Applications of Game Theory

Wide range of applications of game theory
- Originally: in economics
- Now: ubiquitous, also in computer science and AI
  - robotics
  - cloud computing
  - social networks
  - resource management
- ...

(Tim will talk about some of them, and/or others, on Wednesday.)
Applications of Game Theory

Security Games

Motivation

Setting

Formalization

Strategies and Payoffs

Equilibria

Theoretical Results

Summary

Security Games

Today: Security games [Tambe et al., 2007ff.]

- infrastructure security games (air travel, ports, trains)
- green security games (fisheries, wildlife)
- opportunistic crime security games (urban crime)

Some video lectures by M. Tambe:

- https://www.youtube.com/watch?v=wh15TU7sMa8 (Infrastructure security games, 3 mins)
- https://www.youtube.com/watch?v=61yHC5c2c-E (Green security games, 8 mins)
- https://www.youtube.com/watch?v=D4sxZm8-NdM (ICAPS 2017 invited talk, 1 hour)

Common setting in security games:

- attacker and defender
- defender wants to protect targets using patrolling units
- defender chooses probability distribution over routes such that expected damage is minimized given that the probabilities can be observed by attacker

Unobservable vs. observable defense probabilities:

- Unobservable: strategic game
- Observable: extensive game

Example (Security game payoff matrix)

<table>
<thead>
<tr>
<th></th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1,1</td>
<td>3,0</td>
</tr>
<tr>
<td>b</td>
<td>0,0</td>
<td>2,1</td>
</tr>
</tbody>
</table>

Unobservable defense probabilities (strategic game): Only NE is \((a, c)\).

Example (Security game (ctd.))

Observable defense probabilities (extensive game, mixed strategies):

Subgame-perfect equilibrium \((\alpha, d)\).


**Security Games**

**Formalization**

**Definition (Security game)**

A security game is a tuple \( (T, R, \{ S_i \}, U_d^f, U_d^u, U_a^f, U_a^u) \), where:

- \( T = \{ t_1, \ldots, t_n \} \) is a finite set of targets,
- \( R = \{ r_1, \ldots, r_K \} \) is a finite set of resources,
- \( S_i \subseteq 2^T \) is the set of schedules that \( r_i \) can cover. A schedule \( s \in S_i \) is a set of targets that can be covered by \( r_i \) simultaneously.
- \( U_d^f(t_i) \) is the utility of player \( y \in \{ \text{attacker}, \text{defender} \} \), if target \( t_i \) is attacked and is \( x \in \{ \text{covered, uncovered} \} \).
- \( U_a^f \) is the set of coverage vectors for which there is an allocation \( s \) inducing it.

**Example (Federal air marshal service)**

- \( T = \{ f_1, f_2, f_3, f_4, f_5, f_6 \} \)
- \( R = \{ r_1, r_2 \} \)
- \( S_1 = \{ \{ f_1, f_2, f_3 \}, \{ f_4, f_5 \} \} \)
- \( S_2 = \{ \{ f_2, f_3, f_6 \} \} \)
- \( U_d^f(t_i) \) unspecified

**Strategies and Payoffs**

- **Attacker pure strategies**: \( A_a = T \)
- **Attacker mixed strategies**: \( \Delta(T) \)
- **Defender pure strategies**: allocations of resources to schedules, i.e., \( s = (s_1, \ldots, s_K) \in \prod_{i=1}^K S_i \).

**Theoretical Results**

- **Defender mixed strategies**: \( \Delta(\mathcal{S}) \). For \( \alpha_d \in \Delta(\mathcal{S}) \), let \( c_i = \sum_{d=(d_1, \ldots, d_N)\in \mathcal{D}} d_i \cdot \alpha_d(d) \) be the covering probability of target \( t_i \).

**Summary**

- Notation: \( \phi(\alpha_d) = (c_1, \ldots, c_n) \).
- **Example**: \( \tilde{d}_1 = (1, 1, 0) \), \( \tilde{d}_2 = (0, 1, 1) \), \( \alpha_d(\tilde{d}_1) = \alpha_d(\tilde{d}_2) = \frac{1}{2} \).
- Then \( (c_1, c_2, c_3) = (\frac{1}{2}, 1, \frac{1}{2}) \).
- **Payoffs**: Let \( (\alpha_a, \alpha_d) \in \Delta(\mathcal{S}) \times \Delta(T) \) be a mixed strategy profile. Expected utility of player \( y \in \{ a, d \} \):

\[
U_y(\alpha_a, \alpha_d) = \sum_{i=1}^n \alpha_a(t_i) \cdot (c_i \cdot U_d^f(t_i) + (1 - c_i) \cdot U_d^u(t_i))
\]
Definition of best responses, Nash equilibria (NE) and maximinimizers (MM) as usual/expected. Hence omitted here.

More interesting scenario:
- Defender first commits to a mixed defense strategy.
- Attacker observes it over extended time period and learns probabilities.
- Attacker choses response $\alpha_a = g(\alpha_d)$ based on those observations. $g$ is his response function.

Theorem
Defender NE strategies and defender MM strategies are the same.

Theorem
NE strategies are interchangeable.

Theorem
Defender SSE utilities are always at least as large as defender NE utilities.

Definition (Strong Stackelberg equilibrium)
A pair $\langle \alpha_d, g \rangle$ is called a strong Stackelberg equilibrium (SSE) if the following holds:
- $U_d(\alpha_d, g(\alpha_d)) \geq U_d(\alpha'_d, g(\alpha'_d))$ for all $\alpha'_d$;
- $U_a(\tilde{\alpha}_d, g(\tilde{\alpha}_d)) \geq U_a(\tilde{\alpha}_d, g'(\tilde{\alpha}_d))$ for all $\tilde{\alpha}_d$ and all $g'$; and
- tie breaking: $U_d(\tilde{\alpha}_d, g(\tilde{\alpha}_d)) \geq U_d(\tilde{\alpha}_d, \tau(\tilde{\alpha}_d))$ for all $\tilde{\alpha}_d$ and all $\tau(\tilde{\alpha}_d)$ that are attacker best responses to $\tilde{\alpha}_d$.

Definition (Subsets of schedules are schedules property)
A security game satisfies the SSAS property ("subsets of schedules are schedules") if for all $r_i \in R$, for all $s_i \in S_i$, and for all $s' \subseteq s$, also $s' \in S_i$. Remark: SSAS often "natural" to achieve, by "doing nothing".

Theorem
If SSAS holds, then every defender SSE strategy is also a defender NE strategy.

Consequence: When choosing between SSE and NE strategies (assuming being observed or not), for the defender it is unproblematic to restrict attention to SSE strategies. NE interchangeability \(\Rightarrow\) no risk of choosing a "wrong" NE strategy.
Outlook:

- With homogeneous resources and a small restriction on utility functions: then there exists unique defender MM strategy, which is also a unique SSE and NE strategy.
- Theory can be generalized to multiple attacker resources (attacking multiple targets simultaneously).

Summary

- **Case study:** security games (infrastructure, green, opportunistic crime)
- Modeled as Stackelberg games with strong Stackelberg equilibria (SSE)
- **Results:**
  - Though not zero-sum in general, similar results: defender NE = defender MM
  - Nash equilibria interchangeable
  - no equilibrium selection problem
  - Every defender SSE strategy also a NE strategy under reasonable assumption (SSAS)
  - not knowing whether being observed is unproblematic