Shaoyuan Xie

Ph.D. Student, ICS, University of California, Irvine
Tel: (949)368-5560
Email: shaoyux@uci.edu
Homepage: https://daniel-xsy.github.io

Education

University of California, Irvine — Irvine, CA
Ph.D. in Computer Science, Advisor: Professor Qi Alfred Chen — *Expected Jun 2028*

Huazhong University of Science and Technology (HUST) — Wuhan, CN
B.Eng. in Automation, GPA: 3.97 (Top 1st / 212 students) — *Jun 2023*

Internships

Mercedes-Benz Research & Development North America — San Jose, CA
AD Perception | Mentor: Thomas Monninger | Manager: Sihao Ding — *Jun 2025 – Sep 2025*

- Research topic: Leverage VLMs for training better end-to-end autonomous driving system.

Shanghai Artificial Intelligence Laboratory — Shanghai, CN
OpenMMLab | Mentor: Wenwei Zhang | Manager: Kai Chen — *Jun 2023 – Aug 2023*

- Supervised Fine-Tuning (SFT) of InternVL language models.
- Integrated external Python executor to LLM to improve mathematical reasoning capability.

Top-Tier Publications

Summary
2 (1 first-author) in top-tier machine learning conferences (NeurIPS, ICLR)
2 (2 first-author) in top-tier computer vision conferences and journals (TPAMI, ICCV)
3 (1 first-author) in top-tier security conferences (ISOC NDSS)

- **FlyTrap: Physical Distance-Pulling Attack Towards Camera-based Autonomous Target Tracking Systems**
  Shaoyuan Xie, Mohamad Fakih, Junchi Lu, Fayzah Alshammari, Ningfei Wang, Takami Sato, Halima Bouzidi, Mohammad Al Faruque, Qi Alfred Chen
  Network and Distributed System Security Symposium (NDSS), 2026

- **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), 2025

- **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, Qi Alfred Chen, Ziwei Liu, Liang Pan
  International Conference on Computer Vision (ICCV), 2025 (acceptance rate 24% = 2699/11239)

- **Can We Trust Embodied Agents? Exploring Backdoor Attacks against Embodied LLM-Based Decision-Making Systems** (*co-first author)
  Ruochen Jiao*, **Shaoyuan Xie***, Justin Yue, Takami Sato, Lixu Wang, Yixuan Wang, Qi Alfred Chen, Qi Zhu
  International Conference on Learning Representations (ICLR), 2025 (acceptance rate 32.1% = 3689/11500)

- **The Heat is On: Understanding and Mitigating Vulnerabilities of Thermal Image Perception in Autonomous Systems**
  Hrushikesh Varma, **Shaoyuan Xie**, Michael Clifford, Qi Alfred Chen, Takeshi Sugawara, Sara Rampazzi
  Network and Distributed System Security Symposium (NDSS), 2026

- **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 (acceptance rate 15.4% = 211/1369)

- **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), 2023 (acceptance rate 26.1% = 3218/12343)

Other Peer-Reviewed Publications

- **"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
  Proceedings of the 1st ACM Workshop on Large AI Systems and Models with Privacy and Safety Analysis, 2024

- **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

Research Impact

- Email acknowledgements from DJI on autonomous tracking vulnerabilities
- Email acknowledgements from automotive manufacturer on traffic sign recognition vulnerabilities (within Tesla, Toyota, Nissan, Mazda, and Hyundai, hiding for anonymity)

Awards and Honors

- Best Demo, 3rd USENIX Symposium on Vehicle Security and Privacy (2025, *selected for best demo rate 18.2% = 2/11*)
- Honours Bachelor's Degree (2023, *top 1% in univ.*)
- Outstanding Undergraduate Student (2021, *top 1% in univ.*)
- National Scholarship, Ministry of Education of China (2021, *top 0.2% nation-wide*)
- National Scholarship, Ministry of Education of China (2020, *top 0.2% nation-wide*)
- 1st prize in Mathematics Competition of Chinese College Students, Chinese Mathematical Society (2020)
- Provincial Merit Student, Sichuan Provincial Department of Education, (2019, *top 0.4% in high school*)

Academic Services

- *Competition Organizer*: IROS RoboSense (2025), ICRA RoboDrive (2024), ICRA RoboDepth (2023)
- *PC member*: ACM CCS Artifact Evaluation (2024, 2025), NDSS Artifact Evaluation (2025)
- *Reviewer*: CVPR (2023, 2024, 2025), ICCV (2025), TMLR
- *External Reviewer*: USENIX Security (2024, 2025), IEEE S&P (2024), ACM CCS (2024)