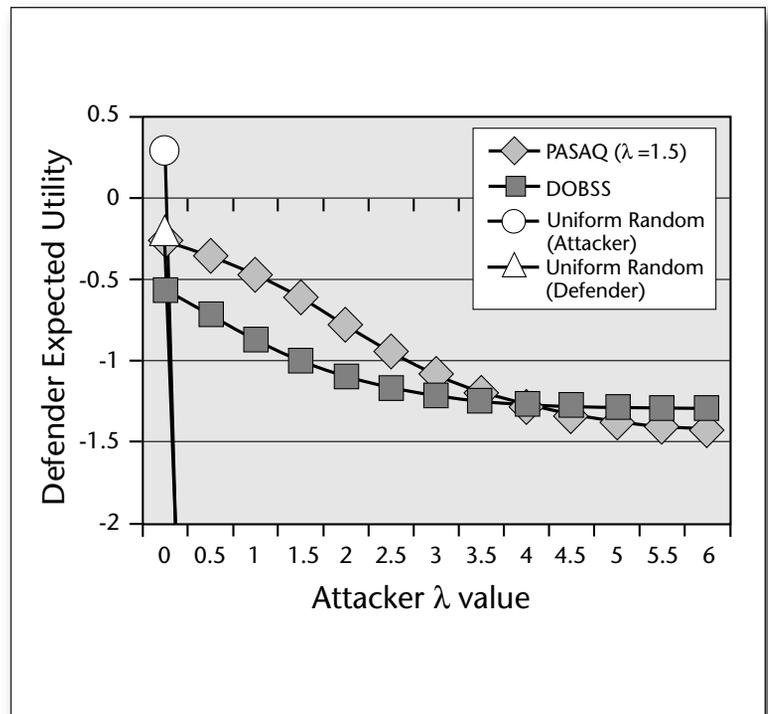
Figure 4. Defender's Expected Utility When Varying λ for Attacker's Strategy(Color).

formed that contained more targets and thus fewer patrol areas in the post-PROTECT figure. Figure 6 depicts a definite pattern in the patrols. While there is a spike in patrols executed on Day 5, there is a dearth of patrols on Day 2. Besides this pattern, the lines in figure 6 intersect, indicating that some days a higher-value target was visited more often while on other days it was visited less often. This means that there was not a consistently high frequency of coverage of higher-value targets before PROTECT.

In figure 7, we notice that the pattern of low patrols on day 2 (from figure 6) disappears. Furthermore, lines do not frequently intersect, that is, higher-valued targets are visited consistently across the week. The top line in figure 7 is the base patrol area and is visited at a higher rate than all other patrol areas.

Adversary Perspective Teams(APT)

