Henger (Henry) Li

Email: hli30@tulane.edu Mobile: +1(504)892-7193
Website: https://henger123.wixsite.com/mysite Github: github.com/HengerLi

Summary

Ph.D. candidate working on **(Deep) Reinforcement Learning**, **Cybersecurity**, and **Game Theory**. Looking for research scientist, applied scientist, machine learning/AI engineer full-time and intern opportunities.

Experience

- **Researching Assistant (Sep 2018 - present)** **Tulane University**

  Proposing a novel model-based reinforcement learning (RL) framework to derive adaptive poisoning attacks against federated learning (FL) system, which significantly outperforms state-of-the-art poisoning attacks even under strong defenses, end up with publications on NeurIPS and ICLR

  Developing practical models for robust moving target defense (MTD) by integrating Stackelberg games, reinforcement learning, and meta-learning, to address important issues including spatial-temporal setting and unknown/uncertain attacker in MTD, with works published on AAMAS, GameSec and MILCOM

  Inventing a new algorithm to maximize the efficiency of group testing for COVID-19 in a noisy adaptive setting to help the local community

  Designing a Spatial-Temporal Moving Target Game to interact with real human players on Amazon Mechanical Turk, with a demo displayed on my personal website

  Building large scale model-based (deep) reinforcement learning frameworks to attack/defend a practical federated learning system; Implementing new algorithms and new defensive framework for robust MTD based on data from National Vulnerability Database (NVD) using HPC cluster, with open source codes published on my Github

- **Teaching Assistant (Sep 2021 - May 2022)** **Tulane University**

  Teaching "Introduction to Computer Science" for Fall 2021 and Spring 2022 in the computer science department of Tulane University

Education

- **Tulane University** New Orleans, USA
  Ph.D. Computer Science *Mar 2018 - Dec 2023(expected)*
- **University of Liverpool** Liverpool, UK
  M.S. Degree Computer Science *Sep 2015 - Dec 2016*
- **Xi'an Jiaotong-Liverpool University** SuZhou, China & Liverpool, UK
  B.S. Degree Applied Mathematics *Sep 2011 - Jun 2015*

Publications

- **Henger Li, Xiaolin Sun, and Zizhan Zheng, "Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework,"** Conference on Neural Information Processing Systems (NeurIPS), Nov. 2022 (Acceptance Rate = 25.6%, selected for scholar award)
- **Henger Li and Zizhan Zheng, "Robust Moving Target Defense against Unknown Attacks: A Meta-Reinforcement Learning Approach,"** Conference on Decision and Game Theory for Security (GameSec), Oct. 2022 (selected for travel award).
- **Henger Li, Wen Shen, and Zizhan Zheng, "Spatial-Temporal Moving Target Defense: A Markov Stackelberg Game Model,"** International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS), May 2020 (long paper).(Acceptance Rate = 23%)
- **Wen Shen, Henger Li, and Zizhan Zheng, "Coordinated Attacks Against Federated Learning: A Multi-Agent Reinforcement Learning Approach,"** ICLR 2021 Workshop on Security and Safety in Machine Learning Systems (ICLR-SecML), May 2021 (selected for travel award).
- **Wen Shen, Henger Li, and Zizhan Zheng, "Learning to Attack Distributionally Robust Federated Learning,"** NeurIPS-20 Workshop on Scalability, Privacy, and Security in Federated Learning (NeurIPS-SpicyFL), Dec. 2020 (selected for oral presentation).
- **Henger Li and Zizhan Zheng, "Optimal Timing of Moving Target Defense: A Stackelberg Game Model,"** Military Communications Conference (MILCOM), Nov. 2019.
- **Paper Under Review: "Learning to Backdoor Federated Learning,"** Mar. 2023 (expected).

Presentations

- **Invited talk:** Learning to Poison/Backdoor Federated Learning, AI TIME Youth PhD Talk Forum (held by Tsinghua University), broadcast live by Bilibili, China Knowledge Centre for Engineering Sciences and Technology, XUETANGX, and KouShare, 2023.
- **Poster presentation:** Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework, *NeurIPS*, New Orleans, LA, 2022.
- **Invited talk:** Meta-Reinforcement Learning for Stackelberg Markov games with unknown follower, Electrical Engineering Department at New York University, 2022.
- **Oral presentation:** Robust Moving Target Defense against Unknown Attacks: A Meta-Reinforcement Learning Approach, *GameSec*, CS department at CMU, Pittsburgh, PA, 2022.
- **Ph.D. qualifying presentation:** Adaptive Attack and Proactive Defense in Cybersecurity, CS department at Tulane University, 2021.
- **Oral presentation** Spatial-Temporal Moving Target Defense: A Markov Stackelberg Game Model, *AAMAS*, Virtual, 2020.
- **Interdisciplinary project presentation:** Learning to pool: Adaptive Group Testing for COVID-19, CS department at Tulane University, 2020.
- **Oral presentation:** Optimal Timing of Moving Target Defense: A Stackelberg Game Model, *MILCOM*, Norfolk, VA, 2019.

Skills Summary

- **Languages** Python, MATLAB, JAVA, JavaScript, HTML, Bash, Latex
- **Frameworks** Pytorch, TensorFlow, Keras, Scikit, Numpy, Git, OpenAI, RLlib
- **Platforms** Linux, Web, Windows, AWS, Microsoft Azure, IBM Cloud, HPC cluster
- **Soft Skills** Leadership, Event Management, Writing, Public Speaking, Time Management

Graduate coursework

Reinforcement Learning (Zheng, Zizhan), Machine Learning (Hamm, Jihun), Information Theory (Mislove, Michael), Distributed Systems (Zheng, Zizhan), Multi-agent Systems (Naumov, Pavel), Algorithms (Wenk, Carola), Computational Complexity (Mettu, Ramgopal), Optimization (Hyman, James), Computer Networks (Zheng, Zizhan), Epidemiology for Public Health (Dorans, Kirsten)

Academic Sevice

- **Sub referee** IJCAI 2021, INFOCOM 2019
- **Journal reviewer** IEEE Transactions on Mobile Computing

Other activities

- **Mentoring Undergraduate Capstone Project (Fall 2019 - Spring 2020)** **Tulane University**

  Harrison Pratt (current software engineer at Microsoft) and Tom Roginsky (current software engineer at General Motors), CS coordinate major research on moving target defense (supported by an NSF REU grant)

- **Mentoring Undergraduate Capstone Project (Fall 2020)** **Tulane University**

  Sarper Tutuncuoglu (current software engineer at AWS), independent study on moving target defense

References

- **Zizhan Zheng** Assistant Professor, Advisor, PhD Committee Chair, Tulane University
  zzheng3@tulane.edu
- **Jihun Hamm** Associate Professor, PhD Committee Member, Tulane University
  jhamm3@tulane.edu
- **Nicholas Mattei** Assistant Professor, PhD Committee Member, Tulane University
  nsmattei@tulane.edu
- **Sencun Zhu** Associate Professor, PhD Committee Member, Pennsylvania State University
  sxz16@psu.edu