Taha Eghtesad

University Park, PA | (832) 606-0154 | tahaeghtesad@psu.edu | Scholar | LinkedIn | https://tahaeghtesad.github.io | Github

SUMMARY

- **PhD Candidate** and Research Assistant in Computer Science specializing in **machine learning**.
- **Five** years of experience as an academic and industry researcher, developing **reinforcement learning**, **deep learning**, and **statistical reasoning** solutions with **distributed and scalable** frameworks for efficient ML training and deployment.
- Strong publication record with an **h-index of 7 and 134 citations**, featuring contributions to top-tier ML conferences and journals.

EDUCATION

exp. May 2025

Pennsylvania State University, University Park, PA, **Computer Science, Ph.D**., Advisor: Dr. Aron Laszka

Dissertation: *Adversarial Reinforcement Learning for Cyber Attack Prevention, Detection, and Mitigation*

May 2022

University of Houston, Houston, TX, **Computer Science, M.S**., Advisor: Dr. Aron Laszka

Thesis: *Adversarial Deep Reinforcement Learning for Moving Target Defense Automatic Decision-making*

SELECT PUBLICATIONS

Total Citations 134 | H-Index 7 | Conference, Journal, and Magazine Publications 9

- **T. Eghtesad** et al.; *Multi-Agent Reinforcement Learning for Assessing False-Data Injection Attacks on Transportation Networks*; International Conference on Autonomous Agents and Multi-Agent Systems; AAMAS; 2024; **Core Ranking A***; Invited Talk: Auckland, NZ
- **T. Eghtesad** et al.; *Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense*; GameSec; 2020; Invited Talk: University of Maryland – College Park
- O. Akgul, **T. Eghtesad**, et al.; *Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem*; USENIX Security; 2023; **Core Ranking A***; **Distinguished Paper Award**

SELECT EXPERIENCE

Aug 2022 – present

Doctoral Dissertation, *Adversarial Reinforcement Learning for Cyber Attack Prevention, Detection, and Mitigation*

- **Applied reinforcement learning** to solve **cybersecurity** challenges in transportation, chemical plants, and computer security by developing novel multi-agent RL algorithms for automated decision-making, enabling autonomous threat detection and mitigation.
- Devised and evaluated a **hierarchical multi-agent** reinforcement learning algorithm that successfully attacked a simulated transportation system, **increasing total vehicle travel time by 50% compared** to the no-attack baseline.
- Devised and evaluated a **competitive multi-agent** reinforcement learning algorithm that effectively mitigated attacks on chemical plants, **limiting state deviation to only 17%** under attack compared to nominal operating conditions.
- Leveraged **software engineering principles** and the Slurm workload manager to implement a **scalable, distributed** computing environment using **MPI**, enabling **efficient evaluation** of multi-agent reinforcement learning algorithms in the context of cyberattacks.
- Relevant Skills: Python, Pytorch, SkLearn, matplotlib, numpy, Reinforcement Learning, DDPG, PPO, Multi-Agent Learning, Deep Learning, Clustering, Distributed Computing, Linux, Scientific Computing, MATLAB, Object Oriented Development.

July 2024– Aug 2024

Machine Learning Research Intern, Triconex at Schneider Electric, Lake Forest, CA

- Collaborated on US patents for Automated Layers of Protection Analysis (LOPA) by performing requirement analysis of safety controllers.
- Applied **supervised and reinforcement learning** solutions for LOPA of safety controllers of Industrial Control Systems.
- Applied adversarial reinforcement learning to **mitigate safety hazards** in Industrial Control Systems.
- Relevant Skills: Cyber-physical and safety system research, statistical modeling, single and multi-agent reinforcement learning.

Aug 2021–Aug 2022

Object Detection for Ridership Data Acquisition, Research Assistant, University of Houston

- Ensured high-quality training and evaluation data for computer vision models by annotating 7000 frames for detection and tracking.
- Trained and **optimized** YOLOv6 **object detection** models to achieve a **10-fold 91% detection rate** for passengers in annotated images.
- Incorporated and **fine-tuned** SORT **object tracking** algorithms to accurately assign boarding/alighting stops to passengers in 24 x 30-second videos, demonstrating an **84% assignment accuracy**.
- Deployed a **containerized** solution on the transit authority's infrastructure, enabling automated ridership data collection and analysis.
- Relevant Skills: Computer Vision, Deep Learning, Pytorch, Object Detection, Object Tracking, Distributed Computing.