YULONG CAO

2371 Leslie Circle ◇ Ann Arbor, MI 48105
(734) · 680 · 4632 ◇ yulongc@umich.edu ◇ kikacaty.github.io

RESEARCH INTERESTS

- Trustworthy machine learning, responsible AI
- Autonomous vehicle: training, testing and simulation

EDUCATION

University of Michigan, Ann Arbor *Sep 2017 - Present*
Advisor: Prof. Morley Mao
Ph.D. in Computer Science & Engineering
University of Michigan, Ann Arbor *May 2017*
B.S. in Computer Science & Engineering
Shanghai Jiao Tong University *August 2017*
B.S. in Electrical and Computer Engineering

WORK EXPERIENCE

NVIDIA, Mentored by Danfei Xu and Chaowei Xiao, Jan 2022 - April 2022
Secure and Safe Prediction for Autonomous Driving Systems *Remote*

· Analyzed vulnerabilities of trajectory prediction in autonomous driving systems and its implications to downstream tasks.
· Built robust trajectory prediction models against adversarial attacks.
· Designed domain specific augmentation for generating realistic and diverse traffic scenarios for improving trajectory prediction model performance.

NIO, Mentored by Yueqiang Cheng May 2021 - August 2021
Adversarial Attacks and Defense on ADAS *Remote*

· Analyzed vulnerabilities of adaptive cruise control and automated lane centering under ADAS.
· Proposed and implemented adversarial attacks that fool the commercial ADAS (openpilot) and demonstrate the attack consequences in the simulator (Carla).
· Proposed defense against patch-based adversarial attacks under the ADAS settings.

Bytedance, Mentored by Yunhan Jia May 2020 - August 2020
AIOps Infrastructure for Enterprise Security *Mountain View, CA*

· Built big data flow based data collection pipeline for AI empowered operation infrastructure.
· Designed a general framework for AI empowered KPI monitoring, anomaly detection and analysis.
· Released a service for anomaly detection and analysis on network traffic between data centers incorporating several supervised and unsupervised machine learning algorithms.

PUBLICATIONS (* INDICATES EQUAL CONTRIBUTION)

1. **Yulong Cao**, Danfei Xu, Xinshuo Weng, Zhuoqing Mao, Anima Anandkumar, Chaowei Xiao, Marco Pavone, Robust Trajectory Prediction against Adversarial Attacks, To appear on the 6th Conference on Robot Learning (*CoRL'22*) (**Oral**), in Auckland, New Zealand, Dec. 2022.

2. **Yulong Cao**, Sri Hrushikesh, Pirouz Naghavi, Takeshi Sugawara, Z. Morley Mao, Sara Rampazzi, You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks, To appear on the 32nd USENIX Security Symposium (*Security'*23), in Anaheim, USA, Aug. 2023.

3. **Yulong Cao**, Chaowei Xiao, Anima Anandkumar, Danfei Xu, and Marco Pavone, AdvDO: Realistic Adversarial Attacks for Trajectory Prediction, To appear as a poster on European Conference on Computer Vision (*ECCV'*22), Tel-Aviv, Oct. 2022.

4. **Yulong Cao***, Ningfei Wang*, Chaowei Xiao*, Dawei Yang*, Jin Fang, Ruigang Yang, Qi Alfred Chen, Mingyan Liu, and Bo Li, Security of Multi-Sensor Fusion based Perception in Autonomous Driving Under Physical-World Attacks, Proceedings of the 42nd IEEE Symposium on Security and Privacy (*Oakland'*21), Online, May. 2021.

5. **Yulong Cao**, Yanan Guo, Takami Sato, Qi Alfred Chen, Z. Morley Mao, and Yueqiang Cheng, Remote Adversarial Attack on Automated Lane Centering, Posters and talks at the 3rd Workshop on Automotive & Autonomous Vehicle Security (*AutoSec'*22), Online, April, 2022

6. **Yulong Cao**, Jiachen Sun, Chaowei Xiao, Qi Alfred Chen, and Z. Morley Mao, Delving into the Remote Adversarial Patch in Semantic Segmentation, Posters at ICML 2021 Workshop on Socially Responsible Machine Learning. July. 2021.

7. **Yulong Cao**, Jiaxiang Ma, Kevin Fu, Sara Rampazzi, and Z. Morley Mao, Automated Tracking System for LiDAR Spoofing Attacks on Moving Targets, Posters and talks at the 3rd Workshop on Automotive & Autonomous Vehicle Security (*AutoSec'*21) **(Best Demo Award Runner-up)**, Online, Feb, 2021

8. **Yulong Cao**, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Park Won, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao, Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving, Proceedings of the 26th ACM Conference on Computer and Communications Security (*CCS'*19), London, UK, November 2019.

