






Taha Eghtesad | PhD Candidate

University Park, Pennsylvania

 /tahaeghtesad  Personal Website  tahaeghtesad@psu.edu  Google Scholar  /in/tahaeghtesad

EDUCATION

- **Doctor of Philosophy, Computer Science** Aug 2022 – Present
PENNSYLVANIA STATE UNIVERSITY; ADVISOR: DR. ARON LASZKA
Approved I-140 Immigrant Petition for Alien Workers based on National Interest Waiver
Recipient of Graduate Fellowship for \$71,000/yr University Park, PA
- **Master of Science, Computer Science** Aug 2018 – May 2022
UNIVERSITY OF HOUSTON; ADVISOR: DR. ARON LASZKA
Recipient of Graduate Fellowship for \$41,000/yr HOUSTON, TX
- **Bachelor of Science, Computer Engineering – Software** Sep 2013 – Feb 2018
SHAHID BEHESHTI UNIVERSITY
Lead ACM-ICPC Team in West Asia Regional Contest
Lead AI Challenge and IranOpen 2D Soccer Simulation Team Tehran, Iran

AREAS OF EXPERTISE AND RESEARCH

Machine Learning, Reinforcement Learning, Strategic Decision-Making, Computer Security, Software Engineering

PUBLICATIONS

- T. Eghtesad et al; Hierarchical Multi-Agent Reinforcement Learning for Assessing False-Data Injection Attacks on Transportation Networks; AAMAS'24; **Core Ranking A***; *accepted for publication*
- T. Eghtesad et al; Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense; GameSec'20
Invited Talk: Gamesec'20 Conference, University of Maryland – College Park ([Presentation](#))
- O. Akgul, T. Eghtesad, et al; Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem; USENIX Security'23; Core Ranking A*; **Distinguished Paper Award (Top %5)**
- O. Akgul, T. Eghtesad, et al; Exploring Challenges and Benefits of Bug-Bounty Programs; WSIW'20
- S. Eisele, T. Eghtesad, et al; Safe and Private Forward-Trading Platform for Transactive Microgrids; TCPS; Dec 2020
- S. Eisele, T. Eghtesad, et al; Blockchains for Transactive Energy Systems: Opportunities, Challenges, and Approaches; IEEE Computer Magazine; Sep 2020
- C. Barreto, T. Eghtesad, et al; Cyber-attacks and mitigation in blockchain based transactive energy systems; ICPS'20
- S. Eisele, T. Eghtesad, et al; Decentralized Computation Market for Stream Processing Applications; IC2E'22
- S. Eisele, T. Eghtesad, et al; Mechanisms for Outsourcing Computation via a Decentralized Market; DEBS'20

SCHOLARLY EXPERIENCE

- **Doctoral Dissertation** Pennsylvania State University
RESEARCH ASSISTANT (FUNDED BY NSF) AUG 2022 – PRESENT
Title: *Adversarial Reinforcement Learning for Cyberattack Prevention, Detection, and Mitigation*
 - Developed a state-of-the-art **multi-agent deep reinforcement learning** framework for **detection** of security breaches in public transportation networks at an operation level by observation of traffic patterns. **Game theoretic** analysis ensures strategic **adaptability** to a variety of attacks such as false data injection, social engineering, and physical tampering. Our approach suggests a **92% correct detection rate** within **3 minutes** of the attack.
 - Devised a novel **deep reinforcement learning** framework for **mitigation** of false data injection attacks on sensor and actuator signals in **networked computer systems**. Strategic modeling of the interaction of false data injection agents and the system controller ensures mitigation against a **worst-case attack scenario** with stealthy attackers. Analysis of the framework shows **9.7%** deviation of the system from **nominal operations** in a worst-case attack.

