Game Theory and Security

MILIND TAMBE

AI & Multiagent Systems Research for Social Impact

Public Health

Conservation

Public Safety and Security

Key Research Challenge

Optimize Our Limited Intervention Resources

Outline

Public Safety and Security:
Stackelberg Security Games

Conservation/Wildlife Protection:
Green Security Games

9/11/2022

Date: 10/13/2022 (from ny1.com)

Around the World (2002-2005)

11 July 2006: Mumbai

ARMOR Airport Security: LAX(2007)

Erroll Southers

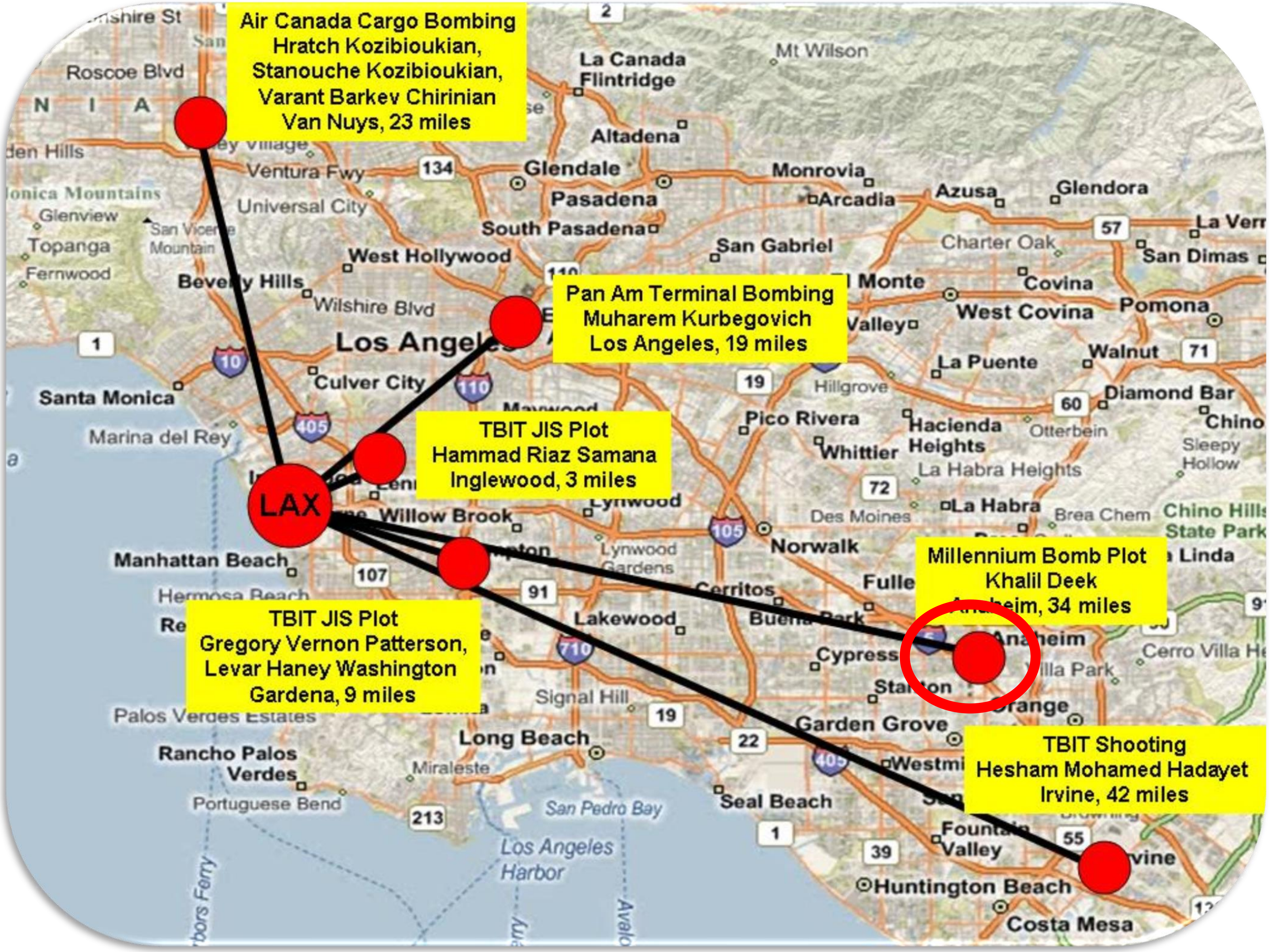
LAX Airport, Los Angeles

LAX Airport Case: Optimize Limited Security Resources

Eight Inbound Roads, Eight Terminals: Limited Staff, Canines

How to optimize limited security resources?

Background on LAX Airport Threats: Surveillance Opportunity



Game Theory for Security Resource Optimization

New Model: Stackelberg Security Games, key aspects for tractability

Set of targets, payoffs based on targets covered or not

Stackelberg Leader-Follower formulation

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

Game Theory for Security Resource Optimization

New Model: Stackelberg Security Games

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

Model: Stackelberg Security Games

Can we use Stackelberg Security Games for security resource optimization?

Stackelberg: Defender commits to randomized strategy, adversary responds

Security optimization: Not 100% security; increase cost/uncertainty to attackers

Challenges faced: Massive scale games

Adversary

Defender

	Terminal #1	Terminal #2
Terminal #1	4, -3	-1, 1
Terminal #2	-5, 5	2, -1

ARMOR at LAX
Basic Security Game Operation [2007]


Kiekintveld


Pita

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

Mixed Integer Program

Pr (Canine patrol, 8 AM @Terminals 2,5,6) = 0.17

Canine Team Schedule, July 28								
	Term 1	**Term 2**	**Term 3**	**Term 4**	**Term 5**	**Term 6**	**Term 7**	**Term 8**
8 AM		Team1			Team3	Team5		
9 AM			Team1	Team2				Team4
…	…	…	…	…	…	…	…	…

OK IF YOU DO NOT FOLLOW THIS SLIDE
Mixed Integer Program [2007]


Kiekintveld


Pita

j →

i ↓

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

We are trying to Find xi

$$\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j$$ ← Maximize defender expected utility

$$s.t. \sum_i x_i = 1$$ ← Defender mixed strategy

$$\sum_{j \in Q} q_j = 1$$ ← Adversary response

$$0 \le (a - \sum_{i \in X} C_{ij} x_i) \le (1 - q_j) M$$ ← Adversary best response

SECURITY GAME PAYOFFS [2007]
Previous Research Provides Payoffs in Security Games

	Target #1	Target #2	Target #3
Defender #1	2, -1	-3, 4	-3, 4
Defender #2	-3, 3	3, -2	….
Defender #3	….	….	….

+ Handling Uncertainty

$$\max \sum_{i \in X} \sum_{j \in Q} R_{ij} \times x_i \times q_j$$

Maximize defender expected utility

ARMOR:
Optimizing Security Resource Allocation [2007]

First application: Computational game theory for operational security

January 2009

- January 3rd — *Loaded 9/mm pistol*
- January 9th — *16-handguns, 1000 rounds of ammo*
- January 10th — *Two unloaded shotguns*
- January 12th — *Loaded 22/cal rifle*
- January 17th — *Loaded 9/mm pistol*
- January 22nd — *Unloaded 9/mm pistol*

ARMOR AIRPORT SECURITY: LAX [2008]
Congressional Subcommittee Hearings

Commendations
City of Los Angeles

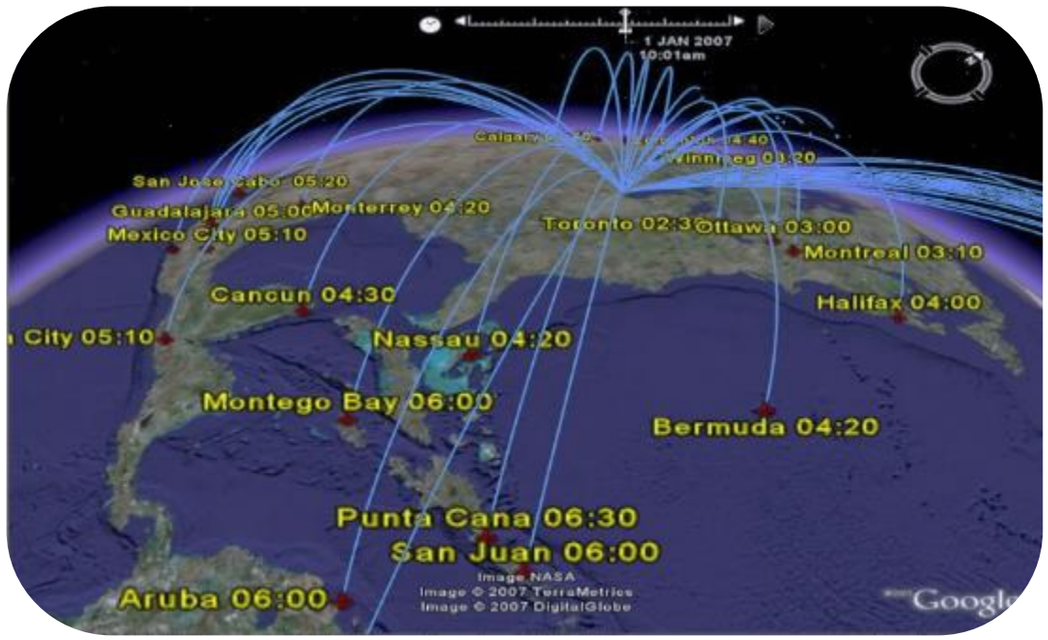
Erroll Southers testimony
Congressional subcommittee

Newsweek

ARMOR…throws a digital cloak of invisibility….

Federal Air Marshals Service [2009]

Visiting Freedom Center: Home of Federal Air Marshals Service



	Strategy 1	Strategy 2	Strategy 3	Strategy 4
Strategy 1	IRIS 1000 flights/day Actions: ~10^{41}			
Strategy 2				
Strategy 3				
Strategy 4				

Scale Up Difficulty [2009]


Kiekintveld


Jain

x_i Defender mixed strategy

1000 flights, 20 air marshals:

10^{41} combinations

$$\max_{x,q} \sum_{i \in X} \sum_{j \in Q} R_{ij} x_i q_j$$

$$s.t. \sum_i x_i = 1, \sum_{j \in Q} q_j = 1$$

$$0 \le (a - \sum_{i \in X} C_{ij} x_i) \le (1 - q_j) M$$

	Attack 1	Attack 2	Attack …	Attack 1000
1 ,2, 3 ..	5,-10	4,-8	…	-20,9
1, 2, 4 ..	5,-10	4,-8	…	-20,9
1, 3, 5 ..	5,-10	-9,5	…	-20,9
…				
…	← **10^{41} rows**			

Scale Up [2009]
Exploiting Small Support Size


Kiekintveld


Jain

Small support set size:
Most x_i variables zero

1000 flights, 20 air marshals:

10^{41} combinations

~~$X_{123} = 0.0$~~

$X_{124} = 0.239$

~~$X_{135} = 0.0$~~

$X_{378} = 0.123$

	Attack 1	Attack 2	Attack …	Attack 1000
~~1 ,2, 3 ..~~	~~5, 10~~	~~4, 8~~	…	~~-20,9~~
1, 2, 4 ..	5,-10	4,-8	…	-20,9
~~1, 3, 5 ..~~	~~5, 10~~	~~9,5~~	…	~~20,9~~
...				
...	← **10^{41} rows**			

New Exact Algorithm for Scale up


Kiekintveld


Jain

Incremental strategy generation: First for Stackelberg Security Games

Primary

	Attack 1	Attack 2	…	Attack 6
1,2,4	5,-10	4,-8	…	-20,9

Secondary (LP Duality Theory)
Best new pure strategy

	Attack 1	Attack 2	…	Attack 6
1,2,4	5,-10	4,-8	…	-20,9
3,7,8	-8,10			

	Attack
1,2,4	5,-10
3,7,8	-8,10
…	…

GLOBAL OPTIMAL
1000 defender strategies
NOT 10^{41}

lity Theory)
re strategy

IRIS: Deployed FAMS [2009-]

Significant change in FAMS operations

Transportation Security Administration

Office of Law Enforcement/Federal Air Marshal Service

Milind Tambe

In recognition and appreciation of your outstanding achievement in developing the Intelligent Randomization In Scheduling (IRIS) program to advance the mission of the Office of Law Enforcement/Federal Air Marshal Service.

