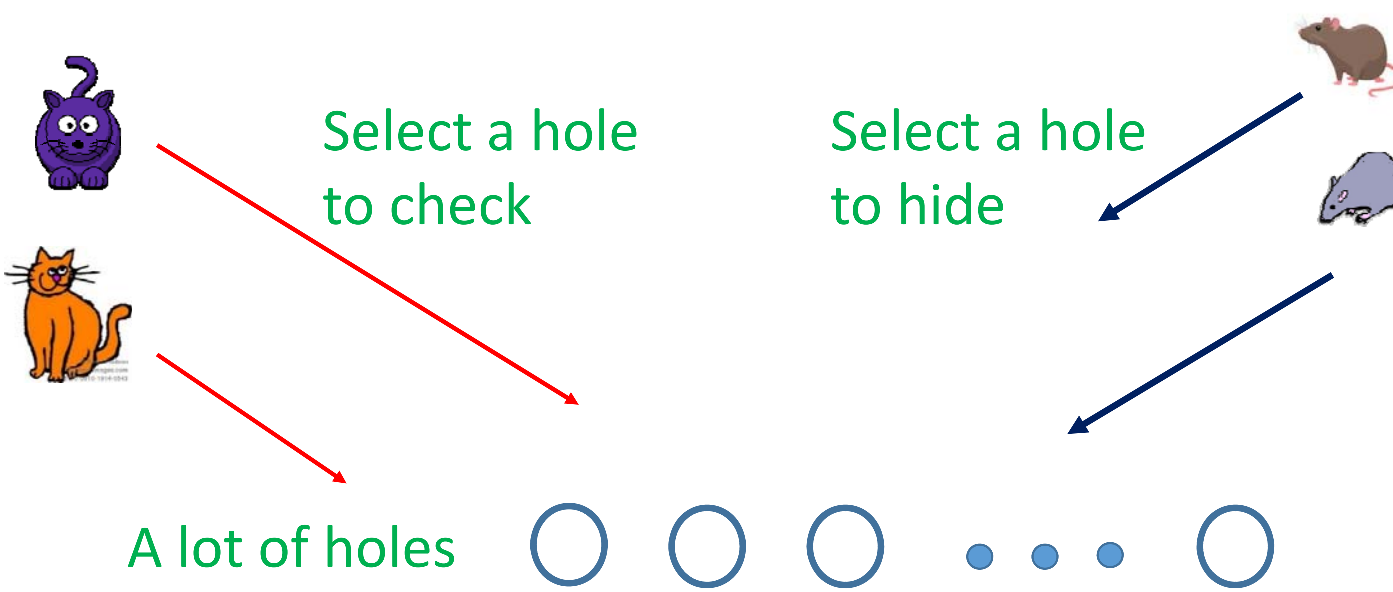
Game Theory
– An Outside Party Perspective

Jun Zhang
Department of Electrical Engineering and Computer Science
University of Wisconsin-Milwaukee
junzhang@uwm.edu

What does game theory do for security?

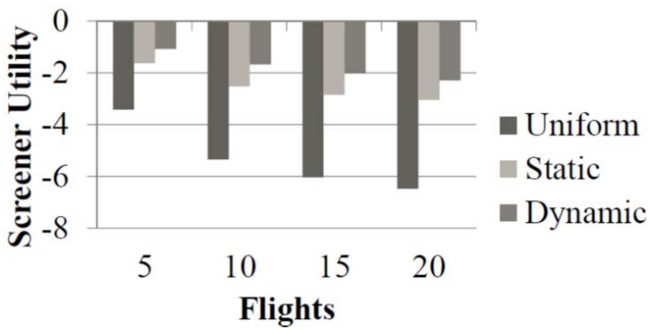


Select a hole to check

Select a hole to hide

A lot of holes

Utility figure:
from Brown’s thesis



- Game theory: allows cats to generate their best strategy given: 1) fewer cats than holes and 2) mice can learn the cats’ strategy and best exploit it
- Potential benefit to security: allow for “intelligent” adversaries, efficient use of resources and improved security
- Does it solve the “needle-in-hay-stack problem?” No

How does game theory work?

