CERIAS
The Center for Education and Research in Information Assurance and Security

2025 - PDR - 2FK-XHB - Sensor Scheduling in Intrusion Detection Games with Uncertain Payoffs - jbhargav@purdue.edu - Jayanth Bhargav

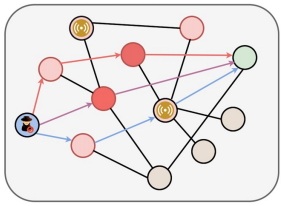
Sensor Scheduling in Intrusion Detection Games with Uncertain Payoffs

Jayanth Bhargav, Shreyas Sundaram, Mahsa Ghasemi

Overview

Goal: Efficiently schedule a set of sensors for monitoring and intrusion detection
Approach: Model the interactions between defender and intruder as a 2-player game
Key Challenges:

- Exponentially many scheduling strategies for defender - Combinatorial strategy space
- Unknown sensor models - Need to learn and adapt scheduling strategies online



Problem Formulation

Player 1 – Defender

- Strategy space: I; $m = |I|$
- Mixed-Strategy: $x \in \Delta_{|I|}$
- Strategy costs: $c_i \in \mathbb{R}_{>0}$; $i \in I$
- Payoff Matrix: $A' \in \mathbb{R}^{m \times n}$

$$A'_{ij} = \log(p_{miss}(i,j)) + c_i$$

- Defender's Optimization Problem

$$\min_{x \in \Delta_{|I|}} x^T A' y$$

Game
$\mathcal{G}' = \{A', B'\}$

Player 2 – Intruder

- Strategy space: J; $n = |J|$
- Mixed-Strategy: $y \in \Delta_{|J|}$
- Strategy costs: $r_j \in \mathbb{R}_{>0}$; $j \in J$
- Payoff Matrix: $B' \in \mathbb{R}^{m \times n}$

$$B'_{ij} = -\log(p_{miss}(i,j)) + r_j$$

- Intruder's Optimization Problem

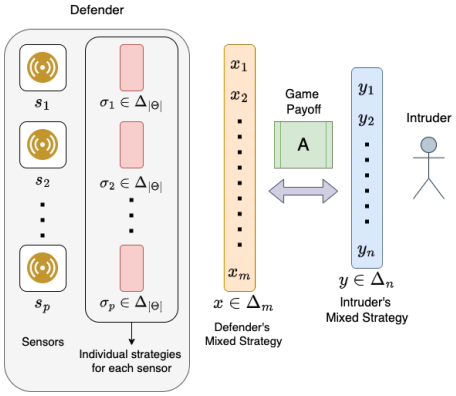
$$\min_{y \in \Delta_{|J|}} x^T B' y$$

Intruder vs Defender Game

- Defender: Schedules a set of sensors to monitor nodes
- Intruder: Chooses a path from a set of paths in the network/graph
- Game Payoff: Probability of Missed-Detection & Strategy Cost

Main Results

- Distributed Weighted Majority (DWM) Algorithm
  - Fast and scalable algorithm to estimate Nash equilibrium
  - Theoretical guarantees for convergence
  - Individual scheduling strategies for each sensor
- Online Learning and Adaptation of Strategies
  - Upper Confidence Bound (UCB) style algorithm for learning the game
  - Online learning under bandit feedback from sensor detection events
  - Order optimal regret bounds: $\tilde{\mathcal{O}}(\sqrt{|\mathcal{S}|^2|\Theta||J|T})$



Strategy Space	Running Time (seconds) Linear Program	Weighted Majority	Distributed Weighted Majority
16 x 50	3.22	2.73	**2.68**
64 x 50	7.90	3.04	**2.65**
256 x 50	24.88	6.09	**4.66**
1024 x 50	75.72	12.15	**6.99**

Acknowledgement: This material is based upon work supported by the Office of Naval Research (ONR) and Saab, Inc. under the Threat and Situational Understanding of Networked Online Machine Intelligence (TSUNOMI) program (grant no. N00014-23-C-1016). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the ONR and/or Saab, Inc.

PURDUE UNIVERSITY
CERIAS