Unleashing Dec-MDPs in Security Games: Enabling Effective Defender Teamwork

Eric Shieh, Albert Xin Jiang, Amulya Yadav, Pradeep Varakantham*, and Milind Tambe

University of Southern California
***Singapore Management University**

Deployed Security Game Applications

- Ports & Port Traffic (2011)
  - *US Coast Guard*

- Airports & flights (2007)
  - *Transportation Security Agency (TSA)*
  - *Federal Air Marshal Service (FAMS)*

Goal of Paper: Add complex defender coordination – missing from previous work

Security in Metro Systems

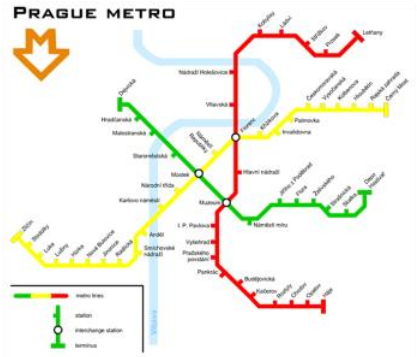
- Key example where coordination is needed
- Examples of London and Madrid (other areas in the world also targeted)

July 7, 2005 London bombings:
Suicide bombers killed 52 civilians and injured over 700 targeting London Underground and bus

2004 Madrid train bombings:
Bombs killed 191 people and wounded 1,800.

Security Game (Example Metro)

- Domain: Metro System (subway/rail)
- 2 player Stackelberg game
  - *1st player: Defender (e.g. police)*
    - Multiple resources
    - Conducts multiple patrols
  - *2nd player: Attacker (e.g. terrorist)*
    - Conducts surveillance of defender's strategy
    - Chooses station/target to attack

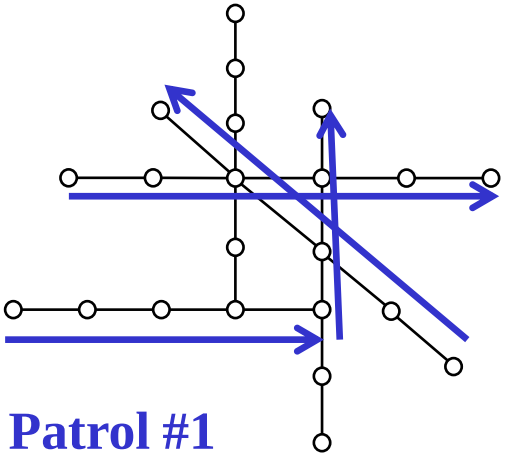


USC Viterbi School of Engineering *Teamcore Research Group*

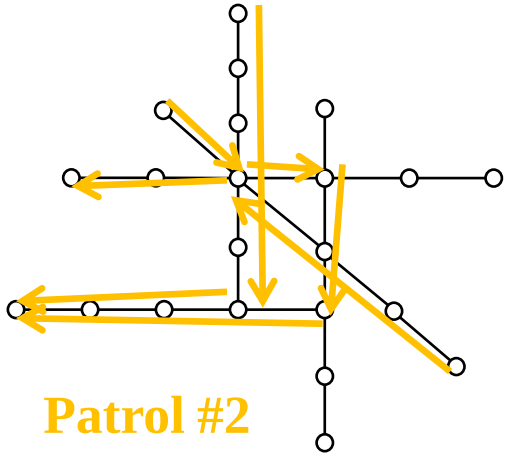
Sample Patrol Strategy (Patrol #1)

Sample Metro System

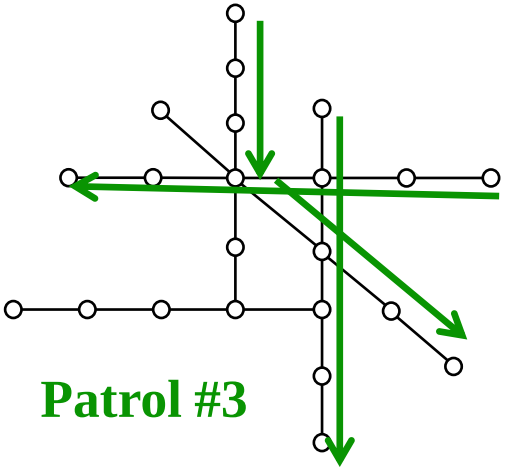
Various Patrol Strategies



Patrol #1



Patrol #2



Patrol #3

Sample Defender Strategy	
Patrol #1	30%
Patrol #2	10%
Patrol #3	15%
…	…

Challenge: Joint Activity (Patrol #4)

Sample Metro System

t_1 t_2 t_{20} t_7 t_{16} t_{17} t_{18} t_{19} t_6 t_{11} t_{22} t_{12}

Not easily decomposable!