- Assume:
  - Finite detection resources (e.g., metal detectors, TSA agents [body search], microwave detectors, explosive detectors, and CT scanners)
  - Terrorists can learn our security strategies and counter in the optimal way
- Generate our optimal strategy by solving a max-min problem like this (Brown, 2015, USC)

$$\begin{array}{rl}
\max\limits_{d_\theta, n_{\psi,\xi}} & \sum_\theta W_\theta d_\theta \\
\forall \theta, \tau, m, \xi \in \theta. & d_\theta \leq U_\sigma(\vec{x}^1_\xi, \ldots, \vec{x}^\eta_\xi, \mu^\tau_{\xi,m}), \\
\forall \tau, \xi. & \vec{x}^\tau_\xi = \frac{\sum_\psi n^\tau_{\psi,\xi} \vec{E}_{\psi,\xi} + (N^\tau_\xi - \sum_\psi n^\tau_{\psi,\xi}) \vec{E}_{\delta,\xi}}{N_\xi}, \\
\forall \tau. & n^\tau_{\psi,\xi} \in conv(P^\tau)
\end{array}$$

- But what’s the basic idea here?

Basic idea through a simple example

- Suppose we have: N holes, one cat, and one mouse
- The game: “Stackelberg game”
  - The mouse chooses a hole to hide
  - The cat chooses a hole to search
  - If they choose the same hole, the cat wins; otherwise, the mouse wins
  - The mouse can learn the cat’s strategy and counter in the best way (e.g., if the cat [definitely] chooses the first hole, the mouse will not choose the first hole)
- The game theory question: what’s the cat’s best strategy?

Example continued

- The cat's general strategy: select the ith hole with probability p_i
- The mouse's optimal counter: choose the jth hole if p_j is the smallest among all p_is, i.e., min
- The cat's optimal strategy: make p_j as large as possible, i.e., max
- The result: "Stackelberg equilibrium", max-min
  - The cat chooses a random hole with probability $1/N$ for each hole
  - The mouse does the same
- Another way to view the result: the cat's optimal strategy presents maximum entropy (uncertainty) for the mouse

A real (security) game

- Cats
  - Cats of different types (different detector types), each with different effectiveness
  - Multiple cats of each type
  - Cat teams and their different effectiveness
  - The number of cats and cat teams
- Mice
  - Also come in different types (different risk levels)
  - The cats do not know which type of mice is coming to hide (only know a prior)
- Consequences
  - Some miss detections (e.g., missed explosives) are more costly than others (e.g., missed guns)
- Results: large LP (linear programming) problems (e.g., page 3)

Related work

- “Probability-based” resource allocation (Jacobson et al, 2006-13)
  - Optimizing resource allocation to maximize probability of detection
  - Under-screening is better than over-screening
- How it compares with game theory: let’s look at a simple example
  - Two passengers, one with risk level 1 and one with risk level 2 (higher probability of bringing in dangerous material)
  - But suppose we can only check one of them
  - Probability based: will check the higher risk level passenger
  - Game theory: will pick a random passenger to check
- More general criticisms of game theory from literature
  - Assumptions not realistic; solutions too complex to compute, etc.
- Potential remedies (Bier et al, 2009): game theory inspired solution
  - Use the basic max-min idea and find suboptimal formulations and/or solutions

Test game theory on real airport data

- How? Start with data collecting at a real airport, including
  - Detection resources: the number, type, and effectiveness of detection resources
  - Passenger arrival rate: number of people per hour
  - Passenger clear rate constraint: the minimum number of passengers that need to be cleared per hour
  - The two rates maybe different at different time of day and different day of the week
  - Cannot collect terrorist data easily – simulate using a model (with type, risk level, and banned-material parameters)
- Next
  - Simulate the airport using the data collected above
  - Generate game theory optimal detection resource allocation strategy
  - Test this on simulated airport data
- Finally
  - Compare the game theory PD and PFA with a bench mark (e.g., the current TSA resource allocation)

The problem of "needle in the hay stack"

- What is the problem?
  - No dangerous materials get through or
  - PD < 10^{-9} , with reasonable PFA, or passenger clearance rate (e.g., 10000 per hour)
- At present time, a possible way to achieve this: have a very large amount of detection resources
- Without that, any technique, including game theory, may not be able to achieve that.
- Example:
  - 1 mouse, m cats to check N holes, m<N.
  - Optimal GT cat strategy: check each hole with p=m/N
  - PD = m/N; to achieve high PD, need more cats

Summary and Future Work

- Game theory is a new and potentially promising approach for improving security and resource allocation
- The best part: allows to account for “intelligent” terrorists
- But it does not solve the “needle-in-hay-stack problem”
- Future work:
  - Test game theory with real airport data
  - Develop game theory inspired approaches