Designing the Game to Play: Payoff Manipulation in Security Games

Zheyuan Ryan Shi[1,2], Ziye Tang[2],
Long Tran-Thanh[3], Rohit Singh[4], Fei Fang[2]

Swarthmore College[1]**, Carnegie Mellon University**[2],
University of Southampton[3], World Wide Fund for Nature[4]

Societal Challenges

Infrastructure Patrol

Wildlife Patrol

Transportation Patrol

Go Beyond Patrols

Go Beyond Patrols

Namibia

Poaching Fine: 200K → 25M
Imprisonment: 20y → 25y

the namibian

Increases in poaching fines, sentences coming

News - National | 2017-02-22 Page no: 1

THE environment minister yesterday announced proposed increases to penalties for poaching. Making the announcement in parliament yesterday, minister Pohamba Shifeta said the fine for elephant and rhino poaching would increase from the current maximum of N$200 000 to N$25 million, and the period of imprisonment from the current 20 to 25 years.

Go Beyond Patrols

Australian Government
Great Barrier Reef
Marine Park Authority

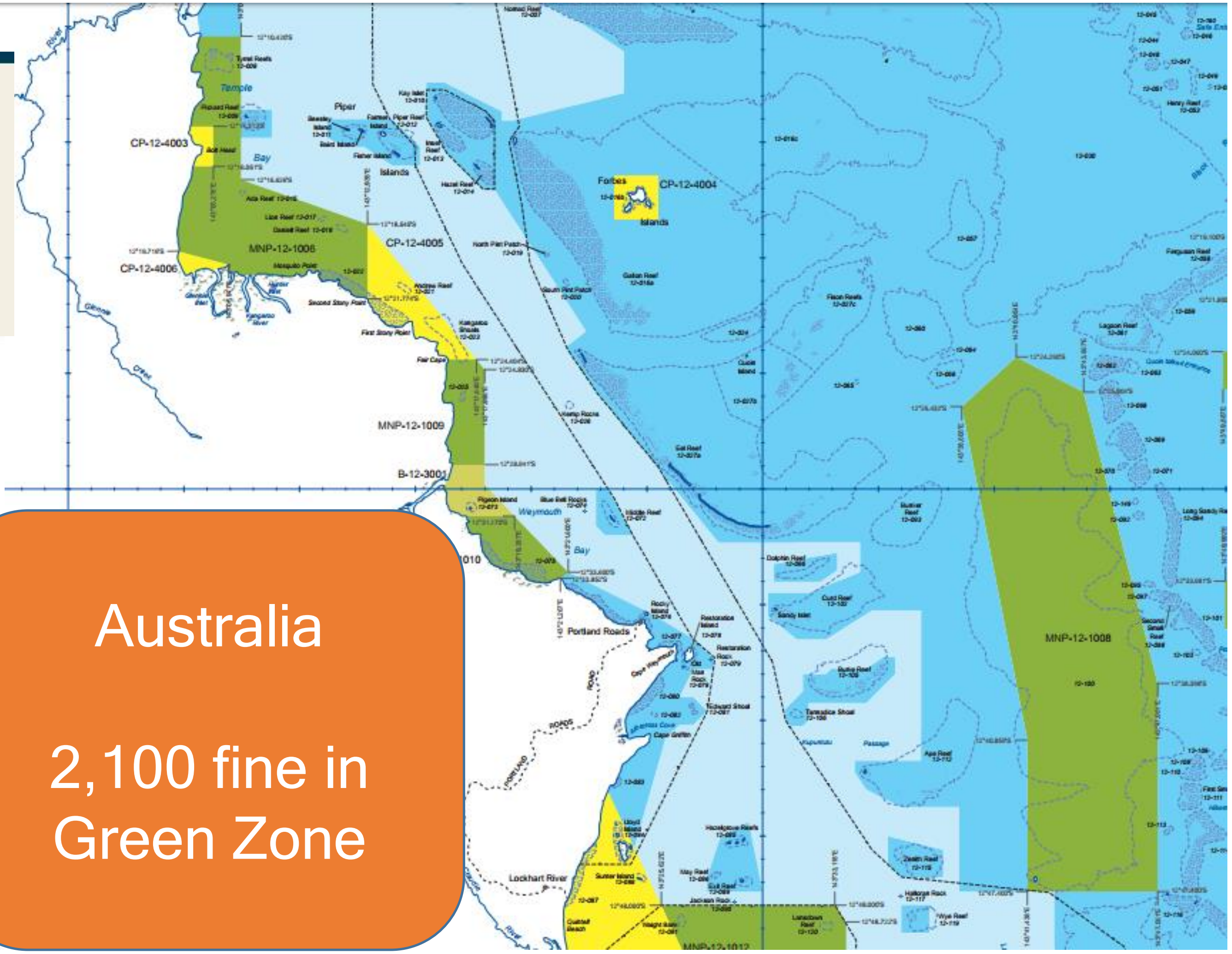
Cairns fishers warned: Fish in a green zone and risk a $2100 fine

