Game Theory for Security: Key Algorithmic Principles, Deployed Systems, Research Challenges

Milind Tambe
University of Southern California

with:

Current/former PhD students/postdocs: Matthew Brown, Francesco DelleFave, Fei Fang, Benjamin Ford, William Haskell, Albert Jiang, Thanh Nguyen, Yundi Qian, Eric Shieh, Amulya Yadav, Rong Yang, Chao Zhang, Bo An, Manish Jain, Chris Kiekintveld, Rajiv Maheswaran, Janusz Marecki, Praveen Paruchuri, James Pita, Jonathan Pearce, Jason Tsai, Pradeep Varakantham, Zhengyu Yin

Other collaborators: Fernando Ordonez (USC), Richard John (USC), David Kempe (USC), H Jo Albers (Oregon State), Vince Conitzer (Duke), Kevin Leyton-Brown (UBC), Sarit Kraus (BIU, Israel), M. Pechoucek (CTU, Czech R), Ariel Procaccia (CMU), Tuomas Sandholm (CMU), Y. Vorobeychik (Vanderbilt), Martin Short (GATech), Jeff Brantingahm (UCLA), Andrew Lemieux (NCSR)….
Security allocation: (i) Target weights; (ii) Opponent reaction

<table>
<thead>
<tr>
<th></th>
<th>Target1 #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>4, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Target #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>

Adversary
### Game Theory: Security Resource Optimization

**Stackelberg Games**

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

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target #1</strong></td>
<td>4, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td><strong>Target #2</strong></td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Stackelberg Games
Randomization: Increase Cost and Uncertainty to Attackers

- Security allocation: (i) Target weights; (ii) Opponent reaction
- Stackelberg: Security forces commit first
- Optimal allocation: Weighted random
  - Strong Stackelberg Equilibrium

<table>
<thead>
<tr>
<th></th>
<th>Target1 #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>4, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Target #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Research Contributions:
Game Theory for Security

Algorithmic game theory:
- Massive games
- Uncertainty

Behavioral game theory:
- Exploit human behavior models

Deployed security decision-aids

Algorithmic Game Theory in the Field
Applications: Deployed Security Assistants

Ports & port traffic
US Coast Guard

Airports, access roads & flights
TSA, Airport Police

Metro trains (crime)
LA Sheriff’s/TSA

Environmental crime
US Coast Guard & others

- Scale-up: Incremental strategies, marginals
- Uncertainty
- Real-world evaluation

Publications 2007-:
AAMAS, AAAI, IJCAI
Airport Security: Mapping to Stackelberg Games

**ARMOR:** LAX (2007-)

**GUARDS:** TSA (2011)
ARMOR MIP [2007]
Solving for a Single Adversary Type

<table>
<thead>
<tr>
<th>Term #1</th>
<th>Term #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defend#1</td>
<td>2, -1</td>
</tr>
<tr>
<td>Defend#2</td>
<td>-3, 1</td>
</tr>
</tbody>
</table>

\[
\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j \\
\text{s.t. } \sum x_i = 1 \\
\sum q_j = 1
\]

Maximize defender expected utility

Defender strategy

Adversary strategy

\[0 \leq (a - \sum_{i \in X} C_{ij} x_i) \leq (1 - q_j) M\]

Adversary best response

Handling Uncertainty
Solving for a Single Adversary Type

\[ 0 \leq (a - \sum_{i \in X} C_{ij} x_i) \leq (1 - q_j) M \]
**1000 Flights, 20 air marshals: \(10^{41}\) combinations**