This 2nd day of September, 2011

James B. Current
Studies, Research and Analysis
Office of Flight Operations

September 2011: Certificate of Appreciation (Federal Air Marshals)

Questions?

Lesson 1: Immersion & Partnership

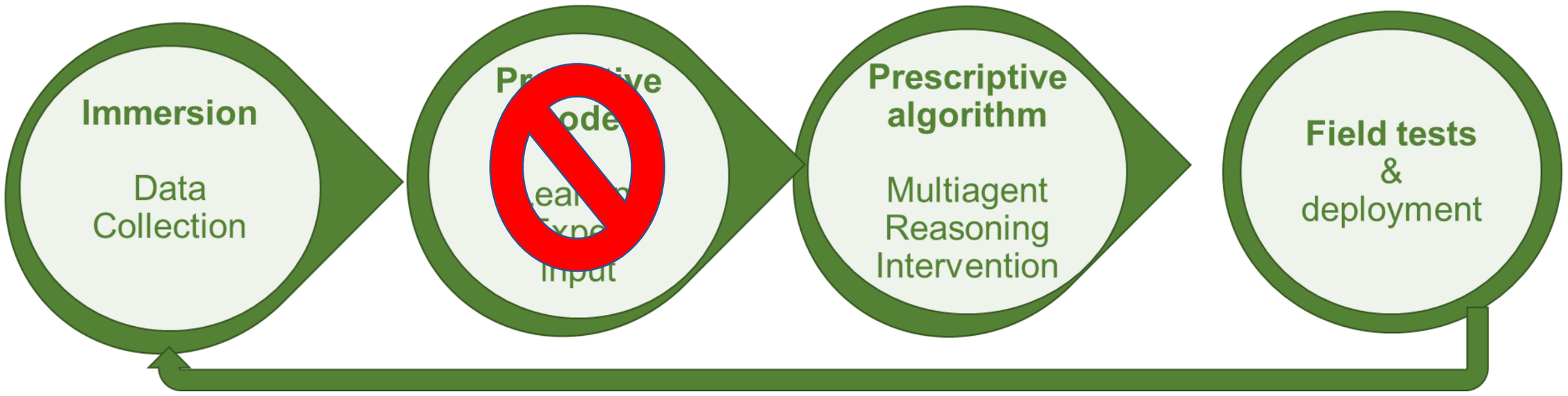
Source: GAO. | GAO-20-125

- Understanding their counter-terrorism experience

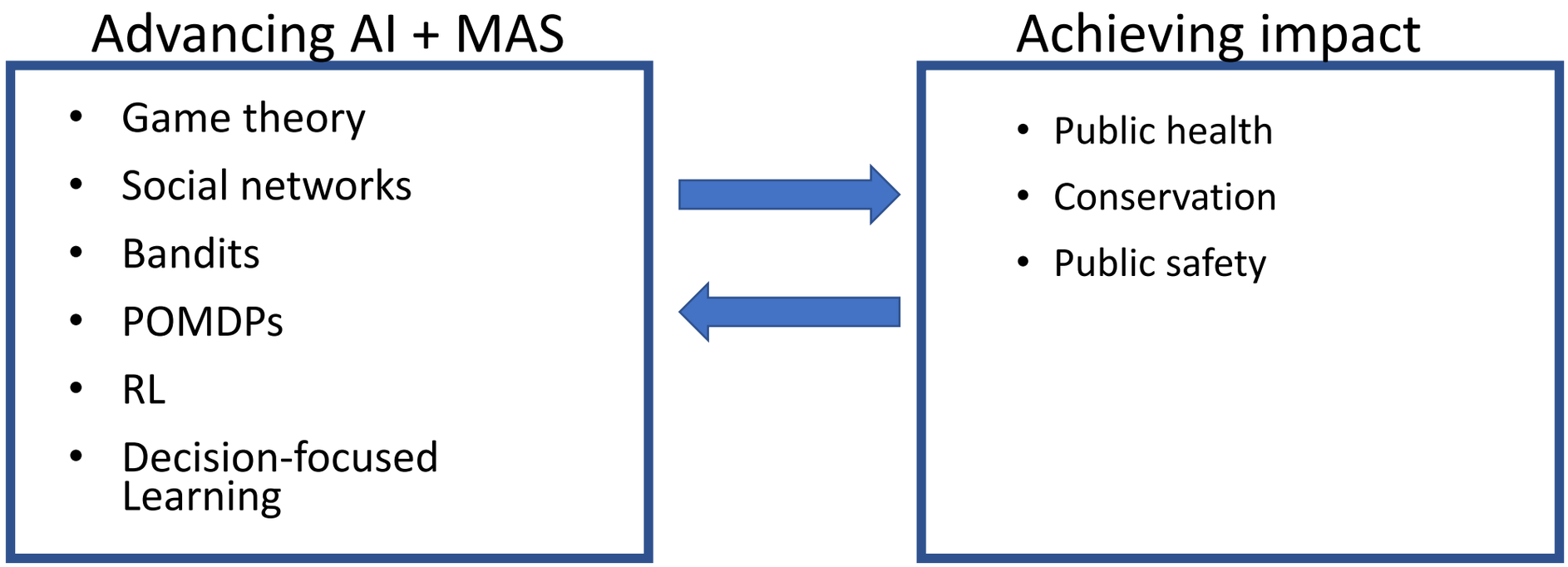
Erroll Southers

Date: 10/13/2022

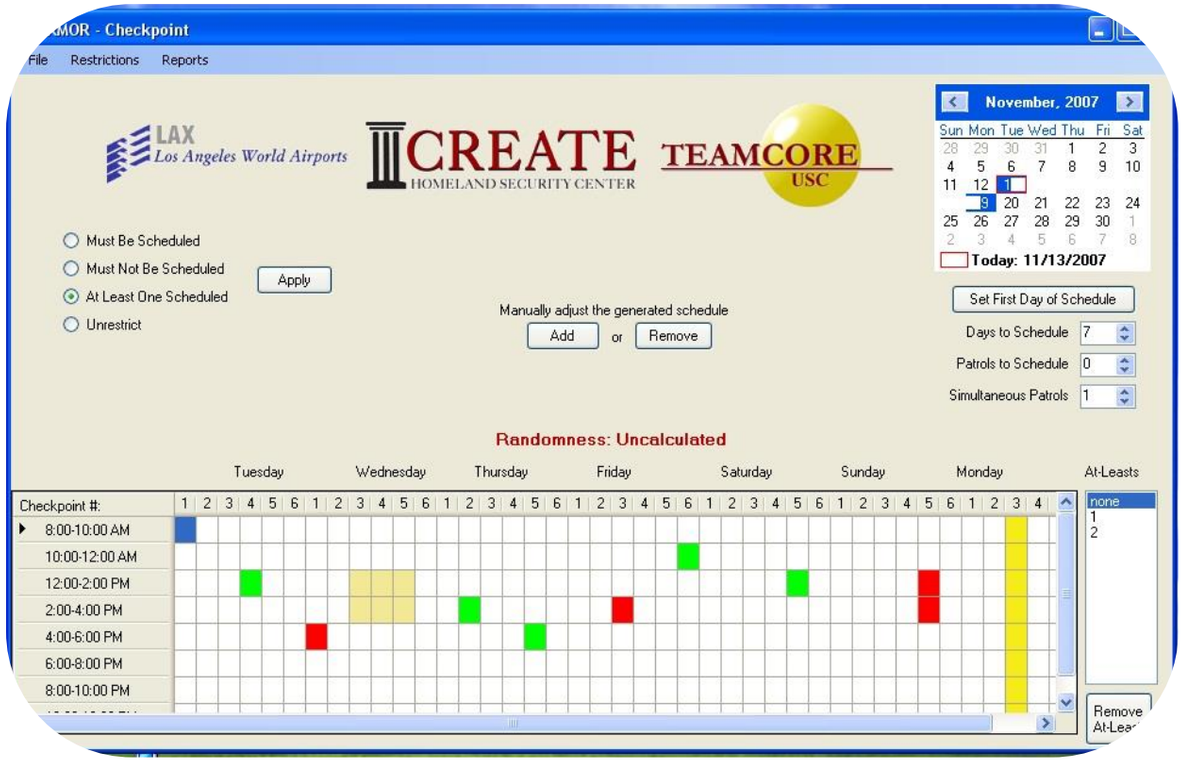
Lesson 1: Immersion & Data to Deployment Pipeline
Partnership with Govt or non-Govt agency throughout



Lesson 2: AI Innovation & Social Impact Goes Hand-in-Hand



Lesson 3: Need for Human Supervision? but Simplify Interaction



ARMOR Transition

ARMOR at LAX, IRIS with FAMS: Both Needed Six Months of Evaluation

- Evaluation: complex

Cost-benefit papers

Savings

- $30 Million in ARMOR
- $35 Million in PROTECT
- > benefit of IRIS

Risk Analysis, Vol. 40, No. 3, 2020 DOI: 10.1111/risa.13403

Assessing the Benefits and Costs of Homeland Security Research: A Risk-Informed Methodology with Applications for the U.S. Coast Guard

Detlof von Winterfeldt,[1,*] R. Scott Farrow,[2] Richard S. John,[1] Jonathan Eyer,[1] Adam Z. Rose,[1] and Heather Rosoff[1]

J. Benefit Cost Anal. 2020; 1–22 © The Author(s), 2020. Published by Cambridge University Press on behalf of the Society for Benefit-Cost Analysis
doi:10.1017/bca.2020.24

Scott Farrow* and Detlof von Winterfeldt

Retrospective Benefit–Cost Analysis of Security-Enhancing and Cost-Saving Technologies

Some lessons

- Impact evaluation is complicated

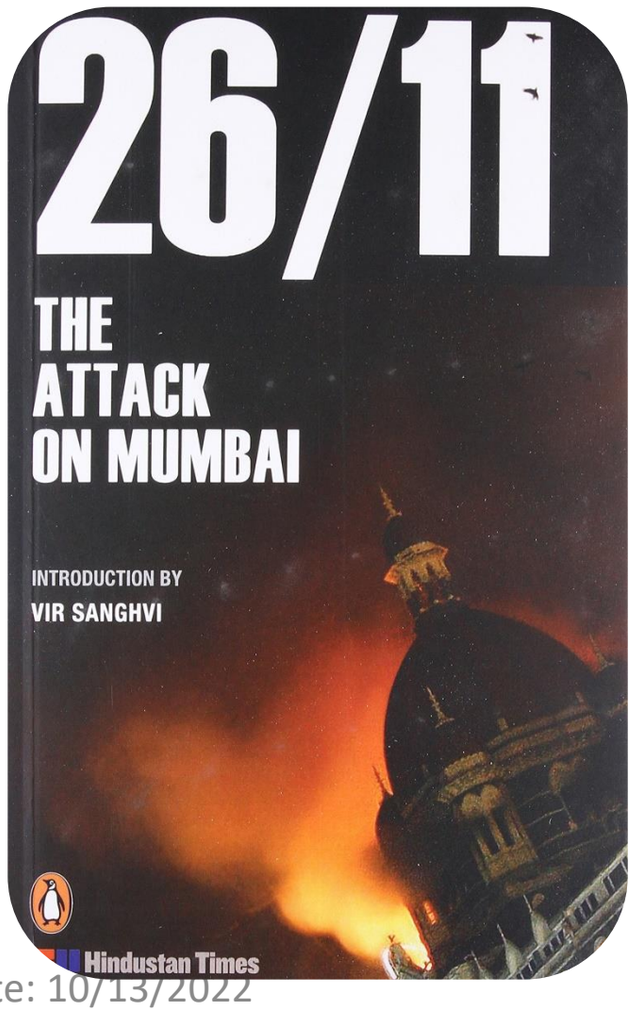
- Must respect others with other areas of expertise: partnership and humility

- Need new publication venues for AI for social impact:
  - If its not a methodological advance AI conferences did not care,
  - *Problematic for AI for social impact because impact evaluation is difficult and AI conferences at the time didn't seem to care*

- Did not set an end date! There must be an end date

26 Nov 2008, Mumbai
Police Checkpoints: Network Security Game

Jain



Road networks:

20,000 roads, 15 checkpoints

150 edges
2 Checkpoints
150-choose-2 strategies

Zero-Sum Network Security Game [2013]

