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

Milind Tambe
University of Southern California

Current PhD students/postdocs: Matthew Brown, Francesco DelleFave, Fei Fang, Sahil Garg, William Haskell, Albert Jiang, Thanh Nguyen, Yundi Qian, Eric Shieh, Rong Yang, Chao Zhang

Former PhD students/postdocs: 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(Sandia)
Outline and Plan

- Introduction and tutorial basics (3 minutes)
- Motivation
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Assume:
- Not much or no familiarity with non-cooperative game theory
- Not much with linear programming

Compressing a semester long courses into 3 hours!
- Tradeoffs necessary
- Active area of research: some questions may lead to new research...

Focus on game theory relevant to “security games”

Paper and pencil: We will do some problem solving
Published ~50 papers:

- AAMAS, AAAI, IJCAI, ECAI, IAAI
- JAIR, JAAMAS, AI Journal
- Interfaces, Journal ITM
Outline and Plan

- Introduction and tutorial basics
- Motivation (15 min)
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Motivation: Allocating Limited Security Resources
Many Targets      Few Resources

How to assign limited resources to defend the targets?

Game Theory: Bayesian Stackelberg Games
Game Theory: Stackelberg Games

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

<table>
<thead>
<tr>
<th></th>
<th>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>5, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Target #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Game Theory: Stackelberg Games

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

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Target1</th>
<th>Target2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Target #1</td>
<td>-1, 1</td>
</tr>
<tr>
<td></td>
<td>5, -3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target #2</td>
<td>2, -1</td>
</tr>
<tr>
<td></td>
<td>-5, 5</td>
<td></td>
</tr>
</tbody>
</table>
Game Theory: Stackelberg Games

- 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>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>5, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Target #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Deployed Security Assistants:
Ports, Airports, Port traffic, Air traffic, Trains

**Ports & port traffic**
*Coast Guard (2011-)*

**PROTECT:** Port patrols and Ferry escorts

**Airport & flight**
*TSA, FAMS, LAX PD (2007-)*

**ARMOR:** LAX

**IRIS:** FAMS

**GUARDS:** TSA

**TRUSTS:** Fare evasion

**Metro trains**
*LASD (2013)*
Port Security Threat Scenarios

- US Ports: $3.15 trillion economy
- Examples of possible threats
  - Boat bombs
  - Attack oil tanker
  - Attack on a ferry

USS Cole after suicide attack

Attack on a ferry

French oil tanker hit by small boat
PROTECT: Port Protection Patrols
US Coast Guard

Port of Boston (April 2011)

Port of New York (Feb 2012)

Port of Los Angeles (July 2012)

Next steps: National Deployment
Staten Island Ferry: over 20 million people a year (60,000 passengers a day on weekdays)
ARMOR: Deployed at LAX 2007

- Randomized schedule: (i) target weights; (ii) surveillance
Undercover, in-flight law enforcement

Not enough air marshals:
Allocate air marshals to flights?
Unpredictability, constraints

Massive scheduling problem
~27,000 domestic flights
~2,000 international flights

100 flights, 10 officers:
$1.7 \times 10^{13}$ combinations
TRUSTS: Tactical Randomization for Urban Security in Transit Systems

LA Sheriff’s dept:
- *Ticketless travelers*
- *Crime suppression*
- *Counter terrorism*

*Fare Evasion*  
*Counter-Terrorism*
Other Domains

Global Tiger Initiative

Forest protection

Overfishing

- Customs and Border Protection
- Health supplies check
- Pollution checks
- Robot patrolling
How to assign limited resources to defend the targets?

*Game Theory: Bayesian Stackelberg Games*

*Many important research challenges*
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
  - Introduction to game theory
  - Introduction to security games
  - Introduction to linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Game Theory

- From Economics, but used in law, politics, biology…
- Focus on non-cooperative game theory
John von Neumann
Normal Form Games
(STRATEGIC FORM GAMES)

Problem/game representation:
- List of players, strategies, payoffs
- Simultaneous
- Zero-sum here but not necessary

Solution?

<table>
<thead>
<tr>
<th></th>
<th>Paper</th>
<th>Stone</th>
<th>Scissors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>0, 0</td>
<td>1, -1</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Stone</td>
<td>-1, 1</td>
<td>0, 0</td>
<td>1, -1</td>
</tr>
<tr>
<td>Scissors</td>
<td>1, -1</td>
<td>-1, 1</td>
<td>0, 0</td>
</tr>
</tbody>
</table>
Prisoner’s Dilemma
### Prisoner’s Dilemma

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cooperate</strong></td>
<td>1 month, 1 month</td>
<td>3 years, Free</td>
</tr>
<tr>
<td><strong>Defect</strong></td>
<td>Free, 3 years</td>
<td>1 year, 1 year</td>
</tr>
</tbody>
</table>
## Solution Concept in Strategic Form Games I: Dominance

<table>
<thead>
<tr>
<th></th>
<th>Cooperate</th>
<th>Defect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cooperate</td>
<td>1 month, 1 month</td>
<td>3 years, Free</td>
</tr>
<tr>
<td>Defect</td>
<td>Free, 3 years</td>
<td>1 year, 1 year</td>
</tr>
</tbody>
</table>
Cooperation would be better for both! But, rational for both to defect!

- Game theory: What rational agents would do

Los Angeles
Merril Flood and Melvin Drescher (RAND)
**Apply Dominance Here?**

<table>
<thead>
<tr>
<th></th>
<th>Fight</th>
<th>Don’t Fight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>-500,-500</td>
<td>-300,-1000</td>
</tr>
<tr>
<td>Bob</td>
<td>-1000,-300</td>
<td>100,100</td>
</tr>
</tbody>
</table>
Solution Concept in Strategic Form Games II: Pure Strategy Nash Equilibrium

- No player wants to deviate
- Self-enforcing: stable!
- Mutual best response
- Dominance subset Nash

<table>
<thead>
<tr>
<th></th>
<th>Fight</th>
<th>Don’t Fight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fight</td>
<td>-500, -500</td>
<td>-300, -1000</td>
</tr>
<tr>
<td>Don’t Fight</td>
<td>-1000, -300</td>
<td>100, 100</td>
</tr>
</tbody>
</table>
“Nash’s theory of noncooperative games should now be recognized as one of the outstanding intellectual advances of the twentieth century...comparable to that of the discovery of the DNA double helix in the biological sciences.” Economist Roger Myerson (Nobel)
Chicken

- Payoffs
- Nash Equilibria?
- What if we don’t pick the same one?
<table>
<thead>
<tr>
<th></th>
<th>Fight</th>
<th>Lock</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>6.3</td>
<td>0.5</td>
<td>1.7</td>
</tr>
<tr>
<td>1.7</td>
<td>2.5</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Solution Concept in Strategic Form Games III: Iterated Dominance
Solution Concept in Strategic Form Games III: Iterated Dominance

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alex</strong></td>
<td><strong>Fight</strong></td>
<td><strong>Lock</strong></td>
<td><strong>Help</strong></td>
</tr>
<tr>
<td><strong>Fight</strong></td>
<td>6,3</td>
<td>0,5</td>
<td>1,7</td>
</tr>
<tr>
<td></td>
<td>1,7</td>
<td>2,5</td>
<td>0,6</td>
</tr>
</tbody>
</table>
Solution Concept in Strategic Form Games III: Iterated Dominance

Bob

Fight	Lock	Help

6,3	1,7	

Alex

Fight	Run
### Solution Concept in Strategic Form Games III: Iterated Dominance

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fight</td>
<td>6,3</td>
</tr>
<tr>
<td>Lock</td>
<td>0,5</td>
</tr>
<tr>
<td>Help</td>
<td>1,7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Alex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fight</td>
<td>1,7</td>
</tr>
<tr>
<td>Run</td>
<td>2,5</td>
</tr>
<tr>
<td></td>
<td>0,6</td>
</tr>
</tbody>
</table>
## Matching Pennies

### Pure Strategy Nash Equilibrium?

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heads</td>
<td>1,-1</td>
</tr>
<tr>
<td>Tails</td>
<td>-1,1</td>
</tr>
</tbody>
</table>

Alex's strategy: Heads or Tails

Bob's strategy: Heads or Tails
Solution Concept in Strategic Form Games IV: Mixed Strategy Nash Equilibrium (Randomization)

- Mixed Strategies
- Heads with Probability 0.5
- Tails with Probability 0.5
**COMPUTE** \( P \) **and** \( Q \)

<table>
<thead>
<tr>
<th></th>
<th>( P )</th>
<th>( 1-P )</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fight</strong></td>
<td><strong>Don’t Fight</strong></td>
<td></td>
</tr>
<tr>
<td><code>Q</code></td>
<td>-500,-500</td>
<td>-300,-1000</td>
</tr>
<tr>
<td><code>1-Q</code></td>
<td>-1000,-300</td>
<td>100,100</td>
</tr>
</tbody>
</table>
**COMPUTE $P$ and $Q$**

Alex:

$EU \ (Fight) = P \times -500 \ + \ (1-P) \times -300$

$EU \ (Don’t \ Fight) = P \times -1000 \ + \ (1-P) \times 100$

$\Rightarrow P \times -500 \ + \ (1-P) \times -300 = P \times -1000 \ + \ (1-P) \times 100$

$\Rightarrow P \times 500 \ + \ (1-P) \times -400 = 0$

$\Rightarrow P = 4/9$

<table>
<thead>
<tr>
<th></th>
<th>Alex</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fight</td>
<td>$P$</td>
<td>$1-P$</td>
</tr>
<tr>
<td></td>
<td>$-500,-500$</td>
<td>$-300,-1000$</td>
</tr>
<tr>
<td>Don’t Fight</td>
<td>$-1000,-300$</td>
<td>$100,100$</td>
</tr>
</tbody>
</table>
How many mixed strategy Nash Equilibria in our Fight/No-Fight Game?