- ARMOR out of memory

**Not enumerate all combinations:**

- Branch and price: Incremental strategy generation
Small support set size:
- Many $x_i$ variables zero

$$\max_{x,q} \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j$$

$s.t. \sum_{i} x_i = 1, \sum_{j} q_j = 1$

$$\begin{array}{c}
\sum_{i} x_i = 1, \sum_{j} q_j = 1 \\
x_123 = 0.0 \\
x_124 = 0.239 \\
x_378 = 0.123
\end{array}$$

$$0 \leq (a - \sum_{i \in X} C_{ij} x_i) \leq (1 - \sum_{q_j}) M$$

$$x_i \in [0...1], \quad q_j \in \{0,1\}$$

1000 flights, 20 air marshals:

<table>
<thead>
<tr>
<th>Attack 1</th>
<th>Attack 2</th>
<th>Attack ...</th>
<th>Attack 1001</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,2,3..</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
</tr>
<tr>
<td>1,2,4..</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
</tr>
<tr>
<td>1,3,5..</td>
<td>5,-10</td>
<td>-9,5</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>10^41 rows</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### IRIS: Incremental Strategy Generation

#### Exploit Small Support

<table>
<thead>
<tr>
<th>Master</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack 1</td>
<td>Attack 2</td>
<td>Attack 3</td>
<td>Attack 6</td>
<td></td>
</tr>
<tr>
<td>1,2,4</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
<td>-20,9</td>
</tr>
<tr>
<td>1,2,4</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
<td>-20,9</td>
</tr>
<tr>
<td>3,7,8</td>
<td>-8, 10</td>
<td>-8,10</td>
<td>...</td>
<td>-8,10</td>
</tr>
</tbody>
</table>

#### Slave (LP Duality Theory)

*Best new pure strategy: Minimum cost network flow*

**Converge**

<table>
<thead>
<tr>
<th>攻撃1</th>
<th>攻撃2</th>
<th>攻撃3</th>
<th>攻撃4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,2,4</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
</tr>
<tr>
<td>3,7,8</td>
<td>-8, 10</td>
<td>-8,10</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

**500 rows**

**NOT 10^{41}**
“…in 2011, the Military Operations Research Society selected a USC project with FAMS on randomizing flight schedules for the prestigious Rist Award, the first non-Department of Defense winner in history”

-R. S. Bray (TSA)

Statement before Transportation Security Subcommittee
US House of Representatives 2012
Networks: Mumbai Police Checkpoints [2013] (with Conitzer et al)

- 2 targets; 2 sources
- 108 nodes
- 150 edges

2 Defender resources.
Double Oracle: Large number of defender and attacker actions

<table>
<thead>
<tr>
<th>Path #1</th>
<th>Path #2</th>
<th>Path #3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check #1</strong></td>
<td>5, -5</td>
<td>-1, 1</td>
</tr>
<tr>
<td><strong>Check #2</strong></td>
<td>-5, 5</td>
<td>1, -1</td>
</tr>
</tbody>
</table>

**Defender oracle**

<table>
<thead>
<tr>
<th>Path #1</th>
<th>Path #2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check #1</strong></td>
<td>5, -5</td>
</tr>
<tr>
<td><strong>Check #2</strong></td>
<td>-5, 5</td>
</tr>
</tbody>
</table>

**New checkpoint block attack paths**

\[
\max_{z, \lambda} - \sum_j (1 - z_j) a_j T_{t_j} \\
\text{s.t. } z_j \leq \sum_e A_{je} \lambda_e \\
\sum_e \lambda_e \leq k \\
\lambda_e, z_j \in \{0, 1\} \\
\lambda_e, z_j \in [0, 1]
\]
Double Oracle: Mumbai Police Checkpoints [2013]
Incremental Strategy Generation
Counter-insurgency strategies: Social networks

Cyber networks
Port Security Threat Scenarios

- US Ports: $3.15 trillion economy
- Examples of possible threats

USS *Cole* after suicide attack

Attack on a ferry

French oil tanker hit by small boat
PROTECT: Randomized Patrol Scheduling [2013]
Coordination (Scale-up) and Ferries (Continuous Space/time)
PROTECT: Randomized Patrol Scheduling [2013] Coordination (Scale-up) and Ferries (Continuous Space/time)
Ferries: Scale-up with Mobile Resources & Moving Targets