Large Combinatorial Problem:

N – defender patrols

K – # resources

$\mathbf{N^K}$ – exponential increase

Joint Activity

Challenge: Execution Uncertainty

Stackelberg Security Game (SSG)

Adversary

Defender	Attack t_1 at 8 AM	Attack t_1 at 9 AM	…	Attack t_8 at 5 PM	Defender Strategy
Patrol #1	7, -4	-2, 3	…	-2, 3	30%
Patrol #2	-7			-2, 3	10%
Patrol #3	-7			4, -3	15%
…					

10^{21} or higher defender strategies; does not fit into memory!

Problem Statement

- How to efficiently compute the defender's optimal patrol strategy assuming a strategic adversary
  - *Multiple defender resources (allowing joint activities)*
  - *Execution uncertainty of the defender resources*
  - *Exponential number of possible defender strategies (due to multiple coordinated resources and uncertainty)*

Contributions

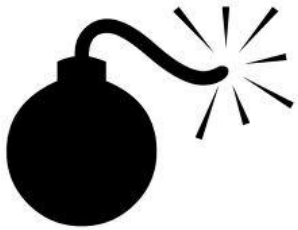
- New general SSG model to handle **execution uncertainty** + **coordination** in Security Games
  - *Integrate Decentralized Markov Decision Problems (Dec-MDP) and Security Games*
    - Dec-MDP: Coordination under uncertainty [*Bernstein2002*, *Becker2004*]
  - *Blends two research areas: Security Games and Dec-MDPs*
- New algorithms to solve the SSG
  - *Use of column generation framework*
  - *Fast heuristics to scale up*

Outline

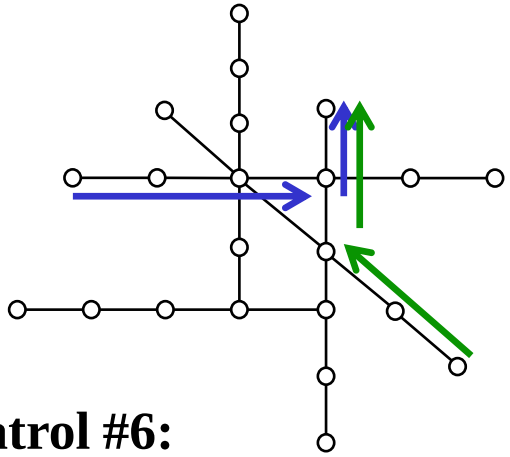
- Introduction
- Background/Contributions
  - *Planning under uncertainty (Dec-MDPs)*
  - *Column generation framework (Scalability)*
- Evaluation
- Summary

Dec-MDP

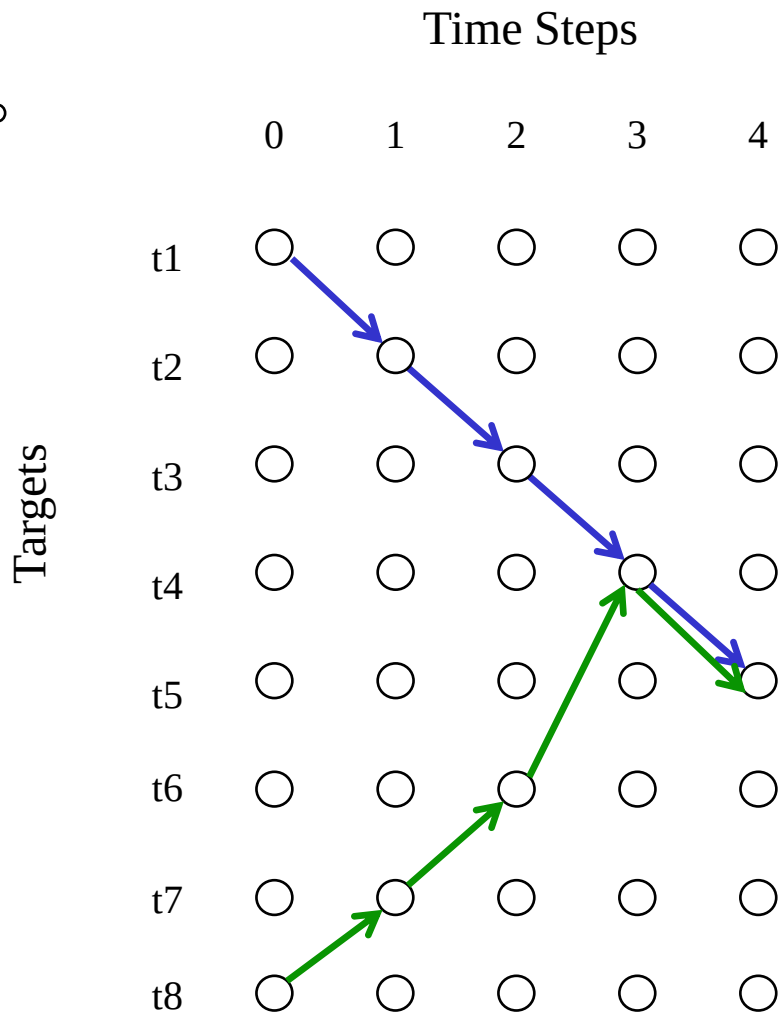
- Decentralized Markov Decision Process: multi-agent planning under uncertainty
  - *Multiple agents (defender resources)*
  - *No communication (underground)*
  - *Uncertainty in execution (delays)*
- Example: Full Scale Exercise
  - *Actual deployment of 23 teams of different resources*