To obtain a better understanding of how the adversary views the potential targets in the port, the USCG created the Adversarial Perspective Team (APT), a mock attacker team. The APT provides assessments from the terrorist perspective and as a secondary function, assesses the effectiveness of the patrol activities before and after deployment of PROTECT. In their evaluation, the APT incorporates the adversary's known intent, capabilities, skills, commitment, resources, and cultural influ-
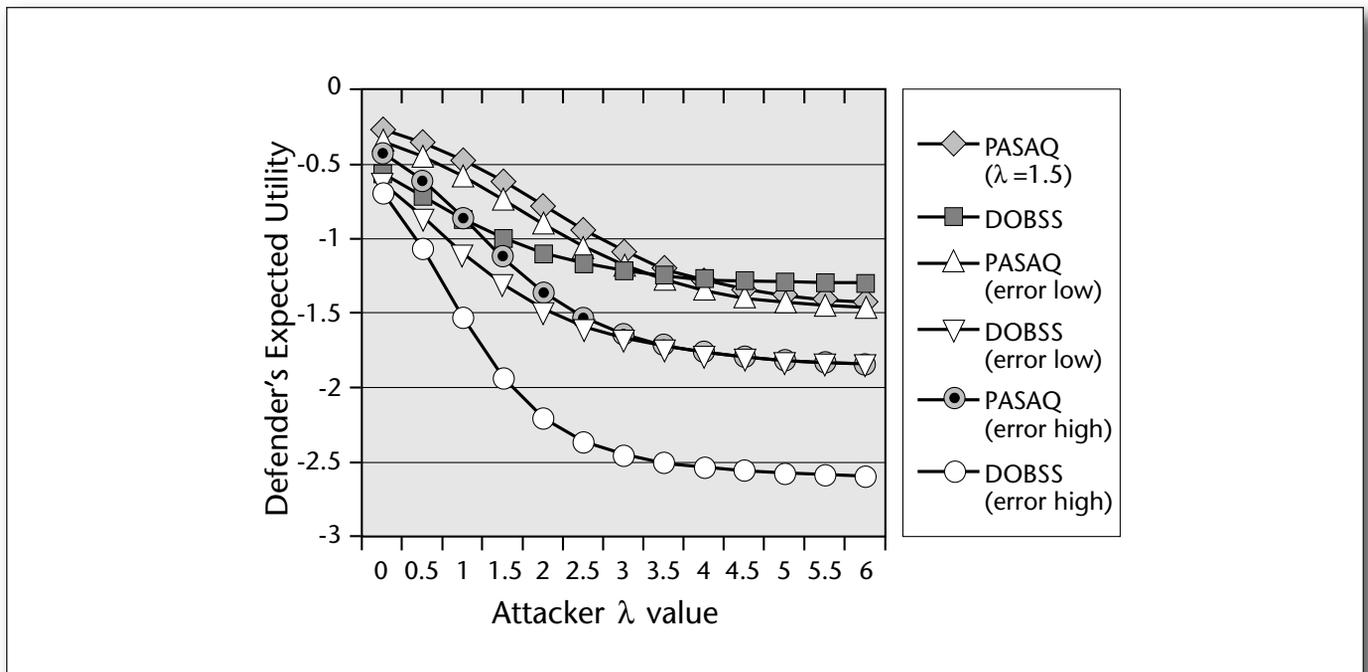
Figure 5. Defender's Expected Utility: Execution Noise(Color).
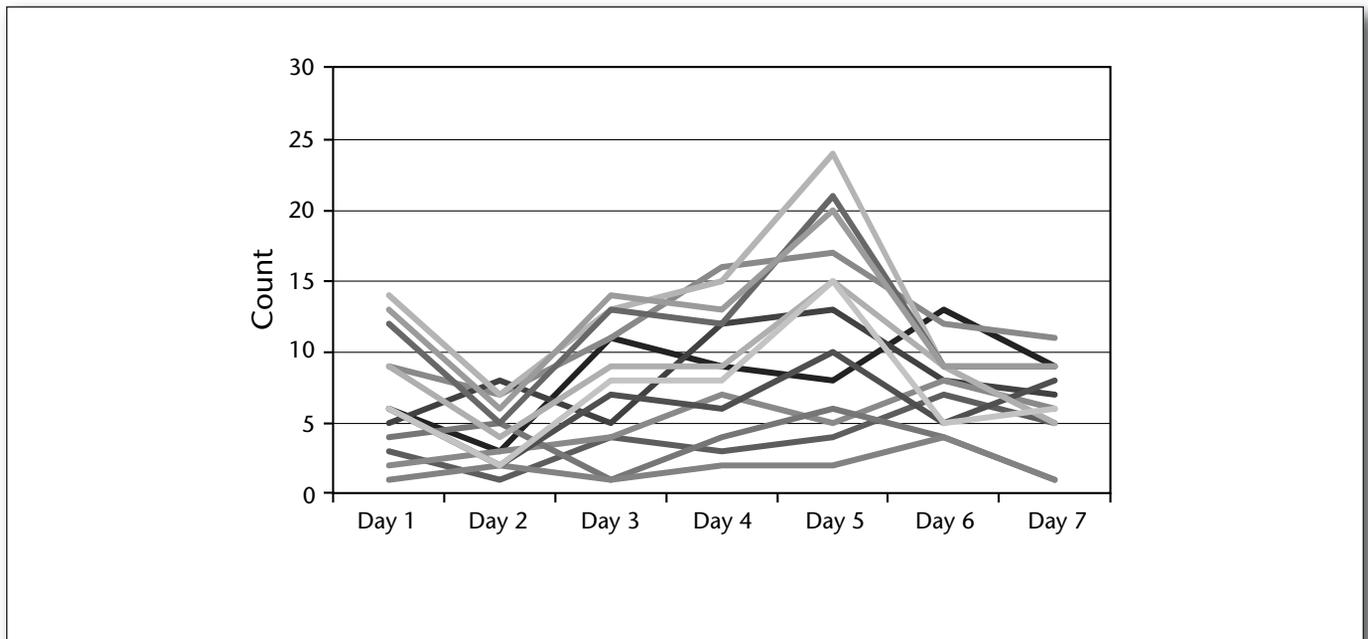
Figure 6. Patrol Visits per Day by Area — Pre-PROTECT(Color), One Line Per Area.