- Dominance < Pure strategy < Mixed strategy NE
**Exercise: COMPUTE $P$ and $Q$**

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P</strong></td>
<td></td>
</tr>
<tr>
<td><strong>1-P</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>R</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q</strong></td>
<td>0,0</td>
<td>-700,700</td>
</tr>
<tr>
<td><strong>1-Q</strong></td>
<td>-100,100</td>
<td>200,-200</td>
</tr>
</tbody>
</table>
Row player: play R with probability of 0.3; L with probability of 0.7

\[ EU(R) = Q \times 0 + (1-Q) \times 100 \]
\[ EU(S) = Q \times 700 + (1-Q) \times -200 \]
\[ Q \times 700 = (1-Q) \times 300 \]
\[ Q = 0.3 \]
Why not deviate from the probabilities of a mixed strategy?

- Why stick to P and Q?
Introduction to game theory

Normal form games

Solution concepts:
- Dominance
- Iterated dominance
- Pure strategy Nash equilibria
- Mixed strategy Nash equilibria
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
  - Introduction to game theory
  - Introduction to security games
  - Introduction to linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Stackelberg Game: Non-Simultaneous Moves

- What is the Nash equilibrium if it were a simultaneous move game?
- **What if not simultaneous move game:**
  - Alex [Leader] commits to strategy first
  - Bob [Follower] optimize against leader’s fixed strategy

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alex</strong></td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>2,1</td>
</tr>
<tr>
<td>b</td>
<td>1,0</td>
</tr>
</tbody>
</table>

Nash Equilibrium: <a,c>

What if leader (Alex) commits to “b”
What will be Bob’s response?
Stackelberg Game: Non-Simultaneous Moves

- What if not simultaneous move game:
  - Alex [Leader] commits to strategy first
  - Bob [Follower] optimize against leader’s fixed strategy

**Leader Commitment ➔ payoff: 3.5 > 2**

<table>
<thead>
<tr>
<th></th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alex</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>2,1</td>
</tr>
<tr>
<td>b</td>
<td>1,0</td>
</tr>
</tbody>
</table>

Nash Equilibrium: <a,c>

Leader commits to uniform random strategy { .5,.5 }
Follower plays d:
Leader payoff: 3.5 > 2
Game Theory: Stackelberg Games

- Security allocation: (i) Target weights; (ii) Opponent reaction
- *Stackelberg*: Security forces commit first
  - *Not simultaneous move*

<table>
<thead>
<tr>
<th></th>
<th>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target #1</strong></td>
<td>5, -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>
First mover advantage in Stackelberg Game

- Can commit to mixed strategy
- Not play simultaneous move Nash equilibrium
- “Stackelberg equilibrium”

Heinrich Freiherr von Stackelberg
1905-1946
Stackelberg Security Games

- Two-person game: defender and attacker
- Targets $T = \{t_1, t_2, \ldots, t_n\}$,
- Defender has $m$ resources
Stackelberg Security Games

- Two-person game – defender and attacker
- Targets $T = \{t_1, t_2, \ldots, t_n\}$, Defender has $m$ resources
- Defender has $m$ resources
- Attacker’s action space:
  \[ A = T \]
Stackelberg Security Games

- Two-person game – defender and attacker
- Targets $T = \{t_1, t_2, \ldots, t_n\}$, Defender has $m$ resources
- Defender has $m$ resources
- Attacker’s action space: $A = T$
- Defender’s action space:
  - *Pure strategies*: example $m=2$: $<t_1,t_2>$, $<t_4,t_6>$ ...
  - *Mixed strategy*: $<t_1,t_2>$ probability of 0.5,
    $<t_4,t_6>$ probability of 0.2
    ....
Two-person game – defender and attacker

Targets \( T = \{t_1, t_2, \ldots, t_n\} \), Defender has \( m \) resources

Utilities (Previous slide)

Attacker’s action space: \( A = T \)

Defender’s action space:

- Pure strategies: \( n \)-choose-\( m \) targets; mixed strategy

General defender strategy more complex:

- Schedules, e.g., one resource \( \{t_1, t_3\} \), second \( \{t_2, t_5, t_6\} \)....
- \( \langle \{t_1, t_3\}, \{t_2, t_5, t_6\} \rangle \)
Are security games always zero-sum?

*NO!*

In real domains attackers and defenders often have different preferences

- Weighting casualties, economic consequences, symbolic value, etc.
- Player may not care about the other’s cost (e.g., cost of security, cost of carrying out an attack)

Weaker assumption:

- Attack on a defended target better than attack on the same target if undefended (for the defender)
- Opposite for attackers (attackers prefer to attack undefended targets)
Two-person game: defender and attacker

Targets T = \{t_1, t_2, \ldots, t_n\},

Defender has m resources

Actions covered previous

Utilities

**Attacker:** \( U^c_a(t_i) < U^u_a(t_i) \)

Utility(Covered) < Utility (Uncovered)

**Defender:** \( U^c_d(t_i) > U^u_d(t_i) \)

Utility(Covered) > Utility (Uncovered)

Not zero-sum!

\[
U^c_a(t_i) + U^c_d(t_i) \neq 0
\]

\[
U^u_a(t_i) + U^u_d(t_i) \neq 0
\]
Is This a Stackelberg Security Game?

<table>
<thead>
<tr>
<th></th>
<th>Target #1</th>
<th>Target #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target #1</td>
<td>5, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Target #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Stackelberg Game Model

- Leader(defender): commits to a mixed strategy
- Follower(attacker): chooses strategy after observing defender mixed strategy

Strong Stackelberg Equilibrium (SSE)

- Defender commits to optimal strategy assuming attacker will:
  - Choose best response
  - Break ties in defender’s favor
### Stackelberg Security Games: Towards Compact Representation

**Duplicates**

Adversary

<table>
<thead>
<tr>
<th>Target #1</th>
<th>Target #2</th>
<th>Target #3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target #1</strong></td>
<td>5, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td><strong>Target #2</strong></td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
<tr>
<td><strong>Target #3</strong></td>
<td>-5, 5</td>
<td>-1, 1</td>
</tr>
</tbody>
</table>
Stackelberg Security Games: Towards Compact Representation

What if 4 targets, 2 resources: How many entries?
No two resources on same target

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
<th>T3</th>
<th>T4</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1, T2</td>
<td>5, -3</td>
<td>2, -1</td>
<td>-3,3</td>
<td>-4,4</td>
</tr>
<tr>
<td>T1, T3</td>
<td>5, -3</td>
<td>-1, 1</td>
<td>3,-3</td>
<td>-4,4</td>
</tr>
<tr>
<td>T1, T4</td>
<td>5, -3</td>
<td>-1,1</td>
<td>3,-3</td>
<td>4,-4</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Adversary
### Example Security Game

<table>
<thead>
<tr>
<th></th>
<th>Covered</th>
<th>Uncover</th>
<th>Uncover</th>
<th>cover</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
<td>0</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

\[
4 \times T \quad \text{instead of} \quad \binom{T}{k} \times T
\]
Example: SSG

- 2 Targets
- 2 Resources
- Write down in normal form

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Uncovered</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Example

- 2 Targets
- 2 Resources

<table>
<thead>
<tr>
<th>Covered</th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Uncovered</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Covered</th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>{t_1, t_2}: &lt;1, 1&gt;</td>
<td></td>
</tr>
<tr>
<td>Uncovered</td>
<td>{t_1}: &lt;1, 0&gt;</td>
<td></td>
</tr>
<tr>
<td>Uncovered</td>
<td>{t_2}: &lt;0, 1&gt;</td>
<td></td>
</tr>
<tr>
<td>Uncovered</td>
<td>{}: &lt;0, 0&gt;</td>
<td></td>
</tr>
</tbody>
</table>
Example

- 2 Targets
- 2 Resources

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Uncovered</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${t_1, t_2}$: $&lt;1, 1&gt;$</td>
<td>4, 0</td>
<td></td>
</tr>
<tr>
<td>${t_1}$: $&lt;1, 0&gt;$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${t_2}$: $&lt;0, 1&gt;$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${}$: $&lt;0, 0&gt;$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example

- 2 Targets
- 2 Resources

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Uncovered</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${t_1, t_2}$: &lt;1, 1&gt;</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${t_1}$: &lt;1, 0&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${t_2}$: &lt;0, 1&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>${}$: &lt;0, 0&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example

- 2 Targets
- 2 Resources

<table>
<thead>
<tr>
<th></th>
<th>( t_1 )</th>
<th>( t_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Uncovered</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>( t_1 )</th>
<th>( t_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( { t_1, t_2 } ): (&lt;1, 1&gt;)</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( { t_1 } ): (&lt;1, 0&gt;)</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>( { t_2 } ): (&lt;0, 1&gt;)</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( {} ): (&lt;0, 0&gt;)</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Nash Equilibrium?

