

# 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

PhD, Department of Computer Science  
Supervisor: Prof. Yuguang "Michael" Fang  
JC STEM Lab of Smart City, WINET Laboratory

Hong Kong SAR  
Sep. 2024 - Now

### Shanghai Jiao Tong University

Master, School of Computer Science  
Outstanding Graduate (2024)

Shanghai, China  
Sep. 2021 - Apr. 2024

### Southeast University

Bachelor, School of Information Engineering  
GPA: 3.89/4.0

Nanjing, China  
Sep. 2017 - Jul. 2021

## RESEARCH INTERESTS

Multi-agent collaborative perception, autonomous driving, AI security, foundation models for multi-agent systems, parameter-efficient fine-tuning.

## PUBLICATIONS

**Published & Accepted:** (# Equal contribution, \* Corresponding author)

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.

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.

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.

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.

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.

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.

**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.

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%)

**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.

**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.

**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.

**Preprints & Under Review:**

Z. Fang, Z. Lin, S. Hu, **Y. Tao**, Y. Deng, X. Chen, and Y. Fang. “Dynamic Uncertainty-aware Multimodal Fusion for Outdoor Health Monitoring,” *arXiv preprint arXiv:2508.01001*, 2025.

**Y. Tao**#, S. Hu#, Y. Hu, H. An, H. Cao, and Y. Fang. “GCP: Guarded Collaborative Perception with Spatial-Temporal Aware Malicious Agent Detection,” *arXiv preprint arXiv:2501.02450*, 2025.

**Y. Tao**, S. Hu, H. An, Z. Fang, H. Cao, and Y. Fang. “Adaptive Attack on Multi-Agent Collaborative Perception,” *Under Review*, 2025.

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,” *arXiv preprint arXiv:2502.07807*, 2025.

**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
WEICHAH POWER Scholarship, Shanghai Jiao Tong University . . . . .	Oct. 2023
Excellent League Member, Shanghai Jiao Tong University . . . . .	Apr. 2022
National Student Research Training Program Excellence Award ( <b>Leader</b> ) . . . . .	Oct. 2020
Excellence Prize, 2nd International Data Competition, IKCEST ( <b>top 3%</b> ) . . . . .	Oct. 2020
Sun Qingyun Innovation Scholarship, Southeast University (<1% <b>annually</b> ) . . . . .	Jun. 2020
Finalist, 36th Mathematical Contest in Modeling (MCM), COMAP ( <b>top 1%</b> ) . . . . .	Apr. 2020
First Prize, 12th National Information Security Contest, China ( <b>top 8%</b> ) . . . . .	Aug. 2019
First Prize, 15th Advanced Mathematics Competition, Jiangsu ( <b>top 10%</b> ) . . . . .	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:**

CVPR 2026, ACM MM 2025, ICML 2025, ICLR 2025, AAAI 2025, ICRA 2025, IUI 2025, IJCNN 2025  
IEEE ISBI 2025, IEEE ICC 2025, IEEE GLOBECOM 2023-2025, IEEE ICC 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)