Transition Graph Representation

A, 15 min
B, 10 min
C, 5 min

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>
Ferries: Scale-up with Mobile Resources & Moving Targets
Transition Graph Representation

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><img src="image" alt="A, 5 min" /></td>
<td><img src="image" alt="A, 10 min" /></td>
<td><img src="image" alt="A, 15 min" /></td>
</tr>
<tr>
<td>B</td>
<td><img src="image" alt="B, 5 min" /></td>
<td><img src="image" alt="B, 10 min" /></td>
<td><img src="image" alt="B, 15 min" /></td>
</tr>
<tr>
<td>C</td>
<td><img src="image" alt="C, 5 min" /></td>
<td><img src="image" alt="C, 10 min" /></td>
<td><img src="image" alt="C, 15 min" /></td>
</tr>
</tbody>
</table>

- **A**, 15 min
- **B**, 10 min
- **C**, 5 min

*Ferry:* Scale-up with Mobile Resources & Moving Targets
Ferries: Scale-up with Mobile Resources & Moving Targets
Patrol Routes

- Patrols protect nearby ferry location
- Solve as in the normal ARMOR program

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

Ferry Patrols protect nearby ferry location
Solve as in the normal ARMOR program
Ferries: Scale-up with Mobile Resources & Moving Targets
Challenges to Scale-up

- $Pr([(B,5), (C,10), (C,15)]) = 0.17$
- $Pr([(A,5), (A,10), (B,15)]) = 0.07$
- $Pr([(B,5), (C,10), (B,15)]) = 0.13$
- $Pr([(A,5), (A,10), (A,15)]) = 0.03$

Exponential numbers of potential routes for patrol boats!
Ferries: Scale-up with Mobile Resources & Moving Targets
Instead of Routes. Marginals Over Segments

- Reason with probability flow over each segment; NOT exponential routes

\[ N^T \text{ variables} \]

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

Ferry
Ferries: Scale-up with Marginals Over Separable Segments

Significant Speedup

Marginals obey flow constraints

\[ N^2T \] variables

\[ N^T \] variables

Extract: \[ \Pr([(B,5), (C, 10), (C,15)]) = 0.17 \]

\[ \Pr([(B,5), (C,10), (B,15)]) = 0.13 \]

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td></td>
<td>0.10</td>
<td>0.03</td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td></td>
<td>0.30</td>
<td>0.13</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
U.S. Coast Guard protects the Staten Island Ferry: I feel safe!

By shortysmom | Posted September 8, 2013 | Staten island, New York
**Ferries: Scale-up with Mobile Resources & Moving Targets**

- Marginals**: Probabilities on “links” separate

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

- Pr\(([(B,5), (C,10), (C,15)]\) = 0.17
- Pr\(([(B,5), (C,10), (B,15)]\) = 0.13

- Marginals Over Segments Exploit Separability

**Ferry Scale-up with Mobile Resources & Moving Targets**
Outline: “Security Games” Research

Scale-up, Uncertainty

Airports
Flights
Roads
Ports
Trains
Environment

2007  2009  2011  2012  2013  2013-

- **Scale-up**: Incremental strategies, marginals
- **Uncertainty**: MDP, Anchor bias, Quantal Response, Learning
- **Real-world evaluation**
TRUSTS: Frequent adversary interaction games
Marginals for Patrols Against Fare Evaders

- Unfortunately, frequent interruptions in patrols
  - Defender action execution uncertainty

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

- 0.10
- 0.30
- 0.13
- 0.17
TRUSTS: Frequent adversary interaction games
Uncertainty in Defender Action Execution

- Markov Decision Problems *in Security games*

- Randomized MDP policies

<table>
<thead>
<tr>
<th></th>
<th>5 min</th>
<th>10 min</th>
<th>15 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A, 5 min</td>
<td>A, 10 min</td>
<td>A, 15 min</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min</td>
<td>B, 10 min</td>
<td>B, 15 min</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

