YIHANG TAO

83 Tat Chee Avenue, Kowloon, Hong Kong
(+852) 92856274 | yihang.tommy@my.cityu.edu.hk | yihangtao.github.io

EDUCATION

City University of Hong Kong — Hong Kong SAR
PhD, Department of Computer Science — Sep. 2024 - Now
Supervisor: Prof. Yuguang "Michael" Fang
JC STEM Lab of Smart City, WINET Laboratory

Shanghai Jiao Tong University — Shanghai, China
Master, School of Computer Science — Sep. 2021 - Apr. 2024
Outstanding Graduate (2024)

Southeast University — Nanjing, China
Bachelor, School of Information Engineering — Sep. 2017 - Jul. 2021
GPA: 3.89/4.0

Research Interests

Autonomous Driving, Spatial Intelligence, Generative Model, AI Security.

PUBLICATIONS

First Author (* Equal contribution)

[Under Review] **Y. Tao***, Y. Guo*, S. Hu, Y. Ma, Z. Fang, S. Kwong, and Y. Fang. "Learning to Generate Driving Scene Across Agents," *Under Review.*

[CVPR'26] **Y. Tao**, S. Hu, H. An, Z. Fang, H. Cao, and Y. Fang. "Learning Mutual View Information Graph for Adaptive Adversarial Collaborative Perception," *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2026. [CCF-A]

[ICRA'25] **Y. Tao**, S. Hu, Z. Fang, and Y. Fang. "Directed-CP: Directed Collaborative Perception for Connected and Autonomous Vehicles via Proactive Attention," *IEEE International Conference on Robotics and Automation (ICRA)*, Atlanta, USA, 2025. [CCF-B]

[AAAI'25] S. Hu*, **Y. Tao***, G. Xu, Y. Deng, X. Chen, Y. Fang, and S. Kwong. "CP-Guard: Malicious Agent Detection and Defense in Collaborative Bird's Eye View Perception," *The 39th Annual AAAI Conference on Artificial Intelligence (AAAI)*, Philadelphia, USA, 2025. **(Oral Presentation, <5%)** [CCF-A]

[TDSC, Major Revision] **Y. Tao***, S. Hu*, Y. Hu, H. An, H. Cao, and Y. Fang. "GCP: Guarded Collaborative Perception with Spatial-Temporal Aware Malicious Agent Detection," *IEEE Transactions on Dependable and Secure Computing (TDSC), Major Revision.* [CCF-A]

[TGCN] **Y. Tao**, J. Wu, Q. Pan, A. K. Bashir, and M. Omar. "O-RAN-Based Digital Twin Function Virtualization for Sustainable IoV Service Response: An Asynchronous Hierarchical Reinforcement Learning Approach," *IEEE Transactions on Green Communications and Networking (TGCN)*, vol. 8, no. 3, pp. 1049-1060, Sep. 2024.

[GLOBECOM'23] **Y. Tao**, J. Wu, X. Lin, S. Mumtaz, and S. Cherkaoui. "Digital Twin and DRL-Driven Semantic Dissemination for 6G Autonomous Driving Service," *IEEE Global Communications Conference (GLOBECOM)*, Kuala Lumpur, Malaysia, Dec. 2023, pp. 2075-2080. [CCF-C]

[LNET] **Y. Tao**, J. Wu, X. Lin, and W. Yang. "DRL-Driven Digital Twin Function Virtualization for Adaptive Service Response in 6G Networks," *IEEE Networking Letters (LNET)*, vol. 5, no. 2, pp. 125-129, Jun. 2023.

Collaborative Author

[CVPR'26] H. An, Y. Xiaohui, G. Hua, **Y. Tao**, H. Cao, X. Yu, and Y. Fang. "RecoverMark: Robust Watermarking for Localization and Recovery of Manipulated Faces," *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2026. [CCF-A]

[TDSC] H. An, G. Hua, W. Du, H. Cao, **Y. Tao**, G. Xu, S. Rahardja, and Y. Fang. "Decoder Gradient Shields: A Family of Provable and High-Fidelity Methods Against Gradient-Based Box-Free Watermark Removal," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2026. [CCF-A]

[TMC] S. Hu, **Y. Tao**, G. Xu, X. Qian, Y. Deng, X. Chen, S. Kwong, and Y. Fang. "CP-uniGuard: A Unified, Probability-Agnostic, and Adaptive Framework for Malicious Agent Detection and Defense in Multi-Agent Embodied Perception Systems," *IEEE Transactions on Mobile Computing (TMC)*, 2025. [CCF-A]

[NeurIPS'25] Y. Guo, S. He, Y. Lu, H. An, **Y. Tao**, H. Zhu, J. Liu, and Y. Fang. "Neptune-X: Active X-to-Maritime Generation for Universal Maritime Object Detection," *The 39th Annual Conference on Neural Information Processing Systems (NeurIPS)*, ***Spotlight***, San Diego, USA, Dec. 2025. [CCF-A]

[NeurIPS'25] S. Hu, X. Han, J. Jiang, **Y. Tao**, Z. Fang, Y. Dai, S. Kwong, and Y. Fang. "Distribution-Aligned Decoding for Efficient LLM Task Adaptation," *The 39th Annual Conference on Neural Information Processing Systems (NeurIPS)*, San Diego, USA, Dec. 2025. [CCF-A]

