Junxiao (Cody) WANG

AIGC Researcher | Developer/Engineer Python/PyTorch

jxiao.wang github.com/wangjunxiao linkedin.com/in/junxiao-wang
(+86) 13478902794 wangjunxiao@live.com scholar.google.com
Born Weihai, China, 1991

Several years of experience applying machine learning models *efficiently*, *faithfully*, *securely*, and *privately* in distributed systems. Enjoys designing better problem-solving methods for challenging tasks, and learning new technologies and tools, and contributing to open source and tech communities by sharing knowledge and experience.

Broadly interested in artificial intelligence system with a special focus on generative AI, distributed machine learning, AI security, privacy and interpretability.

Latest Highlight

- **Scalable pretraining and adaptation for LLMs:**
  (1) Private Training Large-scale Models with Efficient DP-SGD. The annual conference on neural information processing systems (NeurIPS) 2025, San Diego, CA, USA. FlashDP
  TL;DR: Pre-training Llama-13B with 4 A100 GPUs, and achieves a 90% throughput compared to the Non-DP.
  (2) Scalable Zeroth-Order Fine-Tuning for Extremely Large Language Models with Limited GPU Memory. The conference on language modeling (COLM) 2025, Montreal, Canada. zo2
  TL;DR: Fine-tuning extraordinarily large models, such as OPT-175B, on a mere 18GB GPU.

- **Multimodal LLMs for interactive scenarios:**
  (1) Autonomous Workflow for Multimodal Fine-Grained Training Assistants Towards Mixed Reality. The annual meeting of the association for computational linguistics (ACL) 2024, Bangkok, Thailand. AutonomousDialogAgent4AugmentedReality
  TL;DR: Autonomous workflows integrating MLLM agents into LEGO brick assembly in a pilot XR environment.
  (2) Conversational Education at Scale: A Multi-LLM Agent Workflow for Procedural Learning and Pedagogic Quality Assessment. The conference on empirical methods in natural language processing (EMNLP) 2025, Suzhou, CN. WikiHowAgent
  TL;DR: The workflow based on multiple LLM agents simulates teacher-student dialogues and evaluates teaching quality.
  (3) Trustworthy AI Psychotherapy: Multi-Agent LLM Workflow for Counseling and Explainable Mental Disorder Diagnosis. ACM conference on information and knowledge management (CIKM) 2025, Seoul, Korea. mental_health_multiagent
  TL;DR: Multi-agent AI system that simulates therapist-client dialogues to generate explainable mental health diagnoses.

Profession & Skills

Programming	Python (PyTorch), Golang, Java, C/C++.
Services	CVPR25/26, ICCV23/25, ECCV24, NeurIPS25, ICLR26, IJCAI24/25, ECAI25, AISTATS24/25/26.
Misc Tools	Git, LaTex, Markdown, Linux.

Projects & Experiences

Apr 2024 – Mar 2023 — **Pre-Trained Models, KAUST, Python (PyTorch)**

- Implementation of *Faithful Interpretation* for Concept Bottleneck models.
- Implanting triggerable but invisible *Trojans* onto BERT via random encoding perturbations.
- Rebalancing the *Slow-Learning Modalities* towards the Prototypes.
- Implementation of intervening at *Diffusion* timesteps for safe AIGC generation.
- Publications: KDD23, NeurIPS23, NeurIPS24, CVPR23, ICLR24.
- : FVLC, Modal-Imbalance-PMR, TrojanAttack.

Faithful Interpretation | Concept Bottleneck | Trojan | Modality Rebalance | Diffusion

Mar 2023 – Mar 2021 — **Distributed Machine Learning, HONG KONG POLYTECHNIC UNIVERSITY, Python (PyTorch)**

- *Gradient Inversion* protection based on Random Matrix theory.
- *Knowledge Editing* based on TF-IDF and Filter Pruning implemented with NNI.
- Implementation of CLIP based *FL Framework* with Parameter-Efficient Fine-Tuning.
- Publications: INFOCOM22, IJCAI22, WWW22, WWW23, TMC, Network.
- : GradDefense, Unlearning, PromptFL.

