Security Games

Thursday, September 28, 2023 10:57 AM

Defender (leader)

→ n targets $\{1, \dots, n\} = [n]$

→ Set of strategies/moves

$\mathcal{E}$ = set of feasible defence strategies

$\mathcal{E} \subseteq \{0,1\}^n$, $\bar{e} \in \mathcal{E}$

$e_i = 1$ if i is defended
$= 0$ o.w.

r_i = reward if defended while attacked ≥ 0

c_i = cost o.w. ≤ 0

Attacker:

Can attack "one" target.

→ set of strategies/moves $= [n]$.

s_i = reward if i not defended while attacked ≥ 0

ξ_i = cost o.w. ≤ 0.

★ Pure Play $\bar{e} \in \mathcal{E}$, $i \in [n]$.

$(\bar{e}, i)$

$e_i = 1$ if target i defended
$= 0$ o.w.

payoff of def $\underline{(\bar{e}, i)} = r_i e_i + (1 - e_i) c_i$

payoff attack $(\bar{e}, i) = \underline{\xi_i e_i + s_i (1 - e_i)}$

★ Mixed Play: $\underline{\bar{p} \in \Delta(\mathcal{E})}$, $\bar{y} \in \Delta([n])$
$= (y_1, \dots y_n)$

$$\text{payoff of def}(\bar{p}, \bar{y}) = \sum_{e \in \mathcal{E}} \sum_{i \in [n]} (p_e \cdot y_i)\left(r_i e_i + (1 - e_i) c_i\right)$$

$$= \sum_{i \in [n]} y_i \left(\sum_{e \in \mathcal{E}} p_e \left(r_i e_i + (1 - e_i) c_i\right)\right)$$

$$= \sum_{i \in [n]} y_i \left(r_i \left(\sum_{e \in \mathcal{E}: \dots} p_e\right) + c_i \left(1 - \left(\sum_{e \in \mathcal{E}: \dots} p_e\right)\right)\right)$$

$$= \sum_{i \in [n]} y_i \left(r_i \underbrace{\left(\sum_{\substack{e \in \mathcal{E}: \\ e_i = 1}} p_e \right)}_{\in [0,1]} + c_i \left(1 - \sum_{\substack{e \in \mathcal{E} \\ e_i = 1}} \right) \right)$$

Marginal probability of target i being defended.

$$\bar{x} \in \mathcal{P} = \left\{ \left(\sum_{e \in \mathcal{E}} p_e \cdot \bar{e} \right) \in [0,1]^n \;\middle|\; \bar{p} \in \Delta(\mathcal{E}) \right\}.$$

$$= \sum_{i \in [n]} y_i \left(r_i x_i + c_i (1 - x_i) \right)$$

Goal: Compute Stackelberg strategy of the defender.

★ Defender's Best Response Problem (DBR):

$\bar{w} \in \mathbb{R}_+^n \quad \bar{w} \geq 0.$

$$\underset{e \in \mathcal{E}}{\arg\max} \sum_{i \in [n]} (e_i \cdot w_i) \quad \text{(Combinatorial Problem)}.$$

$$= \boxed{\underset{e \in \mathcal{E}}{\arg\max} \langle \bar{e}, \bar{w} \rangle}$$

Suppose attacker is playing. $\bar{y} \in \Delta([n])$

Then the best strategy of the defender is:

$$\underset{x \in \mathcal{P}}{\arg\max} \sum_{i \in [n]} y_i \left(\underline{r_i} x_i + c_i (1 - x_i) \right)$$

$$= \ldots + \left(\sum y_i \cdot c_i \right) \times$$

$$\arg\max_{x \in P} \sum_{i \in [n]}$$

$$= \sum_{i \in [n]} x_i \big((r_i - c_i) \cdot y_i \big) + \sum_{i \in [n]} y_i \cdot c_i$$

independent of $\bar{x}$.

$$= \sum_{i \in [n]} \Big(\sum_{e \in E} p_e \cdot e_i \Big) \underbrace{\big((r_i - c_i) y_i \big)}_{w_i \geq 0}$$

$$= \sum_{e \in E} p_e \sum_{i \in [n]} (e_i \cdot w_i)$$

$$= \max_{\bar{p} \in \Delta(E)} \sum_{e \in E} p_e \underbrace{\big(\langle \bar{e}, \bar{w} \rangle \big)}$$

net payoff from $\bar{e} \in E$ when attacker is playing $\bar{y}$.

$$\boxed{= \max_{e \in E} \langle \bar{e}, \bar{w} \rangle}$$

Thm: If (DBR) problem can be solved in poly-time then S.E. can be found in poly-time.