Patrol strategy for two resources



Patrol #6:
Resource 1
Resource 2

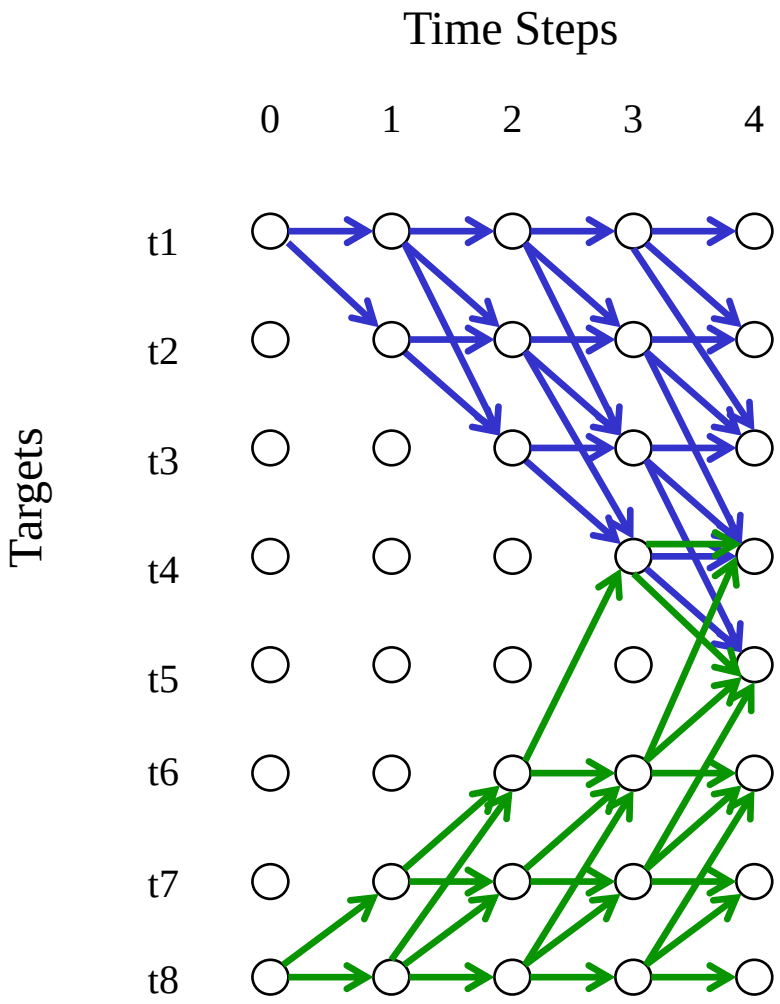


Policy for two resources

- Multiple paths to handle **execution uncertainty**

- Actions for each state

Patrol Policy #6:
Resource 1
Resource 2



Dec-MDPs and Security Games

- Challenges:
  - *Security Games– Never investigate coordination under uncertainty*
  - *Dec-MDPs – Not account for adversarial agent*
- Objective: Develop efficient methods to compute defender patrol strategies to address execution uncertainty and coordinated activities
- Contribution: **First** study to utilize Dec-MDP and security games

Outline

- Introduction
- Background/Contributions
  - *Planning under uncertainty (Dec-MDPs)*
  - *Column generation framework (Scalability)*
- Evaluation
- Summary

