Comp Sci 288: AI for Social Impact

Lecture 2: Case Studies from past 15 years of work

MILIND TAMBE
Announcements

• Over to TFs

• Questions?
This seminar series is bringing together a diverse set of perspectives that spans across algorithmic fairness, human-centered computing, and sustained deployment.

**Jan 25:** Danielle Belgrave, Ph.D.
Microsoft Research Cambridge (UK)

**Feb 1:** Omer Reingold, Ph.D.
Stanford University

**Feb 8:** Heather Lynch, Ph.D.
Stony Brook University

**Feb 22:** Munmun De Choudhury, Ph.D.
Georgia Institute of Technology

**Mar 8:** Courtney Cogburn, Ph.D.
Columbia University

**Mar 15:** Lauren Wilcox, Ph.D
Georgia Institute of Technology, Google

**Mar 22:** Tiffany Veinot, MLS, Ph.D.
University of Michigan

**Mar 29:** Kush Varshney, Ph.D.
Thomas J. Watson Research Center, IBM

**Apr 5:** Christopher Le Dantec, Ph.D.
Georgia Institute of Technology

**Apr 12:** Nyalleng Moorosi, Ph.D.
Google AI

**Apr 19:** Michael J. Mina, MD, Ph.D.
Harvard T.H. Chan School of Public Health, Harvard Medical School
Goals of next two lectures

• Summarizing 15 years of research on AI for social impact

• How to “AI for Social Impact” via case studies:
  • Types of problems solved, AI tools available to solve them
  • Challenges in applying AI tools
  • Challenges in measuring impact
  • Ethical challenges
  • Pitfalls

• Chronological ordering

• Partnership lessons

• General lessons learned
Goals of next two lectures

• Summarizing 15 years of research on AI for social impact

• How to “AI for Social Impact” via case studies:
  • Types of problems solved, AI tools available to solve them
  • Challenges in applying AI tools
  • Challenges in measuring impact
  • Ethical challenges
  • Pitfalls

• You may have different technical backgrounds

• Understand the problem and model used, not essential to understand details of the algorithms used – you can pick that up for your project if necessary
AI & Multiagent Systems Research for Social Impact

- Public Health
- Conservation
- Public Safety and Security
Key Research Challenge

Optimize Our Limited Intervention Resources
Optimizing Limited Intervention Resources

Social Networks & Bandits

Green security games

Conservation

Public Safety & Security

Stackelberg security games
Three Common Themes
Multiagent systems, Data-to-deployment pipeline, Interdisciplinary partnerships

Immersion
Data Collection

Predictive model
Learning/Expert input

Prescriptive algorithm
Multiagent Reasoning Intervention

Field tests & deployment

Social networks

Game theory

Date: 4/11/2021
Three Common Themes
Multiagent systems, Data-to-deployment pipeline, Interdisciplinary partnerships

Field test & deployment: Social impact is a key objective

Lack of data is a norm: Must be part of project strategy
Three Common Themes
Multiagent systems, Data-to-deployment pipeline, Interdisciplinary partnerships

Empower non-profits to use AI tools; avoid being gatekeepers to AI4SI technology
Outline

Public Safety and Security: Stackelberg Security Games

Conservation/Wildlife Protection: Green Security Games
11 July 2006: Mumbai

**Train of Terror**

Mumbai continues to be the prime target for terrorist groups. It has borne the brunt of seven attacks in the past 13 years.

- **Explosive used**: High-quality explosives. Most likely RDX (Cyclonite/dinitrooxymetane).
- **Quantity of explosive**: At least 5 kg per blast, mostly packed into bags or tiffin boxes.
- **Where were bombs placed?**: In the baggage racks where commuters keep their bags and tiffin boxes.
- **How many bombers were there?**: At least 20, 2 for each coach and a logistic team of 6 people.
- **Why attack the first class compartments?**: It is easier to enter a first class compartment at peak hour than a second-class coach filled with up to 5 kg of explosives.

**Warning**

- JAN 9, 2006: Bombed from three pairs of trains in Mumbai
- JAN 30, 2006: Powder and 2 kg of RDX from 2 pairs of trains
- MAY 5, 2006: 2,000 kg of RDX in a train
- MAY 12, 2006: Cartridges and grenades saved
- MAY 14, 2006: Three AK-47s and earphones saved

Erroll Southers

LAX Airport, Los Angeles

Glasgow: June 30, 2007
Background on LAX Airport Threats: Surveillance Opportunity