Published: 02/06/2017

To support Reef recovery, the Cairns area w… be the target of a month-long compliance blitz which … recreational fishers poaching from green zones … firmly in its sights.

With areas off Cairns ranked among the Great Barrie… Reef's most prolific illegal recreational fishing hotspots, the Great Barrier Reef Marine Park Authority and its partners are cracking down on anyone breaking the zoning rules and threatening Reef resilience.

Recreational fishers doing the wrong thing can expect t… receive an $1800 fine, which will increase to $2100 fro… July 1.



Australia

2,100 fine in Green Zone

Go Beyond Patrols → Design the Game to Play

Australian Government
Great Barrier Reef
Marine Park Authority

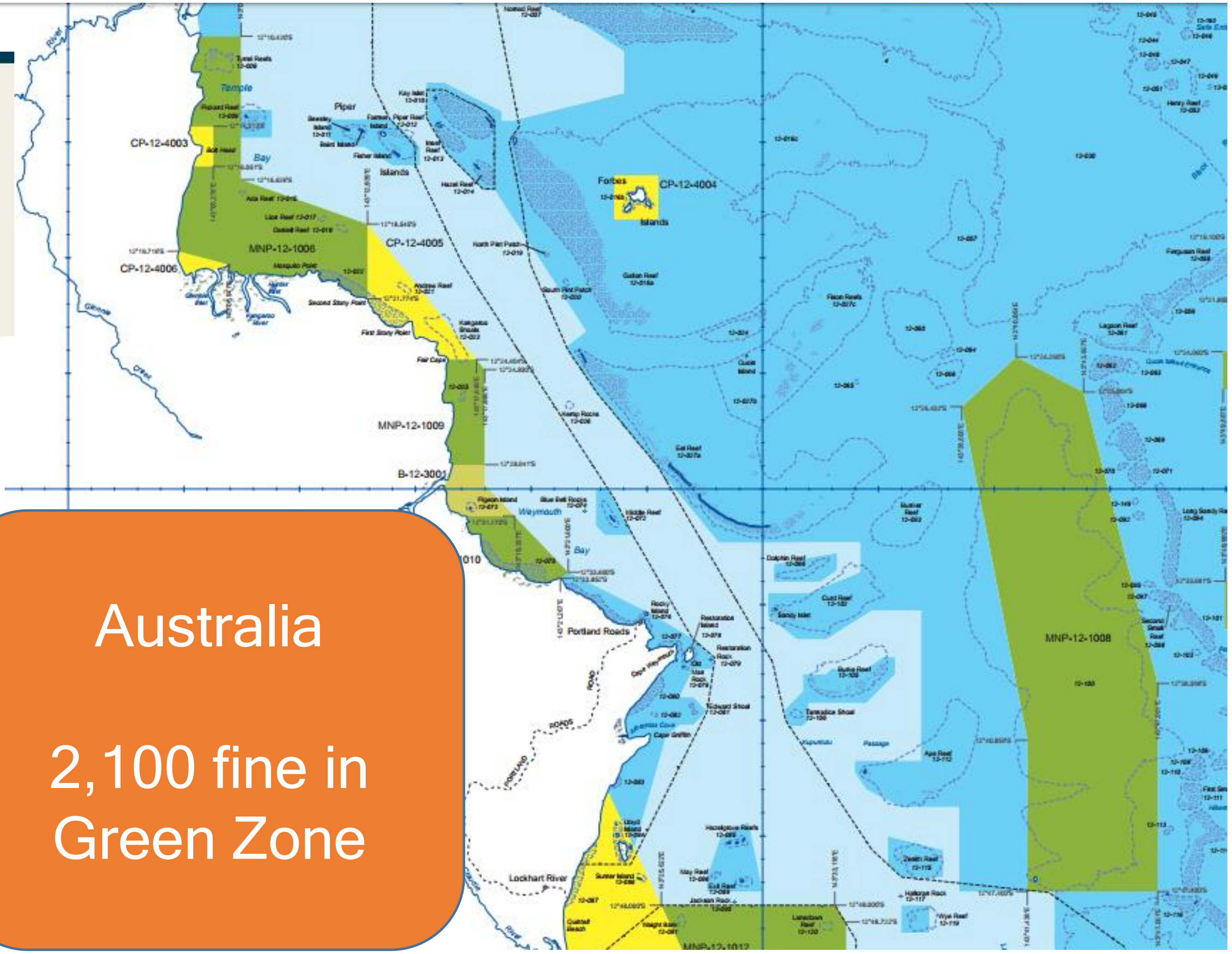
Cairns fishers warned: Fish in a green zone and risk a $2100 fine