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${t_1, t_2}$: $&lt;1, 1&gt;$</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${t_1}$: $&lt;1, 0&gt;$</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>${t_2}$: $&lt;0, 1&gt;$</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${}$: $&lt;0, 0&gt;$</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
**Example**

- Nash Equilibrium?

<table>
<thead>
<tr>
<th></th>
<th>( t_1 )</th>
<th>( t_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {t_1, t_2}: \langle 1, 1 \rangle )</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( {t_1}: \langle 1, 0 \rangle )</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>( {t_2}: \langle 0, 1 \rangle )</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( {}: \langle 0, 0 \rangle )</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

Weakly dominated
Example

Nash Equilibrium?

\(<\{t_1, t_2\}, t_2>\) is a Nash Equilibrium (pure strategy)

Defender’s utility is -1

<table>
<thead>
<tr>
<th>{t_1, t_2}: &lt;1, 1&gt;</th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
</tbody>
</table>

| \{t_1\}: <1, 0>     | \(t_1\) | 4, 0   | \(-2, 3\) |

| \{t_2\}: <0, 1>     | \(t_1\) | 0, 2   | \(-1, 1\) |

| {}: <0, 0>          | \(t_1\) | 0, 2   | \(-2, 3\) |

It is NOT a Stackelberg equilibrium strategy!
Example

- Stackelberg Equilibrium?

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${t_1, t_2}$: $&lt;1, 1&gt;$</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${t_1}$: $&lt;1, 0&gt;$</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>${t_2}$: $&lt;0, 1&gt;$</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${}$: $&lt;0, 0&gt;$</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
**Example**

- Stackelberg Equilibrium?
  - *Commitment so attacker attacks t1*

<table>
<thead>
<tr>
<th></th>
<th>$t_1$</th>
<th>$t_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>${t_1, t_2}$: $&lt;1, 1&gt;$</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${t_1}$: $&lt;1, 0&gt;$</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>${t_2}$: $&lt;0, 1&gt;$</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>${}$: $&lt;0, 0&gt;$</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Example

- Stackelberg Equilibrium?
  - *Commitment so attacker attacks t1*
  - *Could cover t2 at 100%; attacker attacks t1, payoff to defender is 0*

<table>
<thead>
<tr>
<th>Set</th>
<th>t₁</th>
<th>t₂</th>
</tr>
</thead>
<tbody>
<tr>
<td>{t₁, t₂}: &lt;1, 1&gt;</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{t₁}: &lt;1, 0&gt;</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>{t₂}: &lt;0, 1&gt;</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{}: &lt;0, 0&gt;</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Example

- **Stackelberg Equilibrium?**
  - *Commitment so attacker attacks t1*
  - *Could cover t2 at 100%; attacker attacks t1, payoff to defender is 0*
  - *Could we improve defender’s payoff?*

<table>
<thead>
<tr>
<th></th>
<th>( t_1 )</th>
<th>( t_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( {t_1, t_2} ): &lt;1, 1&gt;</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( {t_1} ): &lt;1, 0&gt;</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>( {t_2} ): &lt;0, 1&gt;</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( {} ): &lt;0, 0&gt;</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
**Example**

- **Strong Stackelberg Equilibrium:**
  - **Defender:** defend \( t_1, t_2 \) 50%, \( t_2 \) 50%; defender’s utility is 2
  - **Attacker:** break ties in favor of defender:
    - attack \( t_1 \)

<table>
<thead>
<tr>
<th>Action</th>
<th>( t_1 )</th>
<th>( t_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( t_1, t_2 )</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>( t_1 )</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>( t_2 )</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{}</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Example

Strong Stackelberg Equilibrium:

- Defender: defend \{t_1, t_2\} 50%, \{t_2\} 50%; defender’s utility is 2
- Attacker: break ties in favor of defender: WHY??

attack \(t_1\)

<table>
<thead>
<tr>
<th>({t_1, t_2}): \langle 1, 1 \rangle</th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>({t_1}): \langle 1, 0 \rangle</th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>({t_2}): \langle 0, 1 \rangle</th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>({}): \langle 0, 0 \rangle</th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

Increase \(\{t_2\}\) to 50% + \(\epsilon\)
Example

- Defender: defend\{t_1, t_2\} 50\%, \{t_2\} 50\%;
- Also Nash equilibrium strategy for the defender

<table>
<thead>
<tr>
<th>{t_1, t_2}: &lt;1, 1&gt;</th>
<th>t_1</th>
<th>t_2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{t_1}: &lt;1, 0&gt;</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>{t_2}: &lt;0, 1&gt;</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{}: &lt;0, 0&gt;</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>
Example

- \{t_1, t_2\} 50\%, \{t_2\} 50\%
- Happens to be also a Nash Equilibrium strategy:
- Best responding to attacker’s NE strategy

<table>
<thead>
<tr>
<th></th>
<th>(t_1)</th>
<th>(t_2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>{t_1, t_2}: &lt;1, 1&gt;</td>
<td>4, 0</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{t_1}: &lt;1, 0&gt;</td>
<td>4, 0</td>
<td>-2, 3</td>
</tr>
<tr>
<td>{t_2}: &lt;0, 1&gt;</td>
<td>0, 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td>{}: &lt;0, 0&gt;</td>
<td>0, 2</td>
<td>-2, 3</td>
</tr>
</tbody>
</table>

\(t_2\): attacker’s NE strategy
Uncertainty in Attacker Surveillance
Stackelberg vs Nash

- Defender commits first:
  - Attacker conducts surveillance
  - Stackelberg (SSE)

- Simultaneous move game:
  - Attacker conducts no surveillance
  - Mixed strategy Nash (NE)

How should a defender compute her strategy?

For security games (*):

Set of defender strategies

\[
\text{NE} \supseteq \text{SSE}
\]
Summary: Part II

- Stackelberg games
- Stackelberg Security games (SSG)
- Compact representation
- Strong Stackelberg Equilibrium (SSE)
- SSE vs Nash
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
  - Introduction to game theory
  - Introduction to security games
  - Introduction to linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Operations research: “Abstract programming”

Mathematical program, refers to an optimization problem:

- A set of input variables
- Optimization objective expressed as function of input variables
  - Maximize or minimize
- Set of constraints on input variables, as mathematical functions
Example

Maximize \[ Z = 2x_1 + x_2 \]

Subject to the following constraints or restrictions:

\[ x_1 + x_2 \leq 5 \]
\[ x_2 \geq 2 \]
\[ x_1 \geq 0 \]

Find values of variables: \( x_1 \) & \( x_2 \)
Manufacturing Problem

Resources

- 20000 board-feet wood
- 4000 labor hours
- 2000 ounces glue
- 3000 square feet leather
- 500 square feet of glass

Profit

- $45 per chair
- $80 per table
- $110 per desk
- $55 per bookcase

Chair: 5 Wood, 10 labor hours, 3 glue, 4 leather
Table: 20 wood, 15 labor hours, 8 glue
Desk: 15 wood, 25 labor, 15 glue, 20 leather
Bookcase: 22 wood, 20 labor, 10 glue, 20 glass
A web site for learning about linear programming, with a specific example to solve a maximization problem:

Maximize \( p = 45x + 80y + 110z + 55w \) subject to:
- \( 5x + 20y + 15z + 22w \leq 20000 \)
- \( 10x + 15y + 25z + 20w \leq 4000 \)
- \( 3x + 8y + 15z + 10w \leq 2000 \)
- \( 4x + 20z \leq 3000 \)
- \( 20w \leq 500 \)

The solution provided is:

Optimal Solution: \( p = 146000/7; x = 400/7, y = 1600/7, z = 0, w = 0 \)
Maximize (or minimize) \( c_1 x_1 + c_2 x_2 + \ldots + c_n x_n \) (Objective function)

Subject to constraints:

\[
a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n \sim b_i \quad i=1\ldots m \quad (\text{structural constraints})
\]

\[
x_j \geq 0 \quad j=1\ldots n \quad (\text{non-negativity constraints})
\]

Why is this a LINEAR program?

