Towards a Science of Security Games:
Key Algorithmic Principles, Deployed Systems, Research Challenges

Milind Tambe
Helen N. and Emmett H. Jones Professor in Engineering
University of Southern California

with:

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

Other collaborators:
Fernando Ordonez (USC & U Chile), Richard John (USC), David Kempe (USC), Shaddin Dughmi (USC) &
Craig Boutilier (Toronto), Jeff Brantingahm (UCLA), Vince Conitzer (Duke), Sarit Kraus (BIU, Israel), Andrew Lemieux (NCSR), Kevin Leyton-Brown (UBC), M. Pechoucek (CTU, Czech R), Ariel Procaccia (CMU), Tuomas Sandholm (CMU), Martin Short (GATech), Y. Vorobeychik (Vanderbilt), …
Global Challenges for Security:
Game Theory for Security Resource Optimization
Security allocation:
- Targets have weights
- Adversary surveillance

<table>
<thead>
<tr>
<th>Defender</th>
<th>Target #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>
Example Model: Stackelberg Security Games

Security allocation:
- Targets have weights
- Adversary surveillance

<table>
<thead>
<tr>
<th>Defender</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security allocation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Targets have weights</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Adversary surveillance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adversary</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target #1</strong></td>
<td>4, -3</td>
</tr>
<tr>
<td><strong>Target #2</strong></td>
<td>-5, 5</td>
</tr>
</tbody>
</table>
Example Model: Stackelberg Security Games

Security allocation:
- Targets have weights
- Adversary surveillance

<table>
<thead>
<tr>
<th>Defender</th>
<th>Target #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
Stackelberg Security Games

Security Resource Optimization: Not 100% Security

- Random strategy:
  - Increase cost/uncertainty to attackers
- Stackelberg game:
  - Defender commits to mixed strategy
  - Adversary conducts surveillance; responds
- Stackelberg Equilibrium: Optimal random?

<table>
<thead>
<tr>
<th></th>
<th>Target #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

**Computational game theory:**
- Massive games

**Behavioral game theory:**
- Exploit human behavior models

+ Planning under uncertainty, learning...

**Computational Game Theory in the Field**
Applications: Deployed Security Assistants

Ports & port traffic
US Coast Guard

Airports, access roads & flights
TSA, Airport Police

Urban transport
LA Sheriff’s/TSA
Singapore Police

Environment
US Coast Guard, WWF, WCS…
Decision aids based on computational game theory in daily use
- Optimize limited security resources against adversaries

Applications yield research challenges: Science of security games
- Scale-up: Incremental strategy generation & Marginals
- Uncertainty: Integrate MDPs, Robustness, Quantal response

Current applications (wildlife security): Interdisciplinary challenge
- Global challenges: Merge planning/learning & security games

Research Challenges: Scale-up, Uncertainty

Airports | Flights | Roads | Ports | Trains | Environment

2007 | 2009 | 2011 | 2012 | 2013 | 2013-

Evaluation I: Scale up? Handle uncertainty?

Evaluation II: Real-world deployments
(Patience)

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

ARMOR: LAX (2007)

GUARDS: TSA (2011)

- 6 plots against LAX
ARMOR Operation [2007]  
Generate Detailed Defender Schedule

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

**Mixed Integer Program**

\[ \text{Pr(Canine patrol, 8 AM @ Terminals 2,5,6)} = 0.17 \]
\[ \text{Pr(Canine patrol, 8 AM @ Terminals 3,5,7)} = 0.33 \]

### Canine Team Schedule, July 28

<table>
<thead>
<tr>
<th></th>
<th>Term 1</th>
<th>Term 2</th>
<th>Term 3</th>
<th>Term 4</th>
<th>Term 5</th>
<th>Term 6</th>
<th>Term 7</th>
<th>Term 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 AM</td>
<td>Team1</td>
<td></td>
<td></td>
<td></td>
<td>Team3</td>
<td>Team5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 AM</td>
<td>Team1</td>
<td>Team2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Team4</td>
</tr>
<tr>
<td>10 AM</td>
<td>Team3</td>
<td>Team5</td>
<td>Team2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ARMOR MIP [2007]
Generate Mixed Strategy for Defender

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

\[
\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j
\]

s.t. \[\sum x_i = 1\]

\[\sum q_j = 1\]