Scalability

7 targets
4 targets/patrol
2 defender resources
3 defender activities

⟶ 3.8 x 10^{10} pure strategies for defender

		Target #1	Target #2	…
x_1	{Patrol 1, Patrol 1}	7, -4	-2, 3	…
x_2	{Patrol 1, Patrol 2}	-7, 7	4, -3	…
x_3	{Patrol 1, Patrol 3}	7, -4	-2, 3	…
	…	…	…	
⋮	…			
x_n	…			

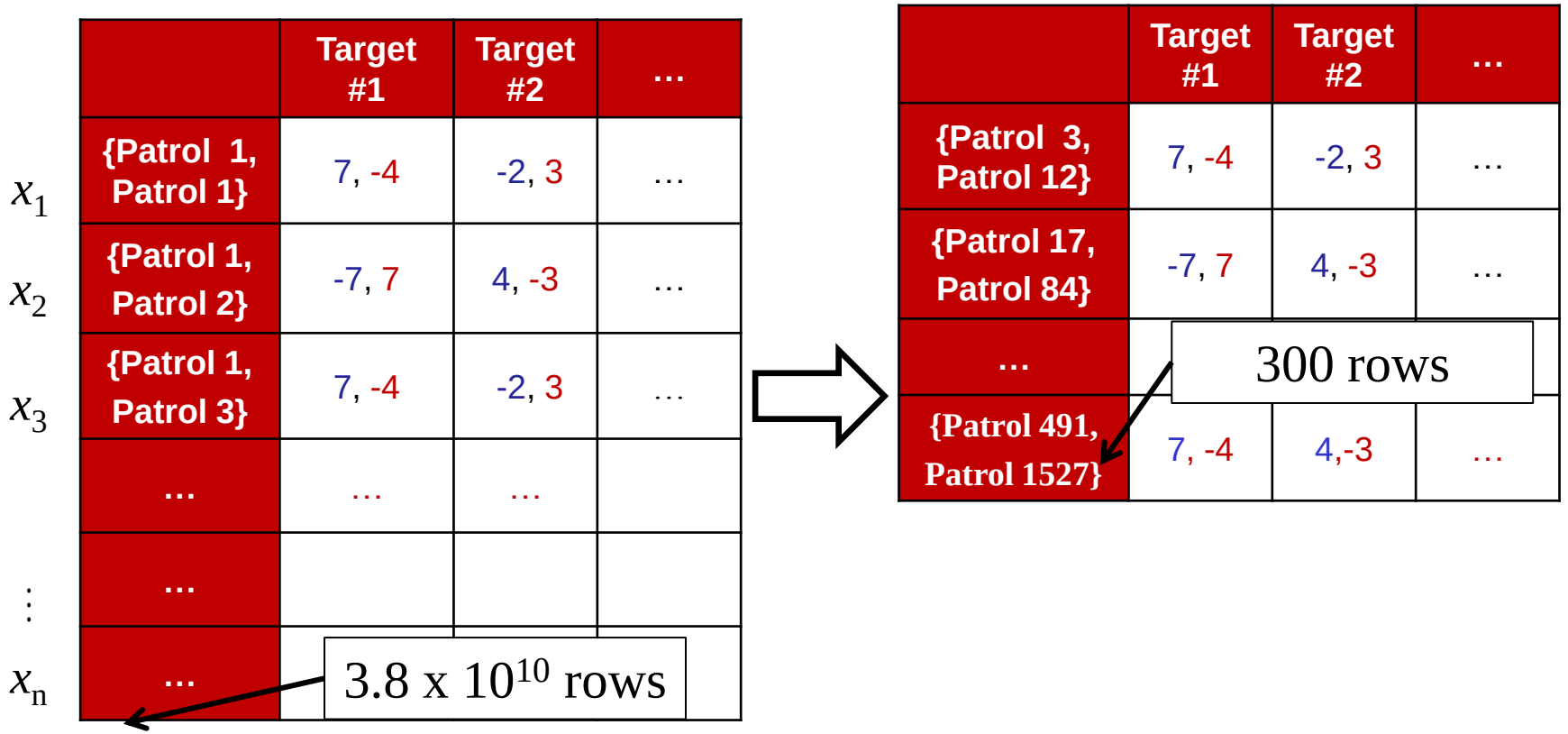
3.8 x 10^{10} rows

$x_1 = 0.0$
$x_2 = 0.0$
$x_3 = 0.05$
$x_4 = 0.0$
⋮
$x_{3422} = 0.174$
$x_{3423} = 0.0$
⋮
$x_{22845} = 0.207$
⋮
$x_n = 0.0$