\( \sim \) refers to either =, \(\leq\) or \(\geq\).
Linear Programming

- Compute maximin solution
- (which is also the) Stackelberg solution
2-person zero-sum game

- Maximin: “Best worst case”
  - *a strategy that maximizes my payoff, assuming my opponent could choose any strategy that minimizes my payoff.*

\[
\arg \max_p \min_q U_1(p, q)
\]

- Minimax: a strategy that minimizes my opponent’s payoff, assuming he could choose any strategy that maximizes his own payoff.

\[
\arg \min_p \max_q U_2(p, q)
\]

- Zero-sum games: Maximin = Minimax
Zero-sum game: Find defender strategy for this security game using linear programming

- Find Maximin
- Reduce defender’s harm the most

<table>
<thead>
<tr>
<th>Defender</th>
<th>T1</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x1</td>
<td>0,0</td>
<td>-700,700</td>
</tr>
<tr>
<td>x2</td>
<td>-100,100</td>
<td>200,-200</td>
</tr>
</tbody>
</table>
Maximin LP

Defender maximizes her value $V$ while opponent tries to minimize $\text{Max } V$

Constraints:
- $x_1 + x_2 = 1$
- $x_1 \geq 0$
- $x_2 \geq 0$
- $\ldots$

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td>x1</td>
<td>0,0</td>
<td>-700,700</td>
</tr>
<tr>
<td>x2</td>
<td>-100,100</td>
<td>200,-200</td>
</tr>
</tbody>
</table>
Maximin LP

Defender maximizes her value $V$ while opponent tries to minimize

- Max $V$
- $x_1 + x_2 = 1$
- $x_1 \geq 0$
- $x_2 \geq 0$

Defender’s expected value if T1 attacked:

- $x_1 \cdot 0 + x_2 \cdot -100$
  - Cannot be $< V$
  - Must be $\geq V$

---

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$x_1$</td>
<td>0,0</td>
<td>-700,700</td>
</tr>
<tr>
<td>$x_2$</td>
<td>-100,100</td>
<td>200,-200</td>
</tr>
</tbody>
</table>
Defender maximizes her value $V$ while opponent tries to minimize

- **Max $V$**
- $x_1 + x_2 = 1$
- $x_1 \geq 0$
- $x_2 \geq 0$
- $x_1 \cdot 0 + x_2 \cdot -100 \geq V$

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>x1</strong></td>
<td>0,0</td>
<td>-700,700</td>
</tr>
<tr>
<td><strong>x2</strong></td>
<td>-100,100</td>
<td>200,-200</td>
</tr>
</tbody>
</table>
Maximin LP

Defender maximizes her value V while opponent tries to minimize

- Max V
- $x_1 + x_2 = 1$
- $x_1 \geq 0$
- $x_2 \geq 0$
- $x_1 \cdot 0 + x_2 \cdot -100 \geq V$
- $x_1 \cdot -700 + x_2 \cdot 200 \geq V$

We find this leads to a solution where $V = -70$. with $x_1 = 0.3$, $x_2 = 0.7$
Defender maximizes her value V while opponent tries to minimize

- Max V
- \( x_1 + x_2 = 1 \)
- \( x_1 \geq 0 \)
- \( x_2 \geq 0 \)
- \( x_1 \times 0 + x_2 \times -100 \geq V \)
- \( x_1 \times -700 + x_2 \times 200 \geq V \)
Defender maximizes her value V while opponent tries to minimize

- **Max V**
  - $x_1 + x_2 = 1$
  - $x_1 \geq 0$
  - $x_2 \geq 0$
  - $x_1 \times 50 + x_2 \times -50 \geq V$
  - $x_1 \times -700 + x_2 \times 200 \geq V$

### Maximin LP: Trial

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>Attacker</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>x1</strong></td>
<td>50, -50</td>
<td>-700, 700</td>
<td></td>
</tr>
<tr>
<td><strong>x2</strong></td>
<td>-50, 50</td>
<td>200, -200</td>
<td></td>
</tr>
</tbody>
</table>

Defender

Attacker
Maxmin LP: Trial

Defender maximizes her value $V$ while opponent tries to minimize

- Max $V$
- $x_1 + x_2 = 1$
- $x_1 \geq 0$
- $x_2 \geq 0$
- $x_1 \cdot 50 + x_2 \cdot -50 \geq V$
- $x_1 \cdot -700 + x_2 \cdot 200 \geq V$

<table>
<thead>
<tr>
<th>T1</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td>50, -50</td>
<td>-700, 700</td>
</tr>
<tr>
<td>-50, 50</td>
<td>200, -200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x1</th>
<th>T1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x2</th>
<th>T2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-25</td>
</tr>
</tbody>
</table>
2-person zero-sum game

- Stackelberg Equilibrium strategy = Maximin(Minimax) strategy
- No leader’s advantage
- Nash Equilibrium = Maximin(Minimax)

ırken <p, q> is a Nash Equilibrium if and only if p and q are Maximin(Minimax) strategies.
Recall Payoffs: Zero Sum?

Are security games always zero-sum?

\textit{NO!}

In real domains attackers and defenders often have different preferences and criteria

- \textit{Weighting casualties, economic consequences, symbolic value, etc.}
- \textit{Player may not care about the other’s cost (e.g., cost of security, cost of carrying out an attack)}
Introduction to linear programming
Maximin
Minimax
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Multiple LPs

LP #1: Attacker attacks T1:
Max \((100 \times x_1 - 100 \times x_2)\)

Constraints:
- \(x_1 + x_2 = 1; x_1 \geq 0; x_2 \geq 0\)
- \(0 \times x_1 + 100 \times x_2 \geq\)
  \(700 \times x_1 - 200 \times x_2\)

LP #2: Attacker attacks T2:
Max \((-700 \times x_1 + 100 \times x_2)\)

Constraints:
- \(x_1 + x_2 = 1; x_1 \geq 0; x_2 \geq 0\)
- \(700 \times x_1 + -200 \times x_2 \geq\)
  \(0 \times x_1 + 100 \times x_2\)
Multiple LPs

LP #1: Attacker attacks T1:
Max \((100*x_1 + -100*x_2)\)
Constraints:
- \(x_1 + x_2 = 1; x_1 \geq 0; x_2 \geq 0\)
- \(0*x_1 + 100*x_2 \geq 700*x_1 + -200*x_2\)

LP #2: Attacker attacks T2:
Max \((-700*x_1 + 100*x_2)\)
Constraints:
- \(x_1 + x_2 = 1; x_1 \geq 0; x_2 \geq 0\)
- \(700*x_1 + -200*x_2 \geq 0*x_1 + 100*x_2\)

Choose max of LP1 and LP2

Works for general Stackelberg games
Finding Stackelberg Equilibria

“Multiple LPs”
Multi-linear programming formulation
Conitzer and Sandholm, 2006

\[
\begin{align*}
\max_{\sigma_1} & \quad \sum_{a' \in A_1} p_1(a') u_1(a', a) \\
\text{s.t.} & \quad \sum_{a' \in A_1} p_1(a') u_2(a', a) \geq \sum_{a' \in A_1} p_1(a') u_2(a', a'') \quad \forall a'' \in A_1 \\
& \quad \sum_{a \in A_1} p_1(a) = 1 \\
& \quad p_1(a) \geq 0 \quad \forall a \in A_1
\end{align*}
\]

The formulation above gives the maximum utility of the leader when the follower chooses action \(a\). The Stackelberg equilibrium is obtained by maximizing over all the possible pure strategies for player two.
Solving for Defender Strategies: Mixed-Integer Programs (DOBSS at LAX)

Maximize defender expected utility
\[
\max \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j
\]

Defender strategy
\[
\sum_{i} x_i = 1
\]

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

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

\[
x_i \in [0...1], q_j \in \{0,1\}
\]
Scale Up in Number of Defender Strategies: Do Not Enumerate All Joint Strategies

FAMS: Joint Strategies or Combinations

100 Flight tours
10 Air Marshals

1.73 x 10^{13}
Schedules: ARMOR out of memory

MARGINALS

100,000,000... x 1000...
**Scale Up in Number of Defender Strategies [2009]**

**Marginals of Mixed Strategies: Target Independence (IRIS)**

**ARMOR: 10 flights, 3 air marshals**

**Payoff duplicates: Depends on target covered**

<table>
<thead>
<tr>
<th>ARMOR Actions</th>
<th>Flight combos</th>
<th>Prob</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,2,3</td>
<td>x123</td>
</tr>
<tr>
<td>2</td>
<td>1,2,4</td>
<td>x124</td>
</tr>
<tr>
<td>3</td>
<td>1,2,5</td>
<td>x125</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>120</td>
<td>8,9,10</td>
<td>...</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{max } & \sum_{x,q} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R^l x_i q_j^l \\
\text{s.t. } & x_1, x_2, \ldots, x_{120} = 1, \\
& \sum_{j \in Q} q_j^l = 1, \\
& 0 \leq \sum_{i \in X} C^l_{ij} x_i \leq (1 - q_j^l) M, \\
& x_i \in [0\ldots1], q_j^l \in \{0,1\} \\
\end{align*}
\]