Gradient | Random Matrix | TF-IDF | Filter Pruning | NNI | CLIP | Parameter-Efficient Fine-Tuning

Sep 2019 – Sep 2018 | **Network Intelligence, QMUL, Python/C/C++**

- Online *Traffic Recognition* based on 1D-CNN implemented with TensorFlow and Keras.
- Implementation of adaptive *Sketch Memory Allocation* based on Actor-Critic Framework.
- Implementation of *RFID Integrity Authentication* with protocol redesign.
- Publications: ICA3PP19, CFI19, SmartIoT19, IoTJ, TMC.
- : TrafficCategorization, HBLSketch, RL_MemoryAllocation.

Traffic Recognition | Sketch | Memory Allocation | Actor-Critic | RFID

Dec 2020 – Sep 2016 | **Network Systems, Dalian University of Technology, Python/Golang/Java/C/C++**

- Implementation of efficient *Software Upgrade* with State-Isolated Modular Management.
- Implementation of fine-grained *Control Plane Scheduling* with Queue Management.
- *Data Plane Flow Tracing* based on Probabilistic Packet Tagging implemented with OpenFlow.
- Publications: SIGCOMM18 Demo, ISJ, TNSM, TNSE, IoTJ, OJCOMS.
- : CLICK-UP, FlowTracer, NFVCloud, SDNCloud, SDNDashboard, AgileScheduler.

Software Upgrade | Control Plane | Scheduling | Queue | Data Plane | Flow Tracing | Packet Tagging

Employment

2024 Associate Professor, Guangzhou University (GZHU), Guangzhou, China.
2023 Postdoctoral Fellow, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia.
2021 Postdoctoral Fellow, Hong Kong Polytechnic University (PolyU), Hong Kong, China.
2018 Visitor, Queen Mary University of London (QMUL), London, United Kingdom.

Publications

- Liangyu Wang, **Junxiao Wang**, Jie Ren, Zihang Xiang, David E. Keyes, Di Wang. Private Training Large-scale Models with Efficient DP-SGD. The Annual Conference on Neural Information Processing Systems (NeurIPS) 2025, San Diego, CA, USA. (acceptance rate∼24.5% [5,290/21,500])
- Yuxuan Lu, Guojie Ma, Shiyu Yang, **Junxiao Wang**. Enhancing Inductive Knowledge Graph Completion with Contextual Relation Topology Learning. Knowledge-Based Systems (KBS) 2025.
- Jiahuan Pei, Fanghua Ye, Xin Sun, Wentao Deng, Koen Hindriks, **Junxiao Wang**. Conversational Education at Scale: A Multi-LLM Agent Workflow for Procedural Learning and Pedagogic Quality Assessment. The Conference on Empirical Methods in Natural Language Processing (EMNLP) 2025, Suzhou, China. (acceptance rate∼17.4% [1,418/8,174])
- Yizhi Zhou, **Junxiao Wang**, Yuchen Qin, Xin Xie, Zhipeng Song, Heng Qi. Federated Learning on Heterogeneous and Long-Tailed Data via Disentangled Representation. IEEE Transactions on Mobile Computing (TMC) 2025.