Support Set

Column Generation

- Incremental strategy generation
- Operations research [*Barnhart94*], Security games [*Jain10*]



Column Generation

Master Component: LP with *few* pure strategies

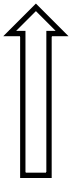
	Target #1	Target #2
Patrol Strategy #1	7, -4	-2, 3
Patrol Strategy #2	-7, 7	4, -3

Slave Component: Patrol Strategy #3 pure strategy

	Target #1	Target #2
Patrol Strategy #1	7, -4	-2, 3
Patrol Strategy #2	-7, 7	4, -3
Patrol Strategy #3	7, -4	4, -3

Column Generation

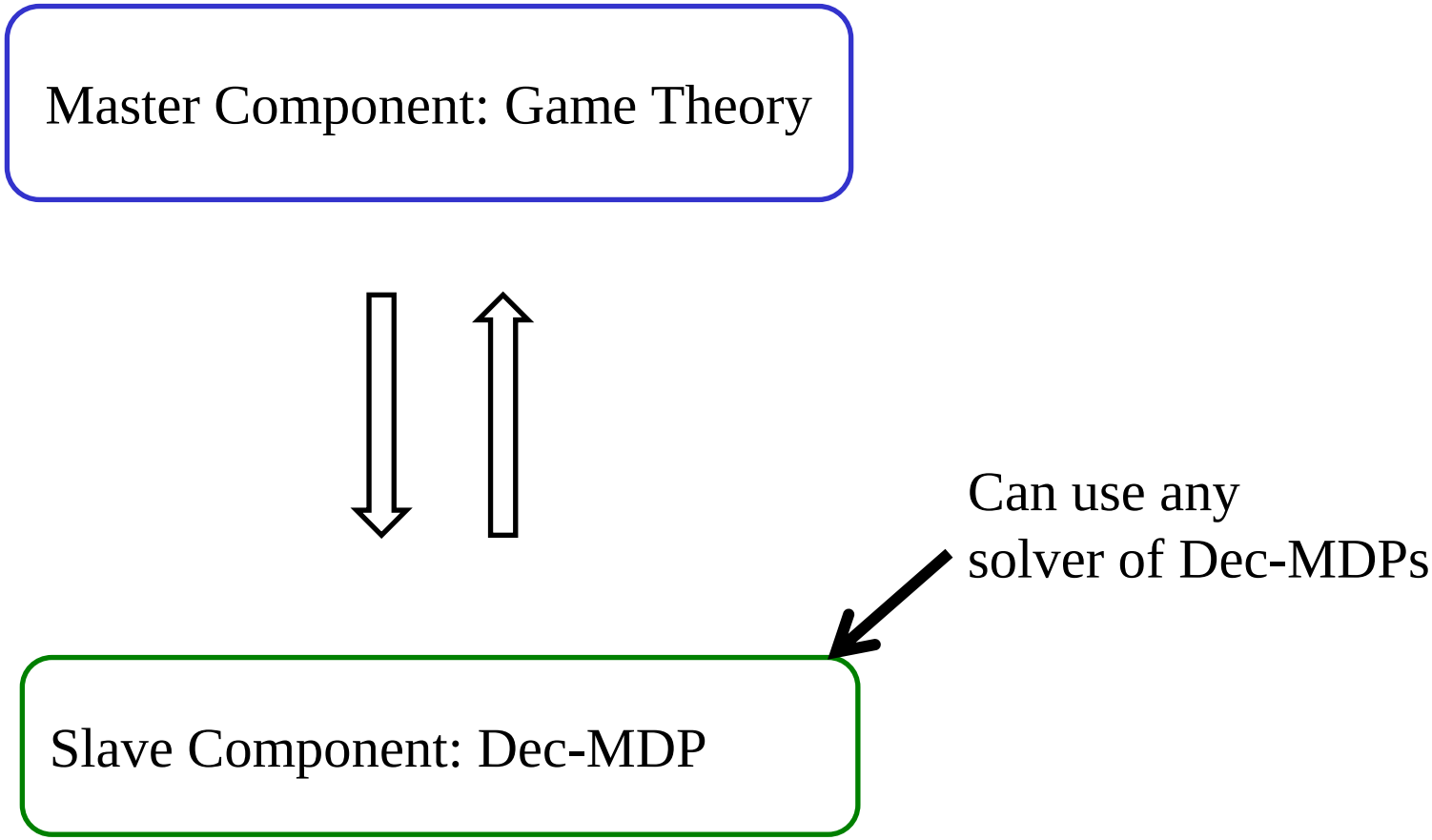
Master Component: LP with *few* pure strategies