- Transition probabilities:
  - A to A: 0.10
  - A to B: 0.07
  - A to C: 0.03
  - B to A: 0.30
  - B to B: 0.05
  - B to C: 0.10
  - C to A: 0.07
  - C to B: 0.15
  - C to C: 0.05
Urban Transportation Security

**COPS**: LA Metro System (Opportunistic Crime)

- Opportunistic security game (OSG)
- Adaptive adversaries strike repeatedly

**STREETS**: Singapore Roads (Reckless Driving)

- Compact game representation (MDP)
- Exploration versus exploration
### Uncertainty in Adversary Decision: Bounded Rationality *(with S. Kraus)*

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

**Your Rewards:**
- 8  
- 5  
- 3  
- 10 
- 1  
- 3  
- 9  
- 4  

**Your Penalties:**
- -3 
- -2 
- -3 
- -2 
- -3 
- -3 
- -2 
- -3 

**Pirate’s Rewards:**
- 4  
- 3  
- 1  
- 5  
- 1  
- 2  
- 5  
- 2  

**Pirate’s Penalties:**
- -8 
- -10 
- -1 
- -8 
- -1 
- -3 
- -11 
- -5 

Uncertainty in Adversary Decision [2009]
Human subjects: Anchoring and $\varepsilon$-Optimality

**ARMOR:** Outperforms uniform random, similar to Maximin

**COBRA:**

$$\max_{x,q} \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j$$

**Anchoring**

$$s.t. \quad x' = (1 - \alpha) x + \alpha (1 / | X |)$$

**$\varepsilon$-optimality**

$$\varepsilon (1 - q_j) \leq (\alpha - \sum_{i \in X} C_{ij} x'_i) \leq \varepsilon + (1 - q_j) M$$
Quantal Response (QR) Model of Adversary [2011]

Not Maximize Expected Utility [McKelvey & Palfrey, 95]

QR: Stochastic choice, better choice more likely

\[
q_j = \frac{e^{\lambda \cdot (EU_{adversary}(x, j))}}{\sum_{j'=1}^{T} e^{\lambda \cdot (EU_{adversary}(x, j'))}}
\]

Fast algorithms: PASAQ, BLADE
Robustness: Bound loss to defender; Not model attacker via QR

\[ \beta \ast (\text{Adversary’s utility loss if deviates from optimal}) \geq (\text{Defender’s utility loss due to adversary deviation}) \]

Results on 100 games

<table>
<thead>
<tr>
<th></th>
<th>Robust wins</th>
<th>Draw</th>
<th>QR wins</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha = .05 )</td>
<td>42</td>
<td>52</td>
<td>6</td>
</tr>
</tbody>
</table>

Defeating MATCH: Learned subjective utility

\[
q_{j} = \frac{e^{\lambda \cdot \text{SEU}_{\text{adversary}}(x, j)}}{\sum_{j' = 1}^{M} e^{\lambda \cdot \text{SEU}_{\text{adversary}}(x, j')}}
\]

\[
\text{SEU}^{a}(j) = w_{1} \times \text{capture prob} + w_{2} \times \text{attack reward} + w_{3} \times \text{attack penalty}
\]

Results on 22 games

<table>
<thead>
<tr>
<th></th>
<th>SU-QR wins</th>
<th>Draw</th>
<th>Robust</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha = .05 )</td>
<td>13</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

Results against security experts

<table>
<thead>
<tr>
<th></th>
<th>SU-QR wins</th>
<th>Draw</th>
<th>Robust</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha = .05 )</td>
<td>6</td>
<td>13</td>
<td>3</td>
</tr>
</tbody>
</table>
Security Games & Quantal Response
Environmental Crime