- Mithat Can Ozgun, Jiahuan Pei, Koen Hindriks, Lucia Donatelli, Qingzhi Liu, **Junxiao Wang**. Trustworthy AI Psychotherapy: Multi-Agent LLM Workflow for Counseling and Explainable Mental Disorder Diagnosis. ACM Conference on Information and Knowledge Management (CIKM) 2025, Seoul, Korea. (acceptance rate∼29.0% [810/2,761])
- Liangyu Wang, Jie Ren, Hang Xu, **Junxiao Wang**, Huanyi Xie, David E. Keyes, Di Wang. Scalable Zeroth-Order Fine-Tuning for Extremely Large Language Models with Limited GPU Memory. The Conference on Language Modeling (COLM) 2025, Montreal, Canada. (acceptance rate∼32.0% [418/1,306])
- Yizhi Zhou, **Junxiao Wang**, Yuchen Qin, Xiangyu Kong, Xin Xie, Heng Qi, Deze Zeng. Federated Learning with Complete Service Commitment of Data Heterogeneity. Knowledge-Based Systems (KBS) 2025.
- Yizhi Zhou, **Junxiao Wang**, Xin Xie, Pengfei Wang, Xibei Jia, Heng Qi, Yuchen Qin. A Survey on Federated Long-Tailed Learning. Chinese Journal of Computers 2024.
- Liangyu Wang, Jie Ren, Hang Xu, **Junxiao Wang**, David E. Keyes, Di Wang. ZO-Offloading: Fine-Tuning LLMs with 100 Billion Parameters on a Single GPU. The NeurIPS Workshop on Adaptive Foundation Models (AFM) 2024, Vancouver, Canada.
- Liangyu Wang, **Junxiao Wang**, Jie Ren, Zihang Xiang, David E. Keyes, Di Wang. FlashDP: Memory-Efficient and High-Throughput DP-SGD Training for Large Language Models. The NeurIPS Workshop on Adaptive Foundation Models (AFM) 2024, Vancouver, Canada.
- Peiran Dong, Bingjie Wang, Song Guo, **Junxiao Wang**, Jie Zhang, Zicong Hong. Towards Safe Concept Transfer of Multi-Modal Diffusion via Causal Representation Editing. The Annual Conference on Neural Information Processing Systems (NeurIPS) 2024, Vancouver, Canada. (acceptance rate∼25.8% [4,043/15,671])
- Tao Guo, Song Guo, **Junxiao Wang**. Explore and Cure: Unveiling Sample Effectiveness with Context-Aware Federated Prompt Tuning. IEEE Transactions on Mobile Computing (TMC) 2024.
- Jiahuan Pei, Irene Viola, Haochen Huang, **Junxiao Wang**, Moonisa Ahsan, Fanghua Ye, Jiang Yiming, Yao Sai, Di Wang, Zhumin Chen, Pengjie Ren, Pablo Cesar. Autonomous Workflow for Multimodal Fine-Grained Training Assistants Towards Mixed Reality. Findings of the Association for Computational Linguistics (ACL) 2024, Bangkok, Thailand. (acceptance rate∼22.1% [974/4,407])
- Yizhi Zhou, **Junxiao Wang**, Xiangyu Kong, Shan Wu, Xin Xie, Heng Qi. Exploring Amplified Heterogeneity Arising from Heavy-Tailed Distributions in Federated Learning. IEEE Transactions on Mobile Computing (TMC) 2024.
- Liangyu Wang, **Junxiao Wang**, Di Wang. Towards Light Adaptation of Large Language Models For Personal Hardware. The ACM MobiSys Workshop on Edge and Mobile Foundation Models (EdgeFM) 2024, Tokyo, Japan.
- Leijie Wu, Song Guo, Yaohong Ding, **Junxiao Wang**, Wenchao Xu, Yufeng Zhan, Anne-Marie Kermarrec. Rethinking Personal-