Published: 02/06/2017

To support Reef recovery, the Cairns area w… be the target of a month-long compliance blitz which … recreational fishers poaching from green zones … firmly in its sights.

With areas off Cairns ranked among the Great Barrie… Reef's most prolific illegal recreational fishing hotspots, the Great Barrier Reef Marine Park Authority and its partners are cracking down on anyone breaking the zoning rules and threatening Reef resilience.

Recreational fishers doing the wrong thing can expect t… receive an $1800 fine, which will increase to $2100 fro… July 1.



Australia

2,100 fine in Green Zone

Stackelberg Security Game

- Simple security game with multiple targets
  - Defender allocates r resources to protect r out of n targets
  - Attacker chooses a target to attack
- If attack on target i succeeds (i unprotected):
  - Defender gets $P_i^d \leq 0$
  - Attacker gets $R_i^a \geq 0$
- If attack on target i fails (i protected)
  - Defender gets $R_i^d \geq 0$
  - Attacker gets $P_i^a \leq 0$
- Strong Stackelberg Equilibrium (SSE)
  - Defender commits to a mixed strategy.
  - Attacker observes defender's strategy, then attacks.
  - Break ties in favor of the defender.

Why Payoff Manipulation Helps

- Defender can modify attacker's payoff arbitrarily

Attacker

Defender

	Target 1	Target 2
Target 1	1, -2	-5, 4
Target 2	-8, 10	10, -20

Why Payoff Manipulation Helps

- Defender can modify attacker's payoff arbitrarily

Attacker

Defender

		Target 1	Target 2
Target 1	5/6 → ϵ	1, -2	-5, 4 → +∞
Target 2	1/6 → $1-\epsilon$	-8, 10	10, -20

Defender's Expected Utility: $-0.5 \rightarrow 10$

Weighted L^1-norm Budget

R_i^a and P_i^a

$\bar{R}_i^a = R_i^a + \epsilon_i$ and $\bar{P}_i^a = P_i^a + \delta_i$

$\bar{R}_i^a$ and $\bar{P}_i^a$

$$\sum_i \mu_i |\epsilon_i| + \theta_i |\delta_i| \leq B$$

Weighted L^1-norm Budget

- Sub-problem: assume attack target i

Maximize defender EU w.r.t.
c: coverage probability
ϵ: change on R^a
δ: change on P^a
($3n$ variables)

