Junxiao Wang

Email: junxiao.wang@kaust.edu.sa
Office: Al-Khawarizmi Building 1, Room 4212-CU02
King Abdullah University of Science and Technology
Thuwal, Saudi Arabia

Introduction

I currently hold the position of **Postdoctoral Fellow** at **KAUST**.
My area of expertise is **artificial intelligence** and **network**, with a focus on security, trustworthy ML and systems. My objective is to develop intelligent agents that are **ubiquitous** and **human-centric**, capable of learning from networked users in a manner that is considerate of limited data and resources.

Experience

King Abdullah University of Science and Technology, CEMSE, *PostDoc* 2023.02 - Now

Project: Interdisciplinary Machine Learning Research encompassing Privacy, Security and Fairness.
Lab: KAUST Provable Responsible AI and Data Analytics Lab Director: Prof. Dr. Di Wang

Hong Kong Polytechnic University, COMP, *PostDoc* 2021.03 - 2023.02

Project: Federated Learning over Mobile Edge Networks and Machine Learning Governance.
Lab: PolyU Edge Intelligence Lab Director: Prof. Dr. Song Guo

Education

Dalian University of Technology, Computer Technology Application, *PhD* 2016.09 - 2020.12

Thesis: Research on Techniques of Performance Guarantee for Software Defined Network Function Virtualization System. Supervisor: Prof. Dr. Keqiu Li, Prof. Dr. Heng Qi

Queen Mary University of London, EECS, *Visiting Student* 2018.10 - 2019.09

Program: China Scholarship Council (CSC)-Funded Joint PhD Program.
Lab: Networks Research Group Supervisor: Prof. Dr. Steve Uhlig

Dalian University of Technology, Computer Systems Organization, *MEng* 2014.09 - 2017.07

Thesis: Research on Request Dispatching for Multi-Controllers in Software Defined Networking.
Program: Master-PhD Combined Program. Supervisor: Prof. Dr. Keqiu Li, Prof. Dr. Heng Qi

Dalian Maritime University, Software Engineering, *BE* 2010.09 - 2014.06

Thesis: Research on Load Balancing Mechanism Based on Floodlight Controller Platform.
Graduate with Honors: Waivers of National Postgraduate Entrance Examination (NPEE), GPA: top 5%

Honors and Awards

NSFC General Program (Participant, 570K CNY, 48 months) 2021.01
Hong Kong PolyU Postdoc Matching Fund (PI, 549K HKD, 24 months) 2020.12
China Scholarship Council Joint PhD Scholarship (PI, 13.8K GBP, 12 months) 2018.06
NSFC General Program (Participant, 640K CNY, 48 months) 2018.01
Outstanding Postgraduate of Dalian University of Technology 2015.12
Final First Prize and Best Creative Award of National University SDN Competition 2015.08
MCM/ICM Media Contest Outstanding Winner 2013.05

Publications

(Note: "⊙" marks the corresponding authors.)

- 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. (Top-level Journal, JCR-Q1)
- 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. (Top-level Conference, 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. (Top-level Conference, acceptance rate∼25.8% [2360/9,155])
- Tao Guo, Song Guo, **Junxiao Wang**$^{\odot}$. pFedPrompt: Learning Personalized Prompt for Vision-Language Models in Federated Learning. The ACM Web Conference (WWW) 2023, Austin, Texas, USA. (Top-level Conference, acceptance rate∼19.2% [365/1,900])
- Leijie Wu, Song Guo, **Junxiao Wang**$^{\odot}$, Zicong Hong, Jie Zhang, Yaohong Ding. Federated Unlearning: Guarantee the Right of Clients to Forget. IEEE Network 2022. (Top-level Journal, JCR-Q1)
- 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. (Top-level Journal, JCR-Q1)
- Rui Zhang, Song Guo, **Junxiao Wang**$^{\odot}$, Xin Xie, Dacheng Tao. A Survey on Gradient Inversion: Attacks, Defenses and Future Directions. International Joint Conference on Artificial Intelligence (IJCAI) 2022, Vienna, Austria. (Top-level Conference, 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. (Top-level Conference, 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. (Top-level Conference, acceptance rate∼19.8% [224/1,129])
- **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. (Top-level Journal, JCR-Q1)
- 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. (Top-level Journal, JCR-Q1)
- **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. (Top-level Journal, JCR-Q1)
- 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. (Top-level Journal, JCR-Q1)
- 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.
- 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.
- 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.
- **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. (Top-level Journal, JCR-Q1)
- **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. (Top-level Journal, JCR-Q1)
- **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.

