Hanjiang Hu

hanjianh@cs.cmu.edu • HanjiangHu • HanjiangHu • cs.cmu.edu/∼hanjianh

EDUCATION

Carnegie Mellon University — **Pittsburgh, USA**
Ph.D. in Electrical and Computer Engineering (ECE) — *2023 - 2026 (expected)*
M.S. in Machine Learning, School of Computer Science — *2023 - present*
Ph.D. in Mechanical Engineering (transferred to ECE) — *2021 - 2022*

Shanghai Jiao Tong University — **Shanghai, China**
M.S. in Control Science and Engineering — *2018 - 2021*
B.Eng. in Mechanical Engineering (Tsien Hsue-shen Honor Program) — *2014 - 2018*

RESEARCH STATEMENT

My research focuses on **safety** and **robustness** at the intersection of robotics, control theory, and machine learning, from provable theories with guarantees to real-world applications in autonomous systems and robotics. Specifically,

- I am working on the provably guaranteed **safety** and formal verification of learning-based dynamical systems for decision-making in robotics, scientific ML and generative AI.
- I am also interested in the adversarial and out-of-distribution **robustness** caused by semantic transformation in the real-world robotics and autonomous driving applications.

AWARDS

- CMU Graduate Student Assembly / Provost Conference Grant for L4DC 2025
- Travel Grants from Princeton ORFE for 2024 Workshop on Optimization, Learning, and Control
- Carnegie Institute of Technology Dean's Fellowship
- Graduate fellowship for MSML from CMU Machine Learning Department
- National Science Foundation Student Travel Grants for CVPR 2022
- SciComm Coverage [link] for SeasonDepth Prediction Challenge at ICRA 2022 by SciComm Winner
- CMU Graduate Student Assembly Travel Grants for ICRA 2022
- Excellent Master Thesis, Shanghai Jiao Tong University, 2021, Top 1%
- Huawei Scholarship, 2019, Top 2.5%
- Outstanding Graduate of SJTU with Tsien Hsue-shen Honor Program, 2018, 4/124
- Second Prize of Excellent Graduation Design of SJTU, 2018, Top 3.5%
- Eleme (Alibaba) Scholarship, 2017, Top 2%

PUBLICATIONS & PRE-PRINTS *** indicates equal contribution, full list can be found [here]**

- **Hu, Hanjiang**, A. Robey, and C. Liu, "Steering dialogue dynamics for robustness against multi-turn jailbreaking attacks," *preprint, under-review*, 2025,[PDF],[code].
- **Hu, Hanjiang** and C. Liu, "On the boundary feasibility for pde control with neural operators," in *The 7th Annual Learning for Dynamics & Control Conference (L4DC)*, PMLR, 2025 [PDF].
- T. Wei, **Hanjiang Hu***, L. Marzari*, K. S. Yun*, P. Niu*, X. Luo, and C. Liu, "Modelverification.jl: a comprehensive toolbox for formally verifying deep neural networks," *International Conference on Computer Aided Verification (CAV)*, 2025, [PDF], [code], [doc].
- H. Cheng*, **Hu, Hanjiang***, and C. Liu, "Robust tracking control with neural network dynamic models under input perturbations," *arXiv preprint*, 2024 [PDF].
- Y. Yang, **Hu, Hanjiang**, T. Wei, S. E. Li, and C. Liu, "Scalable synthesis of formally verified neural value function for hamilton-jacobi reachability analysis," *arXiv preprint*, 2024,[PDF].

- **Hu, Hanjiang**, Y. Yang, T. Wei, and C. Liu, "Verification of neural control barrier functions with symbolic derivative bounds propagation," in *Conference on Robot Learning (CoRL)*, PMLR, 2024, [PDF],[code].

- **Hu, Hanjiang**, J. Lan, and C. Liu, "Real-time safe control of neural network dynamic models with sound approximation," in *The 6th Annual Learning for Dynamics & Control Conference (L4DC)*, PMLR, 2024 [PDF], [code].

- Y. Li, L. Kong, **Hu, Hanjiang**, X. Xu, and X. Huang, "Is your lidar placement optimized for 3d scene understanding?," *Thirty-eighth Conference on Neural Information Processing Systems (NeurIPS),* ***Spotlight (2.5% = 388/15671)***, 2024, [PDF],[code].

- L. Kong, S. Xie, **Hu, Hanjiang**, Y. Niu, W. T. Ooi, B. R. Cottereau, L. X. Ng, Y. Ma, W. Zhang, L. Pan, *et al.*, "The robodrive challenge: Drive anytime anywhere in any condition," *arXiv preprint*, 2024, [PDF].

