PROTECT – A Game Theoretic System to Protect the Ports of United States

Milind Tambe, Bo An, Eric Shieh, Rong Yang
University of Southern California
November 9, 2011
Motivation

• Coast Guard mission: Maritime security
• How to allocate limited security resources?
  – Target weights
  – Adversary monitors defenses, exploits patterns
  – Adversary response
PROTECT: Randomized Patrols

Protect for US Coast Guard is being used at the port of Boston (below)
Contributions of PROTECT

• Previous security applications

  ARMOR: LAX  IRIS: FAMS  GUARDS: TSA

• Key Contributions of PROTECT:
  – 1st time Quantal Response Equilibrium (QRE) used in real world
  – Compact representation of patrol schedules
  – 1st time security application evaluated by Adversarial Perspective Team (APT)
  – 1st time with real data of patrols before/after
Application

PROTECT has been in use at the Port of Boston since April 2011

Being implemented at the Port of New York
Outline

• PROTECT system
• Challenges
• Evaluation
• Future plan
Game Theory: Stackelberg Games

- Security allocation: (i) Target weights; (ii) Opponent reaction

- Stackelberg: Security forces commit first

- Optimal security allocation: Weighted random

<table>
<thead>
<tr>
<th></th>
<th>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>7, -4</td>
<td>-2, 3</td>
</tr>
<tr>
<td>Target #2</td>
<td>-7, 7</td>
<td>4, -3</td>
</tr>
</tbody>
</table>

Adversary
PROTECT System

• Casts the patrolling problem as a Stackelberg game:
  – Two players
    • Defender actions (Coast Guard): Patrol routes
    • Attacker actions (adversaries, terrorists): Attack targets
  – Payoff matrix using defender & attacker actions

• Objective – Compute optimal strategy over patrol routes to defend targets from attack
PROTECT System Overview

Attacker Actions → Game Matrix → Run PASAQ → Sample over Probabilities

Defender Actions: Patrol Schedules

MSRAM Target Data
Example for game matrix formulation

• Patrol # 2794: \{1=T, 5=T, 6=T, 8=Q, 9=Q, 8=T, 6=T, 5=T, 1=T\}
• Row of game matrix for **defender**; attacker’s matrix opposite
• Columns correspond to **target number**

<table>
<thead>
<tr>
<th>Target Number</th>
<th>Patrol Area 1</th>
<th>Patrol Area 2</th>
<th>Patrol Area 3</th>
<th>…</th>
<th>Patrol Area 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrol Area 1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Patrol Area 2</td>
<td>-8.22</td>
<td>-376.54</td>
<td>-54.56</td>
<td>-138.75</td>
<td>-50.83</td>
</tr>
<tr>
<td>Patrol Area 3</td>
<td>-138.75</td>
<td>-50.83</td>
<td>…</td>
<td>578.21</td>
<td></td>
</tr>
<tr>
<td>…</td>
<td>578.21</td>
<td>578.21</td>
<td>…</td>
<td>578.21</td>
<td></td>
</tr>
</tbody>
</table>
# PASAQ output - Probability Distribution of Patrol Areas and Actions

<table>
<thead>
<tr>
<th>Probability</th>
<th>Patrol: Q = Query, O = Observe, T = Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05083</td>
<td>(1:Q), (2:Q), (4:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.05083</td>
<td>(1:Q), (2:T), (4:Q), (2:Q), (1:T)</td>
</tr>
<tr>
<td>0.05083</td>
<td>(1:T), (2:Q), (1:Q), (2:T), (4:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.05083</td>
<td>(1:T), (2:Q), (4:Q), (2:T), (1:Q)</td>
</tr>
<tr>
<td>0.05083</td>
<td>(1:T), (2:T), (4:Q), (2:T), (1:Q), (2:Q), (1:T)</td>
</tr>
<tr>
<td>0.05083</td>
<td>(1:T), (2:T), (4:Q), (2:Q), (1:Q)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (3:Q), (2:T), (4:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:Q), (4:Q), (2:T), (3:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (3:Q), (2:Q), (4:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:T), (2:T), (3:Q), (2:T), (4:Q), (2:Q), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (4:Q), (2:Q), (3:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (4:Q), (2:T), (3:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (3:Q), (2:T), (4:Q), (2:Q), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (4:Q), (2:T), (3:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:T), (2:T), (4:Q), (2:T), (3:Q), (2:T), (1:T)</td>
</tr>
<tr>
<td>0.00221</td>
<td>(1:Q), (2:T), (4:Q), (2:T), (3:Q), (2:T), (1:T)</td>
</tr>
</tbody>
</table>

