A Survey of Advancements in Green Security Games

Joe McCall

CAP5600

Abstract

The field of Green Security Games (GSG) has proven useful in the protection of wildlife. By modelling attackers and defenders as intelligent agents in a repeated simulation we can employ a winning algorithm to deploy scarce resources in actual green security scenarios. This paper summarizes the concept of GSGs, surveys the advancements that have been made, and suggests future opportunities for research.

1 Introduction

The domain of green security entails the struggle between poachers/illegal fishers and rangers charged to protect the wildlife. The rangers are limited in number and have strict constraints applied.

In the field of Artificial Intelligence, Stackelberg Security Games (SSG) have been used to predict potential attacker moves in order to assist in defender strategies. The application of this strategy to green security domains is called Green Security Games (GSG, introduced by [1]). The game abstracts the reality of poachers versus rangers patrolling a vast wildlife area into a grid-based simulation between attackers and defenders, both of which are AI agents. The attacker's goal is to place snares for wildlife without being caught, while the defender's goal is to detect both the snare and the attacker. Furthermore, the attacker behaves human-like and does not always behave optimally.

The game is run in episodes [1]. By simulating multiple rounds of this game, an optimized defender strategy is formed. This strategy is applicable to assist real-world rangers in deciding where and how patrols should be deployed.

Advancements in this field introduce additional constraints, challenge assumptions, and propose novel methods for improving defender strategy. Qian et al. [2] show that the environment must be partially-observable to model the defender's decision to explore new areas or patrol areas known to have snares. Wang et al. [3] introduce the idea that both attackers and defenders leave footsteps that can be used to evade and track. Finally Gholami et al. [4] show that a defender strategy that combines a machine-learning agent with an online learning algorithm that does not rely on prior information can outperform existing models.

2 Methods/Theory

3 Discussions

4 Conclusions

5 References

[1] F. Fang, P. Stone, and M. Tambe, "When security games go green: Designing defender strategies to prevent poaching and illegal fishing," in *Proceedings of the 24th international conference on artificial intelligence*, 2015, pp. 2589–2595.

[2] Y. Qian, C. Zhang, B. Krishnamachari, and M. Tambe, "Restless poachers: Handling exploration-exploitation tradeoffs in security domains," in *Proceedings of the 2016 international conference on autonomous agents & multiagent systems*, 2016, pp. 123–131.

[3] Y. Wang *et al.*, "Deep reinforcement learning for green security games with real-time information," in *Proceedings of the thirty-third aaai conference on artificial intelligence*, 2019, pp. 1401–1408.

[4] S. Gholami, A. Yadav, L. Tran-Thanh, B. Dilkina, and M. Tambe, "Don't put all your strategies in one basket: Playing green security games with imperfect prior knowledge," in *Proceedings of the 18th international conference on autonomous agents and multiagent systems*, 2019, pp. 395–403.