- **Hu, Hanjiang**, Z. Liu, L. Li, J. Zhu, and D. Zhao, "Pixel-wise smoothing for certified robustness against camera motion perturbations," in *The 27th International Conference on Artificial Intelligence and Statistics (AISTATS)*, PMLR, 2024, [PDF], [code].

- Y. Li*, **Hu, Hanjiang***, Z. Liu, X. Xu, D. Zhao, and X. Huang, "Influence of camera-lidar configuration on 3d object detection for autonomous driving," *2024 IEEE International Conference on Robotics and Automation (ICRA)*, 2024, [PDF], [code].

- Z. Liu, Z. Guo, H. Lin, Y. Yao, J. Zhu, Z. Cen, **Hu, Hanjiang**, W. Yu, T. Zhang, J. Tan, *et al.*, "Datasets and benchmarks for offline safe reinforcement learning," *Data-centric Machine Learning Research, PMLR*, 2024, [PDF].

- L. Kong, S. Xie, **Hu, Hanjiang**, L. X. Ng, B. R. Cottereau, and W. T. Ooi, "Robodepth: Robust out-of-distribution depth estimation under corruptions," in *Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS)*, 2023, [PDF].

- L. Kong, Y. Niu, S. Xie, **Hu, Hanjiang**, L. X. Ng, B. R. Cottereau, L. Zhang, H. Wang, W. T. Ooi, R. Zhu, *et al.*, "The robodepth challenge: Methods and advancements towards robust depth estimation," *arXiv preprint*, 2023, [PDF].

- **Hu, Hanjiang**, C. Liu, and D. Zhao, "Robustness verification for perception models against camera motion perturbations," in *2023 International Conference on Machine Learning (ICML) 2nd Workshop on Formal Verification of Machine Learning*, PMLR, 2023, [PDF].

- Z. Liu, Z. Guo, Z. Cen, H. Zhang, Y. Yao, **Hu, Hanjiang**, and D. Zhao, "Towards robust and safe reinforcement learning with benign off-policy data," in *International Conference on Machine Learning (ICML)*, PMLR, 2023, [PDF].

- **Hu, Hanjiang**, Z. Liu, L. Li, J. Zhu, and D. Zhao, "Robustness certification of visual perception models via camera motion smoothing," in *Conference on Robot Learning (CoRL)*, PMLR, 2022, [PDF], [code].

- **Hu, Hanjiang***, Z. Liu*, S. Chitlangia, A. Agnihotri, and D. Zhao, "Investigating the impact of multi-lidar placement on object detection for autonomous driving," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2022, [PDF], [code].

- **Hu, Hanjiang***, B. Yang*, Z. Qiao*, S. Liu, D. Zhao, and H. Wang, "Seasondepth: Cross-season monocular depth prediction dataset and benchmark under multiple environments," *2022 International Conference on Machine Learning (ICML) Safe Learning for Autonomous Driving Workshop, 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, [PDF], [benchmark].

- C. Xu, W. Ding, W. Lyu, Z. Liu, S. Wang, Y. He, **Hu, Hanjiang**, D. Zhao, and B. Li, "Safebench: A benchmarking platform for safety evaluation of autonomous vehicles," *Conference on Neural Information Processing Systems (NeurIPS) 2022*, 2022, [PDF], [benchmark].

- **Hu, Hanjiang**, Z. Liu, W. Chen, and H. Wang, "Domain-invariant similarity activation map contrastive learning for retrieval-based long-term visual localization," *IEEE/CAA Journal of Automatica Sinica (JAS)*, vol. 9, no. 2, pp. 313–328, 2021, [PDF], [code].

- Z. Qiao*, **Hu, Hanjiang***, W. Shi, S. Chen, Z. Liu, and H. Wang, "A registration-aided domain adaptation network for 3d point cloud based place recognition," in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 1317–1322, IEEE, 2021, [PDF], [code].

- **Hu, Hanjiang**, Z. Qiao, M. Cheng, Z. Liu, and H. Wang, "Dasgil: Domain adaptation for semantic and geometric-aware image-based localization," *IEEE Transactions on Image Processing (T-IP)*, vol. 30, pp. 1342–1353, 2020, [PDF], [code].

- **Hu, Hanjiang**, Z. Liu, C. Yang, W. Chen, L. Xie, and H. Wang, "Retrieval-based localization based on domain-invariant feature learning under changing environments," in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 3684–3689, IEEE, 2019, [PDF], [code].

- H. Gu*, **Hu, Hanjiang***, H. Wang, and W. Chen, "Soft manipulator fault detection and identification using anc-based lstm," in *2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pp. 1702–1707, IEEE, 2021, [PDF], [code].

- J. Zhao*, **Hu, Hanjiang***, K. Zhu, H. Wang, and X. Yu, "Distributed rendezvous control of networked uncertain robotic systems with bearing measurements," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 8829–8835, IEEE, 2021.