...
## Actionable Results: Schedule for 20 days

<table>
<thead>
<tr>
<th>Day</th>
<th>Hour: 0000 - 2300</th>
<th>Patrol: Q = Query, O = Observe, T = Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day: 1 Hour: 1500</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (9:Q), (8:Q), (6:T), (5:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 2 Hour: 0300</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (9:T), (8:T), (6:T), (5:T), (1:T), (2:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 3 Hour: 1700</td>
<td>Patrol: [(1:T), (2:T), (4:Q), (2:T), (1:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 4 Hour: 1600</td>
<td>Patrol: [(1:T), (2:Q), (4:Q), (2:T), (1:Q)]</td>
<td></td>
</tr>
<tr>
<td>Day: 5 Hour: 1800</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 6 Hour: 2300</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (7:T), (5:T), (1:T), (2:T), (4:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 7 Hour: 0200</td>
<td>Patrol: [(1:T), (2:Q), (4:Q), (2:T), (1:Q)]</td>
<td></td>
</tr>
<tr>
<td>Day: 8 Hour: 1400</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 9 Hour: 0600</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:Q), (9:Q), (8:T), (6:T), (5:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 10 Hour: 1900</td>
<td>Patrol: [(1:T), (5:T), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 11 Hour: 0600</td>
<td>Patrol: [(1:Q), (2:Q), (4:Q), (2:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 12 Hour: 0000</td>
<td>Patrol: [(1:T), (2:T), (3:Q), (2:T), (4:Q), (2:Q), (1:Q)]</td>
<td></td>
</tr>
<tr>
<td>Day: 13 Hour: 1500</td>
<td>Patrol: [(1:T), (5:T), (7:T), (8:T), (6:T), (5:T), (1:T), (2:T), (4:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 14 Hour: 0200</td>
<td>Patrol: [(1:T), (2:T), (4:Q), (2:T), (1:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 15 Hour: 1400</td>
<td>Patrol: [(1:T), (5:Q), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 16 Hour: 0900</td>
<td>Patrol: [(1:Q), (2:Q), (4:Q), (2:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 17 Hour: 2000</td>
<td>Patrol: [(1:T), (2:T), (4:Q), (2:T), (1:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 18 Hour: 1300</td>
<td>Patrol: [(1:T), (5:Q), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:T), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 19 Hour: 0700</td>
<td>Patrol: [(1:Q), (2:T), (4:Q), (2:Q), (1:T)]</td>
<td></td>
</tr>
<tr>
<td>Day: 20 Hour: 0800</td>
<td>Patrol: [(1:T), (5:Q), (6:T), (8:T), (9:Q), (8:T), (6:T), (5:T), (1:T)]</td>
<td></td>
</tr>
</tbody>
</table>
Outline

• PROTECT system
• Challenges
• Evaluation
• Future plan
Challenges

• Human Adversary
  – Not assume perfectly rational attacker

• Scaling up
  – # of possible schedules exponential

• Modeling CG domain
  – Implementing real world
Human Adversary - QRE

- Game Theory and Human Behavior (IJCAI’11, Yang et al.)

PT = Prospect theory
QRE = Quantal Response Equilibrium
QRE Background

- QRE in games (McKelvey et al, 1995; Weizsäcker, 2003; Yang et al, 2011)
- Model human attacker
- Humans choose better actions at higher frequency
- Noise added to decision/strategy

\[ q_i = \frac{e^{\lambda U_i^a(x)}}{\sum_{j=1}^{n} e^{\lambda U_j^a(x)}} \]

- \( q_i \) = attacker probability
- \( U(x) \) = attacker’s expected utility for target \( x \)
- \( \lambda \) = noise in attacker’s strategy
PASAQ

