Jiachen Sun

BBB 4917, 2260 Hayward St, Ann Arbor, MI 48109
jiachens@umich.edu • +1 (734) 604-1709 • https://web.eecs.umich.edu/∼jiachens/

EDUCATION

University of Michigan, Ann Arbor, MI, United States — Sep 2018 – Present
- Ph.D. Candidate in Computer Science & Engineering
- Advisor: Prof. Z. Morley Mao, IEEE Fellow
- Research Interests: Adversarial ML, Cyber-Physical Security, Networked Systems

Shanghai Jiao Tong University, Shanghai, P.R.China — Sep 2014 – Jun 2018
- B.S.E. in Information Engineering (graduated with honor, **top 5%**)
- Advisor: Prof. Xiaohua Tian
- Research Area: Mobile Computing

University of Washington, Seattle, WA, United States — Jun 2016 – Aug 2016
- Intensive Program in Electrical & Computer Engineering

WORKING EXPERIENCE

Research Assistant in RobustNet Lab, University of Michigan, Ann Arbor — Sep 2018 – Present
- Advisor: Prof. Z. Morley Mao, IEEE Fellow
- Project: Adversarial Machine Learning & Networked System

Research Intern in AI Integrity Team, Meta/Facebook AI — May 2022 – Aug 2022
- Advisor: Dr. Caner Hazirbas and Dr. Ivan Evtimov
- Project: Adversarial Machine Learning

Graduate Computing Student Intern in Lawrence Livermore National Lab — May 2021 – Aug 2021
- Advisor: Dr. Bhavya Kailkhura and Dr. Pin-Yu Chen
- Project: Certified Adversarial Robustness in ML

Algorithm Engineer Intern in AI Lab, DiDi Technology Co. — Sep 2017 – Jan 2018
- Advisor: Dr. Yashu Liu and Prof. Jieping Ye, IEEE Fellow
- Project: Applied Machine Learning

Research Intern in SyNRG Lab, University of Illinois at Urbana-Champaign — Jun 2017 – Sep 2017
- Advisor: Prof. Haitham Hassanieh
- Project: Wireless Sensing & Cyber-physical Security

Research Assistant in IIoT Lab, Shanghai Jiao Tong University — Sep 2016 – Jun 2017
- Advisor: Prof. Xiaohua Tian
- Project: Indoor Localization & Mobile Computing

PUBLICATIONS

Main Publications:

[1] **Benchmarking Robustness of 3D Point Cloud Recognition against Common Corruptions**
Jiachen Sun, Q. Zhang, B. Kailkhura, Z. Yu, C. Xiao, and Z. Mao.
In Submission to *ICML*. 2022.

[2] **A Spectral View of Randomized Smoothing under Common Corruptions: Benchmarking and Improving Certified Robustness**
Jiachen Sun, A. Mehra, B. Kailkhura, P. Chen, D. Hendrycks, J. Hamm, and Z. Mao.
In Submission to *IEEE/CVF ECCV*. 2022.

[3] **Adversarially Robust 3D Point Cloud Recognition Using Self-Supervisions**
Jiachen Sun, Y. Cao, C. Choy, Z. Yu, A. Anandkumar, Z. Mao, and C. Xiao
In Proceedings of *NeurIPS*. 2021. (Acceptance Rate: 2371 / 9122 = 26.0%)

[4] **On Adversarial Robustness of 3D Point Cloud Classification under Adaptive Attacks**
Jiachen Sun, K. Koenig, Y. Cao, Q. Chen, and Z. Mao.
In Proceedings of *BMVC*. 2021. (Acceptance Rate: 437 / 1206 = 36.0%)

[5] **Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures**
Jiachen Sun, Y. Cao, Q. Chen, and Z. Mao.
In Proceedings of *USENIX Security*. 2020. (Acceptance Rate: 63 / 473 = 13.3%, Winter Cycle)

[6] **Harbor: Hybrid Architecture for Collaborative Vehicular Sensing**
X. Zhu†, R. Zhu†, Jiachen Sun, X. Zhang, A. Zhang, Y. Guo, F. Qian, and Z. Mao.
† denotes equal contribution.
In Submission to *USENIX NSDI*. 2022.

[7] **Delving into the Remote Adversarial Patch in Semantic Segmentation**
Y. Cao, Jiachen Sun, C. Xiao, Q. Chen, and Z. Mao.
In Submission to *IEEE/CVF ECCV*. 2022.

