Intrusion Resilience in Game Theoretical APT Models

PI: Alina Oprea, Northeastern University, Boston, MA

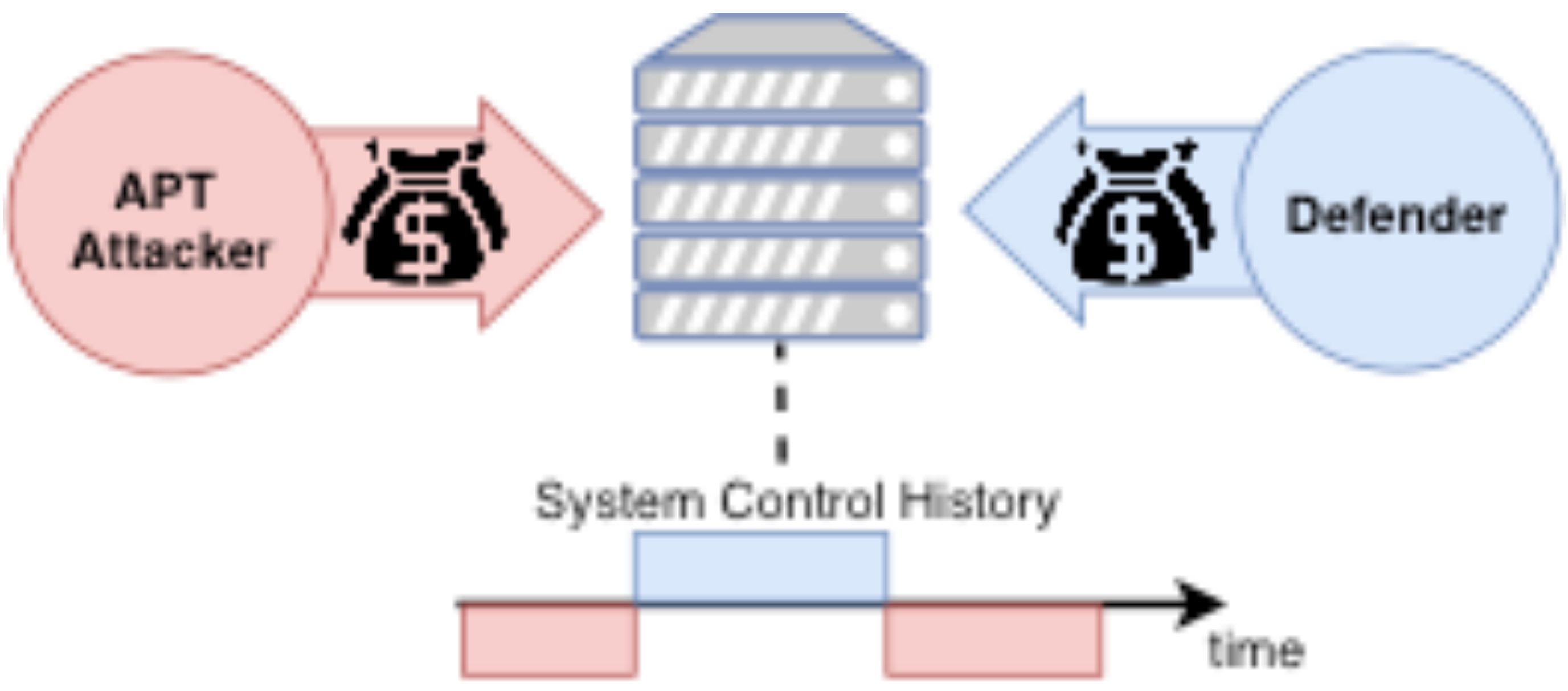
Research assistant: Lisa Oakley, Northeastern University, Boston, MA

Game Theoretical Modeling of APTs

Advanced Persistent Threats (APTs) are long-running, stealthy attacks which circumvent existing security guarantees. Modeling these attacks in a game-theoretical framework can help devise holistic mitigation strategies, while optimizing defense costs.