ences. In addition, it screens attack possibilities and assists in identifying the level of deterrence projected at and perceived by the adversary. For the purposes of this research, the adversary is defined as an individual(s) with ties to al-Qa'ida or its affiliates.

The APT conducted a pre- and post-PROTECT assessment of the system's impact on an adver-
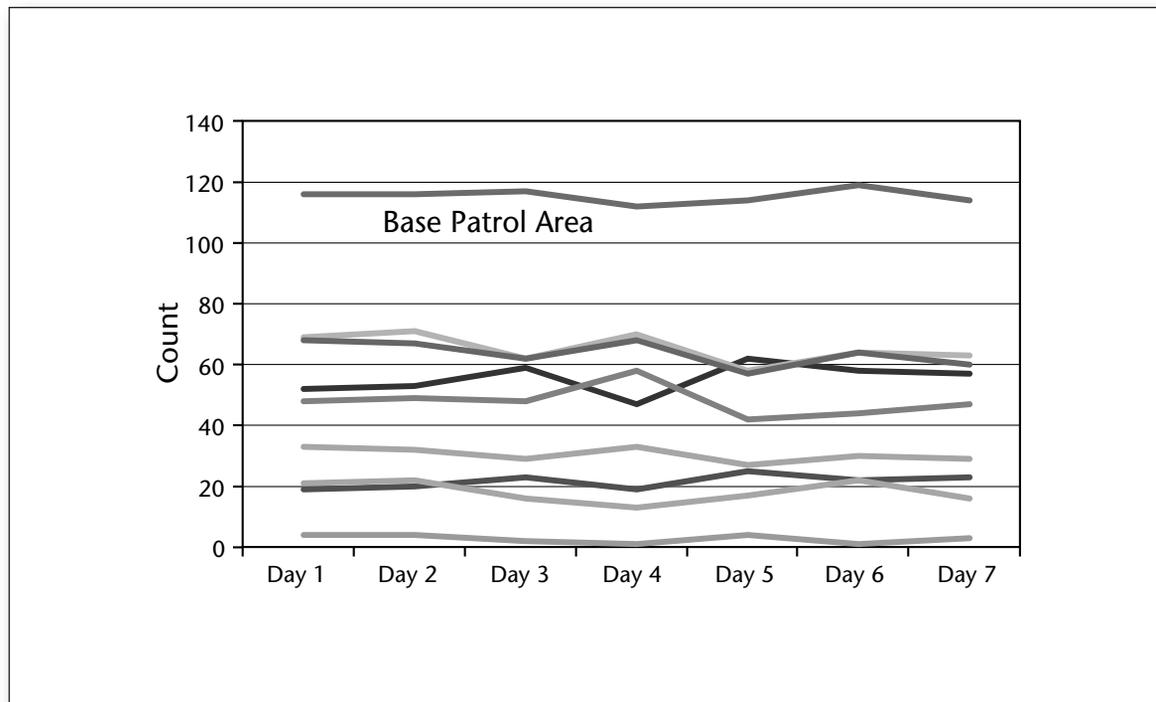
Figure 7. Patrol Visits per Day by Area — Post-PROTECT(Color), One Line Per Area.

sary's deterrence at the Port of Boston. This analysis uncovered a positive trend where the effectiveness of deterrence increased from the pre- to post-PROTECT observations.