ized Client Collaboration in Federated Learning. IEEE Transactions on Mobile Computing (TMC) 2024.

- Songning Lai, Lijie Hu, **Junxiao Wang**, Laure Berti-Equille, Di Wang. Faithful Vision-Language Interpretation via Concept Bottleneck Models. International Conference on Learning Representations (ICLR) 2024, Vienna, Austria. (acceptance rate∼31.0% [2,252/7,262])
- Peiran Dong, Song Guo, **Junxiao Wang**, Bingjie Wang, Jiewei Zhang, Ziming Liu. Towards Test-Time Refusals via Concept Negation. The Annual Conference on Neural Information Processing Systems (NeurIPS) 2023, New Orleans, LA, USA. (acceptance rate∼26.1% [3,222/12,343])
- Tao Guo, Song Guo, **Junxiao Wang**, Xueyang Tang, Wenchao Xu. PromptFL: Let Federated Participants Cooperatively Learn Prompts Instead of Models - Federated Learning in Age of Foundation Model. IEEE Transactions on Mobile Computing (TMC) 2023.
- Peiran Dong, Song Guo, **Junxiao Wang**. Investigating Trojan Attacks on Pre-trained Language Model-powered Database Middleware. ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2023, Long Beach, CA, USA. (acceptance rate∼22.1% [313/1,416])
- Yunfeng Fan, Wenchao Xu, Haozhao Wang, **Junxiao Wang**, Song Guo. PMR: Prototypical Modal Rebalance for Multimodal Learning. IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 2023, Vancouver, Canada. (acceptance rate∼25.8% [2,360/9,155])
- Tao Guo, Song Guo, **Junxiao Wang**. pFedPrompt: Learning Personalized Prompt for Vision-Language Models in Federated Learning. The ACM Web Conference (WWW) 2023, Austin, Texas, USA. (acceptance rate∼19.2% [365/1,900])
- Leijie Wu, Song Guo, **Junxiao Wang**, Zicong Hong, Jie Zhang, Yaohong Ding. Federated Unlearning: Guarantee the Right of Clients to Forget. IEEE Network 2022.
- Xin Xie, Xiulong Liu, **Junxiao Wang**, Song Guo, Heng Qi, Keqiu Li. Efficient Integrity Authentication Scheme for Large-scale RFID Systems. IEEE Transactions on Mobile Computing (TMC) 2022.
- Rui Zhang, Song Guo, **Junxiao Wang**, Xin Xie, Dacheng Tao. A Survey on Gradient Inversion: Attacks, Defenses and Future Directions. International Joint Conference on Artificial Intelligence (IJCAI) 2022, Vienna, Austria. (acceptance rate∼14.9% [679/4,535])
- **Junxiao Wang**, Song Guo, Xin Xie, Heng Qi. Federated Unlearning via Class-Discriminative Pruning. The ACM Web Conference (WWW) 2022, Online. (acceptance rate∼17.7% [323/1,822])
- **Junxiao Wang**, Song Guo, Xin Xie, Heng Qi. Protect Privacy from Gradient Leakage Attack in Federated Learning. IEEE International Conference on Computer Communications (INFOCOM) 2022, Online. (acceptance rate∼19.8% [224/1,129])
- Heng Qi, **Junxiao Wang**, Wenxin Li, Yuxin Wang, Tie Qiu. A Blockchain-driven IIoT Traffic Classification Service for Edge Computing. IEEE Internet of Things Journal (IoTJ) 2021.
- **Junxiao Wang**, Heng Qi, Wenxin Li, Keqiu Li, Steve Uhlig, Yuxin Wang. Dynamic SDN Control Plane Request Assignment in NFV Datacenters. IEEE Transactions on Network Science and Engineering (TNSE) 2021.
- **Junxiao Wang**, Heng Qi, Keqiu Li, Steve Uhlig. Click-UP: Towards the Software Upgrade of Click based Modular Network Function. IEEE Systems Journal (ISJ) 2020.
- Xinping Xu, Wenxin Li, Heng Qi, **Junxiao Wang**, Keqiu Li. Latency-Constrained Cost-Minimized Request Allocation for Geo-distributed Cloud Services. IEEE Open Journal of the Communications Society (OJCOMS) 2020.
- **Junxiao Wang**, Heng Qi, Yang He, Wenxin Li, Keqiu Li. FlowTracer: An Effective Flow Trajectory Detection Solution Based on Probabilistic Packet Tagging in SDN-Enabled Networks. IEEE Transactions on Network and Service Management (TNSM) 2019.
- Keyan Zhao, **Junxiao Wang**, Heng Qi, Xin Xie, Keqiu Li. HBL-Sketch: A New Three-tier Sketch for Accurate Network Measurement. International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP) 2019, Melbourne, Australia.
- Wenrui Zhou, Yuan Cao, Heng Qi, **Junxiao Wang**. An Effective Network Intrusion Detection Framework Based on Learning to Hash. IEEE International Conference on Smart Internet of Things (SmartIoT) 2019, Tianjin, China.
- Wanqian Zhang, **Junxiao Wang**, Sheng Chen, Heng Qi, Keqiu Li. A Framework for Resource-aware Online Traffic Classification Using CNN. International Conference on Future Internet Technologies (CFI) 2019, Phuket, Thailand.
- **Junxiao Wang**, Heng Qi, Keqiu Li, Xiaobo Zhou. Real-Time Link Fault Detection as a Service for Datacenter Network. Journal of Computer Research and Development 2018.
- **Junxiao Wang**, Heng Qi, Keqiu Li, Xiaobo Zhou. PRSFC-IoT: A Performance and Resource Aware Orchestration System of Service Function Chaining for Internet of Things. IEEE Internet of Things Journal (IoTJ) 2018.
- **Junxiao Wang**, Yuchen Huang, Heng Qi, Keqiu Li, Steve Uhlig. CLICK-UP: Towards Software Upgrades of Click-driven Stateful Network Element. ACM SIGCOMM Conference 2018 Demo, Budapest, Hungary.

Education

2020 PhD in Computer Science, Dalian University of Technology (DUT), Dalian, China.
2017 MEng in Computer Science, Dalian University of Technology (DUT), Dalian, China.
2014 BEng in Software Engineering, Dalian Maritime University (DMU), Dalian, China.