Shaoyuan Xie

(949)368-5560 | shaoyux@uci.edu | https://github.com/Daniel-xsy

EDUCATION

University of California, Irvine — Irvine, CA
Ph.D. in Computer Science — Expected Jun 2028
Huazhong University of Science and Technology (HUST) — Wuhan, CN
B.Eng. in Automation, GPA 3.97 / 4.00 (Top 1) — Jun 2023
Honors: Honors Bachelor Degree, National Scholarship (0.2%, 2 years)

PUBLICATION

My research interests focus on the intersection of AI, Security, and Autonomous System

- **Are VLMs Ready for Autonomous Driving? An Empirical Study from Reliability, Data, and Metric Perspectives**
  Shaoyuan Xie, Lingdong Kong, Yuhao Dong, Chonghao Sima, Wenwei Zhang, Qa Alfred Chen, Ziwei Liu, Liang Pan
  (Under Review) Submitted to IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2025
- **FlyTrap: Physical Adversarial Attack Towards Camera-based Autonomous Target Tracking System**
  Shaoyuan Xie, Mohamad Fakih, Fayzah Alshammari, Ningfei Wang, Takami Sato, Halima Bouzidi, Mohammad Al Faruque, Qi Alfred Chen
  (Under Review) Pre-print
- **Exploring Backdoor Attacks against Large Language Model-based Decision Making**
  Shaoyuan Xie*, Ruochen Jiao*, Justin Yue, Takami Sato, Lixu Wang, Yixuan Wang, Qi Alfred Chen, Qi Zhu
  (Under Review) Submitted to International Conference on Learning Representations (ICLR), 2025
- **Benchmarking and Improving Bird's Eye View Perception Robustness in Autonomous Driving**
  Shaoyuan Xie, Lingdong Kong, Wenwei Zhang, Jiawei Ren, Liang Pan, Kai Chen, Ziwei Liu
  IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2024
- **Revisiting Physical-World Adversarial Attack on Traffic Sign Recognition: A Commercial Systems Perspective**
  Ningfei Wang, **Shaoyuan Xie**, Takami Sato, Yunpeng Luo, Kaidi Xu, Qi Alfred Chen
  Network and Distributed System Security Symposium (NDSS), 2025
- **Prompter Says: A Linguistic Approach to Understanding and Detecting Jailbreak Attacks Against Large-Language Models**
  Dylan Lee, **Shaoyuan Xie**, Shagoto Rahman, Kenneth Pat, David Lee, Qi Alfred Chen
  ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis (LAMPS), 2024
- **RoboDepth: Robust Out-of-Distribution Depth Estimation under Corruptions**
  Lingdong Kong, **Shaoyuan Xie**, Hanjiang Hu, Lai Xing Ng, Benoit R Cottereau, Wei Tsang Ooi
  Conference on Neural Information Processing Systems (NeurIPS), Datasets and Benchmarks Track, 2023
- **On the Adversarial Robustness of Camera-based 3D Object Detection**
  Shaoyuan Xie, Zichao Li, Zeyu Wang, Cihang Xie
  Transactions on Machine Learning Research (TMLR), 2024

INTERNSHIPS

Shanghai Artificial Intelligence Laboratory — Shanghai, CN
Research Intern, OpenMMLab — Jun 2023 - Aug 2023

- Developed fine-tuning dataset for InternLM to improve the coding ability
- Incorporated external Python executor to the LLM to improve mathematical reasoning ability, iteratively fine-tuned the LLM, which largely enhances the score on the GSM8k dataset

PROFESSIONAL EXPERIENCE

Workshop Organizer - The RoboDrive Challenge — Yokohama, JP
IEEE International Conference on Robotics and Automation (ICRA) — Jan 2024 - May 2024

- Developed competition toolkit for evaluation for all five tracks

Workshop Organizer - The RoboDepth Challenge — London, UK
IEEE International Conference on Robotics and Automation (ICRA) — Jan 2023 - May 2023

SKILLS

- **Programming Languages:** Python, C, Matlab
- **Machine Learning**: Autonomous Driving, BEV Perception, Adversarial Machine Learning, Large Language Models
- **Miscs**: ROS, MMDet, Vim, Tmux, Git, Latex