Additional Real-World Indicators

The use of PROTECT and APT's improved guidance given to boat crews on how to conduct the patrol jointly provided a noticeable increase in the quality and effectiveness of the patrols. Prior to implementing PROTECT, there were no documented reports of illicit activity. After implementation, USCG crews reported more illicit activities within the port (therefore justifying the effectiveness of the PROTECT model) and provided a noticeable "on the water" presence, with industry port partners commenting, "the Coast Guard seems to be everywhere, all the time." With no actual increase in the number of resources applied, and therefore no increase in capital or operating costs, these outcomes support the practical application of game theory in the maritime security environment.

Outcomes After Boston Implementation

After evaluating the performance and impact of PROTECT at Boston, the USCG viewed this system as a success. As a result, PROTECT is now getting deployed in the Port of New York. We were presented an award for the work on the PROTECT system for the Boston Harbor, which reflects USCG's recognition of the impact and value of PROTECT.

Lessons Learned: Putting Theory into Practice

Developing the PROTECT model was a collaborative effort involving university researchers and USCG personnel representing decision makers, planners, and operators. Building on the lessons reported in Pita et al. (2011) for working with security organizations, we informed the USCG of (1) the assumptions underlying the game-theoretic approaches, for example, full adversary rationality, and strengths and limitations of different algorithms — rather than preselecting a simple heuristic approach; (2) the need to define and collect correct inputs for model development and; (3) a fundamental understanding of how the inputs affect the results. We gained three new insights involving real-world applied research; unforeseen positive benefits because security agencies were compelled to reexamine their assumptions; requirement to work with multiple teams in a security organization at multiple levels of the hierarchy; and the need to prepare answers to end-user practical questions not always directly related to the "meaty" research problems.

The first insight came about when USCG was compelled to reassess its operational assumptions as a result of working through the research problem. A positive result of this reexamination

prompted USCG to develop new PWCS mission tactics, techniques, and procedures. Through the iterative development process, USCG reassessed the reasons why boat crews performed certain activities and whether they were sufficient. For example, instead of "covered" versus "not covered" as the only two possibilities at a patrol point, there are now multiple sets of activities at each patrol point.

The second insight is that applied research requires the research team to collaborate with planners and operators on the multiple levels of a security organization to ensure the model accounts for all aspects of a complex real-world environment. Initially when we started working on PROTECT, the focus was on patrolling each individual target. This appeared to micromanage the activities of boat crews, and it was through their input that individual targets were grouped into patrol areas associated with a PWCS patrol. Input from USCG headquarters and the APT mentioned earlier led to other changes in PROTECT, for example, departing from a fully rational model of an adversary to a QR model.

The third insight is the need to develop answers to end-user questions that are not always related to the "meaty" research question but are related to the larger knowledge domain on which the research depends. One example of the need to explain results involved the user citing that one patrol area was being repeated and hence, randomization did not seem to occur. After assessing this concern, we determined that the cause for the repeated visits to a patrol area was its high reward — order of magnitude greater than the rarely visited patrol areas. PROTECT correctly assigned patrol schedules that covered the more "important" patrol areas more frequently. In another example, the user noted that PROTECT did not assign any patrols to start at 4:00 AM or 4:00 PM over a 60-day test period. They expected patrols would be scheduled to start at any hour of the day, leading them to ask if there was a problem with the program. This required us to develop a layman's briefing on probabilities, randomness, and sampling. With 60 patrol schedules, a few start hours may not be chosen given our uniform random sampling of the start time. These practitioner-based issues demonstrate the need for researchers to not only be conversant in the algorithms and math behind the research, but also be able to explain from a user's perspective how solutions are accurate. An inability to address these issues would result in a lack of real-world user confidence in the model.