**“Marginals”: 10 variables in MIP:**

- \( y_1 = x_{123} + x_{124} + x_{125} \ldots \)
- \( y_1 + y_2 + y_3 \ldots = 3 \)
- \( \text{Sample } y \) (loses combination info)
ARMOR: 10 flights, 3 air marshals

<table>
<thead>
<tr>
<th>ARMOR Actions</th>
<th>Flight combos</th>
<th>Prob</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,2,3</td>
<td>x123</td>
</tr>
<tr>
<td>2</td>
<td>1,2,4</td>
<td>x124</td>
</tr>
<tr>
<td>3</td>
<td>1,2,5</td>
<td>x125</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>120</td>
<td>8,9,10</td>
<td>...</td>
</tr>
</tbody>
</table>

Payoff duplicates: Depends on target covered

<table>
<thead>
<tr>
<th>Attack 1</th>
<th>Attack 2</th>
<th>Attack ...</th>
<th>Attack 6</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>

“Marginals”: 10 variables in MIP:

Sample y (loses combination info)

Sampling difficult if constraints on combinations; interacting tours
### ORIGAMI

<table>
<thead>
<tr>
<th></th>
<th>t1</th>
<th>t2</th>
<th>t3</th>
<th>t4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cover</td>
<td>Uncov</td>
<td>Cover</td>
<td>Uncov</td>
</tr>
<tr>
<td>Defender’s utility</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Attacker’s utility</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Assume no scheduling constraints of return flights etc
Four flights
One marshal

Attacker payoffs

<table>
<thead>
<tr>
<th>Uncovered</th>
<th>Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
ORIGAMI

**Attack Set:**
Set of targets with maximal expected payoff for the attacker

Coverage Probability

<table>
<thead>
<tr>
<th>Flight 4</th>
<th>Flight 3</th>
<th>Flight 2</th>
<th>Flight 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Observation 1
It never benefits the defender to add coverage outside the attack set.
Compute coverage necessary to make attacker indifferent between 3 and 4

\[(1-x) \times 4 + x \times 0 = 3\]

\[X = 0.25\]

Coverage Probability
ORIGAMI

Compute coverage necessary to make attacker indifferent between 3 and 4

\[(1-x) \times 4 + x \times 0 = 3\]

\[X = 0.25\]
Observation 2
It never benefits the defender to add coverage to a subset of the attack set.
ORIGAMI

\[(1-x) \times 4 + x \times 0 = 2\]

\[(1-y) \times 3 + y \times 0 = 2\]

\[x = 0.5\]

\[y = 0.33\]
Coverage Probability

<table>
<thead>
<tr>
<th>Flight 4</th>
<th>Flight 3</th>
<th>Flight 2</th>
<th>Flight 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>0.33</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
ORIGAMI

Coverage Probability

<table>
<thead>
<tr>
<th>Flight 4</th>
<th>Flight 3</th>
<th>Flight 2</th>
<th>Flight 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.75</td>
<td>0.66</td>
<td>0.5</td>
<td>0</td>
</tr>
</tbody>
</table>

Need more than one air marshal!
Coverage Probability

<table>
<thead>
<tr>
<th>Flight 4</th>
<th>Flight 3</th>
<th>Flight 2</th>
<th>Flight 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>0.33</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Can still assign 0.17
Allocate all remaining coverage to flights in the attack set

Fixed ratio necessary for indifference

<table>
<thead>
<tr>
<th>Flight 4</th>
<th>Flight 3</th>
<th>Flight 2</th>
<th>Flight 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.54</td>
<td>0.38</td>
<td>0.08</td>
<td>0</td>
</tr>
</tbody>
</table>

Coverage Probability
## ORIGAMI

<table>
<thead>
<tr>
<th></th>
<th>T1</th>
<th>T2 (0.08)</th>
<th>T3 (0.38)</th>
<th>T4 (0.54)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cover</td>
<td>Uncov</td>
<td>Cover</td>
<td>Uncov</td>
</tr>
<tr>
<td><strong>Defender’s utility</strong></td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td><strong>Attacker’s utility</strong></td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

SSE attacker action: ?  
0.54 * 5 vs 0.38 * 7 vs 0.08 * 3

**T4**
### ORIGAMI

- Four flights
- Two marshals

<table>
<thead>
<tr>
<th></th>
<th>t1</th>
<th>t2</th>
<th>t3</th>
<th>t4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cover</td>
<td>Uncov</td>
<td>Cover</td>
<td>Uncov</td>
</tr>
<tr>
<td>Defender’s utility</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Attacker’s utility</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Assume no scheduling constraints of return flights etc.
ORIGAMI

Four flights
Two marshals

Attacker payoffs

<table>
<thead>
<tr>
<th></th>
<th>Uncovered</th>
<th>Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight 4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Flight 3</td>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>Flight 2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Flight 1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Coverage Probability
Equations

0\*x + (1-x) \* 4 = 

-1\*y + (1-y) \* 3 = 

0\*z + (1-z) \* 2 = 1

4-4x=1 \Rightarrow x = 3/4

3-4y=1 \Rightarrow y = 1/2

2-2z=1 \Rightarrow z = ½

x + y + z = 1.75 < 2; therefore can allocate at least x, y, z.
Equations

YOU SOLVE using ORIGAMI

EQUATIONS?

x' y' z' w'
0*x’ + (1-x’) * 4 = 
-1*y’ + (1-y’) * 3 = 
0*z’ + (1-z’) * 2 = 
0*w’ + (1-w’) * 1

x’+y’+z’+w’=2

x =0.78125...
0*x’ + (1-x’) * 4 = 
-1*y’ + (1-y’) * 3 = 
0*z’ + (1-z’) * 2 = 
0*w’ + (1-w’) * 1 

x’+y’+z’+w’=2

→ x’, y’, z’, w’ are marginal coverages of t4,t3,t2,t1
→ Need to sample 2 targets at a time (2 resources)
→ Sample (t4,t3), (t4,t2), (t4, t1)
Equations

\[0 \times x' + (1-x') \times 4 = \]
\[-1 \times y' + (1-y') \times 3 = \]
\[0 \times z' + (1-z') \times 2 = \]
\[0 \times w' + (1-w') \times 1 = \]

\[x' + y' + z' + w' = 2\]

→ Sample (t4, t3), (t4, t2), (t4, t1)...

*Sampling difficult if constraints on combinations; interacting tours*
Sampling Schedules

Given optimal coverage probabilities for the defender

• How can we construct a sample of joint schedules that implements these probabilities?
• If resources are identical, we can use a simple algorithm
Sampling Joint Schedules

Coverage
Target 1 0.10
Target 2 0.70
Target 3 0.60
Target 4 0.90
Target 5 0.80
Sampling Joint Schedules

Coverage
Target 1 0.10
Target 2 0.70
Target 3 0.60
Target 4 0.90
Target 5 0.80
ERASER

Max Defender Payoff

\[ \max \quad d \quad \text{(5)} \]

Attacker Strategy

\[ a_t \in \{0, 1\} \quad \forall t \in T \quad \text{(6)} \]

Definition

\[ \sum_{t \in T} a_t = 1 \quad \text{(7)} \]

Defender Strategy

\[ c_t \in [0, 1] \quad \forall t \in T \quad \text{(8)} \]

Definition

\[ \sum_{t \in T} c_t \leq m \quad \text{(9)} \]

Best Responses

\[ d - U_\Theta(t, C) \leq (1 - a_t) \cdot Z \quad \forall t \in T \quad \text{(10)} \]

\[ 0 \leq k - U_\Psi(t, C) \leq (1 - a_t) \cdot Z \quad \forall t \in T \quad \text{(11)} \]
Example
Four flights
One marshal