Slave Component: Generates *new* pure strategy

	Target #1	Target #2
Patrol Strategy #1	7, -4	-2, 3
Patrol Strategy #2	-7, 7	4, -3
Patrol Strategy #3	7, -4	4, -3

Decomposition of Column Generation



Dec-MDP Slave Component

TREMOR style algorithm to solve Dec-MDP [*Varakantham09*]

Algorithm 1 SolveSlave($\mathbf{y}, \mathcal{G}$)

1: Input: $\mathbf{y}, \mathcal{G}$
2: Initialize π^j
3: **for all** $r \in R$ **do**
4: $\quad \boldsymbol{\mu}_r \leftarrow \text{ComputeModifiedReward}(\pi^j, \mathbf{y}, \mathcal{G}_r)$
5: $\quad \pi_r \leftarrow \text{SolveSingleMDP}(\boldsymbol{\mu}_r, \mathcal{G}_r)$
6: $\quad \pi^j \leftarrow \pi^j \cup \pi_r$
7: $\mathbf{P}^j \leftarrow \text{ConvertToColumn}(\pi^j)$
8: return $\pi^j, \mathbf{P}^j$

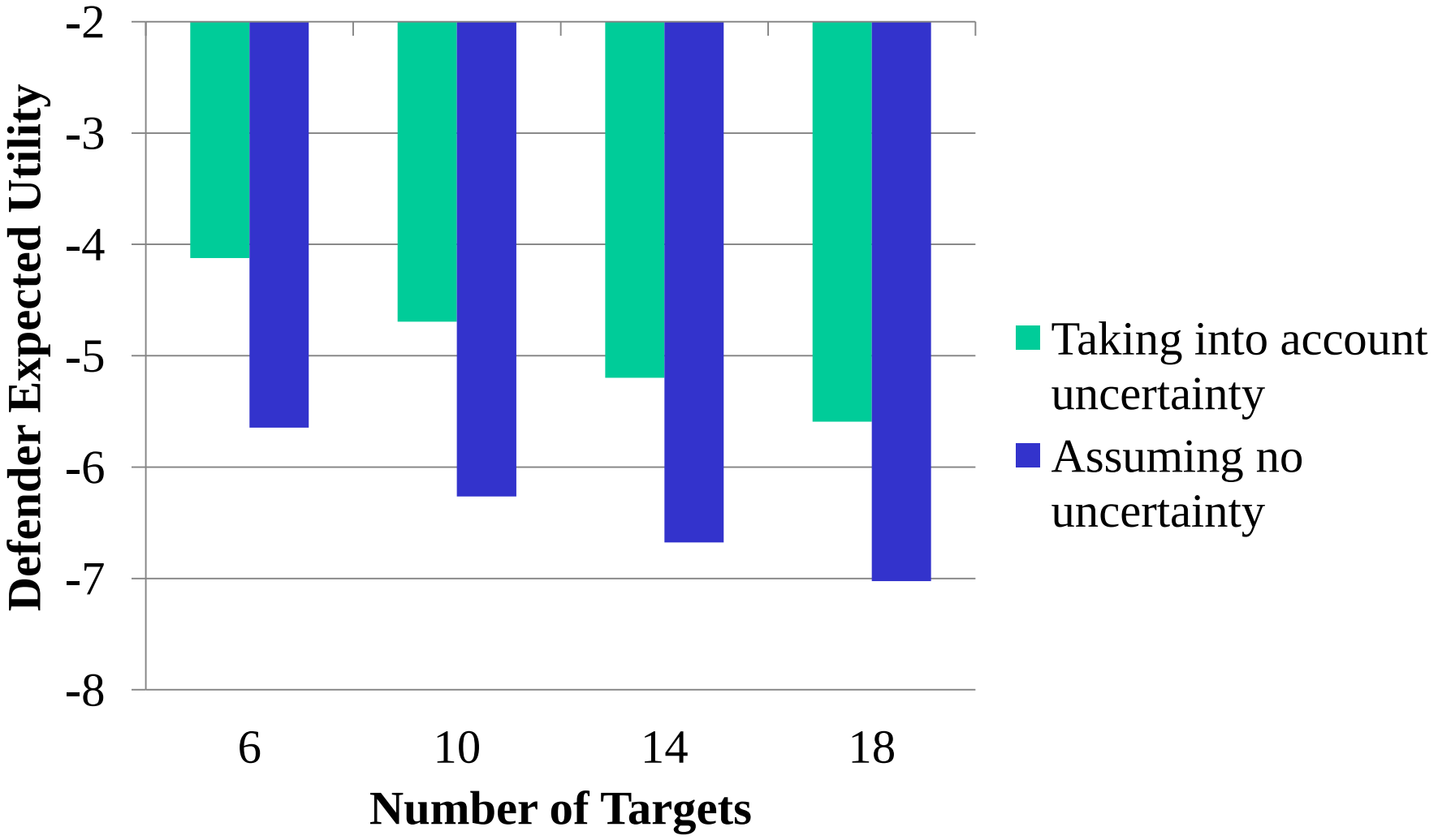
Outline

- Introduction
- Background/Contributions
- Evaluation
- Summary

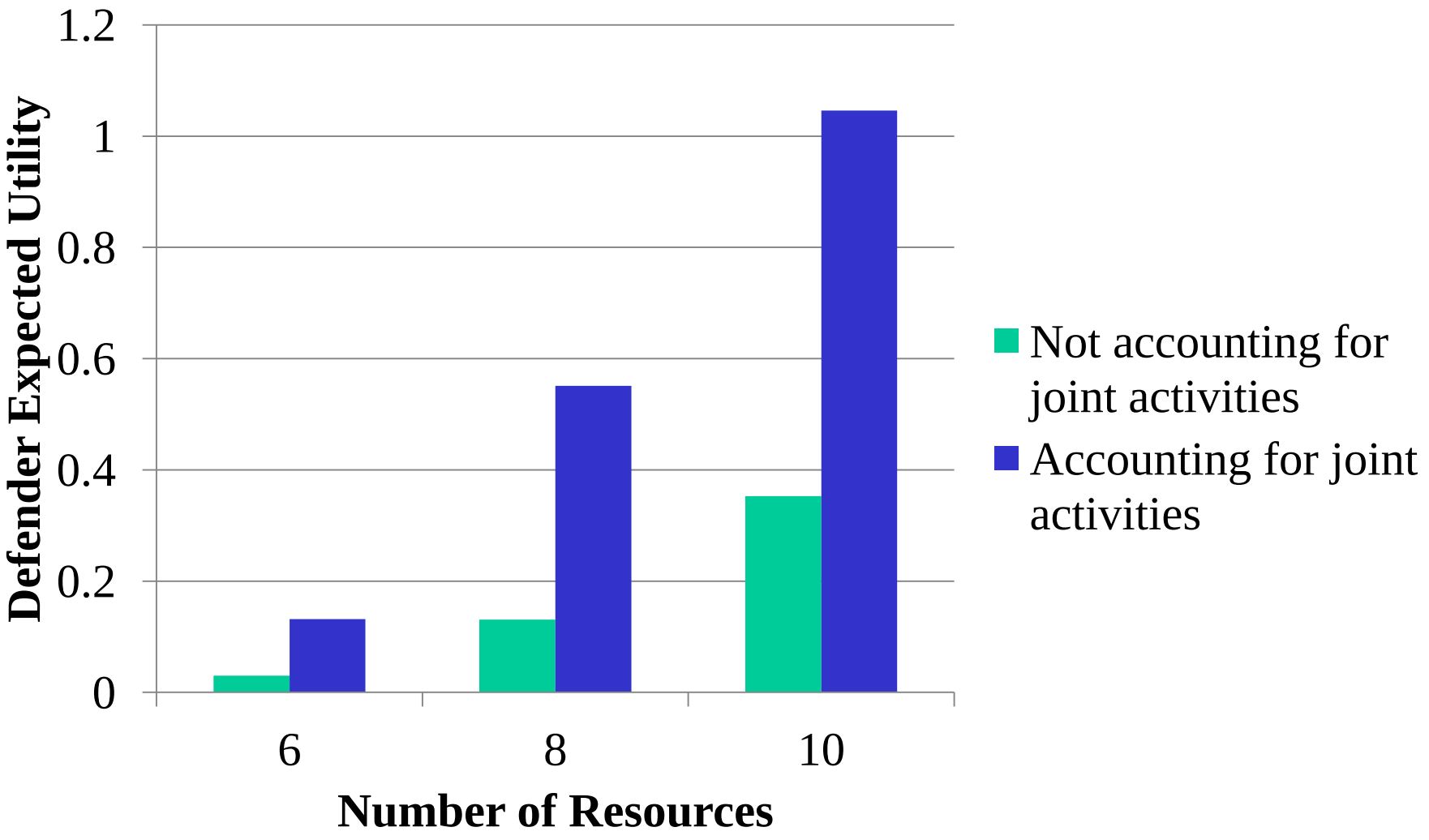
Evaluation

- 30 game instances
- Payoffs range: [-10, 10]
- 8 targets, 8 time steps, 4 resources (unless otherwise noted)
- 5% probability of delay