- J. Zhao, K. Zhu, **Hu, Hanjiang**, X. Yu, X. Li, and H. Wang, "Formation control of networked mobile robots with unknown reference orientation," *IEEE/ASME Transactions on Mechatronics*, 2023.

- Z. Liu, H. Wei, **Hu, Hanjiang**, C. Suo, H. Wang, H. Li, and Y.-H. Liu, "A synchronization approach for achieving cooperative adaptive cruise control based non-stop intersection passing," in *2020 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 236–242, IEEE, 2020.

SELECTED EXPERIENCE

Intelligent Control Lab — **Carnegie Mellon University**
Research Assistant — *Feb. 2023 - Present*

Propose a formal verification framework for the perception model against camera motion perturbations, which is compatible with current incomplete and complete formal neural network verification (VNN) methods.
Work on the formal verification of neural network dynamic models and safe control with verified neural control barrier functions, for various safety-critical problems in robotics and GenAI.

Bosch Center for Artificial Intelligence (BCAI) — **Robert Bosch LLC**
Machine Learning Research Intern — *May 2023 - Aug. 2023*

Work on empirical robustness of vision models against the patch attack, under the DARPA Guaranteeing AI Robustness Against Deception (GARD) program. Propose a model-agnostic defense method to detect the out-of-distribution adversarial patches based on Gaussian Mixture Models.

Safe AI Lab — **Carnegie Mellon University**
Research Assistant — *Aug. 2021 - May 2023*

Work on robust perception with heterogeneous sensing for autonomous driving and robotics.
Investigate the robustness of 3D object detection against the different multi-LiDAR placement.

Mechanical Systems Control Lab — **University of California, Berkeley**
Visiting Student Researcher — *May 2020 - Feb. 2021*

Work on high-quality vehicle detection as ground truth to support the INTERPRET Challenge on NeurIPS 2020

Intelligent Robotics and Machine Vision Lab — **Shanghai Jiao Tong University**
Research Assistant — *Sept. 2017 - May 2021*

Work on SLAM for the delivery robot and outdoor long-term visual localization and perception.

Propose a line of empirical work on robust visual place recognition across different environments. Build the SeasonDepth dataset and benchmark for robust monocular depth prediction and host competition at ICRA.

Robot Machine Vision Group **ASAGE ROBOTS Co. Ltd.**

Robot Algorithm Intern *Sept. 2017 - Jun. 2018*

Work on object detection, segmentation and pose estimation for an intelligent robot grasping system with an eye-in-hand RGBD camera. Won the Third Prize in the 2018 International Conference on Optics and Photonics (ICOPEN) 3-D Sensor Application Design Competition

Automated system group **SAIC Motor Co., Ltd.**

Control Algorithm Intern *May 2017 - Aug. 2017*

Design LQR-based steeling control algorithm for Roewe and Morris Garages (MG) model vehicles. Won the first prize of the 1st SAIC Automotive Software Challenge

ACADEMIC SERVICES

- **Program Committee**: PC member (reviewer) of Workshop on Formal Verification and Machine Learning (WFVML) 2023-2024 and The VerifAI Workshop: AI Verification in the Wild at ICLR 2025, Organizer of the RoboDrive Challenge at ICRA 2024, Organizer of the RoboDepth Challenge at ICRA 2023, lead organizer of SeasonDepth Prediction Challenge at ICRA 2022 and IROS 2022, lead organizer of Workshop on Trustworthy Autonomy and Robotics at ICRA 2022
- **Conference Reviewer**: NeurIPS 2023-2024, ICML 2025, ICLR 2024-2025, CoRL 2024, L4DC 2024, CVPR 2023-2025, ECCV 2024, ICCV 2023-2024, ICRA 2021-2025, IROS 2021-2025, AAAI 2024-2025, ACCV 2024, NeurIPS D&B Track 2021-2024,
- **Journal Reviewer**: JMLR, IEEE T-PAMI, DMLR, RA-L, IEEE T-IP, IEEE T-FR (JFR), IEEE TASE, IEEE/CAA JAS, IJHR

PROFESSIONAL ACTIVITIES

- Invited talk entitled "Real-Time Safe Control of Neural Network Dynamic Models with Sound Approximation" at CMU Learning and Control Seminar, Mar. 2024 , [slides]
- Invited talk entitled "Towards Trustworthy Robotics: Robustness, Safety and Verification" at Shanghai Jiao Tong University, Apr. 2024, [slides]

SKILLS

- **Programming**: Julia, Python, C/C++, MATLAB, Javascript
- **Technologies**: Pytorch, ROS, CARLA, Webots, SolidWorks
- **Languages**: Mandarin (native), English (fluent), Japanese (basic)