Jain

Double oracle: New exact optimal algorithm for scale-up

	Path #1	Path #2	Path #3
Checkpoint strategy #1	5, -5	-1, 1	-2, 2
Checkpoint strategy #2	-5, 5	1, -1	-2, 2

Defender oracle

	Path #1	Path #2
Checkpoint strategy #1	5, -5	-1, 1
Checkpoint strategy #2	-5, 5	2, -1

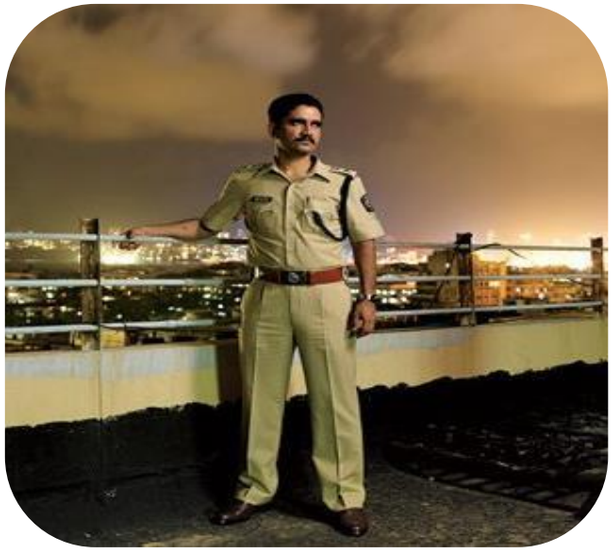
Attacker oracle

	Path #1	Path #2	Path #3
Checkpoint strategy #1	5, -5	-1, 1	-2, 2
Checkpoint strategy #2	-5, 5	1, -1	-2, 2

Presentation at the Indian National Police Academy: Network Security Game [2016]

Road networks:

20,000 roads, 15 checkpoint:
Solved under 20 min



Some lessons

- No “immersion” meant no ability to build up trust

US Coast Guard:
PORT PROTECTION PATROLS DEPLOYED [2011-]

USS Cole after attack

French oil tanker hit by small boat

PROTECT: Port and Ferry Protection Patrols [2011]


Shieh


An

Boston

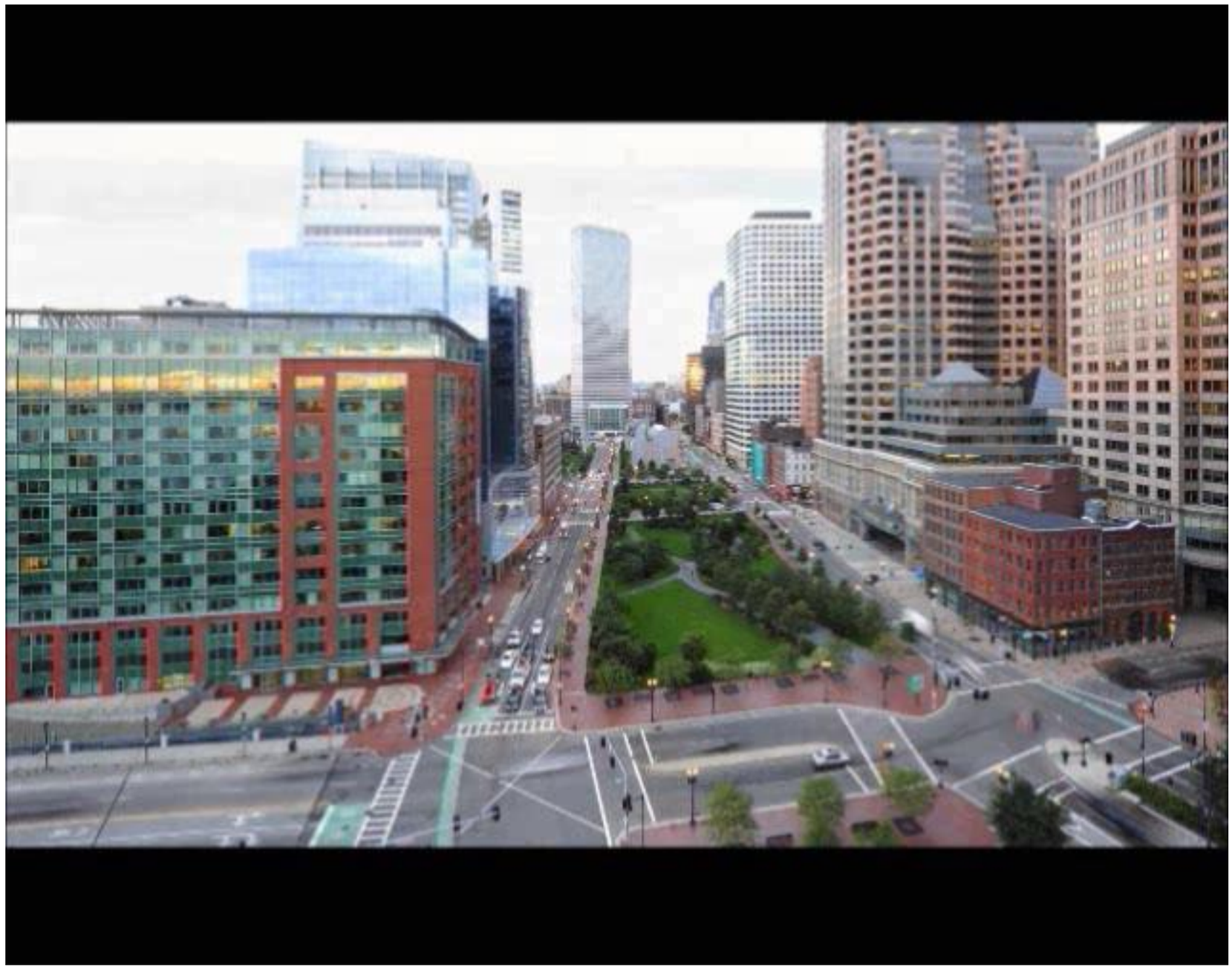
Los Angeles

New York

PROTECT: Port and Ferry Protection Patrols [2011]


Shieh


An



PROTECT: Ferry Protection Deployed [2013]


Fang


Jiang

PROTECT: Ferry Protection Deployed [2013]


Fang


Jiang

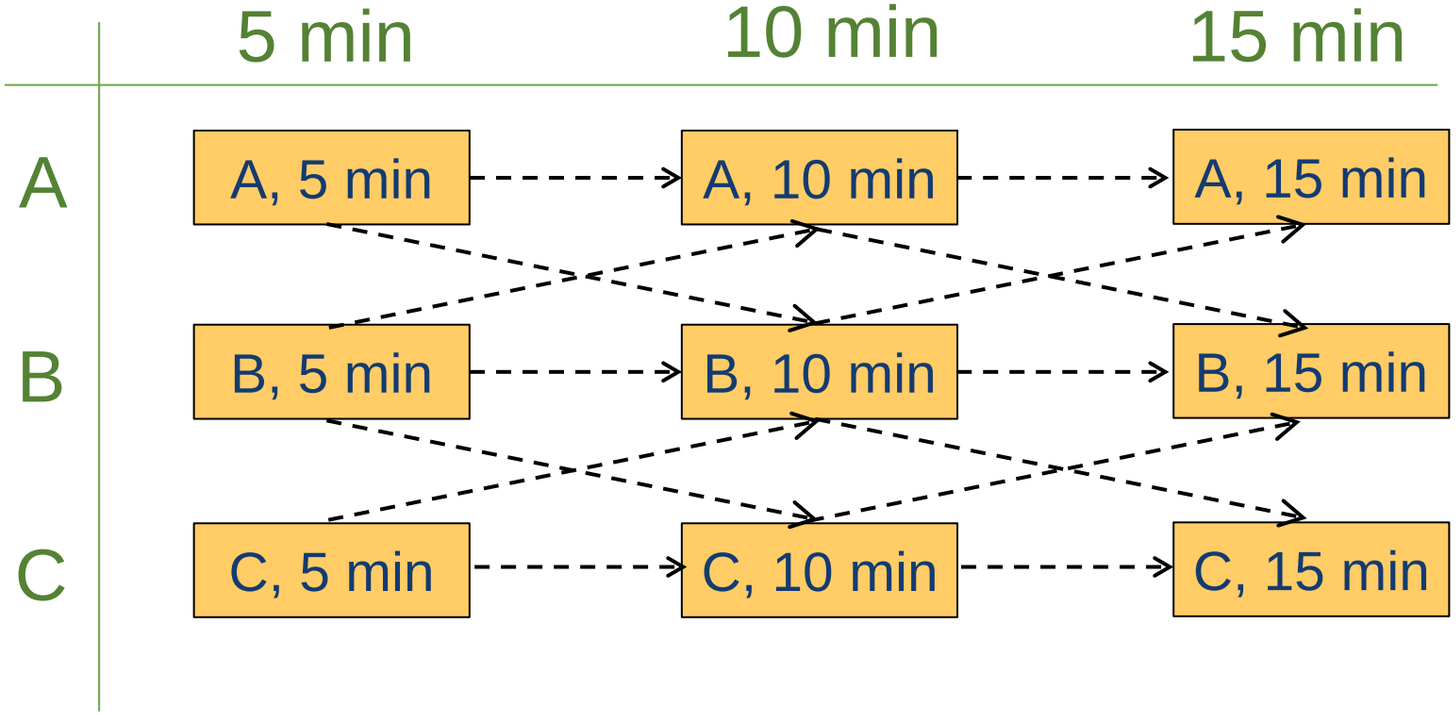
PROTECT: Ferry Protection Deployed [2013]

FERRIES: Mobile Resources & Moving Targets Transition Graph Representation


Fang


Jiang

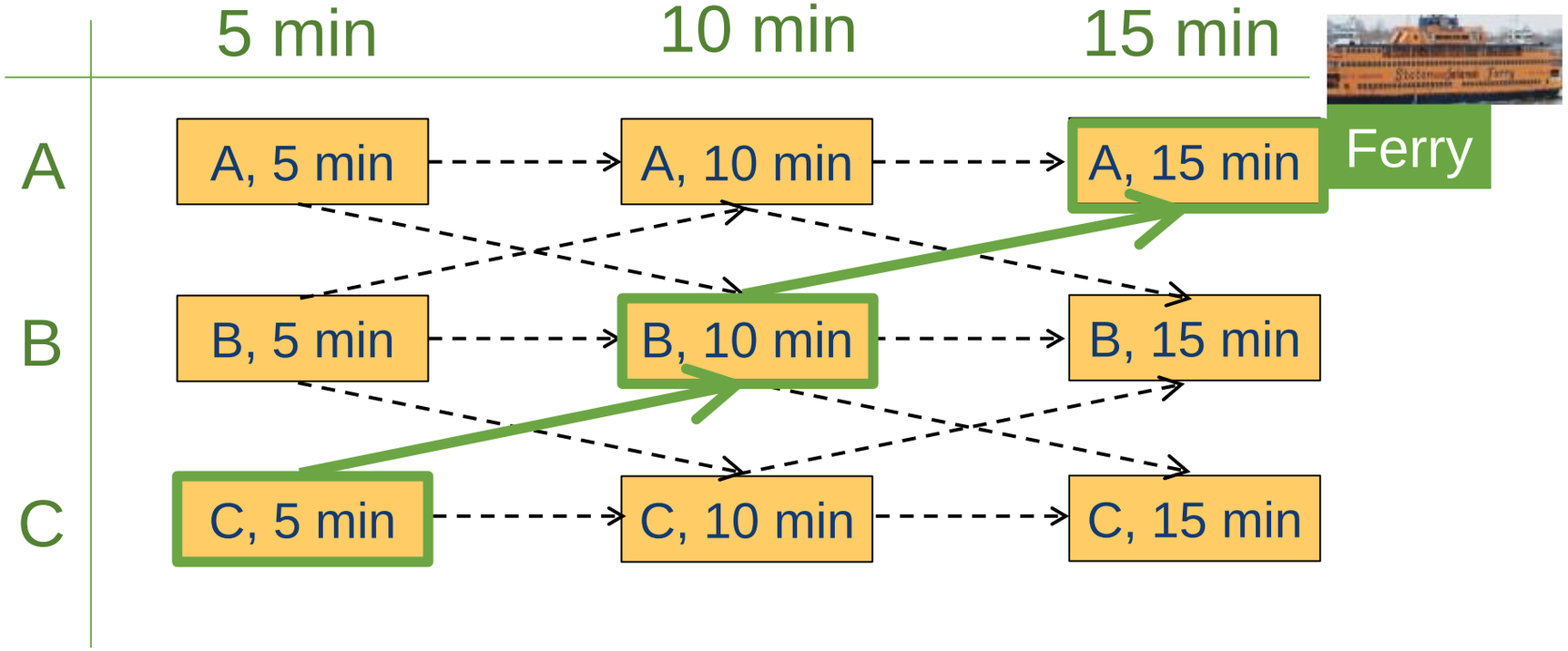
Marginal strategy: New scale-up approach for Stackelberg Security Games