Main Challenges/Goals

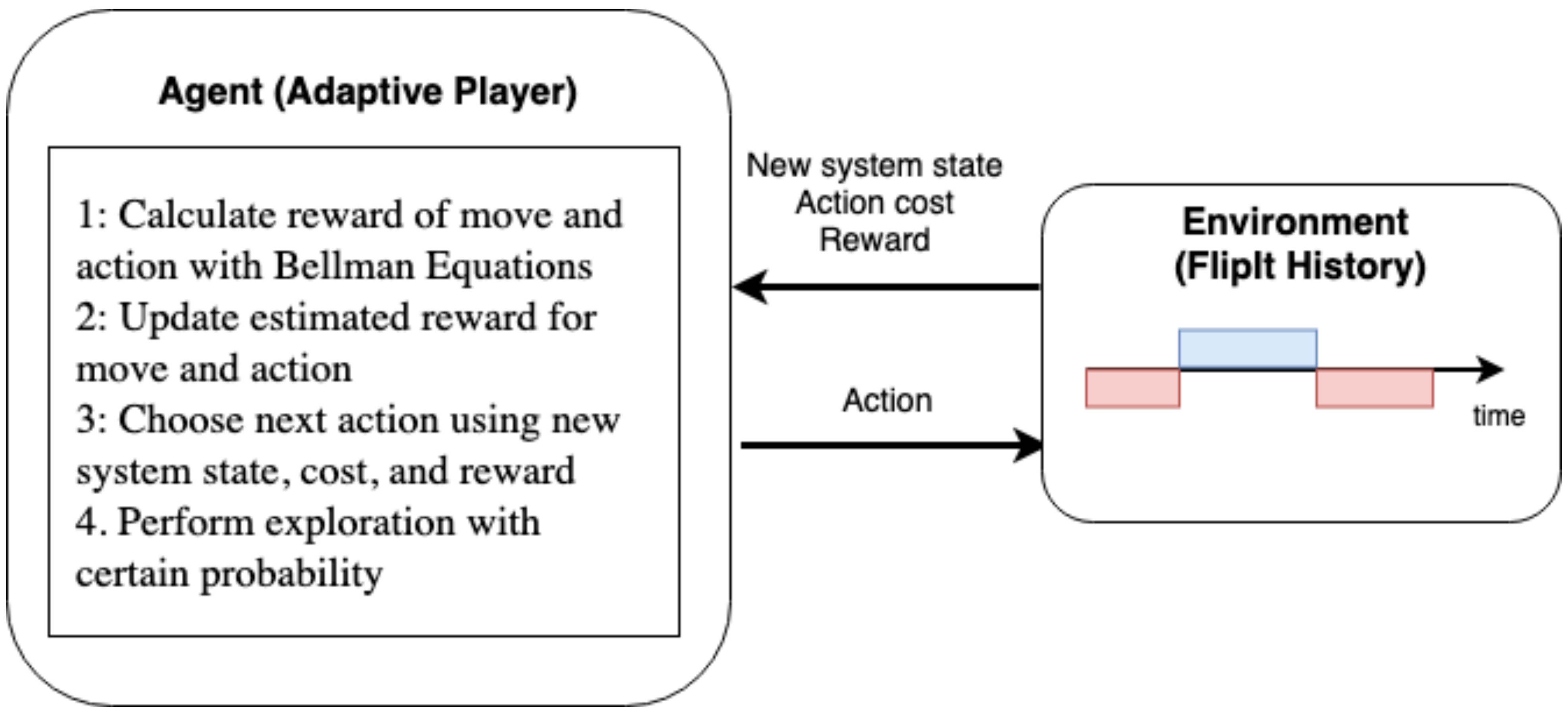
- Use game theory to model adversarial interactions
- Model adaptive play strategies using reinforcement learning (RL) algorithms
- Think holistically about enterprise defense



