Better Security via Randomization: A Game Theoretic Approach and its Operationalization at the Los Angeles International Airport

Milind Tambe, Fernando Ordonez

CREATE: Homeland Security Center
University of Southern California, Los Angeles
Objective: Guarantee Randomness of Security Processes While Meeting Security Quality Requirements

- Limited / uncertain knowledge of opponent(s)
- Opponent monitors defenses, exploits patterns
- Examples: Patrolling, aerial surveillance,…
Research Problem Definition and Results

• Randomize under uncertain adversarial domains

• Research results:
  – Part 1: Plan randomization with quality constraints
    • No adversary model, Information minimization
    • Decision theory
  – Part 2: Strategy randomization with quality constraints
    • Partial adversary models
    • Game theory
  – Part 3: Application to Airport Security
Part I: No Adversary Model Example
Part I: No Adversary Model: Information Minimization

• Intentional plan randomization for security
  – MDP/POMDP: Planning under uncertainty
    • MDP: Markov Decision problems
      – Difficult for adversary to predict even if knows plan

• New algorithms: single agent & teams
  – Reward > Threshold (e.g. fuel)
  – Non-linear program (inefficient but exact), linear program (efficient but inexact)
Example Computational Results for Single Agent

**Conclusion:** Randomization Recommendation is Computationally Solvable
Part II: Security with Partial Adversary Models

Partial model of adversaries:
- Hardline, well-funded, high capability adversary
- Moderate capability adversary

How to randomly allocate security resources:
- k-9 units/officers to terminals
Part II: Model via Bayesian Stackelberg Game

- Agent (police) commit to strategy first, e.g. canine units to terminals
- Adversaries optimize against police strategy
- Bayesian: Probability distribution over different adversary types

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

Adversary

Police
Bayesian Stackelberg Game: New Algorithms

• Mixed-integer linear program (MILP)
  1. Exact Solution: DOBSS
  2. Heuristic solution: ASAP
     ➢ Mixed strategies
        ➢ Weighted randomization: non-uniform
        ➢ E.g. Not 50%-50% split, but 73%-27% split

• Exponential speedups over prior algorithms
Once again, computational solution feasible
PART III: Application at LAX
Assistant for Randomized Monitoring Over Routes (ARMOR) Project

An Interdisciplinary Counter-Terrorism Research Partnership: Los Angeles World Airports & The University of Southern California
PART III: Applications

• **Problem**: Setting checkpoints and allocating K9 units?

• **Approach**: Maximize security through mathematical randomization

• **Goal**: Create software assistants
ARMOR

• Assistant for Randomized Monitoring Over Routes

• DOBSS basis of ARMOR

• ARMOR-Checkpoints

• ARMOR-K9
ARMOR System

Provide inputs, constraints

Schedule evaluation

ARMOR Knowledge Base

DOBSS: GAME THEORY ALGORITHMS

Weights for randomization

Randomized Schedule generation
Knowledge in ARMOR-checkpoint

• **ARMOR-checkpoint base requires knowledge:**
  - Numbers of possible checkpoints
  - Time of checkpoint operation
  - Traffic flow and its impact on catching adversary
  - Estimated target priority for adversary
  - Estimates of cost of getting caught to adversaries
  - Estimates if “different types” of adversaries and their probabilities (e.g. differ in their capabilities)

• **Converted into utilities**
Comparison: ARMOR v/s Non-weighted (uniformed) Random for Canines

- ARMOR: 6 canines
- ARMOR: 5 canines
- ARMOR: 3 canines
- Non-weighted: 6 canines
The Element of Surprise

To help combat the terrorism threat, officials at Los Angeles International Airport are introducing a bold new idea into their arsenal: random placement of security checkpoints. Can game theory help keep us safe?

Security forces work the sidewalk at LAX
Checkpoint Frequency

Checkpoint frequency (Week 1)

Checkpoint frequency (Week 2)

Usage percentage

Checkpoint number

Usage percentage

Checkpoint number
Conclusion

• New algorithms: guarantee randomness while meeting quality requirements
• Computational techniques that allow practical applications
• Initial demonstration with LAX working well
THE END