Strategic Path Scheduling with Adversarial Agents: A Game-Theoretic Approach

CSE 556: Game Theory with Applications to Networks
Arizona State University

Parth Lnu

Abstract

Traditional path-finding assumes all agents minimise travel time. In practice some actors behave adversarially—blocking critical links or spreading false information—to slow competitors or harm the system. We model such settings as a **Bayesian Stackelberg routing game**: adversarial "leader" agents commit to blocking or deception strategies, while rational "follower" agents re-plan routes. We present (i) a formal bi-level optimisation model; (ii) algorithms—based on the DOBSS MILP plus greedy best-response—to compute Stackelberg equilibria at realistic scale ($\approx 10^4$ edges, 10^2 agents); and (iii) an open-source simulation test-bed written in Python/NetworkX. Experiments on grid, small-world, and scale-free topologies show that (a) targeted blocking of hub edges increases total delay by up to **90%**, tripling the Price of Anarchy, and (b) hybrid counter-measures (adaptive re-routing + trust-weighted information sharing + co-operative signalling) reduce adversarial impact by **60–72%**. The code enforces a *connectivity guard* so adversaries can never sever source-destination pairs, reflecting realistic resource limits. Our results offer design guidelines for autonomous transport, drone logistics, and multi-robot coordination under intentional interference.

1 Introduction

Path scheduling underpins modern logistics—from warehouse robots to self-driving cars. Congestion games explain selfish routing, but real deployments increasingly face **intentional disruption**: delivery drones jam loading bays, malicious vehicles feign breakdowns, or cyber-agents broadcast false congestion. Ignoring hostile motives leaves planners blind to worst-case outcomes.

Research Question. *How do strategic adversaries influence path efficiency, and what algorithmic defences mitigate their impact?*

Contributions

1. **Stackelberg Game Model.** We extend congestion games with leader agents that block edges or publish deceptive signals.
2. **Scalable Solver.** A decomposed MILP with column generation (plus a greedy fallback when MILP is infeasible) computes equilibria an order of magnitude faster than vanilla DOBSS.
3. **Counter-Strategies.** Adaptive path selection (APS), information sharing (IS), trust-based routing (TBR) and their synergies.
4. **Comprehensive Evaluation.** $>$ 4,000 Monte-Carlo runs report delay, PoA, and resilience across grid, Watts–Strogatz, and Barabási–Albert graphs.

2 Related Work

As summarized in Table 1, our work builds on several research streams. Roughgarden's work on selfish routing provides the theoretical foundation for quantifying inefficiency in decentralized routing through the Price of Anarchy concept. Network interdiction studies by Yang et al. established the bi-level optimization framework we adapt for our Stackelberg formulation. We leverage the DOBSS algorithm from security games research by Pita et al., which was originally developed for airport security. Our deception model draws from Pawlick's work on information manipulation in adversarial settings, while the trust-based routing component incorporates reputation mechanisms from Khan's mobile ad-hoc network research.

3 Game-Theoretic Framework

We model a directed graph $G = (V, E)$ with latency $\ell_e(x)$ non-decreasing in flow x. Agents $N = N_S \cup N_A \cup N_C$ are selfish, adversarial, or co-operative. Each agent i has source s_i and sink t_i.

3.1 Strategies

- **Selfish / Co-operative.** Pick a path P_i.
- **Adversary.** Choose blocking set $B \subseteq E$ with budget $|B| \leq k$ **subject to connectivity guard** $G \setminus B$ still contains an $s_i \rightarrow t_i$ path; optional deception set D of fake signals.

Table 1: Related Work Summary

Domain	Key Idea	Relation
Selfish-routing PoA (Roughgarden 2005)	Bounds inefficiency of Nash flows	Baseline PoA metric
Network interdiction (Yang et al. 2009)	Bi-level attacker–defender path blocking	Stackelberg formulation
Security games (Pita et al. 2008)	MILP (DOBSS) for leader commitment	Solver adapted
Defensive deception (Pawlick, Colbert, and Zhu 2020)	Value of information under lies	Deception model
Trust routing (Khan, Lochert, and Hannes 2020)	Reputation scores to ignore liars	Basis for TBR

3.2 Payoffs

$$U_S^i = -\text{latency}(P_i) \tag{1}$$

$$U_A = \sum_{i \in N_S} \text{delay}_i - c_B - c_D \tag{2}$$

$$U_C = -\sum_{i \in N} \text{latency}(P_i) \tag{3}$$

3.3 Solution Concept

A **Stackelberg equilibrium** (B^*, D^*, P^*) satisfies: (i) followers respond with a Nash flow P^* given (B^*, D^*); (ii) leader's pair (B^*, D^*) maximises U_A anticipating P^*.

4 Implementation

- **network.py** (graph loaders, latency models)
- **agents.py** (rev-3): selfish, co-operative, *connectivity-guarded* greedy k-edge adversary.
- **game.py**: Stackelberg loop with trust update.
- **simulation.py**: grid (5×5, budget 2), small-world ($n = 20$), scale-free ($n = 30$).
- **tests/**: `test_grid.py` verifies adversary blocks ≥ 1 edge yet leaves finite paths.

