

Research Interests

My research focuses on algorithm–system co-design for efficient and trustworthy foundation-model systems. My current interests center on self-evolving agent systems that learn and adapt through interaction and feedback. Specifically, I study agentic reinforcement learning and in-context learning for continual adaptation in single- and multi-agent systems.

Education

- 2023.8 – Present **Johns Hopkins University**, Baltimore, MD, USA,
Ph.D. in Electrical and Computer Engineering,
Advisor: Prof. Laixi Shi.
- 2021.9 – 2023.6 **Northwestern University**, Evanston, IL, USA,
M.S. in Electrical and Computer Engineering,
Advisor: Prof. Qi Zhu.
- 2017.9 – 2021.7 **Zhejiang Sci-Tech University**, Hangzhou, Zhejiang, China,
B.S. in Electrical Information Engineering.

Publications

* represents equal contribution.

- [1] **Juyang Bai**, Laixi Shi. "MAS-PromptBench: When Does Prompt Optimization Improve Multi-Agent LLM Systems?" *arXiv preprint*, 2026. Short version accepted at the *Conference on Language Modeling (COLM) Workshop on Lifelong Agents: Learning, Aligning, and Evolving*, 2026.
- [2] **Juyang Bai**, Tong Zhou, Shaolei Ren, Xiaolin Xu. "The Map Is Not the Territory: Embedding-Coverage Blacklists for Safe Diffusion Steering" *European Conference on Computer Vision (ECCV)*, 2026.
- [3] Tong Zhou, **Juyang Bai**, Xiaolin Xu, Shaolei Ren. "SafeGuide: Adaptive Inference-Time Safety Control for Diffusion Models" *Preprint*, 2026. Short version accepted at the *International Conference on Learning Representations (ICLR) Workshop on Principled Design for Trustworthy AI*, 2026.
- [4] Siyuan Huang*, Yutong Gao*, **Juyang Bai***, Yifan Zhou*, Zi Yin*, Xinxin Liu, Rama Chellappa, Chun Pong Lau, Sayan Nag, Cheng Peng, Shraman Pramanick. "SciFig: Towards Automating Scientific Figure Generation" *arXiv preprint*, 2026.
- [5] **Juyang Bai**, Md Hafizul Islam Chowdhury, Jingtao Li, Fan Yao, Chaitali Chakrabarti, Deliang Fan. "Phantom: Privacy-Preserving Deep Neural Network Model Obfuscation in Heterogeneous TEE and GPU Systems" *USENIX Security Symposium (USENIX Security)*, 2025.
- [6] Ruochen Jiao, **Juyang Bai**, Xiangguo Liu, Takami Sato, Xiaowei Yuan, Qi Alfred Chen, Qi Zhu. "Learning Representation for Anomaly Detection of Vehicle Trajectories" *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2023.

[7] Blaine Rothrock, Alexander Curtiss, **Juyang Bai**, Josiah Hester. "Towards a Toolkit for Free Living Wearable Development" *ACM International Joint Conference on Pervasive and Ubiquitous Computing and ACM International Symposium on Wearable Computers (UbiComp/ISWC) Adjunct*, 2022.

[8] Xiaojuan Lan, **Juyang Bai**, Meng Li, Jiajun Li. "Fish Image Classification Using Deep Convolutional Neural Network" *International Conference on Computers, Information Processing and Advanced Education (CIPAE)*, 2020.

Honors and Awards

Honors and Scholarships

- 2020.11 Government Scholarship granted by Zhejiang Province, China
- 2020.10 First-class Scholarship granted by Zhejiang Sci-Tech University
- 2020.10 3rd Place China Collegiate Computing Contest-Network Technology Challenge
- 2019.11 Second-class Scholarship & Merit Student granted by Zhejiang Sci-Tech University
- 2019.11 1st Place Softbank Robot Cup Wheeled Robot Sprint Group
- 2019.11 3rd Place Softbank Robot Cup Biped Robot Dance Group
- 2017.9 First-class Scholarship for Freshman granted by Zhejiang Sci-Tech University

Travel Awards

- 2026 The ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems Travel Grant

Research Experience

- 2025.11 – Present **Johns Hopkins University, Baltimore, MD, USA**,
Research Assistant, Advisor: Prof. Laixi Shi.
 - Developed MAS-PromptBench, a benchmark that systematically studies when and how much prompt optimization improves multi-agent LLM performance.
 - Building a prompt optimization framework for multi-agent LLM systems using trace-based reflection to reduce wall-clock optimization time.
- 2025.6 – 2025.11 **Johns Hopkins University, Baltimore, MD, USA**,
Research Assistant, Advisor: Prof. Trac Duy Tran.
 - Investigated hardware-aware pruning of Vision Transformers for sparse image reconstruction, targeting accuracy–latency–power trade-offs on NVIDIA Jetson Nano.
- 2023.8 – 2024.12 **Johns Hopkins University, Baltimore, MD, USA**,
Research Assistant, Advisor: Prof. Deliang Fan.
 - Proposed reinforcement learning–based DNN obfuscation on TEE/GPU systems to protect architectures and weights while retaining full accuracy for authorized users.
- 2022.5 – 2023.5 **Northwestern University, Evanston, IL, USA**,
Research Assistant, Advisor: Prof. Qi Zhu.
 - Designed contrastive learning and semantics-guided reconstruction methods for vehicle trajectory anomaly detection, demonstrating generalization to unseen anomaly patterns.
- 2022.5 – 2023.5 **Northwestern University, Evanston, IL, USA**,
Research Assistant, Advisor: Prof. Josiah Hester.
 - Built a wearable sensing hub integrating IMU, PPG, and ECG sensors for activity analysis, and implemented PPG–ECG fusion for heart rate estimation.

2019.3 – 2021.6 **Zhejiang Sci-Tech University**, *Hangzhou, Zhejiang, China*,

Research Assistant, Advisor: Prof. Meng Li.

- Developed an unmanned ground vehicle (UGV) for indoor inspection and designed a transmission line patrol drone, integrating perception, sensor fusion, and PID control.
- Proposed a DCNN-based approach to fish classification in challenging underwater environments, achieving 89% accuracy with transfer learning and data augmentation.

Professional Service

Organization Top Picks in Hardware and Embedded Security (Web Chair), 2025.

Artifact Evaluation Conference on Machine Learning and Systems (MLSys), 2026.

Committee IEEE Symposium on Security and Privacy (S&P), 2026.

USENIX Conference on Security Symposium (USENIX Security), 2026.

Reviewer Conference on Computer Vision and Pattern Recognition (CVPR), 2026.

Conference on Neural Information Processing Systems (NeurIPS), 2026.

International Conference on Computer-Aided Design (ICCAD), 2025.

Design, Automation & Test in Europe Conference (DATE), 2025, 2026.

IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2024.

Teaching Experience

Fall 2026 **Teaching Assistant**, *EN.520.669 Algorithmic Generative Artificial Intelligence*,
Instructor: Laixi Shi.

Fall 2025 **Teaching Assistant**, *EN.520.344 Introduction to Digital Signal Processing*,
Instructor: Berrak Sisman.

Spring 2025 **Teaching Assistant**, *EN.520.230/231 Mastering Electronics II + Lab*,
Instructor: Amy Foster and Lucas Buccafusca.

Fall 2024 **Teaching Assistant**, *EN.520.231 – Mastering Electronics Lab*,
Instructor: Sathappan Ramesh.

Technical Skills

Programming Python, C/C++, Matlab, CUDA.

Tools Pytorch, Tensorflow.