Wildlife
Queen Elizabeth National Park
Uganda

Fishery
Gulf of Mexico

Forest
Nakai Nam Theun
Forest Area, Laos

No patrols
Higher density
Lower density
PAWS: Protection Assistant for Wildlife Security
Queen Elizabeth National Park, Uganda

\[ q_j = \frac{e^{\lambda \cdot SEU_{adversary} (x, j)}}{\sum_{j'=1}^{M} e^{\lambda \cdot SEU_{adversary} (x, j')}} \]

\[ SEU_{adversary} (x, j) = w_1 \times capture\ prob\ x \]
\[ + w_2 \times attack\ reward \]
\[ + w_3 \times attack\ penalty \]

- SUQR probabilistic parameters
  - Learn distribution from data
- Adversary heterogeneity
- Anonymous & identified poaching data
- Adaptive Resource allocation strategy
- Testing Spring 2014

64 Targets, 16 security resources
3 Captures, 50 Crimes
Uncertainty Space Algorithms: Bayesian and Robust Approaches

Adversary payoff uncertainty

Payoffs +/- Noise

GMC

BRASS

Adversary observation & defender execution uncertainty

Xi +/- Noise

RECON

URAC

Monotonic Maximin (Monotonic adversary)

Monotonic Maximin

Adversary rationality uncertainty

Bayesian

Robust

Quantal Response

Defender's EU

ISG

RECON

MM

URAC-1

a-URAC-1

#Targets

6

7

8

9

-2.5

-1.5

-0.5

0.5

0.5
How Do We Evaluate Deployed Systems?

Evaluating deployed systems: NOT EASY

- Controlled experiments infeasible; No proof of “100% security”

Are we better off than previous approaches? Humans or “simple random”

1. Simulations (including “machine learning” attacker)
2. Human adversaries in the lab
3. Actual security schedules before vs after
4. “Adversary” teams simulate attack
5. Real-time comparison: human vs algorithm
6. Actual data from deployment
7. Domain expert evaluation (internal and external)
Key Conclusions

- Human schedulers:
  - Predictable patterns, e.g., FAMS (GAO-09-903T), US Coast Guard
  - Scheduling burden

- Simple random (e.g., dice roll):
  - Wrong weights, e.g. officers to sparsely crowded terminals
  - No adversary reactions & enumerate large number of combinations?

Multiple deployments, at multiple years: without us forcing them
1. Models and Simulations: Example from IRIS (FAMS)
3. Actual Security Schedules Before vs After: Example from PROTECT (Coast Guard)

Patrols Before PROTECT: Boston

Patrols After PROTECT: Boston
4. Adversary Perspective Team, Supportive data
   Example from PROTECT

- “Mock attacker” team deployed in Boston
  - Comparing PRE- to POST-PROTECT: “deterrence” improved

- Additional real-world indicators from Boston:
  - POST-PROTECT: Actual reports of illegal activity
  - Boston boaters questions:
    - “..has the Coast Guard recently acquired more boats”
5. Real-Time Competition: Human vs Game Theory
Counter-terrorism patrols on LA Metro Trains

- 90 officers, 23 teams, 10 stations
  - *FAMS, LA Sheriffs, AMTRAK police*

- Human scheduler weaknesses:
  - *Significant effort, Errors in schedules*
  - *Station weights ignored*

- Observer’s report on questions:

![Graph showing average agreement between human and game theory]

**Q1** Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9 Q10 Q11 Q12

**Average Agreement**

**Coverage Time**

- Human
- 45 Minutes

NAI 1 NAI 2 NAI 3 NAI 4 NAI 5 NAI 6 NAI 7 NAI 8 NAI 9 NAI 10
6. Tests in the Real World: Algorithmic Game Theory in the Field

**Controlled**
- Game theory vs Random + human
- 21 days of patrol

**Not controlled**

![Graph showing comparisons between Game Theory and Random + Human in the controlled setting.](image)

