Jinghuai Zhang

427 Wilkinson Building, 534 Research Dr, Durham, NC 27705
✉ jinghuai.zhang@duke.edu • https://jzhang538.github.io/jinghuaizhang/ • ☎ 984-259-7626

Research Interests

AI Security and Privacy, Autonomous Driving and Self-supervised Learning.

Education

2021-2023 (expected) **Duke University** – Durham, NC
M.S., Computer Science (GPA: 4.0/4.0 (top 1%))
Advisor: Prof. Neil Zhenqiang Gong

2016-2020 **City University of Hong Kong** – Hong Kong, China
B.S., Computer Science (CGPA: 3.93/4.3 (top 5%), Major GPA:4.09/4.3)
Advisor: Prof. Jianping Wang

Honors and Scholarships

2018-2020 HKSAR Government Scholarship Fund Academic Award with 160,000 HKD Scholarship

2018-2020 Hong Kong, China-Asia-Pacific Economic Cooperation Scholarship

2020 Hong Kong Computer Society Student Sponsorship

2020 Department of Computer Science Outstanding Student Scholarship

2020 The first class honor graduate from City University of Hong Kong

2017-2020 Dean's List of City University of Hong Kong

2015 Second Prize in Provincial Mathematical competition (Zhejiang, China)

Publications

1. Yicheng Liu*, **Jinghuai Zhang***, Liangji Fang, Qinhong Jiang, and Bolei Zhou. "Multimodal Motion Prediction with Stacked Transformer". In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2021. (*co-first authors with equal contributions)
2. Yifan Zhang*, **Jinghuai Zhang***, Jindi Zhang, Jianping Wang, Kejie Lu and Jeff Hong. "A novel learning framework for sampling-based motion planning in autonomous driving". In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI-Oral)*, 2020. (*co-first authors with equal contributions)
3. Zixuan Huang*, **Jinghuai Zhang***, Jing Liao. "Style Mixer: Semantic-aware Multi-Style Transfer Network". In *Pacific Graphics & Computer Graphics Forum*, 2019. (*co-first authors with equal contributions)
4. Yifan Zhang, **Jinghuai Zhang**, Jindi Zhang, Jianping Wang, Kejie Lu and Jeff Hong. "Integrating Algorithmic Sampling-Based Motion Planning with Learning in Autonomous Driving". In *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2022.

Projects

2022 Data Poisoning Based Backdoor Attack to Contrastive Learning. (First author, under review)

2022 Backdoor Attack to Scene Understanding in 3D Vision. (First author, under review)

2022 Empirical Defense against Backdoor Attack in Self-supervised Learning Settings. (under review)

2022 Certified Robustness Guarantees for Point Cloud Models. (First author, under review)

2020 Motion Planning in Autonomous Driving. (HK government research proposal writing experience under Prof.Jianping Wang)

Skills and Qualifications

Standard Exam: GRE: 334 (verbal: 164 quantitative: 170).

Programming languages: Python, C++, Matlab, Java, HTML, SQL.

Teaching Experience

Teaching Assistant, Duke University

Fall 2022 COMPSCI 230 – Discrete Mathematics for Computer Science

Spring 2022 COMPSCI 230 – Discrete Mathematics for Computer Science

Industry Experience

07/2020-04/2021 **Autonomous Driving Group of Sensetime Research**
Intern, Mentor: Liangji Fang
Collect a large-scale motion forecasting dataset (containing 1-2 million cases) with fine-grained intention annotations. Predict intentions and trajectories of vehicles and VRUs with the collected dataset.