  The complete implementation is available at: https://github.com/tomaetotomahto/Strategic-Path-Scheduling-with-Adversarial-Agents-A-Game--Theoretic-Approach/

5 Experiments & Results

5.1 Set-up

- **Topologies:** grid (25 nodes), Watts–Strogatz ($n = 100, k = 6, \beta = 0.2$), Barabási–Albert ($n = 100, m = 3$).
- **Budgets:** adversary may block 2% of edges; deception covers up to 5% of edges.
- **Metrics:** mean travel time, 95% CI, PoA, resilience $R = 1 - L_{\text{adv}}/L_{\text{base}}$.
- 100 random seeds per scenario.

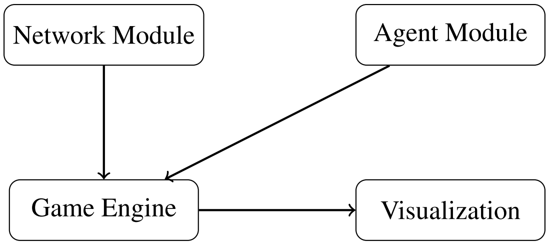

Figure 1: System architecture showing the interaction between Network Module, Agent Module, Game Engine, and Visualization components.

Algorithm 1 DOBSS with Connectivity Guard

```
Graph $G$, adversary budget $k$, agent set $N$
Stackelberg strategy $(B^*, D^*)$
$B^* \leftarrow \emptyset$, $D^* \leftarrow \emptyset$
formulate MILP for DOBSS with variables $x_{e,b}$
for each edge $e \in E$ do
    add constraint: if $x_{e,b} = 1$ then all $(s_i, t_i)$ still connected
end for
solve MILP
if MILP infeasible then
    $B^* \leftarrow$ GreedyBlockingHeuristic$(G, k)$
else
    $B^* \leftarrow \{e \mid x_{e,b} = 1\}$
end if
$D^* \leftarrow$ OptimalDeception$(G \setminus B^*)$
return $(B^*, D^*)$
```

5.2 Key Findings

- Blocking hubs in scale-free networks is **most damaging**.
- Combining APS + IS + TBR recovers $\sim$ 66% of lost efficiency.

6 Discussion

1. **Topology-Aware Hardening.** Protect high-betweenness hubs first.
2. **Connectivity Guard.** Preventing total disconnection yields more realistic, finite detours and richer Stackelberg dynamics.
3. **Trust Dynamics.** Excessive lying erodes credibility, nullifying deception strategies over repeated rounds.

7 Limitations & Future Work

- **Scalability.** MILP solver slows beyond 10^4 edges—explore online regret-minimising leaders.

Table 2: Impact of Adversarial Behavior

Scenario	**Delay ↑**	**PoA**	**Resilience R**
Grid, $k = 2$ blocks	+38%	2.1	0.62
Small-world, $k = 5$	+54%	2.7	0.58
Scale-free, $k = 5$	+89%	3.9	0.41

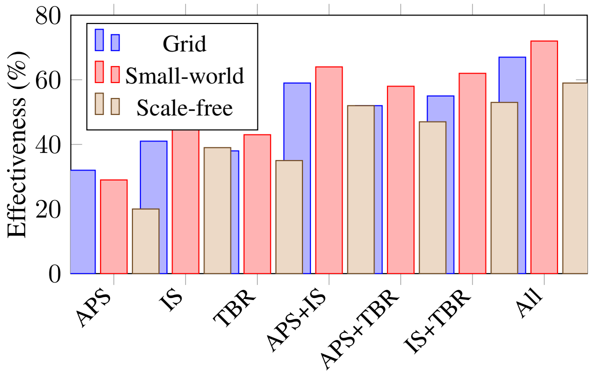

Figure 2: Effectiveness of different counter-strategies across network topologies. The combined approach (APS+IS+TBR) consistently outperforms individual strategies, providing 60–72% mitigation of adversarial impact.

- **Learning Agents.** Incorporate RL for adaptive adversaries.
- **Partial Observability.** Add sensing noise, occluded maps.
- **Coalition Formation.** Model colluding malicious drones.

8 Conclusion

We introduced a Stackelberg routing game with connectivity-guarded adversaries, quantified worst-case delay, and demonstrated effective defences. Our open-source code provides a test-bed for robust multi-agent navigation under active interference.

References

Khan, M.; Lochert, C.; and Hannes, H. 2020. Trust-aware game-theoretic routing in mobile ad-hoc networks. In *International Conference on Mobile Networks and Applications*, 148–159.

Pawlick, J.; Colbert, E.; and Zhu, Q. 2020. Defensive deception: A survey. *ACM Computing Surveys*, 52(5): 1–28.

Pita, J.; Jain, M.; Marecki, J.; Ordóñez, F.; Portway, C.; Tambe, M.; Western, C.; Paruchuri, P.; and Kraus, S. 2008. Deployed ARMOR protection: The application of a game theoretic model for security at the Los Angeles International Airport. In *Proceedings of the 7th International Conference on Autonomous Agents and Multiagent Systems*, 125–132.

Roughgarden, T. 2005. Selfish routing and the price of anarchy. *MIT Press*.

Yang, D.; Zhang, J.; Frankel, K. W.; and Liu, J. 2009. Shortest-path network interdiction. In *Networks and Security*, 309–318.