M. van Dijk, A. Juels, A. Oprea, R. Rivest. FlipIt: the Game of Stealthy Takeover. 2013

Model Setup

1. Consider APT-like attack scenario
2. Use the FlipIt game-theoretical framework
3. Use Markov Decisions Processes (MDP) and Q-Learning to design adaptive strategies
4. Evaluate reinforcement learning model against existing strategies

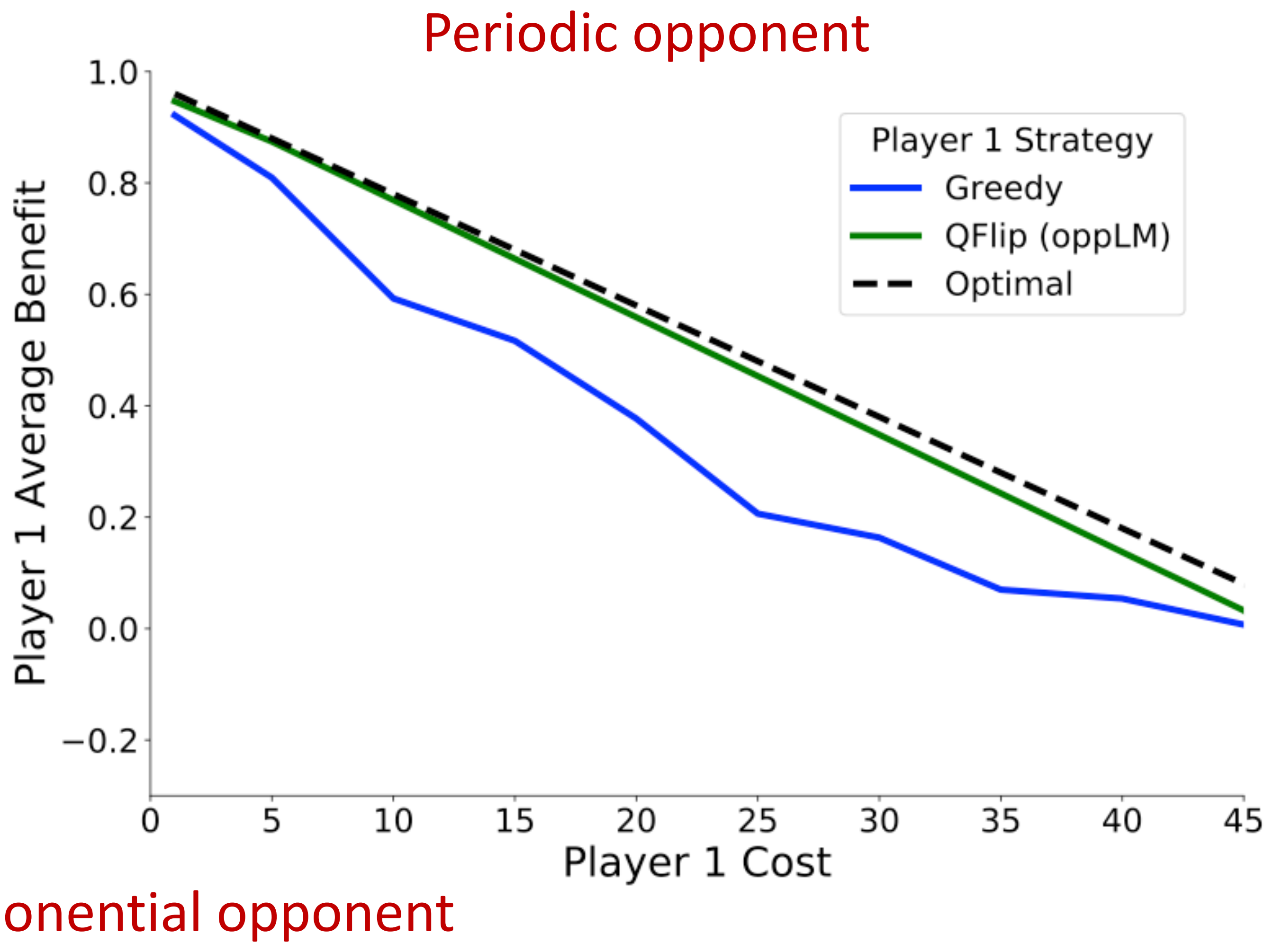


1: Calculate reward of move and action with Bellman Equations
2: Update estimated reward for move and action
3: Choose next action using new system state, cost, and reward
4. Perform exploration with certain probability