![Graph showing data from 2008 to 2012 for various categories such as Total, Miscellaneous, Drugs, and Firearm Violations.](image)
7. Expert Evaluation

Example from ARMOR, IRIS & PROTECT

June 2013: Meritorious Team Commendation from Commandant (US Coast Guard)

July 2011: Operational Excellence Award (US Coast Guard, Boston)

September 2011: Certificate of Appreciation (Federal Air Marshals)

February 2009: Commendations LAX Police (City of Los Angeles)
Summary: Game Theory for Security

Algorithmic game theory

Behavioral game theory

Deployed: PROTECT, ARMOR, IRIS…

Algorithmic Game Theory in the Field
Game Theory for Security: Newer Applications Areas

Software testing
(Kukreja ASE’13)

Privacy audits
(Sinha IJCAI’13)

Random Exam questions
(Li & Conitzer IJCAI’13)

German toll enforcement
(Borndorfer 2012)

Singapore Trains
(Varakantham IAAI’13)
Game Theory for Security:
...just the beginning

tambe@usc.edu
http://teamcore.usc.edu/security

Thank you:
THANK YOU

tambe@usc.edu
http://teamcore.usc.edu/security
1. Models and Simulations: Example from ARMOR (LAX)

ARMOR v/s Non-weighted (uniformed) Random for Canines

- ARMOR: 6 canines
- ARMOR: 5 canines
- ARMOR: 3 canines
- Non-weighted: 6 canines
Evaluation

- Revenue and optimality guarantee

Graphs showing revenue per rider and percentage of upper bound against the number of patrol hours for different colors representing different categories.
Evaluation I: Models “in the lab” II

- ARMOR
- Cyclic Strategy
- Restricted Uniform

Defender Reward

25 Days  50 Days  75 Days  100 Days
Scale up in Security Games: Deployment to Saturation ratio & Hardness (with Leyton-Brown)

**ARMOR Variations**
- Multiple LPs
- DOBSS
- HBGS

**IRIS Variations**
- 400 Schedules
- 500 schedules
- Probability p (400 schedules)
- Probability p (500 schedules)
Robustness – Payoff Noise

![Graph showing the relationship between Defender's Expected Utility and Attacker's λ value](image)

- Blue line: PASAQ(λ=1.5)
- Red line: DOBSS(λ=∞)
- Green line: PASAQ(noise high)
- Orange line: DOBSS(noise high)
Robustness – Observation Noise

Defender's Expected Utility vs. Attacker $\lambda$ value

- PASAQ($\lambda=1.5$)
- DOBSS($\lambda=\infty$)
- PASAQ(noise high)
- DOBSS(noise high)
Robustness – Execution Noise

Defender's Expected Utility vs. Attacker $\lambda$ value

- PASAQ($\lambda=1.5$)
- DOBSS($\lambda=\infty$)
- PASAQ (noise high)
- DOBSS (noise high)
4. Expert Evaluation
ARMOR, IRIS, PROTECT…

“We are satisfied with IRIS and confident in using this scheduling approach.”
James B. Curren, FAMS (2010)

“PROTECT-guided patrols became a source of pride for my boatcrews…. The results have been exceptional,…. “
Rear Admiral Neptun, US Coast Guard (2011)

“LAX is safer today than it was 18 months ago. “
Assistant Chief LAXPD, Erroll Southers, testifying before congressional committee on homeland security: (2008)
Scaling Up Adversary Types [2007]
Problem Decomposition: Type Independence (ARMOR)

<table>
<thead>
<tr>
<th>Term #1</th>
<th>Term #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>5, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Term #1</th>
<th>Term #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4, -2</td>
<td>-1, 0.5</td>
</tr>
<tr>
<td>-4, 3</td>
<td>1.5, -0.5</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\max_{x,q} & \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R_{ij} x_i q_j^l \\
\text{s.t.} & \sum_{i} x_i = 1, \sum_{j} q_j^l = 1 \\
0 & \leq (a^l - \sum_{i \in X} C_{ij} x_i) \leq (1 - q_j^l) M \\
x_i & \in [0...1], q_j^l \in \{0,1\}
\end{align*}
\]
Large Scale Deployment of Game Theoretic Schedules