- Piecewise-linear Approximation of optimal Strategy Against Quantal response algorithm (PASAQ)
- PASAQ faster and provides higher quality strategy

\[
\max_{x,a} \sum_{i=1}^{T} e^{\lambda R_i^a} e^{-\lambda(R_i^a - P_i^d)x_i} \left( (R_i^d - P_i^d)x_i + P_i^d \right) \\
\sum_{i=1}^{T} e^{\lambda R_i^a} e^{-\lambda(R_i^a - P_i^d)x_i} \\
\]

\[
x_i = \sum_{j=1}^{J} a_j A_{ij}, \quad \forall i
\]

\[
\sum_{j=1}^{J} a_j = 1
\]

\[
0 \leq a_j \leq 1, \quad \forall j
\]
Scaling Up

• Graph → Many paths
• Each vertex/patrol area of path has 3 possible actions
• Example: Path of 5 patrol areas = $3^5 = 243$ patrols
• Two Ideas
  – Remove dominated patrols
  – Combine similar patrols
Remove dominated patrols

- 3 Patrol Areas (1, 2, 3); 2 Defender Actions (A, B)
- Payoff(A) > Payoff(B)

<table>
<thead>
<tr>
<th>Patrol #</th>
<th>Patrol Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1,A), (2,A), (3,A), (2,B), (1,B)</td>
</tr>
<tr>
<td>2</td>
<td>(1,B), (2,A), (3,A), (2,B), (1,B)</td>
</tr>
<tr>
<td>3</td>
<td>(1,B), (2,B), (3,A), (2,B), (1,B)</td>
</tr>
</tbody>
</table>

- Patrols 2&3 - dominated
Combine similar patrols

- Same scenario as previous slide, A>B
- Order of targets/actions not impact payoffs
- Represent all 4 patrols as 1 patrol set:
  - \{ (1,A), (2,A), (3,A) \}

<table>
<thead>
<tr>
<th>Patrol #</th>
<th>Patrol Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1,A), (2,A), (3,A), (2,B), (1,B)</td>
</tr>
<tr>
<td>2</td>
<td>(1,B), (2,A), (3,A), (2,B), (1,A)</td>
</tr>
<tr>
<td>3</td>
<td>(1,B), (2,B), (3,A), (2,A), (1,A)</td>
</tr>
<tr>
<td>4</td>
<td>(1,A), (2,B), (3,A), (2,A), (1,B)</td>
</tr>
</tbody>
</table>
Outline

• PROTECT system
• Challenges
• Evaluation
• Future plan
Evaluation

• Simulations in lab
• Expert feedback
• Adversarial team feedback
• Actual before/after data
Robustness Analysis – Observation Noise

![Graph showing the defender's expected utility versus attacker's lambda value for different systems and error conditions.]

- PASAQ ($\lambda=1.5$)
- DOBSS
- PASAQ (error low)
- DOBSS (error low)
- PASAQ (error high)
- DOBSS (error high)
Robustness Analysis – Execution Noise

![Graph showing Defender's Expected Utility vs Attacker λ value]

- **PASAQ (λ=1.5)**
- **DOBSS**
- **PASAQ(error low)**
- **DOBSS(error low)**
- **PASAQ(error high)**
- **DOBSS(error high)**
Robustness Analysis – Payoff Noise

![Graph showing the relationship between defender's expected utility and attacker's lambda value for different strategies and noise levels. The graph includes lines for PASAQ (λ=1.5), DOBSS, PASAQ (noise low), DOBSS (noise low), PASAQ (noise high), and DOBSS (noise high).]
Evaluation – Expert Feedback

- Commander, First Coast Guard District's Operational Excellence Award for the work on the PROTECT project
Evaluation – APT

- APT conducted a pre- and post-PROTECT assessment
- Incorporate adversary’s known intent, capabilities, skills, commitment, resources, and cultural influences
- The effectiveness (in terms of tactical deterrence) increased from the pre- to post-PROTECT observations.
Evaluation – Pre-PROTECT
Evaluation – After PROTECT

Day Trend Analysis (PROTECT)

Patrol Start Finish Point

Count

Patrol 1
Patrol 2
Patrol 3
Patrol 4
Patrol 5
Patrol 6
Patrol 7
Patrol 8
Patrol 9
Outline

• PROTECT system
• Challenges
• Evaluation
• Future plan
Future Work

• Move to New York
• Improved understanding of patrols and behavior at patrol areas
• Include additional attack modes (i.e. Boat Bomb, Swimmer/Diver/Underwater Delivery Systems, Attack by Hijacked Vessel, Sabotage)
• Impact of patrols on deterrence
• Incorporate different assets (aerial)
• Impact of coordination/other gov’t agencies