Summary and Related Work

This article reports on PROTECT, a game-theoretic system deployed by the USCG in the Port of Boston since April 2011 for scheduling their patrols. USCG has deemed the deployment of PROTECT in Boston a success and efforts are underway to deploy PROTECT in the Port of New York, and to other ports in the United States. PROTECT uses an attacker-defender Stackelberg game model, and includes five key innovations.

First, PROTECT moves away from the assumption of perfect adversary rationality seen in previous work, relying instead on a quantal response (QR) model of the adversary's behavior. While the QR model has been extensively studied in the realm of behavioral game theory, to the best of our knowledge, this is its first real-world deployment. Second, to improve PROTECT's efficiency, we generate a novel compact representation of the defender's strategy space, exploiting equivalence and dominance. Third, the article shows how to practically model a real-world (maritime) patrolling problem as a Stackelberg game. Fourth, we provide experimental results illustrating that PROTECT's QR model of the adversary is better able to handle real-world uncertainties than a perfect rationality model. Finally, for the first time in a security application evaluation, we use real-world data: providing a comparison of human-generated security schedules versus those generated through a game-theoretic algorithm and results from an APT's analysis of the impact of the PROTECT system. The article also outlined the insights from the project, which include the ancillary benefits due to a review of assumptions made by security agencies, and the need for knowledge to answer questions not directly related to the research problem.

As a result, PROTECT has advanced the state of the art beyond previous applications of game theory for security. Prior applications mentioned earlier, including ARMOR, IRIS, or GUARDS (Jain et al. 2010, Pita et al. 2011), have each provided unique contributions in applying novel game-theoretic algorithms and techniques. Interestingly, these applications have revolved around airport and air-transportation security. PROTECT's novelty is not only its application domain in maritime patrolling, but also in the five key innovations mentioned above, particularly its emphasis on moving away from the assumption of perfect rationality by using the QR model.

In addition to game-theoretic applications, the issue of patrolling has received significant attention in the multiagent systems literature. These include patrol work done by robots primarily for perimeter patrols that have been addressed in arbitrary topologies (Basilico, Gatti, and Amigoni 2009), maritime patrols in simulations for deterring pirate attacks (Vanek et al. 2011), and in research looking at the impact of uncertainty in adversarial behavior (Agmon et al. 2009). PROTECT differs from these approaches in its use of a QR model of a human adversary in a game-theo-

retic setting, and in being a deployed application. Building on this initial success of PROTECT, we hope to deploy it at more and much larger-sized ports. In so doing, in the future, we will consider significantly more complex attacker strategies, including potential real-time surveillance and coordinated attacks.

Acknowledgments

Note

1. Creating optimal Stackelberg defender strategies that increase the attacker's difficulty of surveillance is an open research issue in the literature; here we choose to maximize unpredictability as the first step.

References

Agmon, N.; Kraus, S.; Kaminka, G. A.; and Sadov, V. 2009. Adversarial Uncertainty in Multi-Robot Patrol. In *Proceedings of the 21st International Jont Conference on Artifical Intelligence,* 1811–1817. Menlo Park, CA: AAAI Press.

Basilico, N.; Gatti, N.; and Amigoni, F. 2009. Leader-Follower Strategies for Robotic Patrolling in Environments with Arbitrary Topologies. In *Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems,* 500–503. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Blair, D. 2010. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. Washington, DC: Senate Select Committee on Intelligence (www.dni.gov/testimonies/20100202 testimony.pdf).

Camerer, C. F. 2003. *Behavioral Game Theory: Experiments in Strategic Interaction.* Princeton, NJ: Princeton University Press.

Conitzer, V., and Sandholm, T. 2006. Computing the Optimal Strategy to Commit To. In *Proceedings of the 7th ACM Conference on Electronic Commerce,* 82–90. New York: Association for Computing Machinery.

