SIMIN LI

Beijing, China | lisiminsimon@buaa.edu.cn | +86 13520138048| Google Scholar | Personal Webpage

RESEARCH INTEREST

I am a second year Ph.D. student from Beihang University, interested in Trustworthy AI for multi-agent reinforcement learning (MARL). My research goal is to make reinforcement learning safe and robust, via probing policy weakness by adversarial attacks and enhancing policy robustness by adversarial defense. My current research includes:

- Realistic adversarial attacks and defenses for MARL.
- Adversarial attacks and defenses driven by multidisciplinary insights and techniques.
- Human computer interaction and human-AI alignment.
- Model robustness evaluation and testing of RL/MARL algorithms.

EDUCATION

Ph.D.	School of Computer Science and Engineering, Beihang University Advisor: Prof. Xianglong Liu.	2021-present
M.S.	School of Computer Science and Engineering, Beihang University Advisor: Prof. Weifeng Lv.	2020-2021
B.S.	School of Electronic Information Engineering, Beihang University	2016-2020

PUBLICATIONS

First-authored Papers

- **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 USENIX Security 2023.*
- **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."*** *Submitted to CVPR 2023.*
- **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.*

Co-authored Papers

- Jun Guo, Yonghong Chen, Yihang Hao, Zixin Yin, Yin Yu, **Simin Li***. (* indicates corresponding author) ***"Towards Comprehensive Testing on the Robustness of Cooperative Multi-agent Reinforcement Learning."*** *CVPR Workshop, 2022.*
- Aishan Liu, Jun Guo, **Simin Li**, Yisong Xiao, Xianglong Liu, Dacheng Tao. ***"A Survey on Adversarial Attacks and Defenses for Deep Reinforcement Learning (in Chinese)."*** *Chinese Journal of Computers (top journal in China), 2023.*
- Jiakai Wang, Aishan Liu, **Simin Li**, Xianglong Liu, Wenjun Wu. ***"A Survey on Adversarial Attacks and Defenses for Deep Reinforcement Learning (in Chinese)."*** *Artificial Intelligence Security (invited), 2023.*
- Pu Feng, Xin Yu, Wenjun Wu, Yongkai Tian, Junkang Liang, **Simin Li**. ***"Hierarchical SPF-RL: Multi-robots Collision Avoidance with Soft Potential Field informed reinforcement learning."*** *Submitted to ICAPS 2023.*

Researches Before Ph.D.

- **Simin Li**, Zhaohao Wang, Yijie Wang, Mengxing Wang, and Weisheng Zhao. "***Magnetization Dynamics Modulated by Dzyaloshinskii-Moriya Interaction in the Double-Interface Spin-Transfer Torque Magnetic Tunnel Junction***." *Nanoscale Research Letters*, 2019. Impact Factor=3.1
- Tengxiang Zhang, Xin Yi, Ruolin Wang, Jiayuan Gao, Yuntao Wang, Chun Yu, **Simin Li**, and Yuanchun Shi. "***Facilitating Temporal Synchronous Target Selection through User Behavior Modeling.***" *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 2019.*
- Wang, Zhaohao, Zuwei Li, Yang Liu, **Simin Li**, Liang Chang, Wang Kang, Youguang Zhang, and Weisheng Zhao. "***Progresses and challenges of spin orbit torque driven magnetization switching and application.***" *IEEE International Symposium on Circuits and Systems (ISCAS)* , 2018.

ACADEMIC SERVICES

2022-2023	Reviewer	CVPR, ECCV, AAAI, Pattern Recognition, etc.
	Program Committee	The Art of Robustness Workshop, CVPR 2023