FERRIES: Mobile Resources & Moving Targets Transition Graph Representation


Fang


Jiang

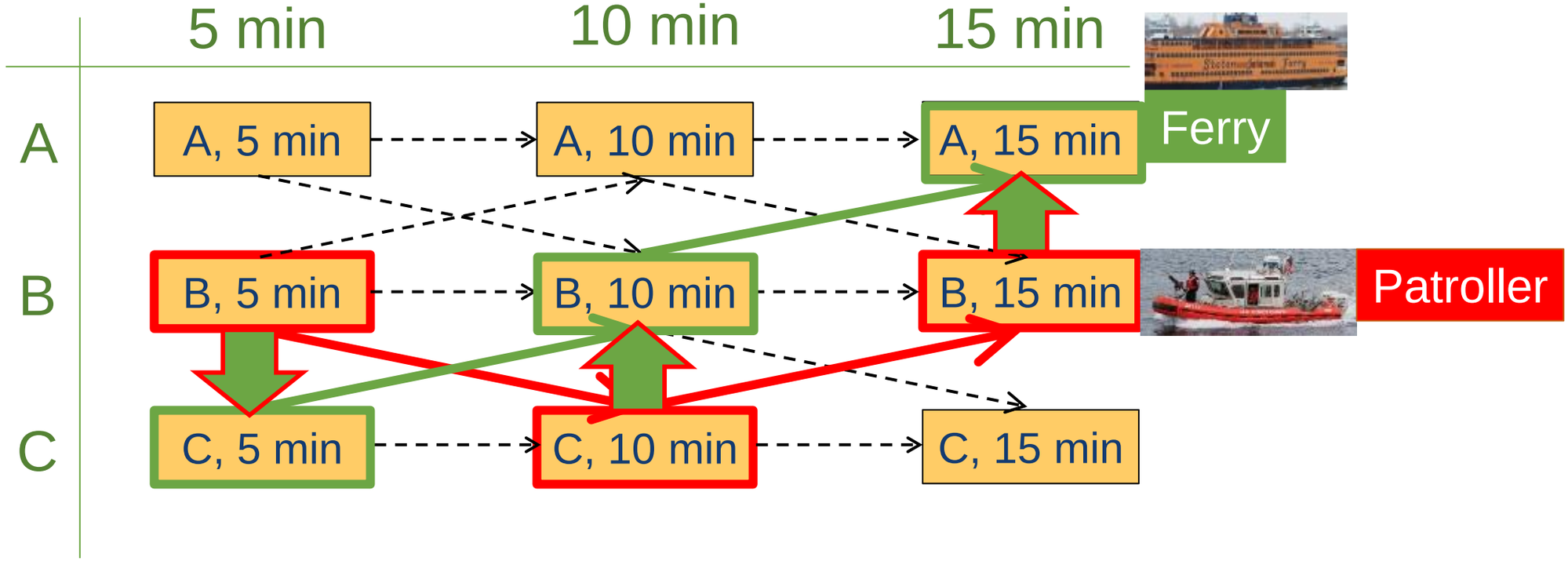


FERRIES: Mobile Resources & Moving Targets Transition Graph Representation


Fang


Jiang

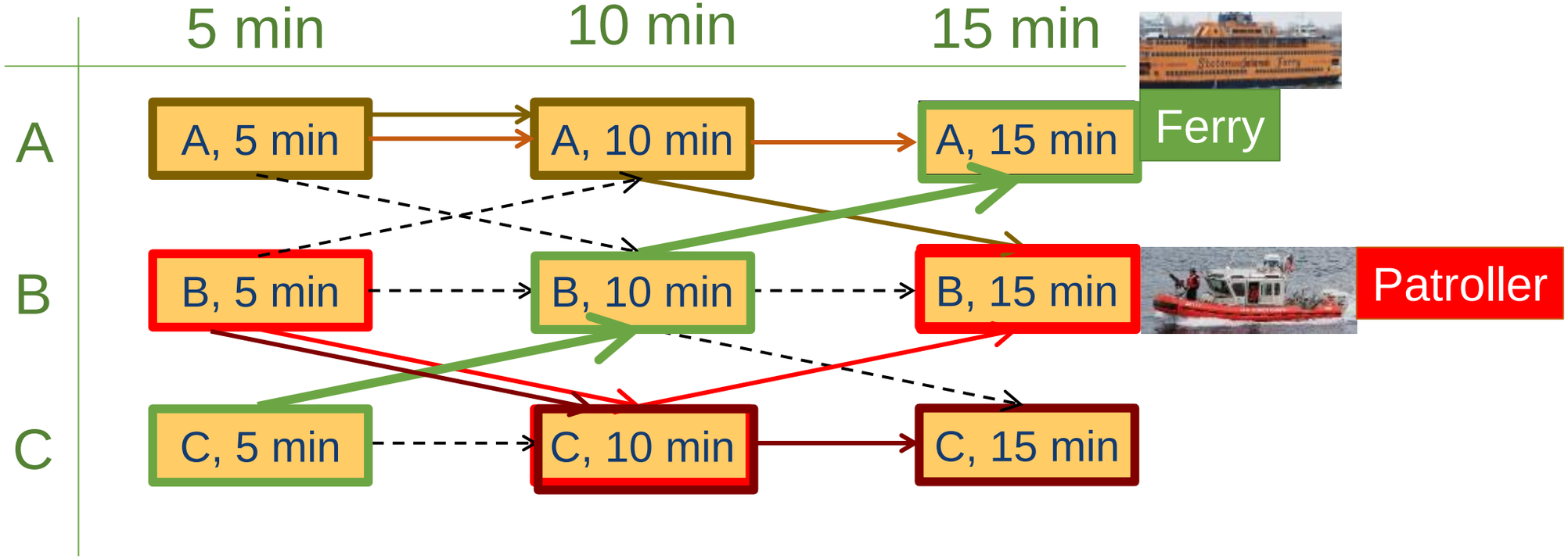
Patrol protects nearby ferry locations



FERRIES: Mobile Resources & Moving Targets Transition Graph Representation


Fang


Jiang



FERRIES: Mobile Resources & Moving Targets Transition Graph Representation

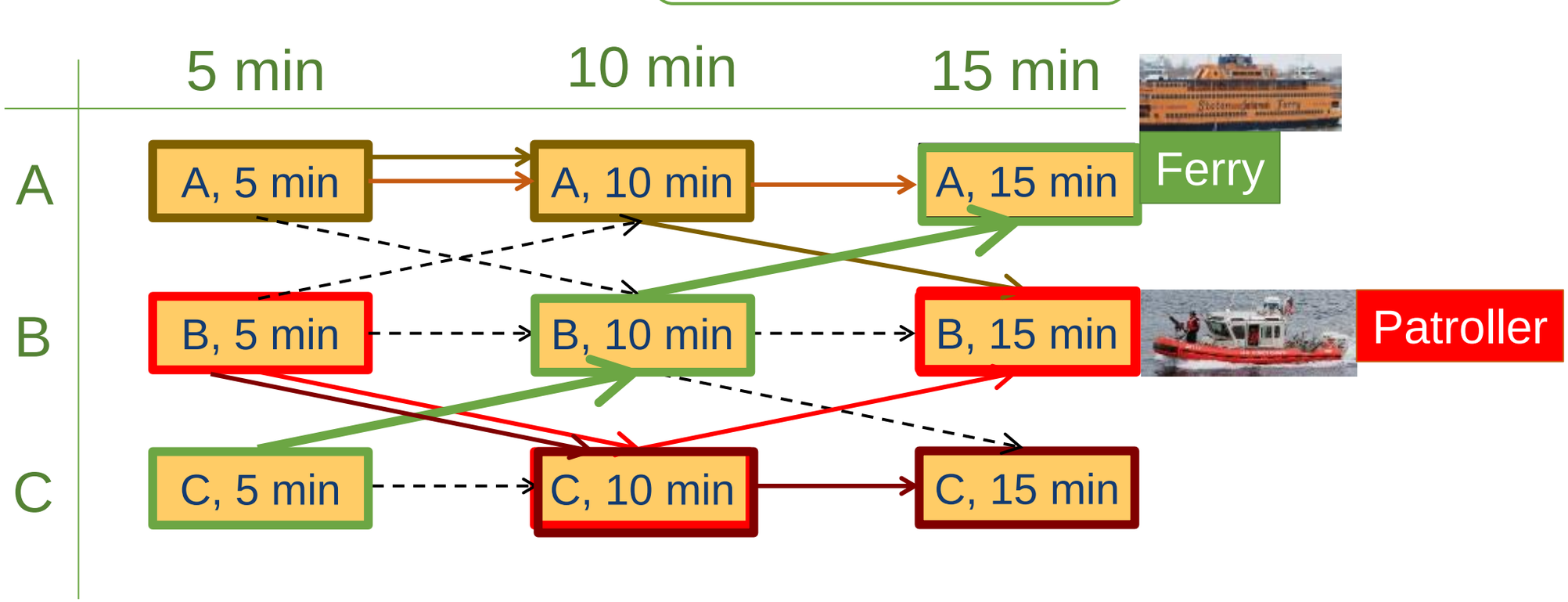

Fang


Jiang

ARMOR style LP: Determine probability for each route

Defender

N^T x_i variables



FERRIES: Scale-Up Transition Graph Representation

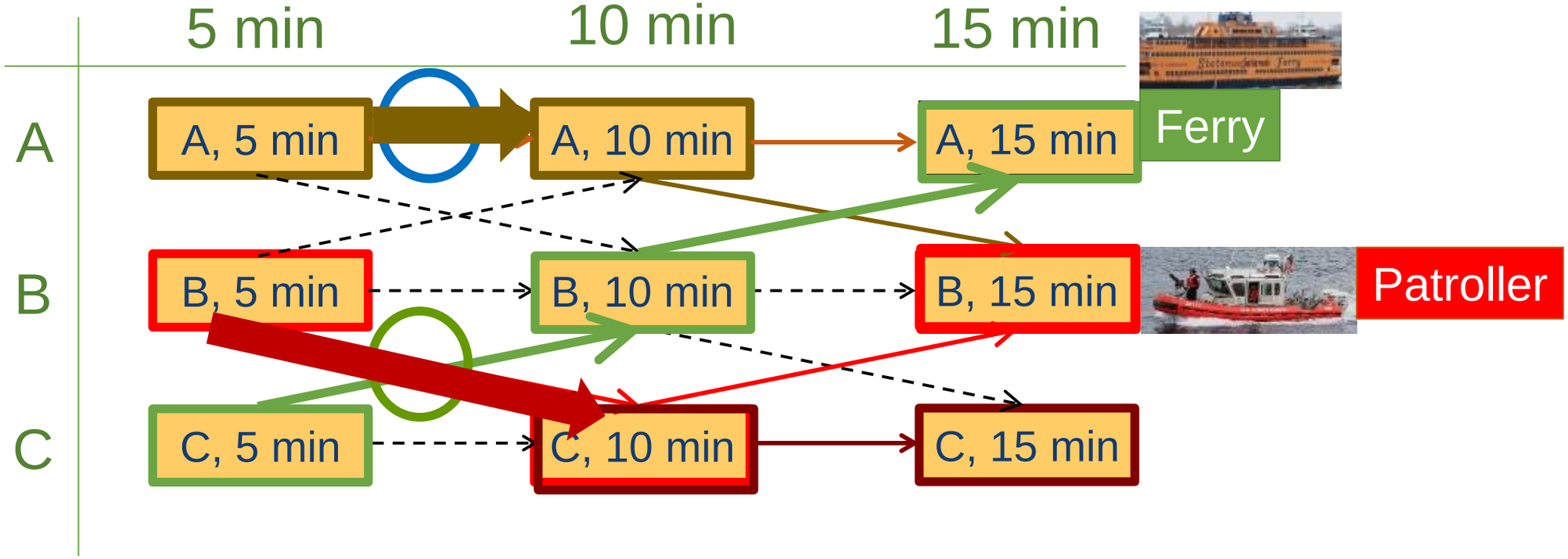

Fang


Jiang

Variables: NOT routes, but marginal probability over each segment

Defender

~~Variables~~



FERRIES: Scale-Up Transition Graph Representation


Fang

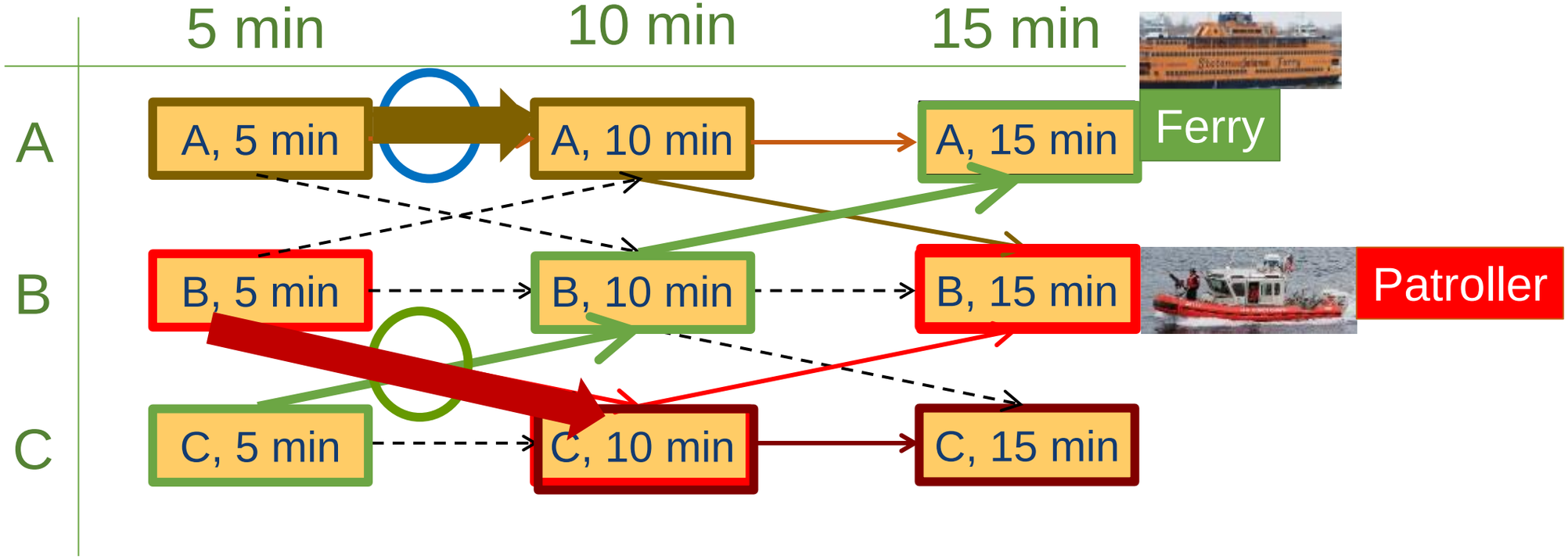

Jiang

Theorem: Marginal representation does not lose any solution quality

Defender

$N^2.T$ x_i variables

N variables



PROTECT: FERRY PROTECTION DEPLOYED [2013-]

CNN iReport

SIGN UP | LOG IN

Main Explore Assignments Profile Upload

g+1 Tweet Share Favorite