Importance of addressing uncertainty

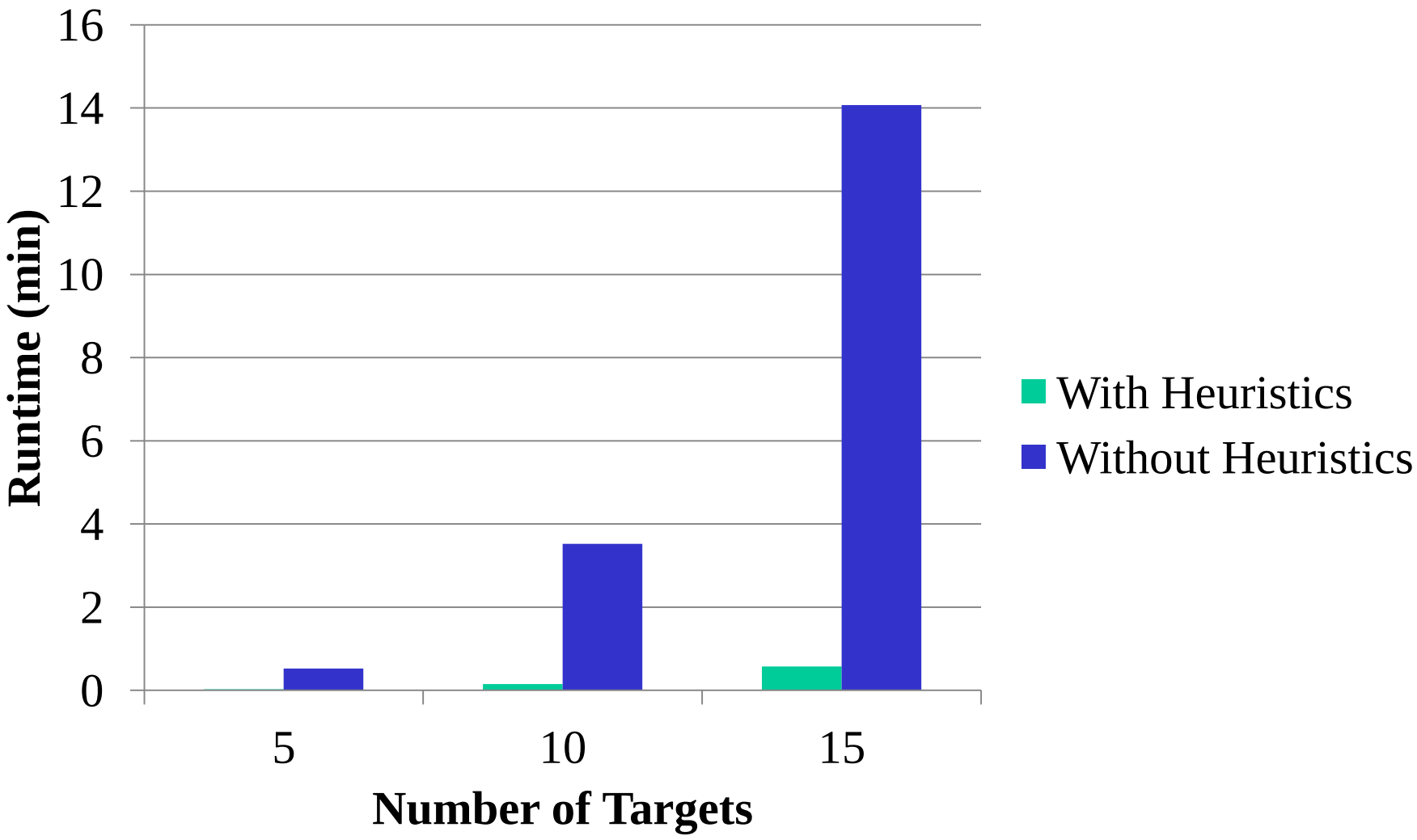


Importance of accounting for joint activities



USC Viterbi School of Engineering Teamcore Research Group

Runtime Improvements



Summary

- Model and solve execution uncertainty + coordination in Security Games
- Combine Dec-MDPs with Game Theory (Security Games)

Thanks!

Contact: eshieh@usc.edu