Assume no scheduling constraints of return flights etc

<table>
<thead>
<tr>
<th></th>
<th>t1</th>
<th>t2</th>
<th>t3</th>
<th>t4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cover</td>
<td>Uncov</td>
<td>Cover</td>
<td>Uncov</td>
</tr>
<tr>
<td>Defender’s utility</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Attacker’s utility</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>
\[
\max d \\
a_1, a_2, a_3, a_4 \in \{0, 1\} \\
a_1 + a_2 + a_3 + a_4 = 1 \\
c_1, c_2, c_3, c_4 \in [0, 1] \\
c_1 + c_2 + c_3 + c_4 = 1 \\
\forall a (1) = 1 \times c_1 + 0 \times (1 - c_1) \\
\forall a (2) = 0 \times c_1 + 1 \times c_2 \\
\forall a (3) = 7 \times c_2 \\
\forall a (4) = 5 \times c_4 \\
\forall d - \forall a (1) \leq (1 - a_1) \times 2 \\
\forall d - \forall a (2) \leq (1 - a_2) \times 2 \\
\forall d - \forall a (3) \leq (1 - a_3) \times 2 \\
\forall d - \forall a (4) \leq (1 - a_4) \times 2 \\
\forall k - \forall a (1) \geq 0 \\
\forall k - \forall a (2) \geq 0 \\
\forall k - \forall a (3) \geq 0 \\
\forall k - \forall a (4) \geq 0 \\
k - \forall a (1) \leq (1 - a_1) \times 2 \\
k - \forall a (2) \leq (1 - a_2) \times 2 \\
k - \forall a (3) \leq (1 - a_3) \times 2 \\
k - \forall a (4) \leq (1 - a_4) \times 2
\]
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>d</strong></td>
<td>2.692308</td>
<td>2.692308</td>
<td>Ud(1)</td>
<td>0</td>
</tr>
<tr>
<td>a1</td>
<td>0</td>
<td></td>
<td>Ud(2)</td>
<td>0.230769</td>
</tr>
<tr>
<td>a2</td>
<td>0</td>
<td></td>
<td>Ud(3)</td>
<td>2.692308</td>
</tr>
<tr>
<td>a3</td>
<td>1</td>
<td></td>
<td>Ud(4)</td>
<td>2.692308</td>
</tr>
<tr>
<td>a4</td>
<td>0</td>
<td></td>
<td>Ua(1)</td>
<td>1</td>
</tr>
<tr>
<td>c1</td>
<td>0</td>
<td></td>
<td>Ua(2)</td>
<td>1.846154</td>
</tr>
<tr>
<td>c2</td>
<td>0.076923</td>
<td></td>
<td>Ua(3)</td>
<td>1.846154</td>
</tr>
<tr>
<td>c3</td>
<td>0.384615</td>
<td></td>
<td>Ua(4)</td>
<td>1.846154</td>
</tr>
<tr>
<td>c4</td>
<td>0.538462</td>
<td></td>
<td>k</td>
<td>1.846154</td>
</tr>
<tr>
<td>SUMa</td>
<td>1</td>
<td></td>
<td>d-Ud(1)</td>
<td>2.692308</td>
</tr>
<tr>
<td>SUMc</td>
<td>1</td>
<td></td>
<td>d-Ud(2)</td>
<td>2.461538</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>d-Ud(3)</td>
<td>6.85E-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>d-Ud(4)</td>
<td>1.59E-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>k-Ua(1)</td>
<td>0.846154</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>k-Ua(2)</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>k-Ua(3)</td>
<td>4.54E-13</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>k-Ua(4)</td>
<td>0</td>
</tr>
</tbody>
</table>
IRIS Speedups: Efficient Algorithms II

Scaling with Targets: Compact

<table>
<thead>
<tr>
<th>Targets</th>
<th>Runtimes (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>0.5</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>1.5</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>2.5</td>
</tr>
<tr>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>17</td>
<td>3.5</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>4.5</td>
</tr>
<tr>
<td>20</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Targets</th>
<th>Runtimes (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4.74s</td>
</tr>
<tr>
<td>11</td>
<td>0.09s</td>
</tr>
<tr>
<td>12</td>
<td>1.57s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>Actions</th>
<th>ARMOR Runtime</th>
<th>IRIS Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAMS Ireland</td>
<td>6,048</td>
<td>4.74s</td>
<td>0.09s</td>
</tr>
<tr>
<td>FAMS London</td>
<td>85,275</td>
<td>----</td>
<td>1.57s</td>
</tr>
</tbody>
</table>
ERASER PROBLEMS?

- Only one target at a time
- If extend to multiple targets with complex schedules, runs into problems
Example: Consider a FAMS game with 5 targets (flights), $T = \{t_1, \ldots, t_5\}$, and three marshals of the same type, $r_1 = 3$. Let the set of feasible schedules be $S_1 = \\{\{t_1, t_2\}, \{t_2, t_3\}, \{t_3, t_4\}, \{t_4, t_5\}, \{t_1, t_5\}\}$. The set of feasible joint schedules is shown below, where column $J_1$ represents the joint schedule $\\{\{t_1, t_2\}, \{t_3, t_4\}\}$.

$$
P = \begin{bmatrix}
J_1 & J_2 & J_3 & J_4 & J_5 \\
\hline
t_1 : & 1 & 1 & 1 & 1 & 0 \\
t_2 : & 1 & 1 & 1 & 0 & 1 \\
t_3 : & 1 & 1 & 0 & 1 & 1 \\
t_4 : & 1 & 0 & 1 & 1 & 1 \\
t_5 : & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
$$

Only two air marshals can be legally used; third one remains unused

Defender: Covered: 1, Uncovered: -5

Attacker: Covered -1, Uncovered: 5
Optimal Strategy

- Defender Uniformly covers J1, J2, J3, J4, J5
- $<0.2, 0.2, 0.2, 0.2, 0.2>$
- Coverage vector = $<0.8, 0.8, 0.8, 0.8, 0.8>$
  - 0.8 coverage of each flight
- ERASER-c answer: $<1,1,1,1,1>$
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Game Theory for Security: Research Challenges

Research challenges

- Scale-up:

- Uncertainty
Research challenges

- **Scale-up:**
  - Defender actions (e.g., 100 flights, 10 FAMS)
  - Adversary actions (e.g., attacking a city)
  - Adversary types

- **Uncertainty:**
  - Adversary decision (bounded rationality),
  - Adversary surveillance
  - Adversary payoff
  - Adversary capabilities...
Deployed real world applications

**Research challenges**

- **Scale-up:**
  - Defender actions (e.g., 100 flights, 10 FAMS)
  - Adversary actions (e.g., attacking a city)
  - Adversary types

- **Key ideas:**
  - **Problem decomposition:** Type independence
  - **Marginals for mixed strategies:** Target independence
  - **Column-generation/Double-oracle:** Small support

- **Uncertainty....**
Scaling Up Adversary Types

Previous Work

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

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

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

P=0.3

Harsanyi Transformation

Previous Linear Programming Techniques
Scaling Up Adversary Types [2007]
Problem Decomposition: Type Independence (ARMOR)

\[ \text{max}_{x,q} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R_{ij} x_i q_j^l \]

s.t. \( \sum_{i} x_i = 1 \), \( \sum_{j \in Q} q_j^l = 1 \)

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

\( x_i \in [0...1] \), \( q_j^l \in \{0,1\} \)
Scaling Up Adversary Types [2007]
Problem Decomposition: Type Independence (ARMOR)

\[
\text{max}_{x, q} \sum_{l} \sum_{j \in Q} \sum_{l} p^{l} R_{ij} x_{i} q_{j}^{l}
\]

\[
0 \leq (a^{l} - \sum_{i \in X} C_{ij}^{l} x_{i}) \leq (1 - q_{j}^{l}) M
\]

\[
x_{i} \in [0...1], q_{j}^{l} \in \{0,1\}
\]
Scaling Up Adversary Types [2007]
Problem Decomposition: Type Independence (ARMOR)

### Problem Formulation

**Objective Function:**

\[
\max_{x,q} \left[ 0.3 \sum \sum R_{ij}^1 x_i q_j^1 + 0.5 \sum \sum R_{ij}^2 x_i q_j^2 + 0.2 \sum \sum R_{ij}^3 x_i q_j^3 \right]
\]

**Subject to:**

\[
\sum x_i = 1
\]

\[
\sum q_j^1 = 1
\]

\[
\sum q_j^2 = 1
\]

\[
\sum q_j^3 = 1
\]

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

---

### Table

<table>
<thead>
<tr>
<th>Term #1</th>
<th>Term #2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Term 1</strong></td>
<td><strong>Term 2</strong></td>
</tr>
<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><strong>Term 1</strong></td>
<td><strong>Term 2</strong></td>
</tr>
<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><strong>Term 1</strong></td>
<td><strong>Term 2</strong></td>
</tr>
<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>

**Parameters:**

- \(P = 0.3\)
- \(P = 0.5\)
- \(P = 0.2\)
ARMOR: Run-time Results

- Multiple LPs (Conitzer & Sandholm’06)
- MIP-Nash (Sandholm et al’05)
- Sufficient for LAX
Scale Up in Number of Defender Strategies: Do Not Enumerate All Joint Strategies

<table>
<thead>
<tr>
<th>Strategy 1</th>
<th>Strategy 2</th>
<th>Strategy 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>784 x 512</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FAMS: Joint Strategies or Combinations

