Ethan Rathbun

EthanRath | Ethan Rathbun | ethanrathbun.com | rathbun.e@northeastern.edu |

Education

Northeastern University, Boston, MA, United States — 2023 - present
PhD in Computer Science, **GPA 4.0/4.0**
Advisors: *Christopher Amato and Alina Oprea*

University of Connecticut, Storrs, CT, United States — 2018 - 2022
BS in Computer Science, **GPA: 3.8/4.0**
BA in Mathematics, **GPA: 3.7/4.0**
Advisors: *Marten van Dijk and Kaleel Mahmood*

Research Experience

Network and Distributed Systems Security Lab at Northeastern University — 2023 - present
Graduate Research Assistant

Lab for Learning and Planning in Robotics at Northeastern University — 2023 - present
Graduate Research Assistant

Secure Computing Lab at University of Connecticut — 2019 - 2023
Undergraduate Research Assistant

Resilient Extraterrestrial Habitats Institute at University of Connecticut — 2021 - 2022
Undergraduate Research Assistant

Publications

Adversarial Inception Backdoor Attacks against Reinforcement Learning
Rathbun, Ethan, Alina Oprea and Christopher Amato.
International Conference on Machine Learning (2025)

Sleepernets: Universal Backdoor Poisoning Attacks Against Reinforcement Learning Agents
Rathbun, Ethan, Christopher Amato, and Alina Oprea.
Advances in Neural Information Processing Systems (2024)

Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense
Singh, Aditya Vikram, **Ethan Rathbun**, Emma Graham, Lisa Oakley, Simona Boboila, Peter Chin, and Alina Oprea
Reinforcement Learning Conference (2025)

Game Theoretic Mixed Experts for Combinational Adversarial Machine Learning
Mahmood, Kaleel*, **Rathbun, Ethan***, Ronak Sahu, Marten Van Dijk, Sohaib Ahmad, and Caiwen Ding
IEEE Access (2025)

Busting the Paper Ballot: Voting Meets Adversarial Machine Learning
Mahmood, Kaleel, Caleb Manicke, **Ethan Rathbun**, Aayushi Verma, Sohaib Ahmad, Nicholas Stamatakis, Laurent Michel, and Benjamin Fuller
The ACM Conference on Computer and Communications Security (2025)

Attacking the spike: On the security of spiking neural networks to adversarial examples
Xu, Nuo, Kaleel Mahmood, Haowen Fang, **Ethan Rathbun**, Caiwen Ding, and Wujie Wen
Neurocomputing (2025)

Distilling Adversarial Robustness Using Heterogeneous Teachers
Deng, Jieren, Aaron Palmer, Rigel Mahmood, **Ethan Rathbun**, Jinbo Bi, Kaleel Mahmood, and Derek Aguiar
International Neural Network Society Workshop on Deep Learning Innovations and Applications (2025)

Back in Black: A Comparative Evaluation of Recent State-Of-The-Art Black-Box Attacks
Mahmood, Kaleel, Rigel Mahmood, **Ethan Rathbun**, and Marten van Dijk
IEEE Access (2022)

Academic Service

Organizing Committee Member

1st Workshop on Coordination and Cooperation in Multi-Agent Reinforcement Learning
Reinforcement Learning Conference 2024

2nd Workshop on Coordination and Cooperation in Multi-Agent Reinforcement Learning
Reinforcement Learning Conference 2025

Program Committee Member

International Conference on Learning Representations 2024, 2025
Advances in Neural Information Processing Systems 2025

Faculty Panel Moderator

2nd Workshop on Coordination and Cooperation in Multi-Agent Reinforcement Learning
Reinforcement Learning Conference 2025

Khoury Security Day 2025
Northeastern University

Talks

Hierarchical Multi-agent Reinforcement Learning for Cyber Network Defense
Reinforcement Learning Conference 2025

Adversarial Inception for Bounded Backdoor Poisoning in Deep Reinforcement Learning
Invited Lecture for CS 4973 / CS 6983: Trustworthy Generative AI at Northeastern University

Teaching Experience

Teaching Assistant, University of Connecticut — Fall - Spring 2023
CSE 2500 – Intro to Discrete Systems

Work Experience

Computer Science Intern, Collins Aerospace, Danbury, CT, United States — Summer 2020

Skills

Programming	Pytorch, Gymnasium, Python, C, Java
Machine Learning	Deep RL, Multi-Agent RL, Adversarial ML
Security	Poisoning, Privacy, and Evasion Attacks against Machine Learning

Last updated: October 3, 2025