9. R. Spencer Hallyburton, Yupei Liu, **Yulong Cao**, Z Morley Mao, and Miroslav Pajic, Security Analysis of Camera-LiDAR Fusion Against Black-Box Attacks on Autonomous Vehicles, Proceedings of the 31th USENIX Security Symposium (*Security'*22), Boston, USA, Aug. 2022.

10. Jiachen Sun, **Yulong Cao**, Christopher Choy, Zhiding Yu, Anima Anandkumar, Z. Morley Mao, and Chaowei Xiao, Adversarially Robust 3D Point Cloud Recognition Using Self-Supervisions, Proceedings of the 35th Conference on Neural Information Processing Systems (*Neurips'*21), Online, Dec. 2021.

11. Jiachen Sun, Karl Koenig, **Yulong Cao**, Qi Alfred Chen, and Z. Morley Mao, On The Adversarial Robustness of 3D Point Cloud Classification, Proceedings of the 32nd British Machine Vision Conference (*BMVC'*21), Online, Nov. 2021.

12. Yanan Guo, Christopher Joseph, Takami Sato, **Yulong Cao**, Qi Alfred Chen, Yueqiang Cheng, An Adversarial Attack on DNN-based Adaptive Cruise Control Systems, Posters at ICCV 2021 Workshop on Adversarial Robustness In the Real World. Oct 11, 2021.

13. Jiachen Sun, **Yulong Cao**, Christopher Choy, Zhiding Yu, Chaowei Xiao, Anima Anandkumar, and Z. Morley Mao, Improving Adversarial Robustness in 3D Point Cloud Classification via Self-Supervisions, Posters at ICML 2021 Workshop on Socially Responsible Machine Learning. July. 2021.

14. Jiachen Sun, **Yulong Cao**, Qi Alfred Chen, Z. Morley Mao, Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures, Proceedings of the 29th USENIX Security Symposium (*Security'*20), Boston, USA, Aug. 2020.

15. David Ke Hong, John Kloosterman, Yuqi Jin, **Yulong Cao**, Qi Alfred Chen, Scott Mahlke, Z. Morley Mao, AVGuardian: Detecting and Mitigating Publish-Subscribe Overprivilege for Autonomous Vehicle Systems, Proceedings of the 5th IEEE European Symposium on Security and Privacy (*EuroS&P'*20), Genova, Italy, June 2020.

16. **Yulong Cao***, Chaowei Xiao*, Dawei Yang*, Jing Fang, Ruigang Yang, Mingyan Liu, Bo Li, Adversarial Objects Against LiDAR-Based Autonomous Driving Systems, Posters and talks at CVPR AMLCV workshop 2019 **(Contributed Talk)**, Long Beach, United States, June 2019.

17. **Yulong Cao**, Qi Alfred Chen, and Z. Morley Mao, Adversarial Machine Learning on LiDAR-based Object Detection in Autonomous Driving: A First Study, Poster and Talks at the 27th USENIX Security Symposium (*USENIX Security'*18), Baltimore, United States, August 2018.

18. Qi Alfred Chen, Eric Osterweil, Matthew Thomas, **Yulong Cao**, Jie Jimmy You, and Z. Morley Mao, Client-side Name Collision Vulnerability in the New gTLD Era: A Systematic Study, Proceedings of the 24th ACM Conference on Computer and Communications Security(*CCS'*17), Dallas, United States, October 2017.

HONORS

- **Best Demo Award Runner-up**: Automated Tracking System for LiDAR Spoofing Attacks on Moving Targets, **Yulong Cao**, Jiaxiang Ma, Kevin Fu, Sara Rampazzi, and Z. Morley Mao, Posters and talks at the 3rd Workshop on Automotive & Autonomous Vehicle Security (*AutoSec*), 2021
- RSC Security Scholar 2020
- Student travel grant (CCS'19, USENIX'20)
- Rackham travel grant (2017, 2018, 2019, 2020)
- University of Michigan Dean's List (2015, 2016).
- 2014 Mathematical Contest in Modeling (MCM), Honorable mention (top 25% worldwide).
- 2014 Shanghai Jiaotong University Scholarship (top 10%) Award (2013,2014).
- UM-SJTU Joint Institute Dean's List (2013, 2014).

ACADEMIC SERVICES

Program Committee

- AAAI'23
- NeurIPS'22
- CVPR'22
- ECCV'22
- ICML'22
- ICCV'21
- ICRA'22
- AdvMLCV'[19,20,21,22] (co-located with CVPR)
- ARRW'[20,21,22] (co-located with ECCV)
- RSEML'21 (co-located with AAAI)
- SSMLS'21,22 (co-located with ICLR)

- SPML'[19,20,21,22] (co-located with ICML)