Tiansheng Huang

PhD student at Georgia Institute of Technology
Email: thuang374@gatech.edu
Phone: (470)301-7963

Education

Georgia Institute of Technology, Atlanta, USA Aug 2022 – Present
- Second year PhD student, School of computer science
- Program Advisor: Prof. Ling Liu.

South China University of Technology, Guangzhou, China Sept 2019 – June 2022
- M.S, School of computer science
- Program Advisor: Prof. Weiwei Lin
- Thesis: Application of Multi-arm Bandit Algorithms in Client Selection of Federated Learning

South China University of Technology, Guangzhou, China Sept 2015 – June 2019
- B.S, School of computer science
- GPA: 3.75 (rank top 10%)

Research Interest

Current interest
- My current research interest lies in distributed machine learning, security/privacy aspect of federated learning, parallel and distributed computing and big data systems.

Previous studied
- Multi-arm bandit
- Online learning
- Resource scheduling on cloud/edge computing

Experience

JD explore academy, Beijing, China March 2022 - June 2022
Research Intern
- Develop Personalized FL algorithms with factorization and sparse compression.
- Program Advisor: Dr. Li Shen

JD explore academy, Beijing, China June, 2021 - Sept 2021
Research Intern
- Develop high efficiency sparse training algorithms for personalized FL.
- Program Advisor: Dr. Li Shen

Honor and Awards

Two years of **National Scholarship** (Top graduate scholarship in China) 2020, 2021
First-Class School Scholarship 2019

Publications

Peer-review Conference

[1] **T. Huang**, S. Hu, KH. Chow, F. Ilhan, S. Tekin, L. Liu, "Lockdown: Backdoor Defense for Federated Learning with Isolated Subspace Training," NeurIPS2023

[2] Y. Sun, L. Shen, **T. Huang**, and D. Tao, "FedSpeed: Larger Local Interval, Less Communication Round, and Higher Generalization Accuracy," ICLR2023

[3] F Ilhan, SF Tekin, S Hu, **T Huang**, KH Chow and L Liu, "Hierarchical Deep Neural Network Inference for Device-Edge-Cloud Systems[C]" Companion Proceedings of the ACM Web Conference (WWW) 2023.

Journal

[4] **T. Huang**, L. Shen, Y. Sun, W. Lin, and D. Tao, "Fusion of Global and Local Knowledge for Personalized Federated Learning," 2022, Transactions on Machine Learning Research (TMLR).
[5] **T. Huang**, W. Lin, L. Shen, K. Li and A. Y. Zomaya, "Stochastic Client Selection for Federated Learning with Volatile Clients," 2022, IEEE Internet of Things Journals (IoT-J).
[6] **T. Huang**, W. Lin, X. Hong , X. Wang, Q. Wu, R. Li, CH. Hsu, AY. Zomaya, "Adaptive Processor Frequency Adjustment for Mobile Edge Computing with Intermittent Energy Supply", 2021, IEEE Internet of Things Journals (IoT-J).
[7] **T. Huang**, W. Lin, W. Wu, L. He, K. Li and AY. Zomaya, "An Efficiency-boosting Client Selection Scheme for Federated Learning with Fairness Guarantee," 2020, IEEE Transactions on Parallel and Distributed Systems (TPDS).
[8] **T. Huang**, W. Lin, C. Xiong, R. Pan and J. Huang, "An Ant Colony Optimization Based Multi-objective Service Replicas Placement Strategy for Fog Computing," 2020, IEEE Transactions on Cybernetics (TCYB).

Under Submission

[9] **T. Huang**, S. Hu, W. Wei, L. Liu, "Silencer: pruning-aware backdoor defense for decentralized federated learning," Under Submission
[10] **T Huang,** S Liu, L Shen, F He, W Lin, D Tao, "Achieving personalized federated learning with sparse local models," Under submission
[11] S. Hu, **T. Huang**, K. Chow, F. İlhan, S. Tekin, L. Liu, "Linking Ethereum Accounts with Transferable Language Model through Pseudo-Supervision", Under submission
[12] S. Hu, **T. Huang**. L.Liu, "Ethereum Account Profiling and De-anonymization via Pseudo-Siamese BERT", Under submission
[13] K. Chow, S. Hu, **T. Huang**, F. İlhan, S. Tekin, L. Liu, "Diversity-driven Privacy Protection Masks Against Unauthorized Face Recognition", Under submission

Projects

Area 1: Security aspect of Federated Learning

Backdoor Defense for Federated Learning (During First year of PhD)

- First to identify poison coupling effect in federated learning.
- Invent isolated subspace training technique to decouple and filter the poisoned parameters.
- Source code available at https://github.com/LockdownAuthor/Lockdown.

Backdoor Defense for Decentralized Federated Learning (During First year of PhD)

- Theoretically identify empirical Fisher information as a reliable indicator of poisoned parameters.
- Empirically study the Fisher-guided pruning technique to purify the poisoned model .
- To increase pruning performance, invent a defense to boost the consensus in the training phase.

Area 2: Efficient Federated Learning/Personalized Federated Learning

Efficient client selection in FL with multi-arm bandit (during master)

- Identify system heterogeneity/selection fairness/ cumulative participation as main factors for federated learning system performance.
- balance system heterogeneity/selection fairness/cumulative participation with UCB/stochastic multi-arm bandit algorithms.

Efficient PFL with low-rank+sparse (with JD.com during master)

- Low-rank+sparse joint compression for personalized federated learning.
- Design a proximal algorithms.to solve the problem with theoretical guarantee.

Efficient PFL with dynamic sparse training (with JD.com during master)

- Formulate the personalized models as a nested network in the global model.
- Propose a dynamic sparse training technique for training time acceleration in PFL.

-