Granted Patents

- Heng Qi, Wenrui Zhou, Yuan Cao, Keqiu Li, **Junxiao Wang**. Abnormal Flow Detection Method based on Automatic Encoder Network, CN201910094284.8
- Wanqian Zhang, Heng Qi, Keqiu Li, **Junxiao Wang**. Abnormal Flow Detection Method with Computing Resource Adaptivity, CN201910067413.4
- Heng Qi, Keyan Zhao, Keqiu Li, **Junxiao Wang**. Elephant Flow Detection Method based on Three-Layer Sketch Framework, CN201910067412.X
- Keqiu Li, Ji Zhao, Heng Qi, **Junxiao Wang**. Gateway Equipment Establishing Method for Providing Edge Computing Service, CN201810419285.0

- Keqiu Li, Zhiqian Zhang, Heng Qi, **Junxiao Wang**. SDN Controller Application Performance Analysis Method based on OpenFlow Protocol, CN201810375977.X
- Heng Qi, Jiabin Qiao, Keqiu Li, **Junxiao Wang**. Service Performance Testing Method for Mixed Cloud, CN201810375893.6
- Keqiu Li, Yuchen Huang, Heng Qi, **Junxiao Wang**. A Kind of Online Method of Combination of Virtual NE based on Click, CN201810255339.4
- Keqiu Li, Chuang Lei, Heng Qi, **Junxiao Wang**. Resource Providing System and Method of Virtualization Platform, CN201710230445.2
- Keqiu Li, Shuyu Li, Heng Qi, **Junxiao Wang**. Virtual Data Center Visual Management Method based on Cairngorm Framework, CN201710225860.9
- Keqiu Li, **Junxiao Wang**, Heng Qi, Haisheng Yu. The Construction Method of Cooperation Layer in a Kind of SDN Architectural Framework, CN201710030607.8

Service Experience

Academic Services

PC Member/Reviewer of International Conference on Artificial Intelligence and Statistics (AISTATS) 2024
Reviewer of International Conference on Computer Vision (ICCV) 2023
Reviewer of IEEE Transactions on Network Science and Engineering (TNSE)

Student Teaching

Shepherd of Doctoral Thesis in KAUST, PolyU and QMUL
Shepherd of Bachelor and Master Thesis in DLUT

Talks

Invited Talks

Title: Privacy Protection in Federated Learning
Ritsumeikan University & CCF Dalian International Seminar | Online 2022.03

Conference Talks

Title: Protect Privacy from Gradient Leakage Attack in Federated Learning
IEEE International Conference on Computer Communications (INFOCOM) | Online 2022.05

Title: Federated Unlearning via Class-Discriminative Pruning
The ACM Web Conference (WWW) | Online 2022.04

Title: CLICK-UP: Towards Software Upgrades of Click-driven Stateful Network Elements
ACM SIGCOMM Conference, Demo Track | Budapest, Hungary 2018.08

Competition Talks

Titile: Centrally Coordinated Replica Selection Architecture in Multi-Controller SDN
The 2nd National University SDN Competition Final | SCUT, Guangzhou 2015.08

Referees

Prof. Dr. Di Wang, CEMSE, KAUST, di.wang@kaust.edu.sa
Prof. Dr. Song Guo, COMP, PolyU, song.guo@polyu.edu.hk
Prof. Dr. Steve Uhlig, EECS, QMUL, steve.uhlig@qmul.ac.uk
Prof. Dr. Keqiu Li, CIC, TJU, keqiu@tju.edu.cn
Prof. Dr. Heng Qi, CS, DLUT, hengqi@dlut.edu.cn

Last updated: *19 September 2023*