Highest attacker
EU at attack target

$$\max_{\boxed{c,\epsilon,\delta}} \quad U_i^d = R_i^d c_i + P_i^d(1-c_i)$$

$$\text{s.t.} \quad \boxed{\begin{aligned} &U_i^a = c_i(P_i^a + \delta_i) + (1-c_i)(R_i^a + \epsilon_i) \\ &\geq U_j^a = c_j(P_j^a - \delta_j) + (1-c_j)(R_j^a - \epsilon_j), \forall j \neq i \end{aligned}}$$

$$\boxed{\sum\nolimits_j (\mu_j \epsilon_j + \theta_j \delta_j) \leq B}$$

Budget constraint

$$\boxed{\sum\nolimits_j c_j \leq r}$$

Defender resource

$$R_j^a - \epsilon_j \geq 0, \quad \forall j \neq i$$

$$P_i^a + \delta_i \leq 0$$

$$c_j, \epsilon_j, \delta_j \geq 0, \quad c_j \leq 1, \quad \forall j \in T$$

- Defender reward R^d
- Defender penalty P^d
- Attacker reward R^a
- Attacker penalty P^a
- Budget B

Weighted L^1-norm Budget

- Sub-problem: assume attack target i

Maximize defender EU w.r.t.
c: coverage probability
ϵ: change on R^a
δ: change on P^a
($3n$ variables)

Highest attacker EU at attack target

$$
\begin{aligned}
\max_{c,\epsilon,\delta} \quad & U_i^d = R_i^d c_i + P_i^d (1 - c_i) \\
\text{s.t.} \quad & U_i^a = \boxed{c_i (P_i^a + \delta_i)} + (1 - c_i)(R_i^a + \epsilon_i) \\
& \geq U_j^a = c_j (P_j^a - \delta_j) + (1 - c_j)(R_j^a - \epsilon_j), \forall j \neq i \\
& \sum_j (\mu_j \epsilon_j + \theta_j \delta_j) \leq B \\
& \sum_j c_j \leq r \\
& R_j^a - \epsilon_j \geq 0, \quad \forall j \neq i \\
& P_i^a + \delta_i \leq 0 \\
& c_j, \epsilon_j, \delta_j \geq 0, \quad c_j \leq 1, \quad \forall j \in T
\end{aligned}
$$

Budget constraint

Defender resource

- Defender reward R^d
- Defender penalty P^d
- Attacker reward R^a
- Attacker penalty P^a
- Budget B

Weighted L^1-norm Budget

Theorem 1

- There is an additive $\max_i \frac{2\rho_0(R_i^d - P_i^d)}{R_i^a}$ -approximation algorithm.

Theorem 2

- With budget $B \leq \min_i\{|P_i^a|, R_i^a\}$ and uniform cost, there exists an optimal solution which manipulates at most two targets.