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

Maximize defender expected utility

Defender mixed strategy

Adversary response

Adversary best response
ARMOR Payoffs [2007]
Previous Research Provides Payoffs in Security Game Domains

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

\[
\text{Maximize defender expected utility}
\]

\[
\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j
\]
ARMOR MIP [2007]  
Solving for a Single Adversary Type

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

ARMOR...throws a digital cloak of invisibility....
**ARMOR**

8 Terminals

Actions: ~100

---

**IRIS**

1000 flights/day

Complex tours

Actions: \(10^{41}\)

---

- **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:

- Most $x_i$ variables zero

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

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

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

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

$10^41$ combinations

1000 flights, 20 air marshals:

<table>
<thead>
<tr>
<th>Attack 1</th>
<th>Attack 2</th>
<th>Attack ...</th>
<th>Attack 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3</td>
<td>5, 10</td>
<td>4, 8</td>
<td>20, 9</td>
</tr>
<tr>
<td>1, 2, 4..</td>
<td>5, -10</td>
<td>4, -8</td>
<td>... -20, 9</td>
</tr>
<tr>
<td>1, 3, 5..</td>
<td>5, 10</td>
<td>-9, 5</td>
<td>... -20, 9</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

$10^41$ rows
IRIS: Incremental Strategy Generation
Exploit Small Support

Master

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

Slave (LP Duality Theory)

Best new pure strategy:
Minimum cost network flow

Converge:
GLOBAL OPTIMAL

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

500 rows
NOT $10^{41}$
“…in 2011, the Military Operations Research Society selected a University of Southern California project with FAMS on randomizing flight schedules for the prestigious Rist Award…”

-R. S. Bray (TSA)
Transportation Security Subcommittee
US House of Representatives 2012
Networks: Mumbai Police Checkpoints[2013]∗

150 edges; 2 Checkpoints
150-choose-2 strategies

*With V Conitzer
### Double oracle: Converge to a global optimal

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

#### Attacker oracle

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

*With V Conitzer*
Double Oracle[2013]
Incremental Strategy Generation: Exploit Small Support

150 edges; 2 Checkpoints

Only six candidate edges for checkpoints
Mumbai Police Checkpoints[2013]
Results of Scale-up

20416 Roads, 15 checkpoints: 20 min
Social networks: e.g., counter-insurgency

Cyber networks:
Outline: “Security Games” Research
Port Security Threat Scenarios

US Ports: $3.15 trillion economy

USS *Cole* after suicide attack

Attack on a ferry

French oil tanker hit by small boat
PROTECT: Randomized Patrol Scheduling [2013]
Port Protection (Scale-up) and Ferries (Continuous Space/time)
PROTECT: Randomized Patrol Scheduling [2013]
Port Protection (Scale-up) and Ferries (Continuous Space/time)
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>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>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 done in ARMOR

Ferry

Exponential Numbers of Patrol Routes
Ferries: Patrol Routes
Exponential Numbers of Patrol Routes

- Patrons protect nearby ferry location; Solve as done in ARMOR
  - \( \text{Pr}([(B,5), (C,10), (C,15)]) = 0.17 \)
  - \( \text{Pr}([(A,5), (A,10), (B,15)]) = 0.07 \)
  - \( \text{Pr}([(B,5), (C,10), (B,15)]) = 0.13 \)
  - \( \text{Pr}([(A,5), (A,10), (A,15)]) = 0.03 \)

\( N_T \) variables
Ferries: Scale-up
Marginal Probabilities Over Segments

- Variables: NOT routes, but probability flow over each segment

<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

Obtain marginal probabilities over segments

\[ N^2 . T \text{ variables} \]

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 0.10</td>
<td>A, 10 min 0.03</td>
<td>A, 15 min 0.07</td>
</tr>
<tr>
<td>B</td>
<td>B, 5 min 0.30</td>
<td>B, 10 min 0.13</td>
<td>B, 15 min 0.17</td>
</tr>
<tr>
<td>C</td>
<td>C, 5 min</td>
<td>C, 10 min 0.17</td>
<td>C, 15 min</td>
</tr>
</tbody>
</table>

Ferry
I feel safe!

