Junxiao WANG

LLM 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, September 11, 1991

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

Skills

Programming	Python (PyTorch), Golang, Java, C/C++
Machine Learning	Quantization, Parameter-Efficient Fine-Tuning, Federated Learning
CV/NLP/Multimodal	Diffusion, GAN, VAE, ViT, CNN, GPT, BERT, GNN, CLIP
PC/Reviewers	AISTAT24, ICCV23, TMC, TNSE, etc.
Misc Tools	Git, LaTex, Linux

Projects & Experiences

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

- Implementation of *Faithful Interpretation* with Concept Bottleneck model.
- Implanting triggerable but invisible *Trojans* in BERT via random encoding perturbation.
- *Slow-Learning Modality Rebalance* based on Prototypes implemented with Python.
- Implementation of *Diffusion Concept Negation* with test-time attention refinement.
- Publications: KDD23, NeurIPS23, CVPR23, ICLR24.
- : 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 Protection* based on Random Matrix theory implemented with Python.
- *Knowledge Editing* based on TF-IDF and Filter Pruning implemented with NNI.
- Implementation of CLIP based *Distributed 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* with Actor-Critic Framework.
- Implementation of *RFID Integrity Authentication* with protocol design.
- 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 Python.
- 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

2023-current	Researcher, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
2021-2023	Researcher, Hong Kong Polytechnic University (PolyU), Hong Kong, China
2018-2019	Researcher, Queen Mary University of London (QMUL), London, United Kingdom

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

Publications

- 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** (Corresponding Author), 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** (Corresponding Author), 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** (Corresponding Author). 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** (Corresponding Author). 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** (Corresponding Author), 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** (Corresponding Author), 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. 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.