Theorem 3

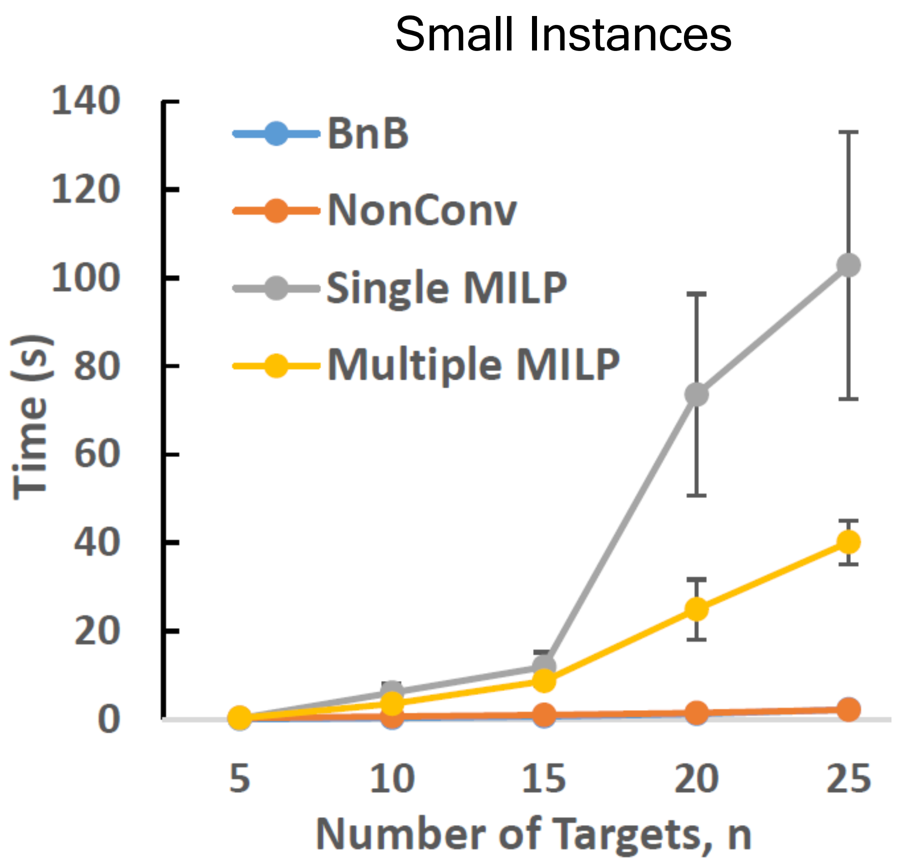
- With budget $B \leq \min_i\{|P_i^a|, R_i^a\}$ and uniform cost, there exists a polynomial-time approximation scheme (PTAS).