99 VIEWS | 0 COMMENTS | 6 SHARES

U.S. Coast Guard protects the Staten Island Ferry: I feel safe!

By shortysmom | Posted September 8, 2013 | Staten Island, New York

Share on Facebook 0

About this iReport

- Not vetted for CNN

Posted September 8, 2013 by

PROTECT: Port Protection Patrols [2013] Congressional Subcommittee Hearing

June 2013: Meritorious Team Commendation from Commandant (US Coast Guard)

July 2011: Operational Excellence Award (US Coast Guard, Boston)

US Coast Guard testimony Congressional subcommittee

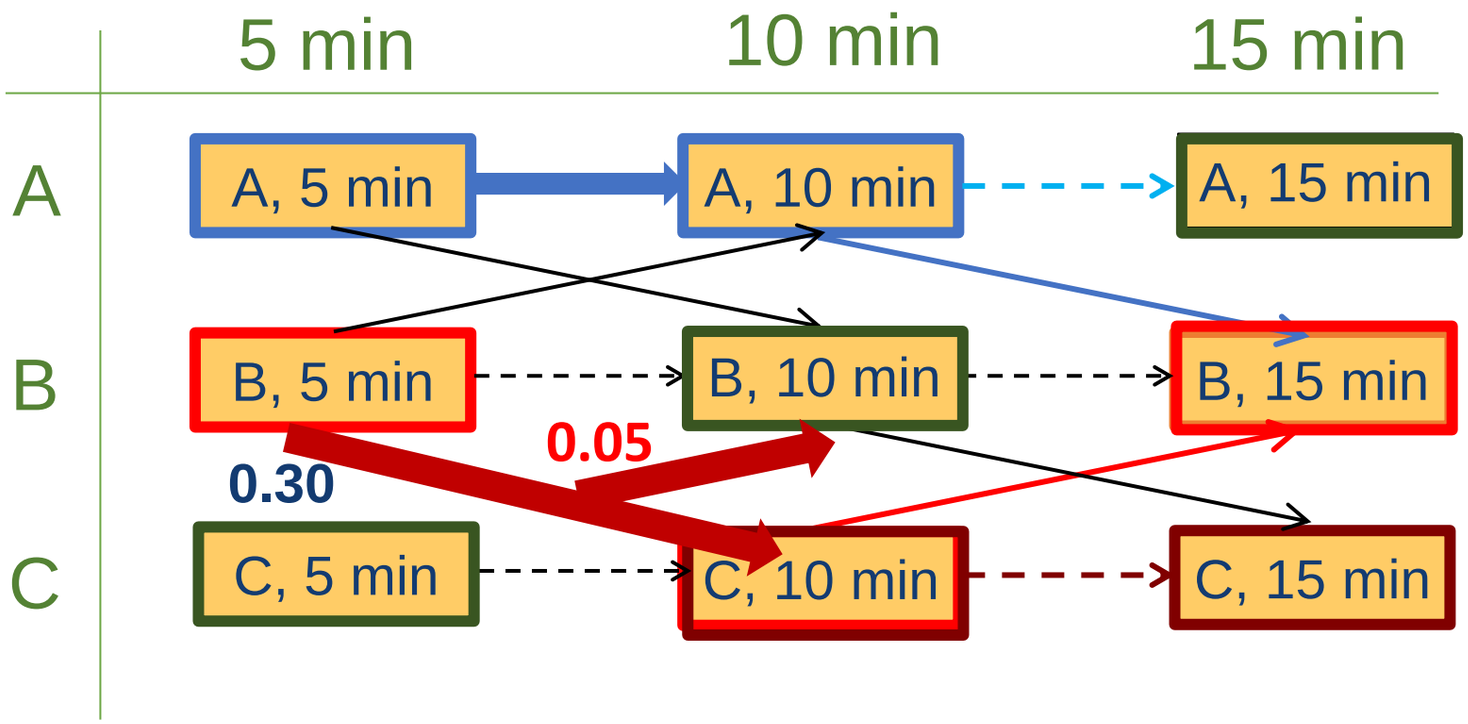
Some lessons

- PROTECT: 2011-2017

Train Patrols
Execution Uncertainty: MDPs


Jiang


Delle Fave



Questions

Evaluation

- “BUT DOES THIS WORK”?

Evaluating Deployed Security Systems Not Easy

How Well Optimized Use of Limited Security Resources?

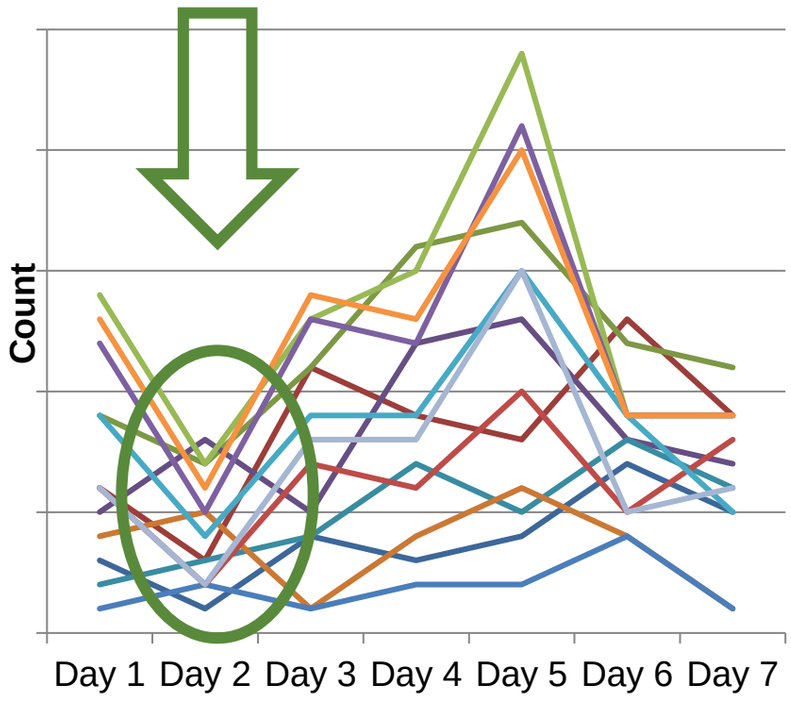
Security Games superior
vs
Human Schedulers/”simple random”

- Lab evaluation
- *Scheduling competitions: Patrol quality unpredictability? Coverage?*
- Field evaluation: Tests against real adversaries
- *Economic cost-benefit analysis*
- *…*

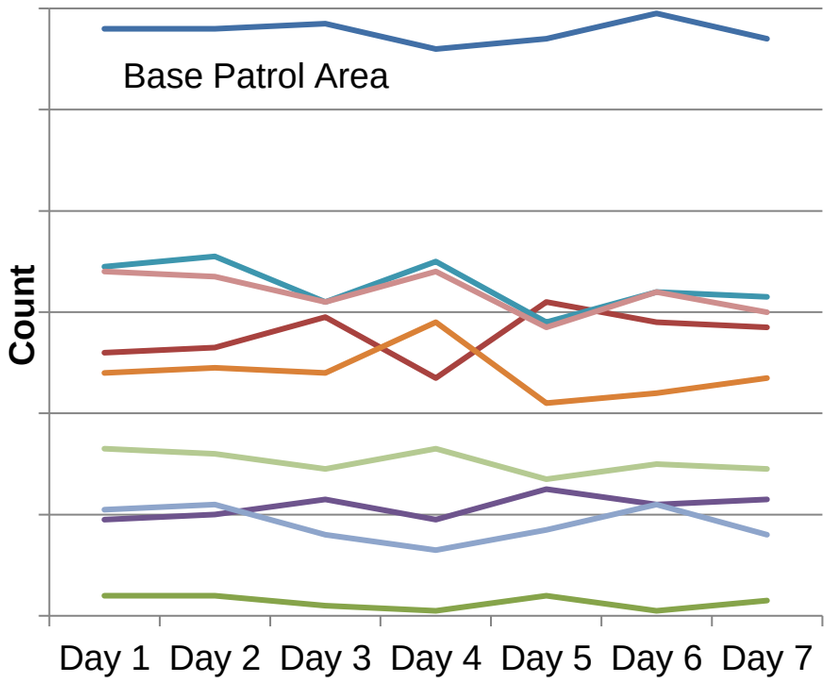
Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort

Patrols Before PROTECT: Boston



Patrols After PROTECT: Boston



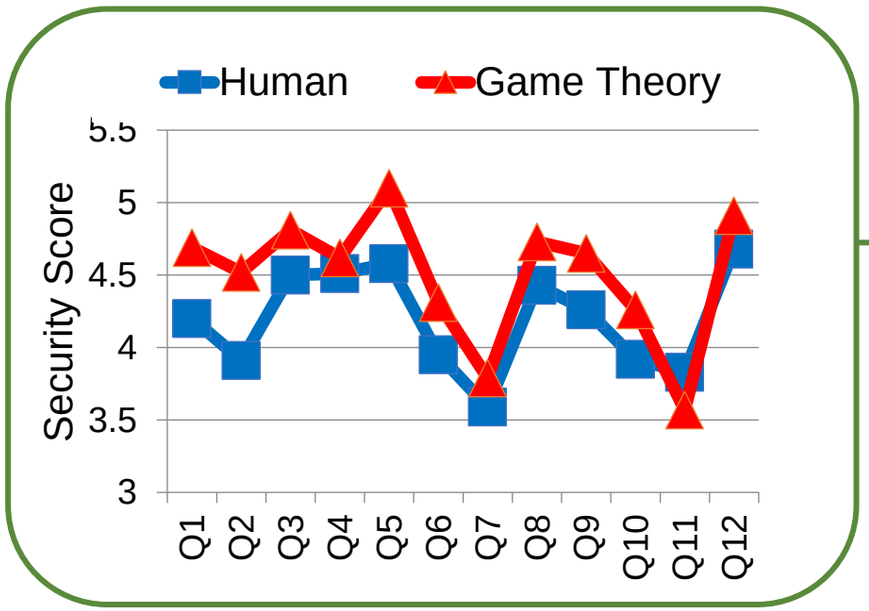
350% increase in defender expected utility

Field Evaluation of Schedule Quality

Improved Patrol Unpredictability & Coverage for Less Effort

FAMS: IRIS Outperformed expert human over six months

Report:GAO-09-903T

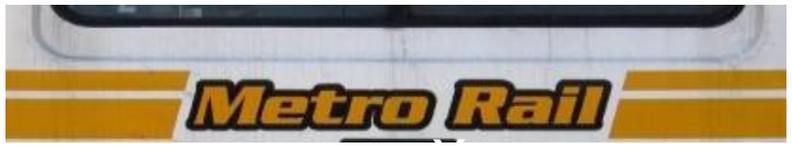


Trains: TRUSTS outperformed expert humans schedule 90 officers on LA trains

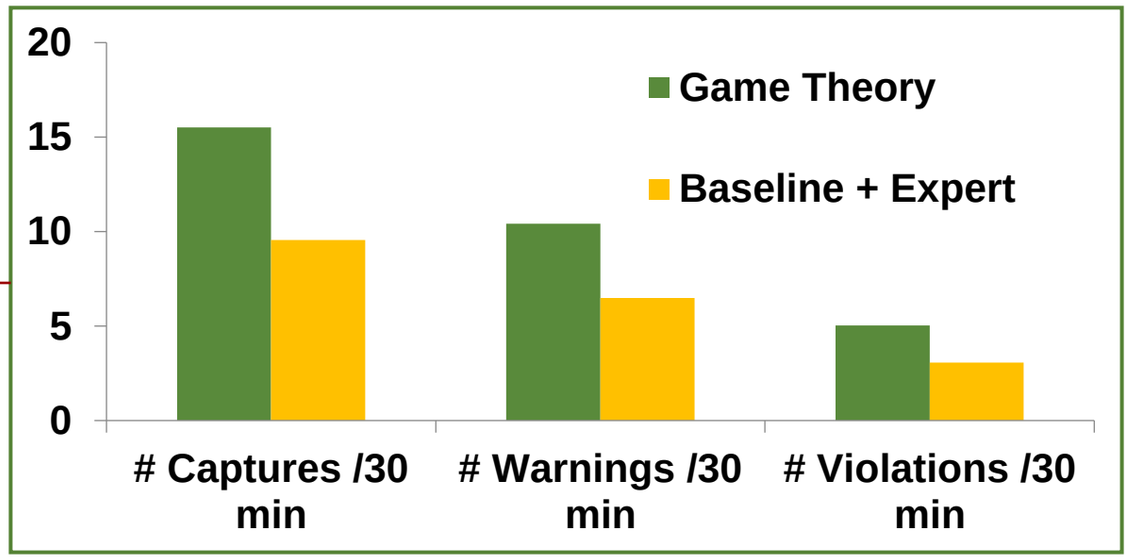
Field Tests Against Adversaries

Computational Game Theory in the Field

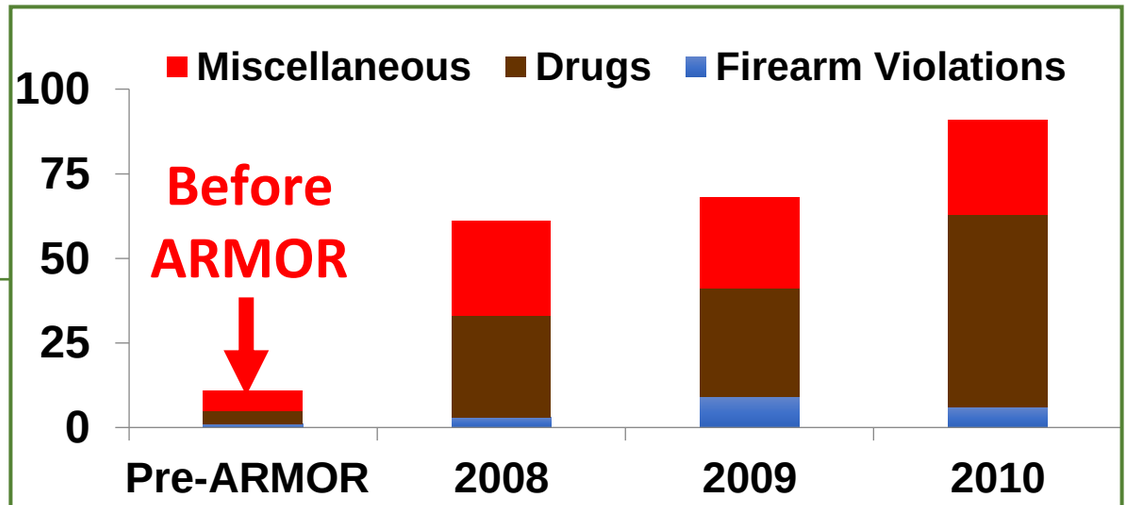
Controlled

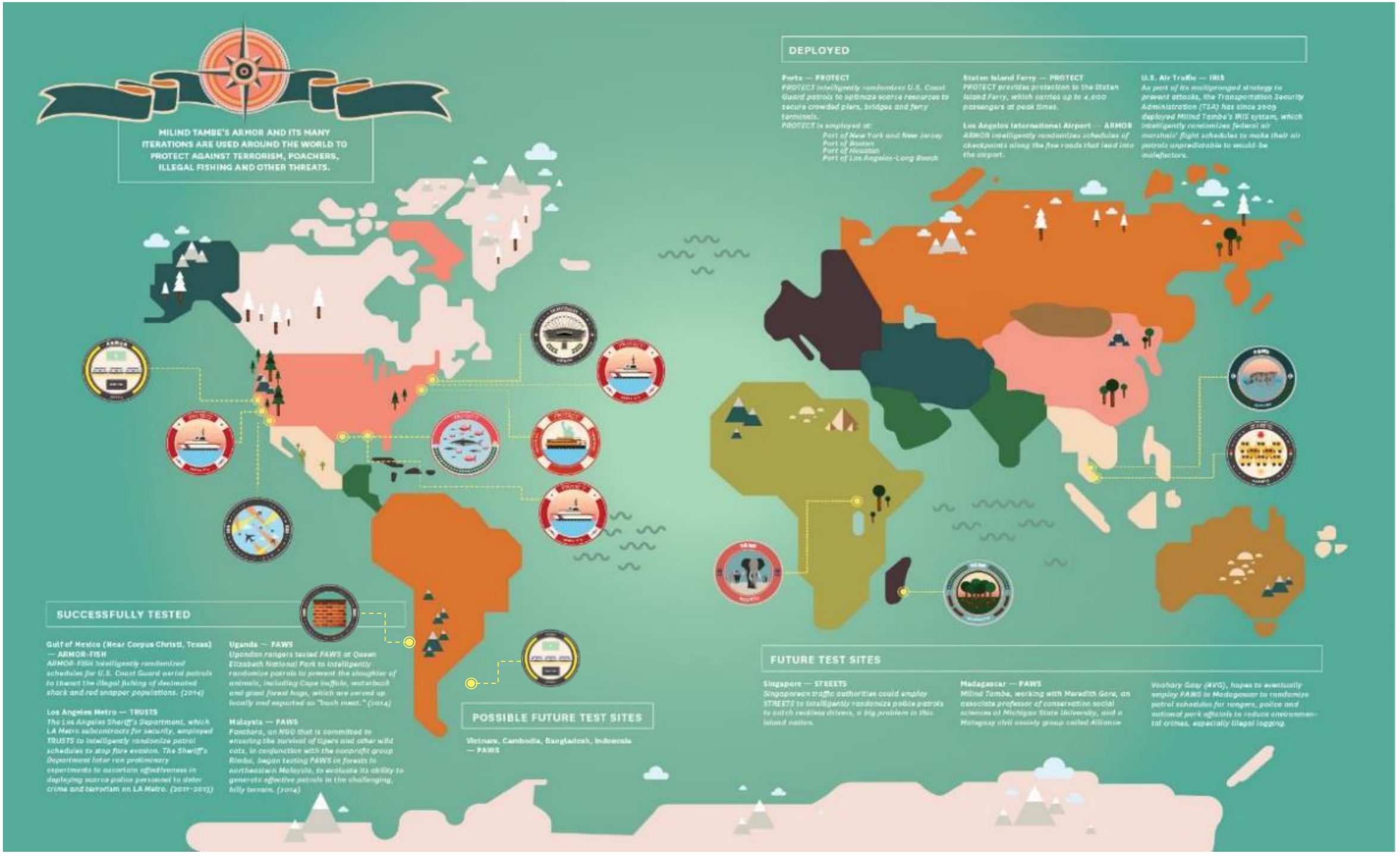


- 21 days of patrol, identical conditions
- Game theory vs Baseline+Expert



Not Controlled





New applications: cybersecurity, protecting of endangered wildlife and fisheries, protecting forests, audit games, drug design against viruses, traffic enforcement, software code testing, adversarial machine learning

Outline

Public Safety and Security:
Stackelberg Security Games

Conservation/Wildlife Protection:
Green Security Games

World Bank Global Tiger Initiative
How I got into AI for Wildlife Conservation

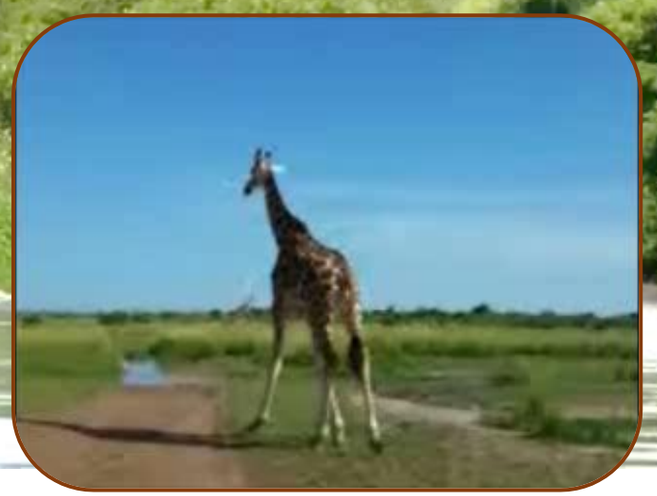
Visiting Uganda & Meeting Andy Plumptre

Date: 10/13/2022

Poaching of Wildlife in Uganda
Limited Intervention (Ranger) Resources to Protect Forests