- 23 Teams / different types (FAMS, Amtrak police, LASD…)
  - Different abilities
  - Coordination
- A schedule was generated for each specific team
- Each team was provided with a handheld
Evaluation (Survey): Preliminary Results

25% Manual
25% Game Theoretic
12 Questions about safety and security at each station
Approximate finite Bayesian Stackelberg game via sampling

Solve the sampled problem using efficient search techniques

Type 1:
- Target 1
- Target 2
- Payoff: 0.500
- Feasible: 0.506

Type 2:
- Target 1
- Target 2
- Target 1
- Target 2
- Payoff: 0.333

Number of Types vs. Runtime (in seconds)

- HUNTER
- HBGS
- DOBSS

Target coverage:
- Covered
- Uncovered

Payoff distribution:
- Target 1
- Payoff range
Uncertainty in Attacker Surveillance [2010]

Stackelberg vs Nash (with Conitzer et al)

- Strong Stackelberg Equilibrium:
  - Defender commits; attacker surveillance

- Mixed Strategy Nash Equilibrium
  - Simultaneous moves; no surveillance

How should a defender compute her strategy?

Security games defender strategies

- NE = Minimax
- SSE
PROTECT: Time spent on acronyms

Erroll’s congress talk: delete intro, add the bit about “worked with our department to create ARMOR”

First civilian honor from USCG from commandant

When introducing ARMOR Pancake, LAX, El AL

I Feel safe URL on ferries?
### Two Insights in ARMOR at LAX
Mapping to Stackelberg Games & Scale-up Challenges

#### Term #1

<table>
<thead>
<tr>
<th>Defend#1</th>
<th>5, -3</th>
<th>-1, 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defend#2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>

#### Term #2

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

**P=0.3**

**P=0.5**

**P=0.2**

<table>
<thead>
<tr>
<th>Defend#1</th>
<th>4, -2</th>
<th>-1, 0.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defend#2</td>
<td>-4, 3</td>
<td>1.5, -0.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Terminal #1</th>
<th>3.3, -2.2</th>
<th>2.3,...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal #2</td>
<td>-3.8, 2.6</td>
<td>...,...</td>
</tr>
</tbody>
</table>

**Previous work**
ARMOR: Scaling Up Adversary Types [2007]
Problem Decomposition via Type Independence

\[
\text{max } x, q \left[ 0.3 \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j \right] + \left[ 0.5 \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j \right] + \left[ 0.2 \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j \right]
\]

s.t.

\[
\sum_{i \in X} x_i = 1
\]

\[
\sum_{j \in Q} q_j = 1
\]

0 ≤ (a^l - \sum_{i \in X} C_{ij}^l x_i) ≤ (1 - q_j^l) M

x_i \in [0...1], q_j^l \in \{0,1\}

P=0.3

\begin{align*}
\text{Term #1} & \quad \text{Term #2} \\
\text{Defend#1} & \quad 5, -3 \quad -1, 1 \\
\text{Defend#2} & \quad -5, 5 \quad 2, -1
\end{align*}

P=0.5

\begin{align*}
\text{Term #1} & \quad \text{Term #2} \\
\text{Defend#1} & \quad 2, -1 \quad -3, 4 \\
\text{Defend#2} & \quad -1 \quad 3, -3
\end{align*}

P=0.2

\begin{align*}
\text{Term #1} & \quad \text{Term #2} \\
\text{Defend#1} & \quad 4, -2 \quad -1, 0.5 \\
\text{Defend#2} & \quad -4, 3 \quad 1.5, -0.5
\end{align*}