

Xiaolin Sun

2734 Calhoun Street | New Orleans, LA 70118 | xsun12@tulane.edu | 315.630.2418

EDUCATION&HONORS

Tulane University, Department of Computer Science, New Orleans, LA

August 2020-Present

Doctoral Student

- Cumulative GPA: 3.94/4.00
- Courses Taken: Reinforcement Learning, Machine Learning, Algorithms, Distributed Systems, Multi-agent Systems, Artificial Intelligence, Computer Vision
- Coding skills: Python, Pytorch

Colgate University, Hamilton, NY

August 2016-May 2020

Bachelor of Arts

- Double Major: Computer Science and Mathematical Economics
- Cumulative GPA: 3.66/4.00, Mathematical Economics GPA: 3.73/4.00, Computer Science GPA: 4.02/4.00
- Dean's Award with Distinction for Academic Excellence (Fall 2016-Fall 2017, Fall 2018- Fall 2019)
- Dean's Award for Academic Excellence (Spring 2018)
- Member of Phi Eta Sigma honor society

EXPERIENCE

Research Assistant

September 2021-Present

Tulane University Computer Science Department

I worked as a research assistant for Prof. Zheng. I have worked projects on multi-agent reinforcement learning and robust reinforcement learning.

Mentor

Tulane University Computer Science Department

Summer 2023

Help high school student on her summer research on Reinforcement Learning and its application in autonomous racing.

Teaching Assistant

September 2020-May 2021

Tulane University Computer Science Department

Holding Lab sessions and office hours for Intro to Computer Science and Computer Organization courses.

Research Assistant

Summer 2018-June 2020

Colgate University Computer Science Department

I worked as a research assistant for Prof. Gember-Jacobson. The project aims at developing a tool that can automatically detect the errors in router configurations that cause the policies violation in a network by using SMT solver to get unsatisfiable cores.

CONFERENCE ATTENDED

Poster Presenter

Aug 1st 2023

Thirty-ninth Conference on Uncertainty in Artificial Intelligence (UAI'23)

- Present the paper *Pandering in a (flexible) representative democracy* during the poster session of the conference

Poster Presenter

Dec 1st 2022

Thirty-sixth Conference on Neural Information Processing Systems (NeurIPS'22)

- Present the paper *Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework* during poster sessions of the conference

Attendee

ACM Special Interest Group on Data Communication (Sigcomm'19)

Aug 19th 2019

- Receive NSF Student Travel Grant to attend the conference

Poster Presenter

Feb 26th 2019

16th USENIX Symposium on Networked Systems Design and Implementation (NSDI'19)

- Presented the poster *Localizing Router Configuration Errors Using Unsatisfiable Cores* during the poster sessions of the conference

SELECTED PUBLICATIONS

- [ICLR'24] [Xiaolin Sun](#) and Zizhan Zheng. *Belief-Enriched Pessimistic Q-Learning against Adversarial State Perturbations*. The Twelfth International Conference on Learning Representations (ICLR). 2024.
- [MASEC'23] [Xiaolin Sun](#) and Zizhan Zheng. *Robust Q-Learning against State Perturbations: A Belief-Enriched Pessimistic Approach*. In 1st Multi-Agent Security Workshop at NeurIPS (MASEC). 2023.
- [UAI'23] [Xiaolin Sun](#), et al. *Pandering in a (Flexible) Representative Democracy* In 39th Conference on Uncertainty in Artificial Intelligence (UAI). 2023.
- [AAMAS'23] [Xiaolin Sun](#), et al. *Does Delegating Votes Protect Against Pandering Candidates?* In 22nd International Conference on Autonomous Agents and Multiagent Systems (AAMAS). 2023. (Extended Abstract)
- [NeurIPS'22] Henger Li*, [Xiaolin Sun](#)* and Zizhan Zheng. *Learning to Attack Federated Learning: A Model-based Reinforcement Learning Attack Framework*. In 36th Conference on Neural Information Processing Systems (NeurIPS). 2022. (*Co-Primary Author)
- [NSDI'19] Ruchit Shrestha, [Xiaolin Sun](#), and Aaron Gember-Jacobson. *Localizing router configuration errors*

using unsatisfiable cores. In 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI). 2019.