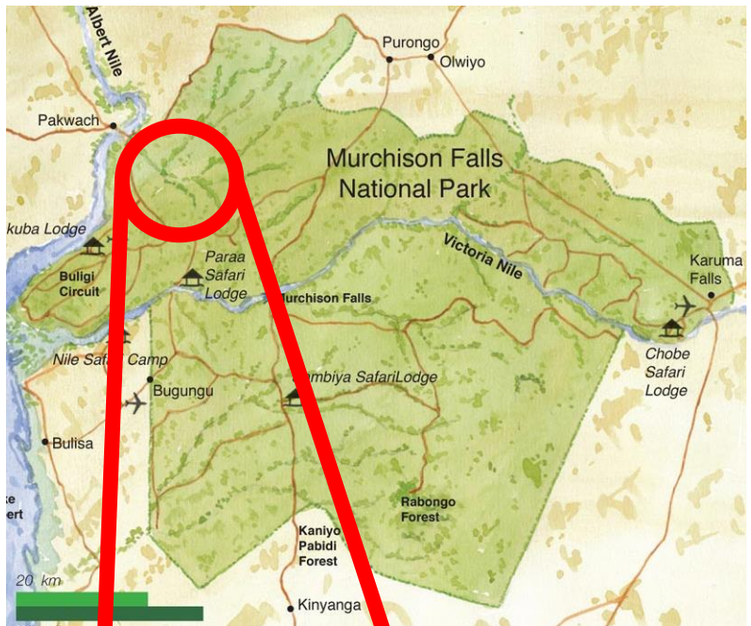
Snare or Trap

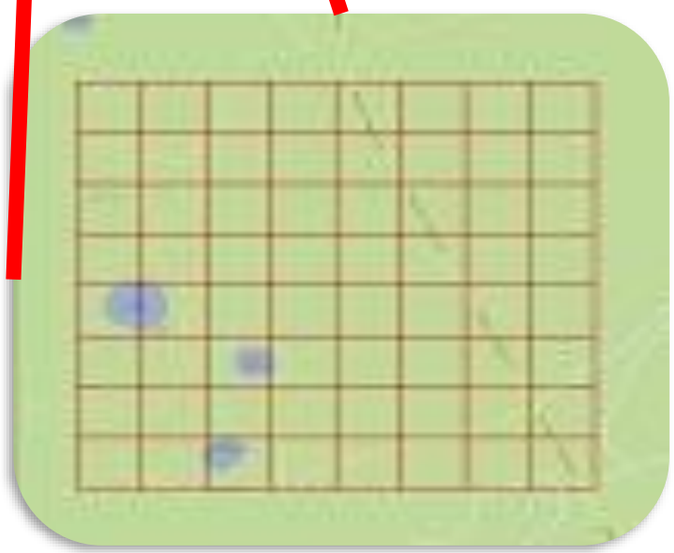
Wire snares



Stackelberg Security Games?

Fang



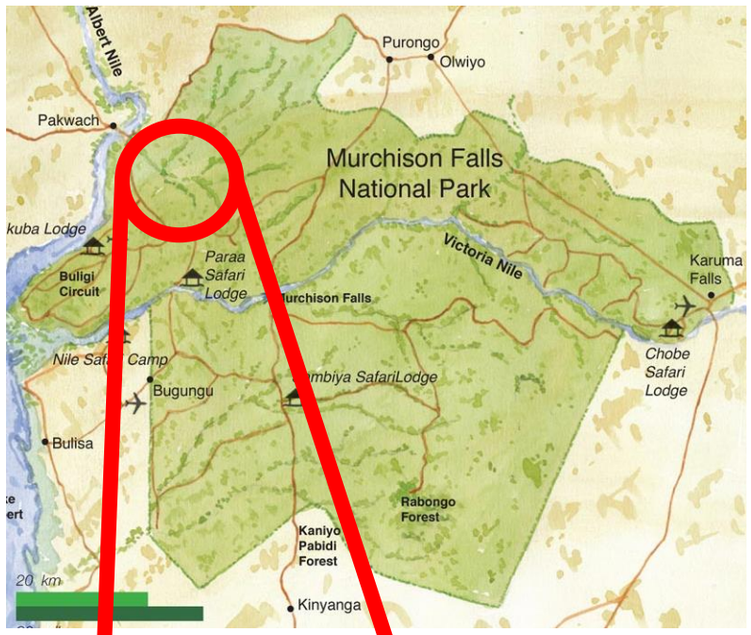


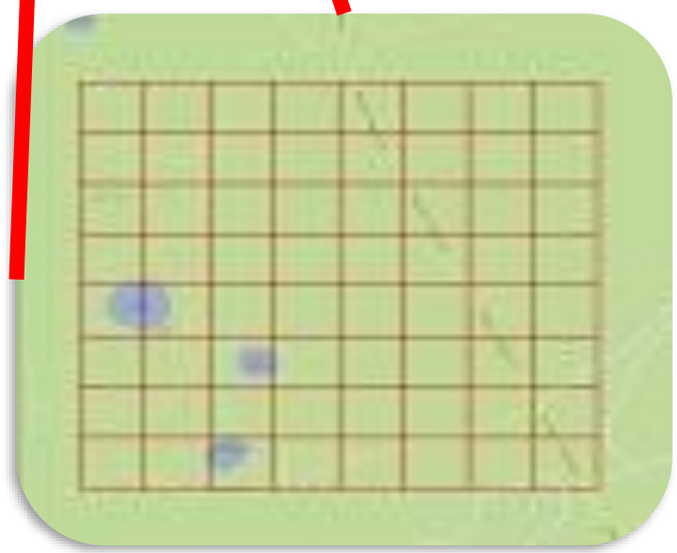
- ***Stackelberg security games (SSG)***

	Area1	Area2
Area1	4, -3	-1, 1
Area2	-5, 5	2, -1

Green Security Games Combine Stackelberg Security Games and Machine Learning

Fang





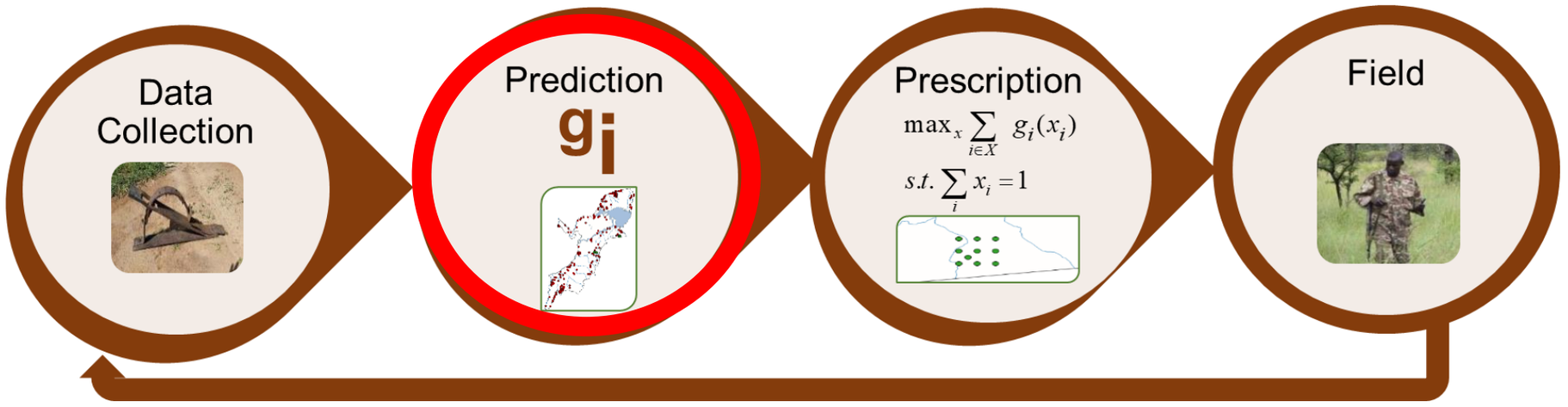
- ***Not fully strategic adversaries***
- ***Boundedly rational poachers, past poaching data***
- ***Learn adversary response model at targets "i"***

