swissQuant
Mastering Complexity

Mathematical Challenge February 2019

Security Games

References

[1] Merrill M Flood. The hide and seek game of von neumann. Management Science, 1972.

[2] Christopher Kiekintveld et al. Computing optimal randomized resource allocations for massive security games. In Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1, 2009.

[3] Praveen Paruchuri et al. Playing games for security: An ef cient exact algorithm for solving bayesian stackelberg games. In Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems-Volume 2, 2008.

[4] James Pita et al. Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. In Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track, 2008.

[5] Aaron Schlenker et al. Don't bury your head in warnings: a game-theoretic approach for intelligent allocation of cyber-security alerts. Proceedings of the 26th IJCAI, 2017.

[6] Jason Tsai et al. Iris-a tool for strategic security allocation in transportation networks. 2009.

Description

Motivation

Security Games are one of the most proli c applications of Game Theory. They were introduced by John von Neumann in [1] with hide and seek, a 2 players adversarial game. In the Security Game settings, we will call hider and seeker, Attacker and Defender respectively. Security Games are frameworks for computing the allocation of resources to optimally protect an environment from different threats. They are modeled as Stackelberg games in which the Defender (the Leader) commits to a strategy and the Attacker (the Follower), after

having observed the commitment of the Defender, chooses the best response in order to maximize his utility.
These representations have been used in different real-world contexts (concerning both physical and non-physical security [5]). The first application of Security Games has been the strategic allocation of resources in order to protect the Los Angeles International Airport [4]. Security Games have also been used in scheduling the Federal Air Marshals (FAMs) abroad U.S. commercial flights [6]. Both these two frameworks have to face new and different challenges. In protecting LAX, the authors had to relax the assumption of certainty about the Attacker type modeling the game as a Bayesian Stackelberg game. In scheduling FAMs, instead, the authors had to deal with a massive Stackelberg game.
In this mathematical challenge, we present the fundamental algorithms used to solve the presented real-world challenges and we propose some interesting questions to reason about.

Technical Details

In [3], the authors have developed an algorithm called DOBSS (Decomposed Optimal Bayesian Stackelberg Solver) to find the Defender's optimal strategy to commit to in an efficient and exact way. The same algorithm has been used to allocate resources at LAX.

DOBSS

We start presenting the MIQP to solve Stackelberg games with single type Attacker and leave to the reader the derivation of the decomposed MILP for Bayesian Stackelberg games.

$$\max_{x,q,a} \sum_{i \in X} \sum_{j \in Q} R_{iq} x_i q_j$$
$$a \geq \sum_{i \in X} C_{ij} x_i$$
$$a - \sum_{i \in X} C_{ij} x_i \leq (1 - q_j) M$$

In the problem definition above x corresponds to the Defender's policy. Each value x_i is the proportion in which the pure strategy i is choosen. In the same way, q is the Attacker's policy. With X and Q we denote respectively the sets of pure strategies of Defender and Attacker. The payoffs of Defender and Attacker will be described by 2x2 matrices R and C. The value R_{ij} and C_{ij} are the rewards for the two players when the Defender follows strategy i and the Attacker strategy j.
We denote with M some large constant value and with a the Attacker maximum reward. Remember that the Attacker has the ability to observe the strategy which the Leader commit to. In this settings, it is straightforward to notice that the Attacker can reach the optimal value with a pure strategy.

♦ **Q1:** *Can you devise a method to compute a?*

To introduce multiple types the authors assigned to each Attacker type l an a priori probability p^l.

- **Q2:** *Extend the previous algorithm in order to handle the Attacker different types without using a full-blown Harsanyi transformation.*
- **Q3:** *Provide a MILP definition of your algorithm. (hint: you will have to perform a change of variable)*

The protection of physical environments may involve the allocation of multiple resources. In this setting the size of the game increases of a combinatorial factor both in terms of strategy space and payoff representation. In [2] the authors proposed a novel representation of the payoff structure to handle this problem.

ERASER

From a payoff perspective the representation of an unattacked target, wether it is covered or not, is identical. To leverage this property the authors have introduced two coverage vectors C and A. Values c_t in C corresponds to the probability that target t is covered. Vector A represents the probabilities of being attacked. As before the Attacker strategy can be restricted to the set of pure strategies without loss of generality.
The Defender utility becomes:

$$U_D(t, C) = c_t U_D^c(t) + (1 - c_t) U_D^u(t)$$

The payoff of the Defender for a covered attack is $U_D^c(t)$. If the attack is not covered the payoff is denoted by $U_D^u(t)$. The Attacker selects the target t^* that gives him the maximum expected payoff given coverage C, breaking ties in favor of the Defender. The resulting MILP is shown below:

$$\begin{aligned} &\max d \\ d - U_D(t, C) &\leq (1 - a_t) Z \\ 0 \leq k - U_A(t, C) &\leq (1 - a_t) Z \end{aligned}$$

The first constraint defines the Defender's expected payoff w.r.t. the attacked target. The second constraint forces the Attacker to select one of the targets that gives him the maximum payoff.

- **Q4:** *Prove that for any feasible coverage vector there exists a corresponding mixed strategy.*

We look forward to your opinions and insights.

Best Quant Regards,

swissQuant Group Leadership Team