Dozier, K. 2011. Bin Laden Trove of Documents Sharpen US Aim. New York: NBC News (www.msnbc.msn.com/id/43331634/ns/us news-security/t/bin- laden-trove-documents-sharpen-us-aim).

Fudenberg, D., and Tirole, J. 1991. *Game Theory.* Cambridge, MA: The MIT Press.

Gilpin, A. 2009. Algorithms for Abstracting and Solving Imperfect Information Games. Ph.D. Dissertation, Carnegie Mellon University, Pittsburgh, PA.

Jain, M.; Tsai, J.; Pita, J.; Kiekintveld, C.; Rathi, S.; Tambe, M.; and Ordóñez, F. 2010. Software Assistants for Randomized Patrol Planning for the LAX Airport Police and the Federal Air Marshal Service. *Interfaces* 40(4): 267–290.

Kiekintveld, C.; Marecki, J.; and Tambe, M. 2011. Approximation Methods for Infinite Bayesian Stackelberg Games: Modeling Distributional Uncertainty. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems,* 1005–1012. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Korzhyk, D.; Conitzer, V.; and Parr, R. 2011. Solving Stackelberg games with Uncertain Observability. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems,* 1013–1020. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

McKelvey, R. D., and Palfrey, T. R. 1995. Quantal Response Equilibria for Normal Form Games. *Games and Economic Behavior* 10(1): 6–38.

Paruchuri, P.; Pearce, J. P.; Marecki, J.; Tambe, M.; Ordóñez, F.; and Kraus, S. 2008. Playing Games with Security: An Efficient Exact Algorithm for Bayesian Stackelberg games. In *Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems,* 895–902. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Pita, J.; Tambe, M.; Kiekintveld, C.; Cullen, S.; and Steigerwald, E. 2011. GUARDS — Game Theoretic Security Allocation on a National Scale. In *Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems,* 37–44. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Rogers, B. W.; Palfrey, T. R.; and Camerer, C. F. 2009. Heterogeneous Quantal Response Equilibrium and Cognitive Hierarchies. *Journal of Economic Theory* 144(4): 1440–1467.

Shieh, E.; An, B.; Yang, R.; Tambe, M.; Baldwin, C.; DiRenzo, J.; Maule, B.; and Meyer, G. 2012. PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems.* Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Tambe, M. 2011. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned.* New York: Cambridge University Press.

Vanek, O.; Jakob, M.; Hrstka, O.; and Pechoucek, M. 2011. Using Multi-Agent Simulation to Improve the Security of Maritime Transit. Paper presented at the 12th International Workshop on Multi-Agent-Based Simulation (MABS). Taipei, Taiwan 26 May.

von Stengel, B., and Zamir, S. 2004. Leadership with Commitment to Mixed Strategies. Technical Report LSE-CDAM-2004-01, CDAM Research Report. London: London School of Economics.

Wright, J., and Leyton-Brown, K. 2010. Beyond Equilibrium: Predicting Human Behavior in Normal Form Games. In *Proceedings of the 24th AAAI Conference on Artificial Intelligence,* 901–907. Menlo Park, CA: AAAI Press.

Yang, R.; Kiekintveld, C.; Ordóñez, F.; Tambe, M.; and John, R. 2011. Improving Resource Allocation Strategy

Against Human Adversaries in Security Games. In *Proceedings of the 22nd International Joint Conference on Artificial Intelligence,* 458–464. Menlo Park, CA: AAAI Press.

Yang, R.; Tambe, M.; and Ordóñez, F. 2012. Computing Optimal Strategy Against Quantal Response in Security Games. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems.* Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Yin, Z.; Korzhyk, D.; Kiekintveld, C.; Conitzer, V.; and Tambe, M. 2010. Stackelberg Versus Nash in Security Games: Interchangeability, Equivalence, and Uniqueness. In *Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems,* 1139–1146. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems.