- Air Canada Cargo Bombing
  Hratch Kozibioukian, Stanouche Kozibioukian, Varant Barkev Chiriinan
  Van Nuys, 23 miles
- Pan Am Terminal Bombing
  Muharem Kurbegovich
  Los Angeles, 19 miles
- TBIT JIS Plot
  Hammad Riaz Samana
  Inglewood, 3 miles
- TBIT JIS Plot
  Gregory Vernon Patterson, Levar Haney Washington
  Gardena, 9 miles
- Millennium Bomb Plot
  Khalil Deek
  Anahiem, 34 miles
- TBIT Shooting
  Hesham Mohamed Hadayet
  Irvine, 42 miles
Can we propose game theory for security resource optimization?
Set of targets, payoffs based on targets covered or not
Stackelberg Leader-Follower formulation
Game Theory for Security Resource Optimization

New Model: Stackelberg Security Games

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

Adversary

Defender

Date: 4/11/2021
**Model: Stackelberg Security Games**

**Stackelberg**: Defender commits to randomized strategy, adversary responds

**Security optimization**: Not 100% security; increase cost/uncertainty to attackers

**Challenges faced**: Massive scale games

<table>
<thead>
<tr>
<th></th>
<th>Terminal #1</th>
<th>Terminal #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal #1</td>
<td>4, -3</td>
<td>-1, 1</td>
</tr>
<tr>
<td>Terminal #2</td>
<td>-5, 5</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
ARMOR at LAX
Basic Security Game Operation [2007]

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

Mixed Integer Program

Pr (Canine patrol, 8 AM @Terminals 2,5,6) = 0.17

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>Team3</td>
<td>Team5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 AM</td>
<td></td>
<td>Team1</td>
<td>Team2</td>
<td></td>
<td>Team4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

Date: 4/11/2021
We are trying to Find $x_i$

Maximize defender expected utility

Defender mixed strategy

Adversary response

Adversary best response

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

subject to

$$\sum_i x_i = 1$$

$$\sum_{j \in Q} q_j = 1$$

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

Target #1 | Target #2 | Target #3
---|---|---
Defender #1 | 2, -1 | -3, 4 | -3, 4
Defender #2 | -3, 3 | 3, -2 | ....
Defender #3 | .... | .... | ....
SECURITY GAME PAYOFFS [2007]
Previous Research Provides Payoffs in Security Games

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

Maximize defender expected utility

\[
\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j
\]
First application: Computational game theory for operational security

January 2009

- January 3rd
  - Loaded 9/mm pistol
- January 9th
  - Loaded 9/mm pistol
  - 16-handguns, 1000 rounds of ammo
- January 10th
  - Two unloaded shotguns
- January 12th
  - Loaded 22/cal rifle
- January 17th
  - Loaded 9/mm pistol
- January 22nd
  - Unloaded 9/mm pistol
ARMOR AIRPORT SECURITY: LAX [2008]
Congressional Subcommittee Hearings

Commendations
City of Los Angeles

Erroll Southers testimony
Congressional subcommittee

ARMOR…throws a digital cloak of invisibility….
New applications: cybersecurity, protecting of endangered wildlife and fisheries, protecting forests, audit games, drug design against viruses, traffic enforcement, software code testing, adversarial machine learning
Questions?
Behind the scenes

- Immersion
  - Data Collection

- Predictive model
  - Learning/Expert input

- Prescriptive algorithm
  - Multiagent Reasoning Intervention

- Field tests & deployment
Lessons in Immersion

• Understanding their counter-terrorism experience
No data-driven predictive model
**AI ADVANCES?**

- Game theory
- Social networks
- Bandits
- POMDPs
- RL
- Decision-focused Learning

**Advancing AI + MAS**

**Achieving impact**

- Public health
- Conservation
- Public safety
AI ADVANCES?

• E.G.: Stackelberg security games from ARMOR
• There wasn’t as much interest in Stackelberg
• NOT JUST Stackelberg, BUT SECURITY GAME
Simplify Interaction
ARMOR Transition
Cost-benefit analysis

Savings
• $30 Million in ARMOR
• $35 Million in PROTECT
• > benefit of IRIS
Some lessons

• Impact evaluation is complicated: Domain experts may not provide scientific evaluation

• Must respect others with other areas of expertise

• No zero-risk application

• Pressure to publish AI advances: if its not a methodological advance AI conferences don’t care
  • Problematic for AI for social impact

• Did not set an end date! There must be an end date
Questions
Visiting Freedom Center: Home of Federal Air Marshals Service

Date: 4/11/2021
Scale Up Difficulty [2009]

\[ x_i \] Defender mixed strategy

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

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

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

1000 flights, 20 air marshals:

10^41 combinations

<table>
<thead>
<tr>
<th>Attack</th>
<th>Attack</th>
<th>Attack</th>
<th>Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>...</td>
<td>1000</td>
</tr>
<tr>
<td>1, 2, 3 ..</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
</tr>
<tr>
<td>1, 2, 4 ..</td>
<td>5,-10</td>
<td>4,-8</td>
<td>...</td>
</tr>
<tr>
<td>1, 3, 5 ..</td>
<td>5,-10</td>
<td>-9,5</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>10^41 rows</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scale Up [2009]
Exploiting Small Support Size

Small support set size:
Most $x_i$ variables zero

1000 flights, 20 air marshals:
$10^{41}$ combinations

<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>
<tr>
<td>...</td>
<td>...</td>
<td>10^{41} rows</td>
<td></td>
</tr>
</tbody>
</table>

X_{123} = 0.0
X_{124} = 0.239
X_{135} = 0.0
X_{378} = 0.123
New Exact Algorithm for Scale up

**Incremental strategy generation:** First for Stackelberg Security Games

### Primary

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

### Secondary (LP Duality Theory)

Best new pure strategy

### Global Optimal

1000 defender strategies

NOT $10^{41}$
IRIS: Deployed FAMS [2009-]

Significant change in FAMS operations

September 2011: Certificate of Appreciation (Federal Air Marshals)
Behind the scenes

1. Immersion
   - Data Collection

2. Predictive model
   - Learning/Expert input

3. Prescriptive algorithm
   - Multiagent Reasoning Intervention

4. Field tests & deployment
26 Nov 2008, Mumbai
Police Checkpoints: Network Security Game

Road networks:
20,000 roads, 15 checkpoints

150 edges
2 Checkpoints
150-choose-2 strategies
## Zero-Sum Network Security Game [2013]

**Double oracle**: New exact optimal algorithm for scale-up

### Defender oracle

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

### Attacker oracle

<table>
<thead>
<tr>
<th>Checkpoint strategy #1</th>
<th>Path #1</th>
<th>Path #2</th>
<th>Path #3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5, -5</td>
<td>-1, 1</td>
<td>-2, 2</td>
</tr>
<tr>
<td>Checkpoint strategy #2</td>
<td>-5, 5</td>
<td>1, -1</td>
<td>-2, 2</td>
</tr>
</tbody>
</table>
Presentation at the Indian National Police Academy: Network Security Game [2016]

Road networks:
20,000 roads, 15 checkpoint: Solved under 20 min
Some lessons

• No “immersion” meant no ability to build up trust
PROTECT: Port and Ferry Protection Patrols [2011]

Boston

Los Angeles

New York
PROTECT: Port and Ferry Protection Patrols [2011]
PROTECT: Ferry Protection Deployed [2013]
PROTECT: Ferry Protection Deployed [2013]
**Marginal strategy**: New scale-up approach for Stackelberg 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>
PROTECT: Port Protection Patrols [2013]
Congressional Subcommittee Hearing

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

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

US Coast Guard testimony
Congressional subcommittee

Date: 4/11/2021
Train Patrols
Execution Uncertainty: MDPs

<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>

Date: 4/11/2021
Questions
Evaluation

• Breakout

• “BUT DOES THIS WORK”?
Evaluating Deployed Security Systems Not Easy

How Well Optimized Use of Limited Security Resources?

Security Games superior
vs
Human Schedulers/”simple random”

- Lab evaluation
- Scheduling competitions: Patrol quality unpredictability? Coverage?
- Field evaluation: Tests against real adversaries
- Economic cost-benefit analysis
- …
Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort

350% increase in defender expected utility
Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort

**FAMS:** IRIS Outperformed expert human over six months

Report: GAO-09-903T

**Trains:** TRUSTS outperformed expert humans schedule 90 officers on LA trains

Date: 4/11/2021
Field Tests Against Adversaries

Computational Game Theory in the Field

Controlled
- 21 days of patrol, identical conditions
- Game theory vs Baseline+Expert

Not Controlled

Before ARMOR

Date: 4/11/2021
Poaching of Wildlife in Uganda
Limited Intervention (Ranger) Resources to Protect Forests

Snare or Trap

Wire snares
Focus on Threat prediction
Diving up the area into 1 Km x 1 Km Grid cells
Learning Poacher Model: Uncertainty in Observations

What uncertainty might you expect as rangers walk to recover snares and report that data?
Learning Poacher Model: Uncertainty in Observations

Positive and unlabeled datasets

Record: No Attack (NEG)

Record: Attack (POS)

Walk more!
Learning Adversary Response Model: Uncertainty in Observations

Ranger patrol
Animal density
Distance to rivers / roads / villages

Probability of snare Per 1 KM Grid Square

Area habitat
Area slope

Training: Filtered Datasets

Predict: Ensemble of Classifiers

Patrol Effort

C₀

C₁

C₂