[8] **On Adversarial Robustness of Trajectory Prediction for Autonomous Vehicles**
Q. Zhang, S. Hu, Jiachen Sun, Q. Chen, and Z. Mao.
In Proceedings of *IEEE/CVF CVPR*. 2022. (Acceptance Rate: 2067 / 8161 = 25.3%)

[9] **EMP: Edge-assisted Multi-vehicle Perception**
X. Zhang, A. Zhang, Jiachen Sun, X. Zhu, Y. Guo, Q. Feng, and Z. Mao.
In Proceedings of *ACM MobiCom*. 2021. (Acceptance Rate: 60 / 299 = 20.0%)

[10] **Automatic Discovery of Denial-of-Service Vulnerabilities in Connected Vehicle Network Stack**
S. Hu, Q. Chen, Jiachen Sun, Y. Feng, Z. Mao, and H. Liu.
In Proceedings of *USENIX Security*. 2021. (Acceptance Rate: 246 / 1295 = 19.0%)

[11] **MPBond: Efficient Network-level Collaboration Among Personal Mobile Devices**
X. Zhu, Jiachen Sun, X. Zhang, Y. Guo, F. Qian, and Z. Mao.
In Proceedings of *ACM MobiSys*. 2020. (Acceptance Rate: 34 / 175 = 19.4%)

[12] **Detecting Anomaly in Large-Scale Network Using Mobile Crowdsourcing**
Y. Li, Jiachen Sun, W. Huang, and X. Tian.
In Proceedings of *IEEE INFOCOM*. 2019. (Acceptance Rate: 288 / 1464 = 19.7%)

[13] **Ghostbuster: Detecting the Presence of Hidden Eavesdroppers**
A. Chaman, J. Wang, Jiachen Sun, H. Hassanieh, and R. Choudhury.
In Proceedings of *ACM MobiCom*. 2018. (Acceptance Rate: 42 / 187 = 22.4%)

Workshop & Demo Publications:

[1] **Towards Robust LiDAR-based Perception in Autonomous Driving**
Jiachen Sun, Y. Cao, Q. Chen, and Z. Mao.
In AdvMLCV Workshop of *CVPR*. 2020. (**Contributed Talk**)

[2] **Improving Adversarial Robustness in 3D Point Cloud Classification via Self-Supervisions**
Jiachen Sun, Y. Cao, C. Choy, Z. Yu, C. Xiao, A. Anandkumar, and Z. Mao.
In SRML Workshop of *ICML*. 2021.

[3] **Replacing the Kariba Dam**
Y. Zhang†, Jiachen Sun†, Y. Yao†. † denotes equal contribution.
UMAP Journal of Undergraduate Mathematics and Its Applications. 2017. (MCM contest paper)

PROJECT EXPERIENCE **Risky Driver Inference Using Statistical Machine Learning** Oct 2017 – Feb 2018

- This project explores the feasibility to detect and infer risky drivers in a sparse data warehouse. We leverage casual inference and XGBoost algorithms to achieve a satisfactory recall.

Indoor Positioning System Based on Crowdsourcing Sep 2016 – Jun 2017

- This project presents an BLE-based indoor localization system. We design a SLAM algorithm by leveraging crowdsourcing. We also improve the RSSI propagation model by extended Kalman filter.

SELECTED HONORS & AWARDS

ACM MobiCom Travel Grant (Virtual)	2020
USENIX Student Grant	2020, 2021
CVPR Workshop on AdvMLCV DeepMind Grant (top 30%)	2020
ACM HotMobile Student Travel Grant	2019
Outstanding Research Scholarship of SJTU (top 1%)	2017 – 2018
Outstanding Winner & INFORMS Award in Mathematical Contest in Modeling (**top 0.1% worldwide**)	2017
Academic Excellence Scholarship of SJTU, A Class (top 1%)	2016 – 2017
Honor Scholarship of Zhiyuan College (top 5%)	2014 – 2015, 2015 – 2016
Academic Excellence Scholarship of SJTU, C Class (top 15%)	2014 – 2015, 2015 – 2016
Champion of Men's 4×100 Meters Relay of SJTU	2015, 2016

COMPUTER SKILLS

Language: Python, Java, C/C++
Tools: PyTorch, TensorFlow, Android Studio, MATLAB, Git, LaTeX

PROFESSIONAL SERVICES

ICML 2022 Reviewer
IEEE CVPR 2022 Reviewer
IEEE IoT Journal 2021 Reviewer
ICML SRML 2021 Technical Program Committee
IEEE ICCV AROW 2021 Technical Program Committee
ACM SIGCOMM 2021 Artifact Evaluation Committee
CVPR AMLCV 2021 Reviewer
IEEE ICCV 2021 Reviewer
ICLR SecML Workshop 2021 Technical Program Committee
IEEE S&P 2021 Shadow Technical Program Committee
ECCV AROW 2020 Technical Program Committee
IET Intelligent Transport Systems Reviewer
ACM EuroSys 2021 Shadow Technical Program Committee
Mentorship for Undergraduates at USENIX Security 2020

REFERENCES

Available upon Request

Updated on Aug 2021