SIMIN LI

Beijing, China | lisiminsimon@buaa.edu.cn | +86 13520138048| siminli.github.io
English: TOEFL 103 | GRE 332+3.5 | IEILTS 8

EDUCATION

Beihang University, Computer Science **Beijing, China**
Ph.D. Student. Advisor: Prof. Xianglong Liu. Also work with Prof. Yaodong Yang. *Sep. 2021-*

Beihang University, Computer Science **Beijing, China**
Master of Science (Advanced to Ph.D. study). Advisor: Prof. Weifeng Lv. *Seq. 2020-Jul. 2021*

Beihang University, Electronic Engineering **Beijing, China**
Bachelor (Summa Cum Laude). Ranked: top 5%. *Seq. 2016-Jul. 2020*

RESEARCH

Overview: I am interested in **robust multi-agent reinforcement learning** (MARL). My research interest includes practical adversarial attack for MARL, robust MARL and robust LLM-based autonomous agents. In early years, I also work on adversarial attack/defense for computer vision, human-computer interaction, graph neural network, multivariate time series forecasting and microelectronics.

Byzantine Robust Cooperative Multi-Agent Reinforcement Learning as a Bayesian Game

- Robust MARL address the uncertainty from unknown agents under software/hardware error or be controlled by adversaries. We systematically formulate this uncertainty in robust cooperative MARL as a Bayesian Adversarial Robust Dec-POMDP, with uncertainties in unknown agents treated as type assigned by nature. Next, we define corresponding equilibrium concept and propose a practical algorithm with almost sure convergence.
- Accepted by ICLR 2024.

Mutual Information Regularization is Provably Robust for Multi-Agent Reinforcement Learning

- In robust MARL, defenders are unaware of each agent fails or not. As number of agents rises, robust MARL face an exponential increase of threat scenarios, making it computationally hard to solve. By formulating robust MARL as an inference problem, we proof that minimizing mutual information is minimizing a lower bound of robustness in MARL under all potential threat scenarios.
- Submitted to ICML 2024.

Attacking Cooperative Multi-Agent Reinforcement Learning by Adversarial Minority Influence

- We propose an adversarial policy for cooperative MARL, such that an adversary unilaterally fools the joint agents to a cooperative worst-case failure. Technically, the adversary maximizes its impact to victims by a modified mutual information metric and fools the victim to worst-case actions learned by a separate MARL algorithm.
- Submitted to IEEE TCYB.

PUBLICATIONS

- **Simin Li**, Jun Guo, Jingqiao Xiu, Xini Yu, Jiakai Wang, Aishan Liu, Yaodong Yang, Xianglong Liu. *Byzantine Robust Cooperative Multi-Agent Reinforcement Learning as a Bayesian Game*. **ICLR 2024**.
- Xin Yu, Rongye Shi, Pu Feng, Yongkai Tian, **Simin Li**, Shuhao Liao, Wenjun Wu. *Leveraging Partial Symmetry for Multi-Agent Reinforcement Learning*. **AAAI 2024**.
- Pu Feng, Xin Yu, Wenjun Wu, Yongkai Tian, Junkang Liang, **Simin Li**. *SPF-RL: Multi-robots Collision Avoidance with Soft Potential Field informed reinforcement learning*. **ICRA 2024**.
- **Simin Li**, Shuning Zhang, Gujun Chen, Dong Wang, Pu Feng, Jiakai Wang, Aishan Liu, Xin Yi, Xianglong Liu. *Towards Benchmarking and Assessing Visual Naturalness of Physical World Adversarial Attacks*. **CVPR 2023**.
- Jun Guo, Yonghong Chen, Yihang Hao, Zixin Yin, Yin Yu, **Simin Li**. *Towards comprehensive testing on the robustness of cooperative multi-agent reinforcement learning*. **Corresponding author. CVPR 2022 workshop**.
- **Simin Li**, Zhaohao Wang, Yijie Wang, Mengxing Wang, Weisheng Zhao. *Magnetization dynamics modulated by Dzyaloshinskii-Moriya interaction in the double-interface spin-transfer torque magnetic tunnel junction*. **Nanoscale Research Letters 2019.**
- Tengxiang Zhang, Xin Yi, Ruolin Wang, Jiayuan Gao, Yuntao Wang, Chun Yu, **Simin Li**, Yuanchun Shi. *Facilitating Temporal Synchronous Target Selection through User Behavior Modeling*. **Ubicomp 2019**.

Work on Progress

- **Simin Li**, Ruixiao Xu, Jun Guo, Pu Feng, Jiakai Wang, Aishan Liu, Yaodong Yang, Xianglong Liu. *Mutual Information Regularization is Provably Robust for Multi-Agent Reinforcement Learning*. **Submitted to ICML 2024**.
- **Simin Li**, Jun Guo, Jingqiao Xiu, Pu Feng, Xin Yu, Jiakai Wang, Aishan Liu, Wenjun Wu, Xianglong Liu. *Attacking Cooperative Multi-Agent Reinforcement Learning by Adversarial Minority Influence*. **Submitted to IEEE TCYB**.
- **Simin Li**, Huangxinxin Xu, Jiakai Wang, Aishan Liu, Fazhi He, Xianglong Liu, Dacheng Tao. *Hierarchical Perceptual Noise Injection for Social Media Fingerprint Privacy Protection*. **Submitted to IEEE TIP (2023.12: Accept with mandatory, required change).**