• Master Thesis

RESEARCH ASSISTANT (FUNDED BY NSF, DoE, ARO)

University of Houston

AUG 2018 – AUG 2022

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

- **Network reconnaissance attacks** is the initial step of sophisticated **adversarial persistent threats** against computer networks. To this extent, we developed a state-of-the-art **multi-agent reinforcement learning** framework that employs **game theoretic** modeling to obfuscate network architecture. This framework systematically alters network and component configurations, proactively defending against reconnaissance attacks by strategic and stealthy actors. The implemented solution enhances defense accuracy, reliability, and sophistication, surpassing the effectiveness of human-supervised ([GitHub](#))

• Bachelor Project

RESEARCH ASSISTANT

Shahid Beheshti University

MAY 2017

Title: *SunHAS: A Home Automation System for Smart Energy Monitoring*

- Developed a home automation system based on ESP8266 Microcontroller (C++), NodeJS, and Casandra for energy monitoring and routine actuation in smart homes. The limitations of Wifi range and number of connected nodes are tackled by turning the set of ESP8266 controllers into a **mesh grid**, enabling deployment of these systems on large-scale residential and commercial buildings reliably and wirelessly. ([GitHub](#))

• Selected Projects

RESEARCH ASSISTANT (FUNDED BY NSF, DoT, DoE, NIST)

University of Houston

AUG 2018 – SEP 2022

Title: *Deep Reinforcement Learning for Model-Based Volt/VAR Optimization*

- Devised a decentralized **deep reinforcement learning** platform based on **DDPG** algorithm for improving **Volt/VAR** optimization of **power grids** in smart and connected communities. **Decentralization** of the computational framework leads to improved training time and better accuracy of the models. Our analysis shows that our RL framework improves the Volt/VAR convergence time **from thousands** of computational steps to a few **hundred steps** to stabilize the power grid. ([GitHub](#))

Title: *Blockchain-based Renewable Transactive Trading Framework in Smart Communities*

- Designed and implemented an **Ethereum-based smart contract** platform for **forward-trading renewable energy** within smart and connected communities. Developed software integration to facilitate seamless interaction between off-chain and on-chain components, maintaining authenticity and accountability of the energy trading contracts in an efficient manner. ([GitHub](#))

Title: *Toward Scalable Bug Bounty Programs*

- Surveyed 156 bug bounty hunters to understand **their motivations and challenges they face** while working in the crowdsourced vulnerability discovery markets. We interviewed 24 participants for a better understanding of the reasons for their dissatisfaction and leaving a program. With a **quantitative and qualitative** assessment, we summarized the key takeaways from the interviews with a numerical ranking. We provided **managerial bullet points** for program directors to improve their program, increasing participation and efficiency while decreasing the wasted time due to invalid reports.

Title: *Computer Vision For Ridership Data Acquisition*

- Trained and applied **computer vision object detection** models to public transit footage for passenger counting. Enabled automated collection of public transit boarding/alighting patterns using camera footage with **computer vision tracking** algorithms. We achieve **91%** accuracy in correctly detecting and counting passengers and assigning them to their boarding/alighting stops. ([GitHub](#))

SKILLS

- **Languages:** Python, Java, C, C++, C#, JavaScript, MATLAB
- **Machine Learning Algorithms:** Decision Tree, SVM, Linear Regression, Linear Programming, Clustering, Bayesian, Deep Learning, Graph Convolution, Graph Attention, Convolutional Neural Network, RL (*Q*-Learning, DDPG, SAC, PPO)
- **Machine Learning Technologies:** TensorFlow, PyTorch, Keras, Pandas, Numpy, SciKit Learn, Matplotlib, Seaborn
- **Software Development Technologies:** J2EE, Spring, Hibernate, ASP.NET, Entity Framework, NodeJS, Express JS, SQL, NoSQL (Redis, Neo4j) with emphasis on clean and maintainable development
- **Big Data and Cloud Technologies:** Information Retrieval, ELK Stack, Map Reduce, Apache Hadoop, Apache Spark, MongoDB, Kubernetes
- **Computer Engineering:** Data Structures, Algorithms, Object Oriented Programming, Design Patterns, Computer Architecture, Computer Networks, Cryptography, Compilers
- **Misc:** \LaTeX , Git, Linux (LPIC-1), Windows (MCSA), CI/CD (Jenkins)