I ride the Staten Island Ferry on a daily basis to and from work. We ferry riders have our own personal protectors in the form of the U.S. Coast Guard. The

U.S. Coast Guard protects the Staten Island Ferry; I feel safe!

Research Challenges:
- Scale-up, Uncertainty
- Environment
- Trains

Evaluation I: Scale up? Handle uncertainty?
Evaluation II: Real-world deployments (Patience)

Airports
Flights
Ports
Roads
Trains
TRUSTS: Frequent adversary interaction games
Patrols Against Fare Evaders

![Diagram showing the interaction between different patrol lengths and fare evaders.](image)
TRUSTS: Frequent adversary interaction
Uncertainty in Defender Action Execution
TRUSTS: Frequent adversary interaction
Uncertainty in Defender Action Execution

Markov Decision Problems in Security games

<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 A, 15 min: 0.03
- B to B, 10 min: 0.05
- B to B, 15 min: 0.10
- C to C, 15 min: 0.15
Urban Transportation Security: MDPs & DEC-MDPs in Security Games

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

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

**DEC-MDPs in Security Games**: Teamwork + Uncertainty
Uncertainty Space Algorithms: Bayesian and Robust Approaches

Adversary payoff uncertainty

Payoff interval; Not point estimate

GMC

BRASS

HUNTER

Adversary observation & defender execution uncertainty

RECON

URAC

Monotonic Maximin (Monotonic adversary)

Adversary rationality uncertainty

Bayesian

Robust

GMC

HUNTER

RECON

URAC

Defender’s EU

0
0.5
1
1.5

5
10

#Targets

ISG RECON URAC
Security Games, Environmental Crime & Bounded Rationality

Wildlife
Queen Elizabeth National Park
Uganda

Nakai Nam Theun
Forest Area, Laos

Fishery
Gulf of Mexico

No patrols
Higher density
Lower density

x
Uncertainty in Adversary Decision: Bounded Rationality
Human Subjects as Poachers

Game 2  Caught!
Total: $1.3 = $1.4 - $0.1

<table>
<thead>
<tr>
<th>Reward if successful</th>
<th>Penalty if caught by rangers</th>
<th>Money earned if successful</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>-1</td>
<td>0.9</td>
</tr>
</tbody>
</table>

Percentage of success

Percentage of failure

End Game
**Uncertainty in Adversary Decision** [2009]  
Human subjects: Anchoring, $\varepsilon$-Optimality*

- **ARMOR:** Outperforms uniform random
- **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

\[
\varepsilon (1 - q_j) \leq (\alpha - \sum_{i \in X} C_{ij} x'_i) \leq \varepsilon + (1 - q_j) M
\]

*With Sarit Kraus*
Quantal Response Model of Adversary [2011]
Not Maximize Expected Utility

Quantal Response: Stochastic choice, better choice more likely

Adversary’s probability of choosing target $j$

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

$$
\max \sum_{j=1}^{T} e^{\lambda \cdot EU_{adversary} (x, j)} = \sum_{j=1}^{T} e^{\lambda \cdot EU_{adversary} (x, j')} = EU_{defend} (x, j)
$$

Subject to:

$$
\sum_{t} x_t = K; \quad 0 \leq x_t \leq 1
$$

Payoff 1  Payoff 2  Payoff 3  Payoff 4

COBRA
ARMOR
### Uncertainty in Adversary Decision [2012]

**Robust vs Modeling Adversaries**

#### Robustness: Bound loss to defender; Not model attacker via QR

<table>
<thead>
<tr>
<th>$\beta$ * (Adversary’s utility loss if deviates from optimal) $&gt;=$ (Defender’s utility loss due to adversary deviation)</th>
</tr>
</thead>
</table>

#### Defeating Robust: Learned subjective utility

$$q_j = \frac{e^{\lambda \cdot SEU^\text{adversary}}(x, j)}{\sum_{j' = 1}^{M} e^{\lambda \cdot SEU^\text{adversary}}(x, j')}$$

$$SEU^a(j) = w_1 \times \text{capture prob} + w_2 \times \text{attack reward} + w_3 \times \text{attack penalty}$$

#### 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>Results</td>
<td>42</td>
<td>52</td>
<td>6</td>
</tr>
</tbody>
</table>

#### 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>Results</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>Results</td>
<td>6</td>
<td>13</td>
<td>3</td>
</tr>
</tbody>
</table>