[GLOBECOM'25] S. Hu, Y. Ma, **Y. Tao**, Z. Fang, Z. Fang, Y. Deng, S. Kwong, and Y. Fang. "Task-Aware Parameter-Efficient Fine-Tuning of Large Pre-Trained Models at the Edge," *IEEE Global Communications Conference (GLOBECOM)*, Taipei, Taiwan, Dec. 2025. [CCF-C]

[JSAC] Z. Fang, J. Wang, Y. Ma, **Y. Tao**, Y. Deng, X. Chen, and Y. Fang. "R-ACP: Real-Time Adaptive Collaborative Perception Leveraging Robust Task-Oriented Communications," *IEEE Journal on Selected Areas in Communications (JSAC)*, 2025. [CCF-A]

[TDSC, Major Revision] S. Hu, **Y. Tao**, Z. Fang, G. Xu, Y. Deng, S. Kwong, and Y. Fang. "CP-Guard+: A New Paradigm for Malicious Agent Detection and Defense in Collaborative Perception," *IEEE Transactions on Dependable and Secure Computing (TDSC), Major Revision.* [CCF-A]

[TMC, Minor Revision] Z. Fang, Z. Lin, S. Hu, **Y. Tao**, Y. Deng, X. Chen, and Y. Fang. "Dynamic Uncertainty-aware Multimodal Fusion for Outdoor Health Monitoring," *IEEE Transactions on Mobile Computing (TMC), Minor Revision.* [CCF-A]

HONORS & AWARDS

Outstanding Academic Performance Award (OAPA), City University of Hong Kong . . . . . Aug. 2025
IEEE Robotics and Automation Society (RAS) Travel Grant for ICRA'25 . . . . . Mar. 2025
Outstanding Graduate, Shanghai Jiao Tong University . . . . . May 2024
WEICHAI POWER Scholarship, Shanghai Jiao Tong University . . . . . Oct. 2023
Excellent League Member, Shanghai Jiao Tong University . . . . . Apr. 2022
National Student Research Training Program Excellence Award (**Leader**) . . . . . Oct. 2020
Excellence Prize, 2nd International Data Competition, IKCEST (**top 3%**) . . . . . Oct. 2020
Sun Qingyun Innovation Scholarship, Southeast University (**<1% annually**) . . . . . Jun. 2020
Finalist, 36th Mathematical Contest in Modeling (MCM), COMAP (**top 1%**) . . . . . Apr. 2020
First Prize, 12th National Information Security Contest, China (**top 8%**) . . . . . Aug. 2019
First Prize, 15th Advanced Mathematics Competition, Jiangsu (**top 10%**) . . . . . Aug. 2018

PROJECT EXPERIENCE

Multi-Agent Collaborative Perception for Autonomous Driving . . . . . 2024 - Present

1) Institution and Supervisor: City University of Hong Kong, Prof. Yuguang Fang

2) Research Focus: Developing robust collaborative perception systems, designing defense mechanisms against adversarial attacks, and deploying on real-world ROS and Jetson-based autonomous driving platforms;

3) Achievements: 3 first-author papers accepted/submitted to top venues (ICRA'25, AAAI'25), 1 RAS travel grant.

Digital Twin and 6G Communications . . . . . 2021 - 2024

1) Institution and Supervisor: Shanghai Jiao Tong University, Prof. Jun Wu

2) Research Focus: Designing digital twin function virtualization for IoV services, developing DRL-based adaptive service response mechanisms, using Unity Software to connect with real-world elevator systems;

3) Achievements: 3 first-author papers published in IEEE journals/conferences, Outstanding Graduate Award.

Ultrasonic Anti-Recording Security System . . . . . 2019 - 2020

1) Institution and Supervisor: Southeast University, Prof. Yubo Song

2) Responsibility: Team leader. Designed ultrasonic anti-recording mechanism based on acoustic parametric array; Implemented SM4-based spread spectrum and DDS waveform generation on STM32F407 microcontroller;

3) Achievements: First prize in National Information Security Contest, 1 patent (CN111064543A), Sun Qingyun Innovation Scholarship.

ACADEMIC SERVICE

Program Committee Member:

ECCV 2026, CVPR 2026, ACM MM 2025-2026, ICML 2025-2026, ICLR 2025, AAAI 2025, ICRA 2025, IUI 2025, IJCNN 2025

IEEE ISBI 2025, IEEE ICC 2025, IEEE GLOBECOM 2023-2025, IEEE ICCC 2024

Journal Reviewer:

IEEE TMC, IEEE TITS, IEEE TCE, Pattern Recognition, Neural Networks, EAAI, IEEE JBHI, IEEE LNET

Session Chair:

IEEE GLOBECOM 2023, MWN Track, Semantic Communications Session

TECHNICAL SKILLS

Programming Languages: Python, MATLAB, C++, C#, JavaScript, Verilog HDL, LaTeX, Markdown

Deep Learning Frameworks: PyTorch, TensorFlow, OpenMMLab (MMDetection, MMSegmentation)

Tools & Platforms: Git, Docker, Linux, CARLA Simulator, SUMO, ROS

Languages: English (IELTS 7.0), Chinese (Native)