Jiyao Liu

github.com/jiyao17 | www.linkedin.com/in/jiyao17 | jiyao.liu@outlook.com | +1 (267) 336 3486

Summary

Jiyao Liu is a third-year Ph.D. candidate at the Department of Computer and Information Sciences at Temple University. His research interests include **AI and privacy/security at edge/on device**, e.g., federated learning, mobile vision, etc. He is actively seeking internships anytime in 2024.

Education

2021 - present **Temple University**, Philadelphia, PA, USA
PhD, Computer and Information Sciences
Advisor: Dr. Yu Wang

2016 - 2020 **North China University of Technology**, Beijing, China
BEng, Information Security

Selected Publications

For full publication list, see my Google Scholar.

[1] **Jiyao Liu**, Xinliang Wei, Xuanzhang Liu, Hongchang Gao, and Yu Wang. "Group-based Hierarchical Federated Edge Learning: Convergence, Group Formation and Sampling". In: *ICPP*. 2023.

Industrial and Academic Experience

Research Intern (Aug. 2023 - Dec. 2023)
Toyota North America, Mountain View, CA, USA

- Topic. Find out items left behind by riding app users (via an in-cabin camera). Responsible for dataset collection, model design, fine-tuning, patent/paper drafting, etc.
- Model. Design new neural network model dedicated to this task, with state-of-the-art object detection techniques. It should i) be easy to train (require small training dataset), ii) be able to handle background interference (e.g., change of illumination, brightness, shadow, etc); iii) be good at generalization, i.e., detecting unknown items; iv) be efficient on mobile devices.
- Dataset. Determine the data to be collected (e.g., class number, background interference, dataset size, etc). Process and organize raw images to create training data for the dedicated model. Instead of synthetic augmentation, use combination of raw images as training data to enhance the model resistance to background noise.

Research Assistant (May. 2021 - current)
Temple University, PA, USA

- Topic. Federated Learning, including communication compression, statistical/systematic heterogeneity, attack and defense, resource allocation, etc.
- Techniques. Compression: top-k, quantization, pruning, etc. Privacy: differential privacy, secure aggregation. Security: gradient reversion, member inference, etc. Heterogeneity: imbalanced data distribution, device sampling, resource allocation optimization, etc.

Skill Set

Programming Languages	C/C++, Python, Java, SQL, x86 Assembly & Disassembly.
Machine Learning	Convex Optimization, Differential Privacy, PyTorch, NumPy, matplotlib.
Cryptography	Encryption, Blockchain, Solidity.
Distributed Systems	networkx, Gurobi, Resource/Task Scheduling/Allocation
Systems & Tools	Linux (Ubuntu), Raspberry PI, Git, CMake, ssh, shell.

Services

Reviewer for IEEE TCC 2023, IEEE IoTJ 2023, IEEE MASS 2023, etc.