100 Flight tours
10 Air Marshals

1.73 x 10^{13} Schedules:
ARMOR out of memory

Two key ideas
- Marginals (IRIS I & II)
- Branch and price (IRIS III)
Many $x_i$ variables zero!
Support set is small

<table>
<thead>
<tr>
<th></th>
<th>Attack 1</th>
<th>Attack 2</th>
<th>Attack ...</th>
<th>Attack 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1,2,3$</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>$1,3,5$</td>
<td>$5,-10$</td>
<td>$-9,5$</td>
<td>...</td>
<td>$-20,9$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$x_{123}=0.0$</td>
<td>$x_{124}=0.239$</td>
<td>$x_{135}=0.0$</td>
<td>$x_{378}=0.123$</td>
<td>$x_n=0$</td>
</tr>
</tbody>
</table>

$1.7 \times 10^{13}$ rows
Scale Up in Number of Defender Strategies: LP Duality for Small Support Set (IRIS III)

<table>
<thead>
<tr>
<th>Attack 1</th>
<th>Attack 2</th>
<th>Attack ...</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>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-8,10</td>
</tr>
</tbody>
</table>

Minimum cost network flow; **Best New Pure Strategy**

“Slave” Problem

![Network diagram with nodes and edges representing resource, targets, and sink]

500 rows

NOT $10^{13}$
IRIS Results

Comparison (200 Targets, 10 Resources)

Runtime (in secs) [log-scale]

- IRIS II
- B&P
- IRIS III

Number of Schedules

ARMOR
Runs out of memory
**Double oracle**: Small support of mixed strategies

---

**Generate mixed strategy solution**

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

---

**Defender best response**

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

**Attacker best response**
Deployed real world applications

**Research challenges**

- **Scale up**
- **Uncertainty**
  - Adversary decision (bounded rationality), Adversary surveillance, Adversary payoffs, capabilities…

**Key ideas:**

- **Anchoring bias**: Limited surveillance
- **Quantal response model**: Bounded rationality
- **Efficient pruning for bayesian games**: Payoffs
- **Equilibrium refinement**: Capability
<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<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>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>3</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>-3</td>
<td>-2</td>
<td>-3</td>
<td>-2</td>
<td>-3</td>
<td>-3</td>
<td>-2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>-8</td>
<td>-10</td>
<td>-1</td>
<td>-8</td>
<td>-1</td>
<td>-3</td>
<td>-11</td>
</tr>
</tbody>
</table>

**Your Rewards:**

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-2</td>
<td>-3</td>
<td>-3</td>
<td>-2</td>
<td>-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-8</td>
<td>-1</td>
<td>-3</td>
<td>-11</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Your Penalties:**

**Pirate’s Rewards:**

**Pirate’s Penalties:**
178 total subjects, 2480 trials, 40 subjects for each setting

Four reward structures, four observation conditions

**DOBSS**: Outperforms uniform random, similar to Maximin
COBRA:

“epsilon optimality”

Anchoring bias: Full observation vs no observation: $\alpha$

Choosing $\alpha$ (even for unlimited observations?)

$$\max_{x, q} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R^l_{ij} x_i q^l_j$$

s.t. $x' = (1 - \alpha) x + \alpha (\mathbb{I}(X | x))$

$$\varepsilon (1 - q^l_j) \leq (a^l - \sum_{i \in X} C^l_{ij} x'_i) \leq \varepsilon + (1 - q^l_j) M$$

No observation: $\alpha = 1$

Full observation: $\alpha = 0$
Addressing Bounded Rationality

- Standard assumption: Attacker perceives any $\varepsilon$-difference in utility and plays utility maximizing strategy.

\[ \text{EU}^\psi(t_2) \geq \text{EU}^\psi(t_1) + \varepsilon \]
\[ \text{EU}^\psi(t_2) \geq \text{EU}^\psi(t_3) + \varepsilon \]

Here $\varepsilon \approx 0$
Addressing Bounded Rationality

- Standard assumption: Attacker perceives any $\varepsilon$-difference in utility and plays utility maximizing strategy.

Attacker chooses $t_2$ and defender receives 2.31
Addressing Bounded Rationality

- Humans may not perceive such minor differences

Attacker chooses $t_3$ and defender receives .23 instead of 2.31
Addressing Bounded Rationality

Solution: Enforce a human perceivable $\varepsilon$- difference

- Set $\varepsilon = 1$ and resolve

Now target $t_1$ is at least 1 unit of utility better than $t_3$ or $t_4$ for the attacker.

If more than 1 target is within $\varepsilon$ of the optimal target, maximize the worst case outcome between them.
Uncertainty: Human Bounded Rationality and Observations

**COBRA:**
- “epsilon optimality”
- Anchoring bias: Full observation vs no observation: $\alpha$

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

**s.t.**
$$x' = (1 - \alpha) x + \alpha (1/ |X|)$$
$$\varepsilon (1 - q_j^l) \leq (\alpha^l - \sum_{i \in X} C_{ij}^l x'_i) \leq \varepsilon + (1 - q_j^l) M$$
Quantal Response Equilibrium

- Error in individual’s response
  - *Still: more likely to select better choices than worse choices*
- Probability distribution of different responses
- Quantal best response:
  \[ q_j = \frac{e^{\lambda U(j,x)}}{\sum_{k=1}^{M} e^{\lambda U(k,x)}} \]

- \( \lambda \): represents error level (=0 means uniform random)
  - *Maximal likelihood estimation* (\( \lambda=0.76 \))
Optimal Strategy against QR

Solve the Nonlinear optimization problem

\[
\max_x \frac{\sum_{j \in Q} \sum_{i \in X} x_i R_{ij} \cdot \prod_{l \in X} e^{\lambda C_{lj} x_l}}{\sum_{k \in Q} \prod_{l \in X} e^{\lambda C_{lk} x_l}}
\]

s.t. \[\sum_{i \in X} x_i \leq \text{Total Resource}\]
\[0 \leq x_i \leq 1, \quad \forall i \in X\]
Subjects are given $8 as the starting budget

For each point they gain, $0.1 real money is paid
Experiment Setting

- 7 payoff structures
  - 4 new, 3 from previous tests with COBRA

- 5 strategies for each payoff structure
  - New methods: BRPT, RPT and BRQR
  - Leading contender: COBRA
  - Perfect rational baseline: DOBSS

- Subjects play all games (randomized orders)
- No feedback until subject finishes all games
Average Defender Expected Utility

Payoff 5  Payoff 6  Payoff 7

-3  -2.5  -2  -1.5  -1  -0.5  0  0.5  1  1.5  2  2.5  3

BRPT  RPT  BRQR  COBRA  DOBSS
BRQR outperforms DOBSS in all 7 payoffs

In payoff 1, 3 and 4, the result is statistically significant

BRQR outperforms COBRA in all 7 payoffs

In payoff 2, 3 and 4, the result is statistically significant
Uncertainty in Adversary Decision [2012]

MATCH

**Builds on QR, exploiting security game structure:**

- Like QR: Adversary response error; better choice more likely
- Bound loss to defender on adversary deviation

\[ \beta \cdot (U^a(q, x) - U^a(\hat{q}, x)) \geq \gamma - U^d(\hat{q}, x) \]

Results on 100 games

<table>
<thead>
<tr>
<th></th>
<th>MATCH 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>
Optimize against an adversary who responds according to QR

- $\lambda = .75$

*Target 4 is a penalty of -9.5*
Optimize against an adversary who responds according to QR

- \( \lambda = .75 \)

*Target 4 is a penalty of -9.5
QR vs MATCH

- Optimize against an adversary who responds according to QR
- $\lambda = .75$

Defender receives utility:
\[ \sum EU(t_i) p_i \]

\[ .64 \times (-0.4) + .22 \times (-0.5) + .10 \times (-2.2) + .04 \times (-9.5) = -0.966 \]

*Target 4 is a penalty of -9.5*
If the choice distribution is incorrect then the result can be bad.