	Area1	Area2
Area1	4, -3	-1, 1
Area2	-5, 5	2, -1

Learning Adversary Response Model: Uncertainty in Observations

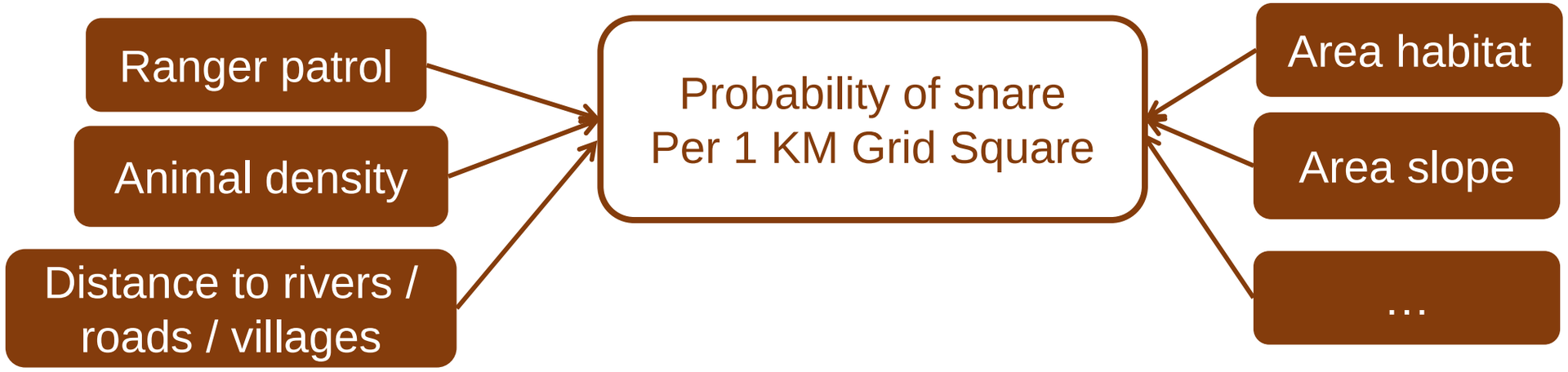

Nguyen

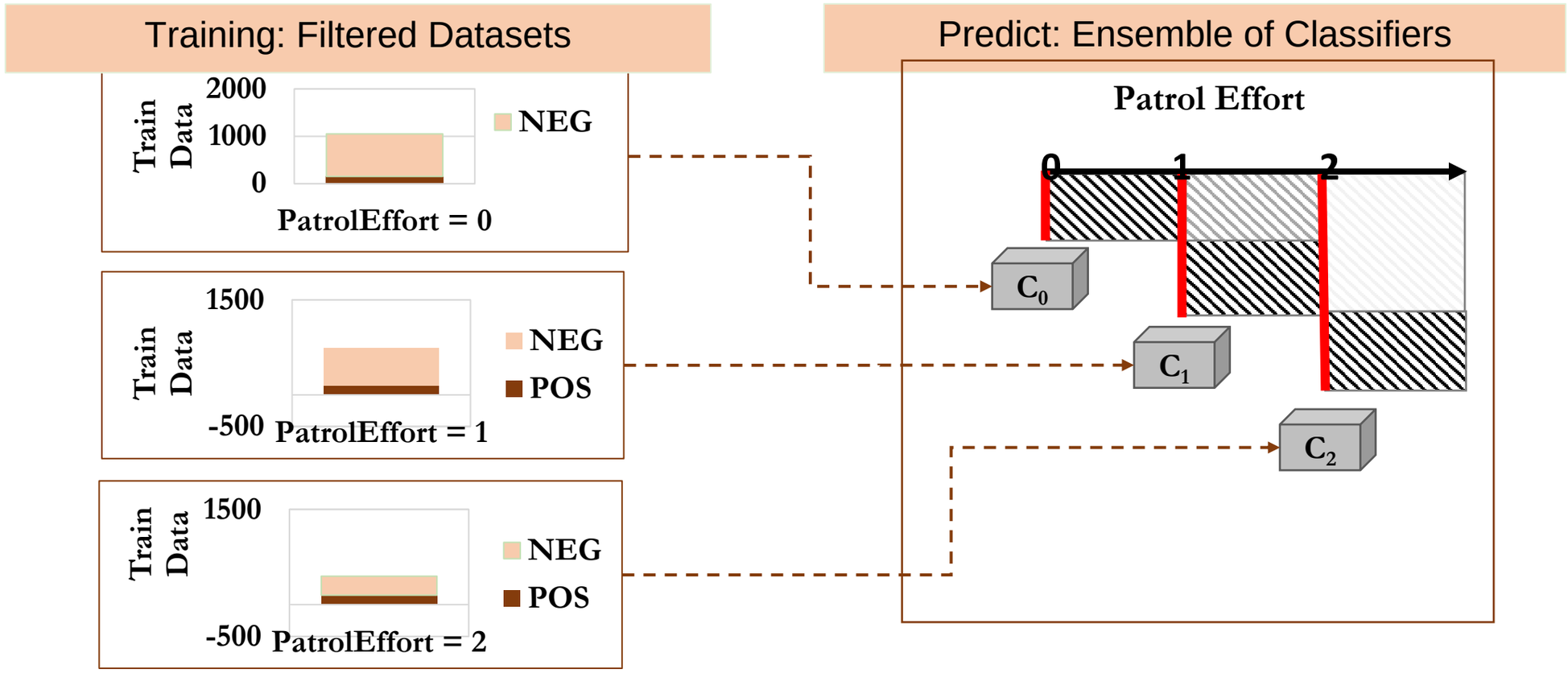

Gholami



Learning Adversary Response Model: Uncertainty in Observations


Nguyen Gholami



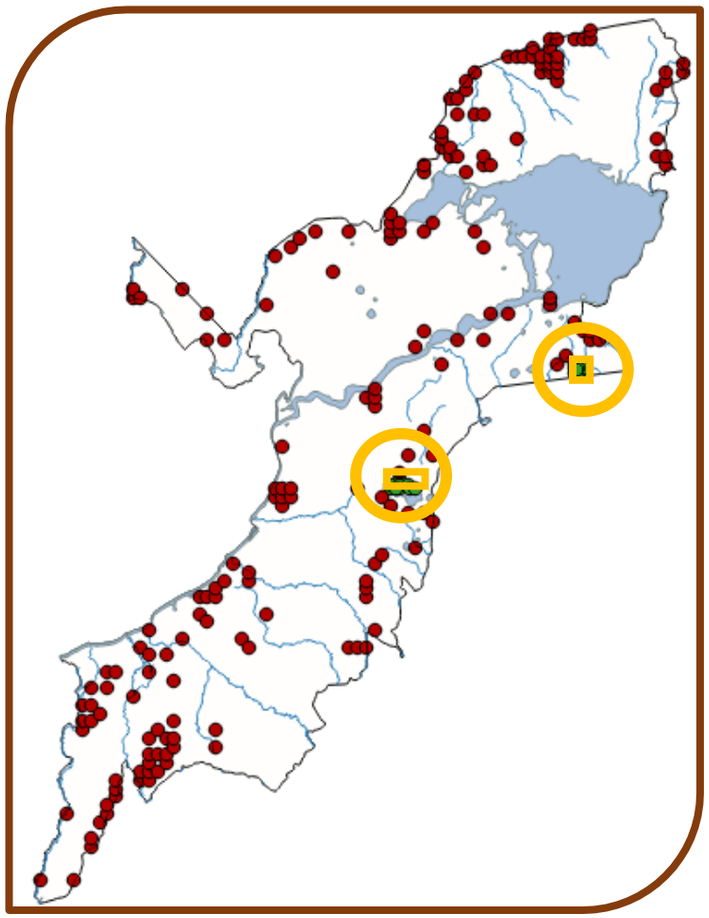


PAWS: First Pilot in the Field
(AAMAS 2017)

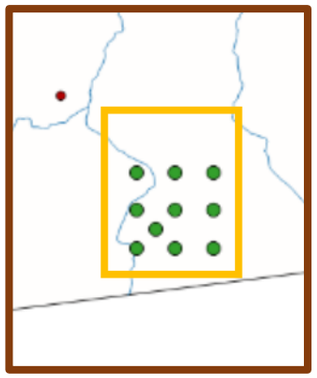

Ford

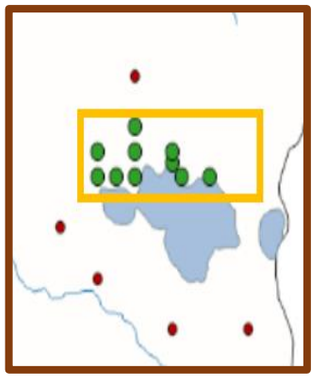

Gholami

- Two 9-sq.km areas, infrequent patrols



- Poached elephant
- 1 elephant snare roll
- 10 Antelope snares



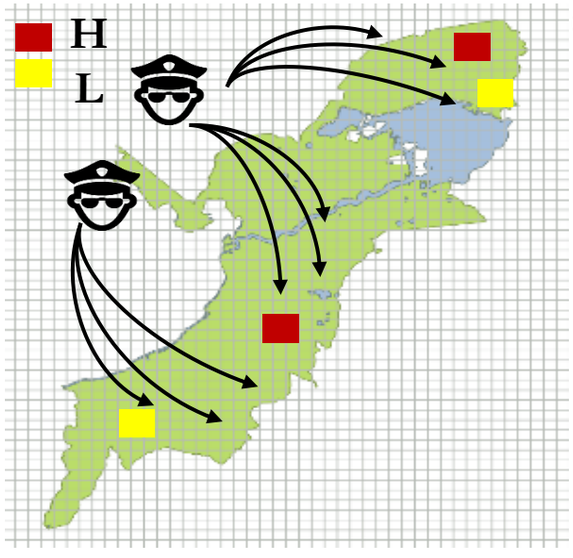


PAWS Predicted High vs Low Risk Areas: 3 National Parks, 24 areas each, 6 months

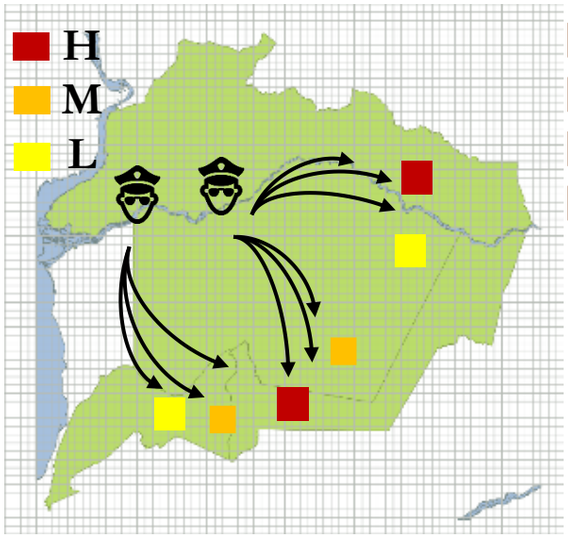
(ECML PKDD 2017, ICDE 2020)

Xu

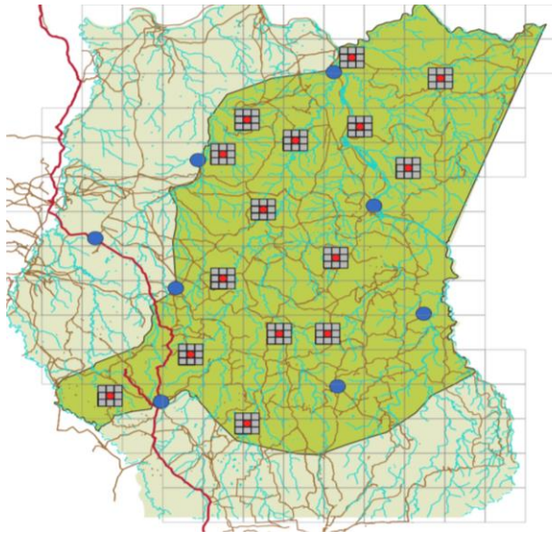
Gholami



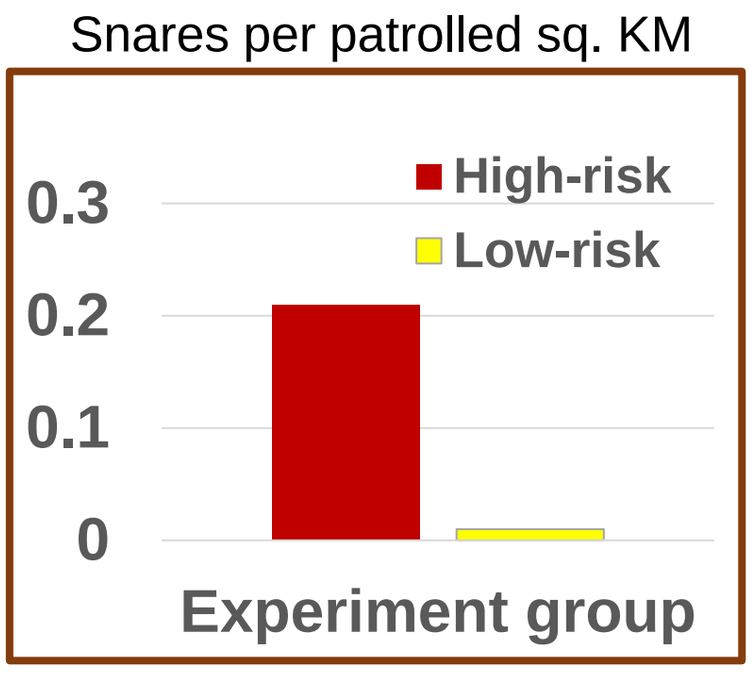
Queen Elizabeth National Park

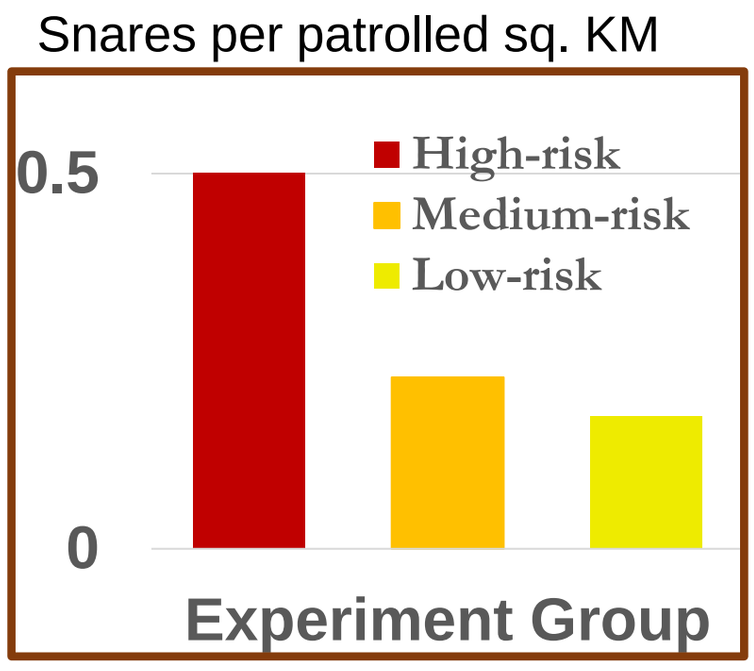


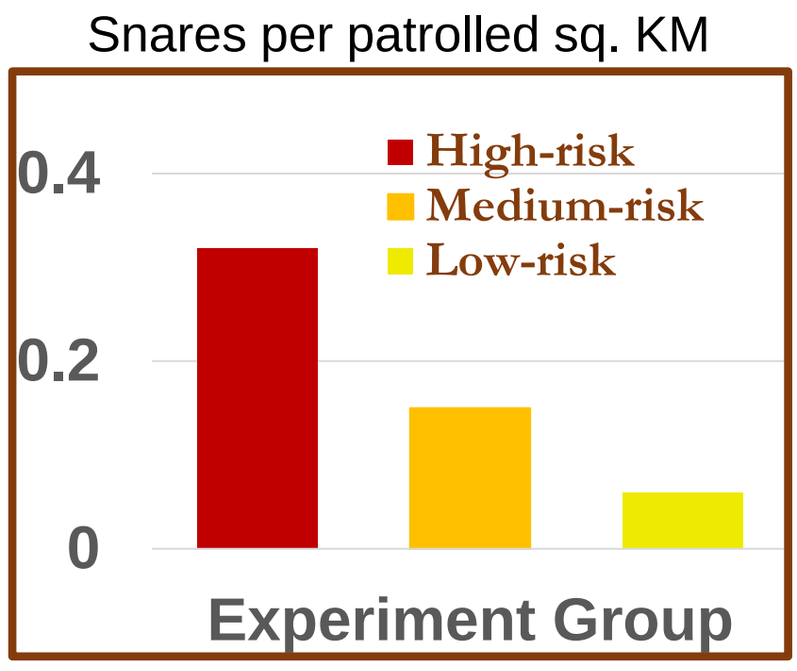
Murchison Falls National Park



Srepok Wildlife Sanctuary







PAWS Real-world Deployment
Cambodia: Srepok Wildlife Sanctuary
(ICDE 2020)

Xu

2019 PAWS: *521 snares/month*

vs

2018: *101 snares/month*

2021 PAWS

1,000 snares found in March

PAWS GOES GLOBAL with SMART platform!!

Protect Wildlife
800 National Parks
Around the Globe