Pf: (C-S'06) $\to$ $j \in [n]$ write LP(j)

$$\max: \; r_j x_j + c_j (1 - x_j)$$

$$\text{s.t. } \; \xi_j x_j + s_j (1 - x_j) \geq \xi_i x_i + s_i (1 - x_i) \quad \forall i \in [n]$$

$$x \in P \iff \bar{x} = \sum_{\bar{e} \in E} p_e \bar{e}$$

$x \in P \Leftrightarrow \quad x = \sum_{\bar{e} \in \mathcal{E}} p_e \bar{e}$

exponentially many vars.

$p_e \geq 0 \quad , \forall e \in \mathcal{E}$

$\sum_{e \in \mathcal{E}} p_e = 1$

$\downarrow$

DLP(i)

exp. many constraints.

$\downarrow$ Ellipsoid.

Poly-time separation oracle.

$\downarrow$

DBR. problem.

Examples:

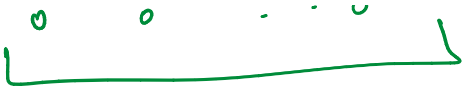
1. ORD. Gates.

n-gates , k-pandora cons.

$\mathcal{E}$ = Subsets of $[n]$ of size $\leq k$.

$DBR = \arg\max_{\bar{e} \in \mathcal{E}} \langle \bar{e}, \bar{w} \rangle \qquad \bar{w} \geq 0$

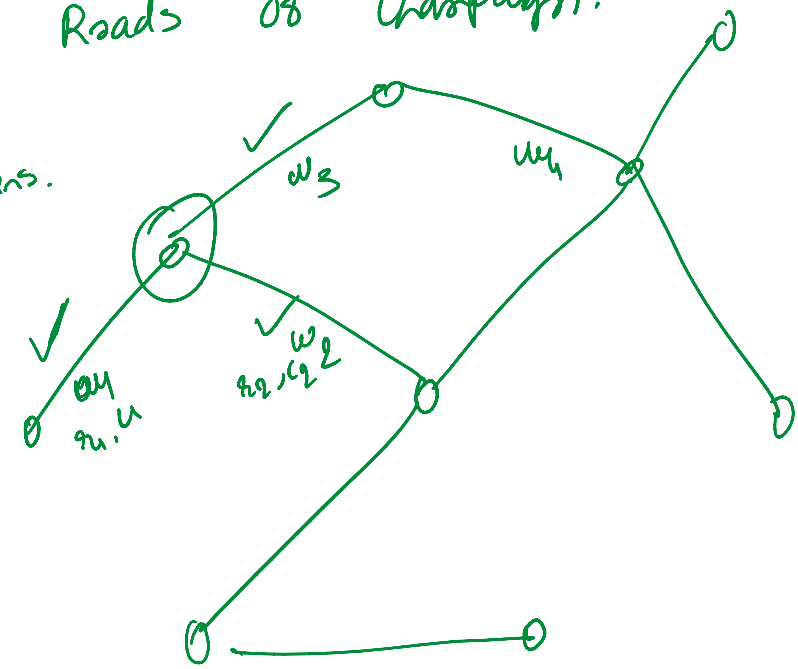
$\underset{0}{w_1} \geq \underset{0}{w_2} \geq \ldots \geq \underset{0}{w_k} \geq \ldots \geq \underset{0}{w_n}$



② Defend Roads of Champaign.

K patrol cars.

n-nodes.



$\mathcal{E}$ = Set of edges defended by k patrol cars.

Road n/w : Goal: maximize the # edges defended.

$$DBR = \max_{\bar{e} \in \mathcal{E}} \langle \bar{e}, \bar{w} \rangle$$

= maximize the total weight of the edges that are covered by k junctions.

≡ max-weight vertex cover problem.

NP-Hard!

③ Air Marshal's Problem:

an AM can defend flight A & flight B if dest. of A = source of B. → #

$S_1, \ldots, S_H$ are all feasible defense strategy based on the #.

set of flights / targets $= \{1, \ldots, N\}$
$w_1 \ldots w_N$.

K AM's $\quad K << N$.

$\mathcal{E} = \quad S \subseteq \{S_1, \ldots, S_H\}$

$$|S| \leq K.$$

$$DBR = \arg\max_{\bar{e} \in \mathcal{E}} \sum_{i \in I}^{N} w_i \, \mathbb{1}_{i \in \bigcup_{T \in S} T}$$

= max coverage problem.

NP-hard!

4 Ports / forests.