Defender receives utility:
\[ \sum EU(t_i) p_i \]
\[ .60 \times (-0.4) + .15 \times (-0.5) + .15 \times (-2.2) + .10 \times (-9.5) = -1.595 \]

*Target 4 is a penalty of -9.5
The SUQR Model

- **Performance**: MATCH significantly outperforms QR-based BRQR
- **Hypothesis**: classic QR integrated with expected value does not well capture the human adversary’s decision-making

**The Quantal Response model (QR)**

- The adversary response:
  \[
  q_t = \frac{e^{R_t^A x_t + P_t^A (1 - x_t)}}{\sum_{t=1}^T e^{R_t^A x_t' + P_t^A (1 - x_t')}}
  \]
- Key parameters:

**Subjective utility function**

\[
\hat{U}_t^A = w_1 x_t + w_2 R_t^A + w_3 P_t^A
\]

**The SUQR model**: a novel integration of QR and subjective utility

- The adversary response:
  \[
  q_t = \frac{e^{(w_1 x_t + w_2 R_t^A + w_3 P_t^A)}}{\sum_{t=1}^T e^{(w_1 x_t' + w_2 R_t^A + w_3 P_t^A)}}
  \]
- Key parameters: \(w_1, w_2, w_3\)
Result 1: SU-BRQR vs MATCH

- AMT workers, 8-target games, 3 resources

<table>
<thead>
<tr>
<th></th>
<th>SU-BRQR</th>
<th>Draw</th>
<th>MATCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha = .05</td>
<td>13</td>
<td>8</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1: SU-BRQR vs MATCH

Conclusion

SU-BRQR significantly outperforms MATCH
Result 2: Security Intelligence Experts

SU-BRQR vs MATCH

<table>
<thead>
<tr>
<th></th>
<th>SU-BRQR</th>
<th>Draw</th>
<th>MATCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha = .05</td>
<td>6</td>
<td>13</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 2: SU-BRQR vs MATCH

Analysis

Rationality of experts

More rational than AMT workers

- Parameter of classic QR: AMT worker: 0.77, security experts: 0.91

- 34 of 44 games: obtained a higher expected value

Security experts are boundedly rational
Result 3: New Game Setting

- AMT workers, 24-target games, 9 resources
  - SU-BRQR vs MATCH with previously learned parameters

<table>
<thead>
<tr>
<th></th>
<th>SU-BRQR</th>
<th>Draw</th>
<th>MATCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha = .05</td>
<td>8</td>
<td>11</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 3: SU-BRQR vs MATCH

- SU-BRQR vs MATCH with re-estimated parameters

<table>
<thead>
<tr>
<th></th>
<th>SU-BRQR</th>
<th>Draw</th>
<th>MATCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha = .05</td>
<td>11</td>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 4: SU-BRQR vs MATCH
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
How Do We Evaluate Deployed Systems?

- Evaluating deployed systems: **NOT EASY**
  - Controlled experiments infeasible; No proof of “100% security”

- Are our systems useful: Are we better off than previous approaches?
  1. Simulations (including “machine learning” attacker)
  2. Human adversaries in the lab
  3. Actual security schedules before vs after
  4. Real-time exercises comparing human vs algorithm schedules
  5. “Adversary” teams simulate attack
  6. Actual data from deployment
  7. Domain expert evaluation (internal and external)
Key Conclusions

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

- Uniform random or simple weighted random:
  - 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
  - Internal evaluations, e.g. LAX by Blue ribbon panel
1. Models and Simulations: Example from IRIS (FAMS)

- Uniform
- Weighted: sum of defender covered
- Weighted: min of defender uncovered
- IRIS

Graph showing comparison of different models and simulations with values from 20 to 250.
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
3. Actual Security Schedules Before vs After: Example from PROTECT (Coast Guard)

Patrols Before PROTECT: Boston

Patrols After PROTECT: Boston

Base Patrol Area
5. Adversary Perspective Team, Supportive data
Example from PROTECT

- “Mock attacker” team deployed in Boston
  - Incorporated adversary’s known intent, capability
  - Comparing PRE- to POST-PROTECT: “deterrence” improved

- Additional real-world indicators from Boston:
  - PRE- to POST-PROTECT: Actual reports of illicit activity
  - Industry port partners comments:
    - “The Coast Guard seems to be everywhere, all the time.”
    (With no actual increase in the number of resources)
6. Before and After Results from the Real World
   -- Not Controlled Experiments

**TRUSTS (3 weeks)**

<table>
<thead>
<tr>
<th>Daily Average</th>
<th>Human</th>
<th>TRUSTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citation Rate</td>
<td>1.11%</td>
<td>1.96%</td>
</tr>
<tr>
<td>Citations/Officer</td>
<td>3.54</td>
<td>6.24</td>
</tr>
</tbody>
</table>

**ARMOR (4 years)**

![Graph showing ARMOR (4 years)]
7. Expert Evaluation
Example from ARMOR, IRIS & PROTECT

February 2009: Commendations
LAX Police (City of Los Angeles)

September 2011: Certificate of Appreciation (Federal Air Marshals)

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

June 2013: Meritorious Team Commendation from Commandant (US Coast Guard)
Federal Air Marshals Service (May 2010):

We have tested IRIS and...have continued to expand the number of flights scheduled using IRIS. Our exact use of IRIS is sensitive information and we can only state that we are satisfied with IRIS and confident in using this scheduling approach.

James B. Curren
Special Assistant, Office of Flight Operations,
Federal Air Marshals Service
4. Expert Evaluation

ARMOR, IRIS, PROTECT…

Erroll Southers: US Congress Committee Hearings 2008
4. Expert Evaluation

ARMOR, IRIS, PROTECT…

US Congress Committee Hearings 2013
Outline and Plan

- Introduction and tutorial basics
- Motivation
- Foundations of game theory and linear programming
- Introduction to security game algorithms
- Research Challenges
- Evaluation
- Future work
Motivation

- Illegal extraction of fuelwood
  - Causes high levels of forest degradation
  - Tanzania’s Kibaha Ruvu Forest Reserves
  - Khao Yai National Park in Thailand
- Deter extractors by patrols
Problem Statement (1)

- **Forest**
  - Large area, surrounded by potential extractors
  - Can be freely visited
Problem Statement (2)

- Extractors
  - Extract fuelwood for home-use
  - Extract along the way back home
  - May be caught on the way back

- Policymaker
  - Distribute patrols within limited budget
  - Maximize the “pristine” area: 100% preserved
Simulation Results (2)

\[ b(x) = 1 - x; \quad c(x) = x; \quad E = 1; \]
Multiple Objectives

- Prior work only considers a single objective
  - Bayesian Stackelberg game: weighted summation over attacker types

- Why multiple objectives?
  - Example: *performance* versus *fuel consumption* in automobile design
  - Impossible to compare objectives due to different types, units, …
  - Multiple solutions are desired to understand trade offs (Pareto frontier)
Los Angeles Metro Rail System

- Barrier-free system with random security inspections
- Goal: Protection from fare evaders, criminals, terrorists
- Outcomes for different adversaries are incomparable
  - Lost ticket revenue, personal / property crimes, massive casualties / destruction
- Security must balance threats when selecting strategy
## Multi-Objective Security Games (MOSG)

- **1** defender, *n* attacker types
  - Probability distribution over attacker types not required
- **One** defender objective for each attacker type
  - Defender payoff is a now vector rather than scalar

<table>
<thead>
<tr>
<th>Defender</th>
<th><strong>T 1</strong></th>
<th><strong>T 2</strong></th>
<th><strong>T 1</strong></th>
<th><strong>T 2</strong></th>
<th><strong>T 1</strong></th>
<th><strong>T 2</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>T 1</strong></td>
<td>5, -3</td>
<td>-1, 1</td>
<td>2, -1</td>
<td>-5, 5</td>
<td>4, -4</td>
<td>-2, 2</td>
</tr>
<tr>
<td><strong>T 2</strong></td>
<td>-5, 5</td>
<td>2, -1</td>
<td>-1, 1</td>
<td>5, -3</td>
<td>-6, 6</td>
<td>1, -2</td>
</tr>
</tbody>
</table>

Defender Payoff = <-1, -5, -2>
Pareto Frontier

- No single solution will optimize all objectives
- Solution concept: Pareto frontier
  - Set of non-dominated solutions
  - Exists in n-dimensional objective space
  - Can be large or even continuous
Security Games with Limited Surveillance

- Finite observation length
- Update using Bayes rule

Defender strategy $X$

$X = \langle 0.4, 0.6 \rangle$

$O_1 = \langle 1, 4 \rangle$

$P(O_1|X)$

$P(O_i|X)$

$P(O_n|X)$

posterior belief $g(X|O_1)$

... 

posterior belief $g(X|O_i)$

... 

posterior belief $g(X|O_n)$

Attack target $f(g(X|O_1))$

... 

Attack target $f(g(X|O_i))$

... 

Attack target $f(g(X|O_n))$

$max_x \sum_o P(O|X)U(X, f(g(X|O)))$
Security Games with Limited Surveillance: Algorithms and Results

Compute defender strategy given an observation length

\[
\begin{aligned}
\max & \quad \sum_{o \in O_{\tau}} \prod_{A \in A} \frac{\tau!}{o_{A}!} x_{A}^{o_{A}} d^{o} \\
\text{s.t.} & \quad x_{A} \in [0, 1] \\
& \quad \sum_{A \in A} x_{A} = 1 \\
& \quad c_{i} = \sum_{A \in A} x_{A} A_{i} \\
& \quad d^{o} = c_{\psi(o)}(R_{\psi(o)}^{d} - P_{\psi(o)}^{d}) + P_{\psi(o)}^{d} \quad \forall o \in O_{\tau}
\end{aligned}
\]

![Graph showing defender expected utility vs. number of observations](image)
THANK YOU!

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