*With Sarit Kraus*
PAWS: Protection Assistant for Wildlife Security [2014]
Repeated Stackelberg Game

Bayesian SUQR: Heterogeneous Poachers

\[ e^{SEU_i(w_1, w_2, w_3)} \]
\[ \sum_k e^{SEU_k(w_1, w_2, w_3)} \]

Learn from crime data: Improve model

Poachers attack targets
Defender calculates mixed strategy
Defender executes randomized patrols

Simulation

Defender Cumulative Expected Utility

PAWS
MAXIMIN
PAWS Test: April 2014
Trials in Queen Elizabeth National Park

Andrew Lemieux with rangers on PAWS patrol in Uganda

- **Game theory:** Improvement over previous approaches
  - *Previous:* Human schedulers or “simple random”

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulated adversary</td>
<td>Compare real schedules</td>
<td>“Mock attackers”</td>
</tr>
<tr>
<td>Human subject adversaries</td>
<td>Scheduling competition</td>
<td>Capture rates of real adversaries</td>
</tr>
<tr>
<td>Expert evaluation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why Does Game Theory Perform Better?  
Weaknesses of Previous Methods

- Human schedulers:
  - Predictable patterns, e.g., US Coast Guard
  - Scheduling effort & cognitive burden

- Simple random (e.g., dice roll):
  - Wrong weights/coverage, e.g. officers to sparsely crowded terminals
  - No adversary reactions

- Multiple deployments over multiple years: without us forcing them
Lab Evaluation via Simulations: Example from IRIS (FAMS)

Defender Expected utility vs Schedule Size

- Uniform
- Weighted random 1
- Weighted random 2
- IRIS

Schedule Size: 50, 150, 250
Field Evaluation of Schedule Quality: Improved Patrol Unpredictability & Coverage

PROTECT (Coast Guard): *350% increase defender expected utility*

**Patrons Before PROTECT: Boston**

**Patrons After PROTECT: Boston**

- Base Patrol Area

- Count

Day 1  Day 2  Day 3  Day 4  Day 5  Day 6  Day 7
Field Evaluation of Schedule Quality:
Improved Patrol Unpredictability & Coverage for Less Effort

**IRIS for FAMS**: Outperformed expert human over six months
Report: GAO-09-903T

**ARMOR at LAX**: Savings of up to an hour a day in scheduling
Field Evaluation: Human vs Game Theory Competition
Counter-terrorism Patrol Scheduling

- 90 officers on LA Metro Trains

- Humans required significant effort
  - *Worse schedules than game theory*

- Observer’s report on questions:

![Graph showing security scores for humans vs game theory over questions Q1 to Q12. The graph plots security scores on the y-axis ranging from 3 to 5.5, and question numbers on the x-axis from Q1 to Q12. The human scores are represented by blue squares, while the game theory scores are represented by red triangles. The graph shows fluctuations in scores across questions with overall game theory scores usually higher than human scores.]

54/59
“Mock attacker” team deployed in Boston

Comparing PRE- to POST-PROTECT: “deterrence” improved

Additional real-world indicators from Boston:

Boston boaters questions:
“..has the Coast Guard recently acquired more boats”

POST-PROTECT: Actual reports of illegal activity
Field Tests Against Adversaries
Computational Game Theory in the Field

**Controlled**

- Game theory vs Random
- 21 days of patrol
- Identical conditions
- Random + Human

**Not controlled**

- Miscellaneous
- Drugs
- Firearm Violations
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: Security Games

Decision aids based on computational game theory in daily use
- Optimize limited security resources against adversaries

Applications yield research challenges: Science of security games
- Scale-up: Incremental strategy generation & Marginals
- Uncertainty: Integrate MDPs, Robustness, Quantal response

Current applications (wildlife security): Interdisciplinary challenge
- Global challenges: Merge planning/learning & security games
Just the Beginning of “Security Games”….

- Follow on research & applications:
  - Privacy audits (Sinha IJCAI’13)
  - Software testing (Kukreja ASE’13)
  - Sport event security (Yin AAAI’14)
  - Singapore train (Varakantham IAAI’13)
  - Exam questions (Li IJCAI’13)

- Our next steps:
  - Startup: ARMORWAY

Game theory in the field

Thank you to sponsors:
THANK YOU

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