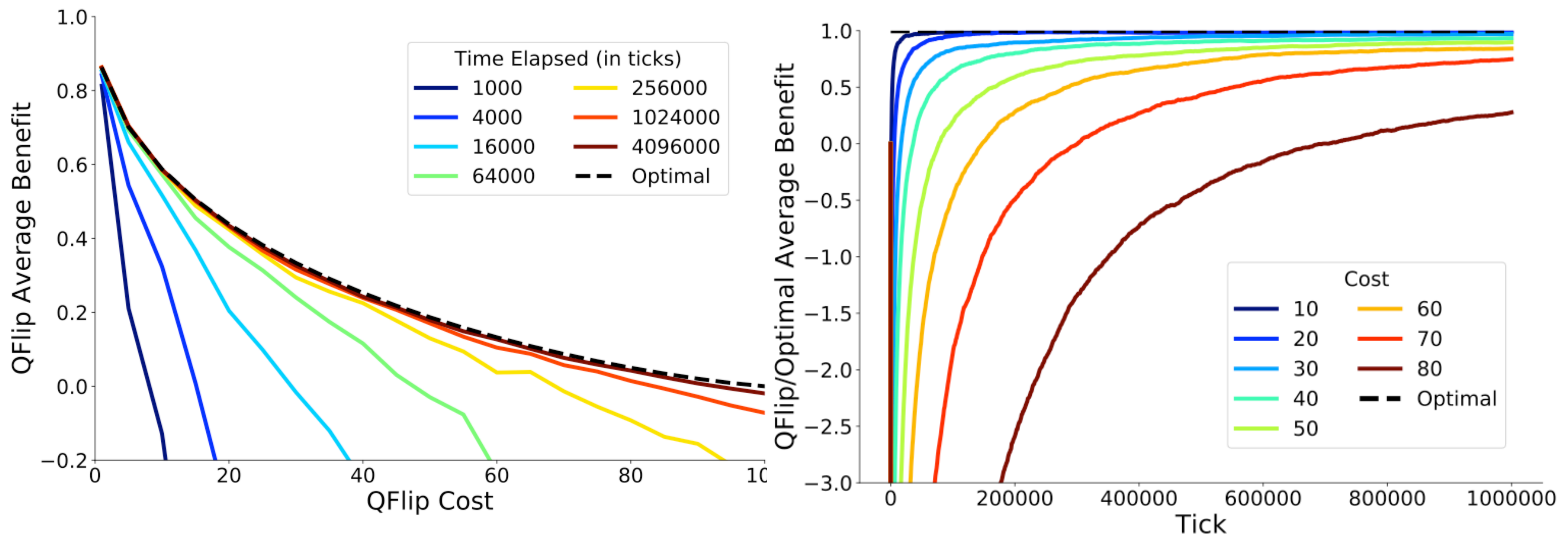
Results

- Theoretical convergence analysis against periodic
- RL strategies converge to optimal
- RL strategies improve upon Greedy

Periodic opponent



Exponential opponent



Impacts

Scientific: Theoretical model can apply to various security scenarios. RL can be used as a tool for adaptive cyber defense.

Societal: Model and tools for dynamic defenses against more sophisticated modern attackers.

Future Research: RL defense against sophisticated attacks, other defenses against RL attacks.

Outreach: QFlip: An Adaptive Reinforcement Learning Strategy for the FlipIt Security Game.

Lisa Oakley and Alina Oprea.

In *Proceedings of the Conference on Decision and Game Theory for Security (GameSec)*, 2019.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 I Alexandria, Virginia

Award ID#: 1717634