Game Theory

8. Interlude: Applications

Albert-Ludwigs-Universität Freiburg

Bernhard Nebel and Robert Mattmüller

Summer semester 2019

1 Applications of Game Theory

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
  - ...

2 Security Games

- Motivation
- Setting
- Formalization
- Strategies and Payoffs
- Equilibria
- Theoretical Results

Security Games
Motivation

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=whl5TO7sMa8` (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)

Security Games
Motivation

Applications of Game Theory
Security Games
Motivation
Setting
Formalization
Strategies and Payoffs
Equilibria
Theoretical Results
Summary

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

Security Games
Setting

Unobservable vs. observable defense probabilities:

- Unobservable: strategic game
- Observable: extensive game

Example (Security game payoff matrix)

Attacker

		c	d
Defender	a	1,1	3,0
	b	0,0	2,1

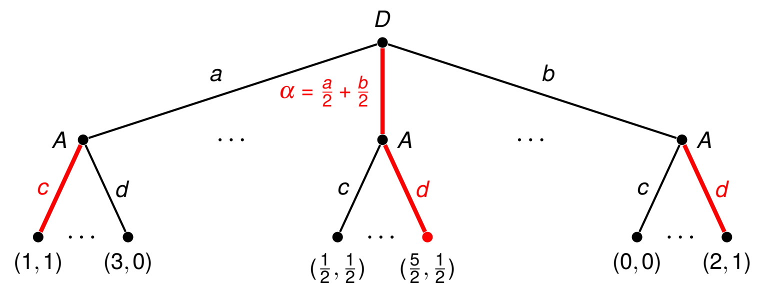
Unobservable defense probabilities (strategic game): Only NE is (a,c).

Security Games
Setting

Applications of Game Theory
Security Games
Motivation
Setting
Formalization
Strategies and Payoffs
Equilibria
Theoretical Results
Summary

Example (Security game (ctd.))

Observable defense probabilities (extensive game, mixed strategies):



Subgame-perfect equilibrium (α, d).

Security Games
Formalization

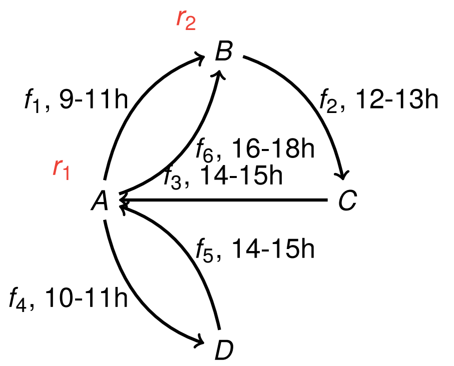
Definition (Security game)

A security game is a tuple $\langle T, R, (S_i), U_d^c, U_d^u, U_a^c, U_a^u \rangle$, where

- $T = \{t_1, \dots, t_n\}$ is a finite set of targets,
- $R = \{r_1, \dots, r_K\}$ 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.
- $U_y^x(t_i)$ is the utility of player $y \in \{\textbf{a}ttacker, \textbf{d}efender\}$, if target t_i is attacked and is $x \in \{\textbf{c}overed, \textbf{u}ncovered\}$.

Security Games
Formalization

Example (Federal air marshal service)



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

Security Games
Strategies and Payoffs

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

  Target t_i is covered in $\bar{s}$ iff $t_i \in s_j$ for at least one j, $1 \le j \le K$. Allocation $\bar{s}$ induces coverage vector $\bar{d} = (d_1, \dots, d_n) \in \{0, 1\}^n$ with $d_i = 1$ iff t_i is covered in $\bar{s}$.

  Let $\mathscr{D}$ be the set of coverage vectors for which there is an allocation $\bar{s}$ inducing it.

Security Games
Strategies and Payoffs

- Defender mixed strategies: $\Delta(\mathscr{D})$. For $\alpha_d \in \Delta(\mathscr{D})$, let $c_i = \sum_{\bar{d}=(d_1,\dots,d_n) \in \mathscr{D}} d_i \cdot \alpha_d(\bar{d})$ be the covering probability of target t_i.

  Notation: $\phi(\alpha_d) = (c_1, \dots, c_n)$.

  Example: $\bar{d}_1 = (1, 1, 0)$, $\bar{d}_2 = (0, 1, 1)$, $\alpha_d(\bar{d}_1) = \alpha_d(\bar{d}_2) = \frac{1}{2}$. Then $(c_1, c_2, c_3) = (\frac{1}{2}, 1, \frac{1}{2})$.
- Payoffs: Let $(\alpha_d, \alpha_a) \in \Delta(\mathscr{D}) \times \Delta(T)$ be a mixed strategy profile. Expected utility of player $y \in \{a, d\}$:

$$U_y(\alpha_d, \alpha_a) = \sum_{i=1}^{n} \alpha_a(t_i) \cdot \left(c_i \cdot U_y^c(t_i) + (1 - c_i) \cdot U_y^u(t_i)\right).$$

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.

Applications of Game Theory
Security Games
Motivation
Setting
Formalization
Strategies and Payoffs
Equilibria
Theoretical Results
Summary

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 α'_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 $\tilde{\alpha}_d$.

Applications of Game Theory
Security Games
Motivation
Setting
Formalization
Strategies and Payoffs
Equilibria
Theoretical Results
Summary

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. □

Applications of Game Theory
Security Games
Motivation
Setting
Formalization
Strategies and Payoffs
Equilibria
Theoretical Results
Summary

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 $s \in S_i$, 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 $\rightsquigarrow$ no risk of chosing 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).

3 Summary

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
    $\rightsquigarrow$ Nash equilibria interchangeable
    $\rightsquigarrow$ no equilibrium selection problem
  - Every defender SSE strategy also a NE strategy under reasonable assumption (SSAS)
    $\rightsquigarrow$ not knowing whether being observed is unproblematic