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 **machine learning** and **systems**, with a focus on FL, trustworthy ML and networking.
My objective is to develop intelligent agents that are **ubiquitous** and **human-centric**, capable of learning from network edge users in a manner that is considerate of limited data and resources.

Work 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

Technical Skills

I possess advanced knowledge and expertise in the field of Machine Learning, including but not limited to: Federated Learning, Prompt Tuning, Multimodal, Unlearning, Gradient Inversion, Backdoors, and Diffusion; Additionally, I am proficient in Distributed Networking Systems, including Software-Defined Networks, Network Functions Virtualization, and Cloud. I am also skilled in various techniques and tools such as Linux, PyTorch, and OpenStack.

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

Hong Kong Polytechnic University Postdoc Matching Fund 2020.12
China Scholarship Council Joint PhD Scholarship 2018.06
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

Refereed Papers

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

- 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.

- 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.
- 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.
- 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.
- **Junxiao Wang**, Song Guo, Xin Xie, Heng Qi. Federated Unlearning via Class-Discriminative Pruning. The ACM Web Conference (WWW) 2022, Online.
- **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.
- **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.
- **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.

Service Experience

Academic Services

(Sub-)Reviewers of ICCV, INFOCOM, CVPR, JSAC, TNET, CSUR, IoTJ, TNSM, TNSE, etc.
Session Chair of IEEE International Conference on Parallel and Distributed Systems (ICPADS) 2019

Student Teaching

Shepherd of PhD Students in Hong Kong Polytechnic University and Queen Mary University of London
Shepherd of Postgraduate Students in Dalian University of Technology

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, DUT, hengqi@dlut.edu.cn