Yin, Z.; Jain, M.; Tambe, M.; and Ordóñez, F. 2011. Risk-Averse Strategies for Security Games with Execution and Observational Uncertainty. In *Proceedings of the 25th AAAI Conference on Artificial Intelligence,* 758–763. Menlo Park, CA: AAAI Press.

Young, S., and Orchard, D. 2011. Remembering 9/11: Protecting America's Ports. Coast Guard Compass: Official Blog of the U.S. Coast Guard (6 September) (coastguard.dodlive.mil/2011/09/remembering-911-protecting-americas-ports).

Bo An is a postdoctoral researcher at the University of Southern California. His research interests include artificial intelligence, multiagent systems, game theory, and automated negotiation. He is the recipient of the 2010 IFAAMAS Victor Lesser Distinguished Dissertation Award. He also won an Operational Excellence Award from the Commander, First Coast Guard District, and the AAMAS'2012 best Innovative Application paper award. He received a Ph.D. degree in computer science from the University of Massachusetts, Amherst.

Eric Shieh is a Ph.D. student at the University of Southern California. His research focuses on multiagent systems and game theory in real-world applications. Prior to joining the doctoral program, he worked as a software engineer for Northrop Grumman. He obtained his M.S. in computer science from the University of Southern California (2005) and B.S. in computer science from Carnegie Mellon University (2003).

Rong Yang is a Ph.D. student in the Department of Computer Science at University of Southern California. Her research interests include artificial intelligence, game theory, and human decision making. She received her M.S. degree from the Department of Electrical and Computer Engineering at the Ohio State University and B.S. degree from Tsinghua University.

Milind Tambe is a professor of computer science at the University of Southern California (USC). He leads the TEAMCORE Research Group at USC, with research focused on agent-based and multiagent systems. He is a fellow of AAAI, recipient of the ACM/SIGART Autonomous Agents Research Award, as well as recipient of the Christopher Columbus Fellowship Foundation Homeland Security Award and the influential paper award from the International Foundation for Agents and Multigent Systems. He received his Ph.D. from the school of computer science at Carnegie Mellon University.

Craig Baldwin is a research scientist and senior program manager at the USCG Research and Development Center where he manages a portfolio of research projects involving application of game theory to improving port security, analysis and modeling of Coast Guard command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems, and major systems acquisition alternatives analyses such as the Offshore Patrol Cutter C4ISR systems alternative analysis.

Joe DiRenzo III is the chief of the Operations Analysis Division at Coast Guard Atlantic Area Portsmouth Virginia. In this role he directs all risk, operations analysis, modeling, and innovation engagement for the command. DiRenzo is a retired Coast Guard officer and former cutter commanding officer. He also serves as the Coast Guard Chair at the Joint Forces Staff College in Norfolk VA. The author of 300 published articles, DiRenzo was the runner up for the Naval Institute's Author of the Year in 2010. Additionally, he is the national codirector of the Joint-University of Southern California National Maritime Risk Symposium. Finally, DiRenzo is a professor of graduate intelligence studies at American Military University.

Lieutenant Commander Ben Maule is the lead operations research analyst for the Operations Analysis Division at Coast Guard Atlantic Area in Portsmouth, Virginia. Maule directs all research projects for the operations analysis division. He received his B.S. in mechanical engineering from the Coast Guard Academy and his M.S. in industrial engineering from Purdue University. Maule is a Coast Guard aviator and has flown Coast Guard helicopters in Kodiak, Alaska, and Traverse City, Michigan.

Lieutenant Garrett Meyer is the chief of the Incident Management Division at U.S. Coast Guard Sector Boston where he is responsible for managing the Coast Guard's Ports and Waterways Coastal Security, Law Enforcement, Maritime Environmental Response, Search and Rescue, and All-Hazards Response missions in the Port of Boston and along the shores of Massachusetts. He has a B.S. and master's degree in management from the United States Coast Guard Academy and the University of Phoenix, respectively.