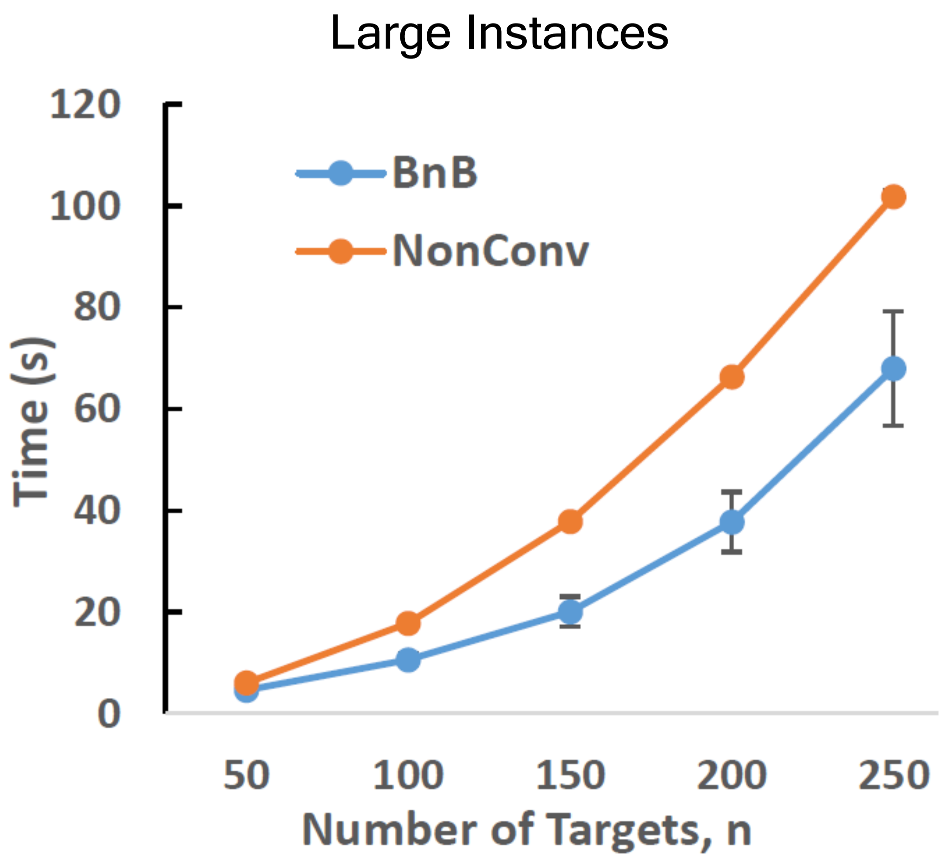
Weighted L^1-norm Budget

Branch and Bound

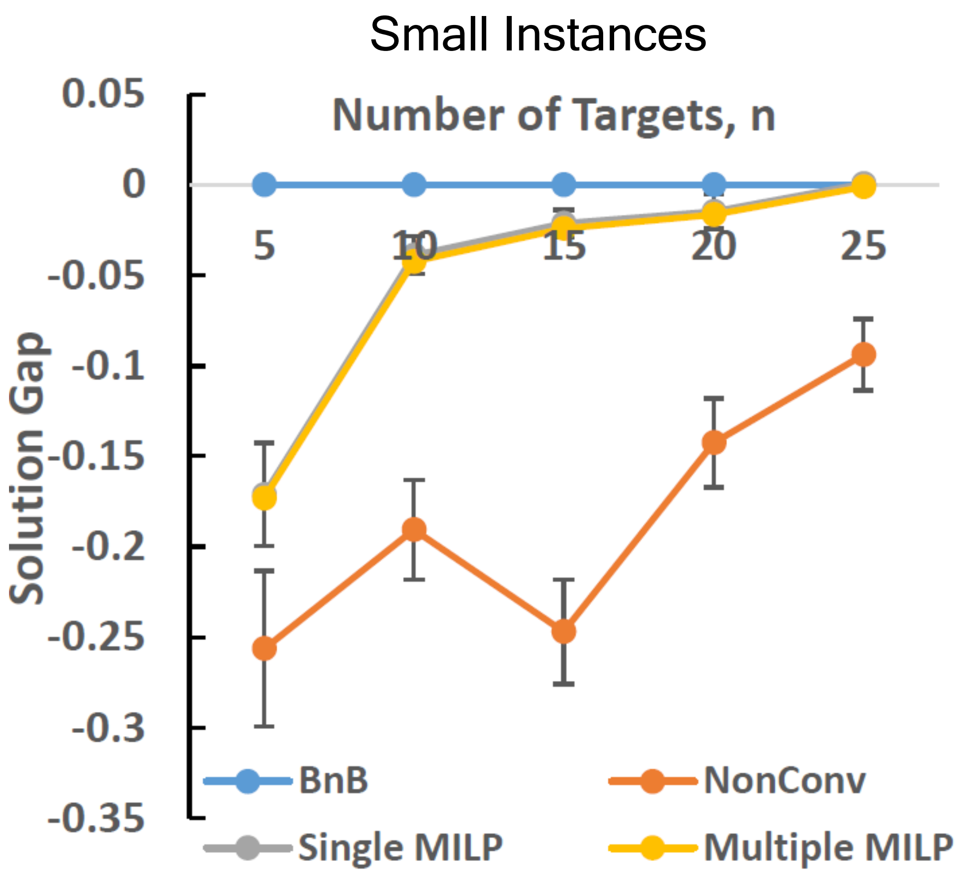
- Each sub-problem assumes an attack target
- Lower bound ← feasible solution
- Upper bound ← budget overuse

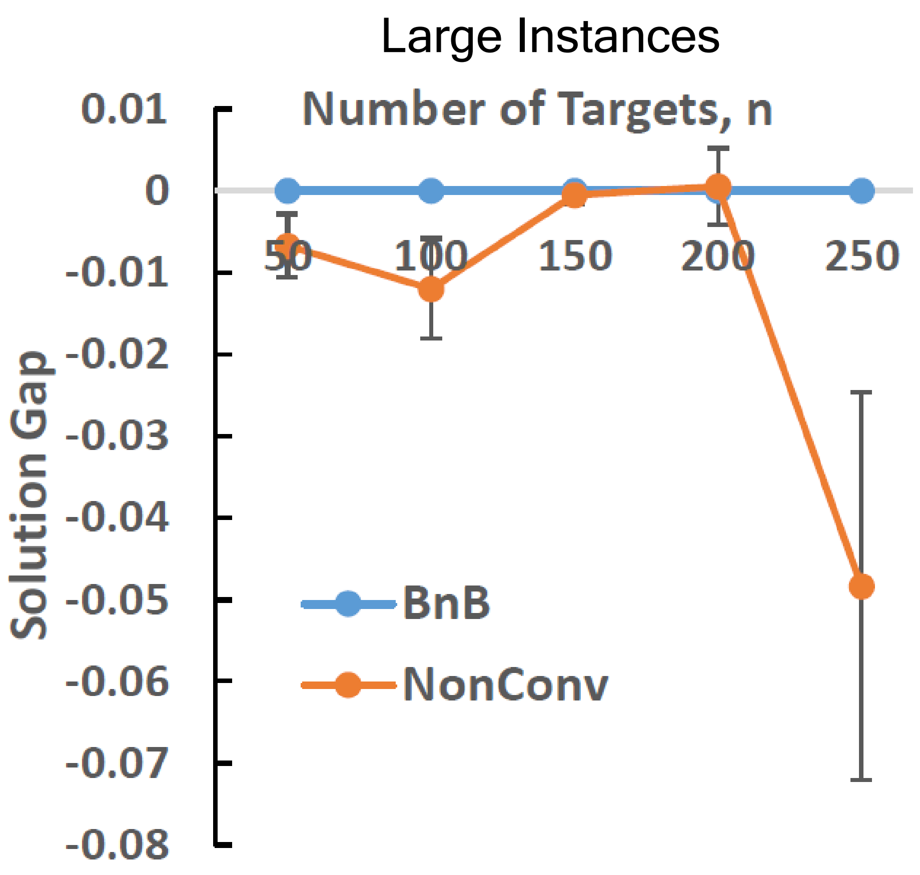
Weighted L^1-norm: Experimental Results - Runtime





Weighted L^1-norm: Experimental Results – Solution Gap





Other Forms of Budget Constraint

Theorem 4 Weighted L^∞-norm Budget

- With budget constraint in weighted L^∞-norm, the problem reduces to a fixed-payoff security game, and admits a $O(n^2 \log n)$ algorithm.

Theorem 5 L^0-norm Budget

- Budget constraint in L^0-norm admits a $O(n^3)$ algorithm.

Related Works

- Audit Games
  - Blocki et al., 2013, 2015
- Incomplete Matrix Games
  - Brill et al., 2016
- Honeypots
  - Schlenker et al., 2018; Horák et al., 2017
- Payoff uncertainty
  - Kiekintveld et al., 2013; Yin and Tambe, 2012; Letchford et al., 2009; Blum et al., 2014
- Mechanism Design (two-layered strategy design)
  - Kang and Wu, 2015; Xue et al., 2016; Sharma and Williamson, 2007; Yang et al., 2012

Conclusions and Future Directions

- We study how to manipulate payoff in SSG under several forms of budget constraints.
- L^1-norm case: branch-and-bound in general, PTAS for a special case
- L^0-norm and L^∞-norm are poly-time solvable

- More complicated constraint settings
- Implications for zero-poaching

Thank you!

Zheyuan Ryan Shi
ryanshi@cmu.edu

Ziye Tang
ziyet@andrew.cmu.edu

Long Tran-Thanh
l.tran-thanh@soton.ac.uk

Rohit Singh
rsingh@wwfnet.org

Fei Fang
feifang@cmu.edu