Jianrong Lu | CV

lujianrong@hust.edu.cn ● jianrong-lu.github.io

Education

Huazhong University of Science and Technology (HUST), Wuhan, China Sept. 2020 -
M.Eng. in Cyberspace Security **Major GPA: 4.0/4.0**
School of cyber Science and Engineering Supervisor: Shengshan Hu

Fu Zhou University, Fu Zhou, China Sept. 2016 - Jun. 2020
B.S. in Information and Computing Science **Major GPA: 3.44/4.0**
School of Mathematics and Computer Science

Courses Highlight: Distributed System (100/100), Machine Learning and Security (98/100), Database Design and Implementation (95/100), Distributed Computing (94/100), Combinatorial Optimization (91/100), The C Programming Language (90/100), Computer Graphics (90/100).

Research Interests

My research focuses on providing fundamental understandings of **how Federated Learning (FL) is influenced by system-level variability in the computing infrastructure, and statistical variability in the training data, under adversarial settings**. Inspired by the theoretical or experimental insights, I seek to design system- and data-aware distributed/federated training algorithms that are byzantine-robust or superior in generalization performance. Specific research focuses are as follows:

Federated Learning [1, 2, 3, 4, 5, 6, 7, 8, 9]: Aim to build a FL system with endogenous safety and security.

Algorithm Robustness [1, 5, 6, 7, 8, 9]: Improve the reliability of FL algorithms in adversary environments.

Algorithm Performance [2, 3]: Design communication/computation-efficient FL algorithms with better model generalization.

Medical Image Analysis [4]: Improve the efficiency and precision of medical image segmentations.

In the future, I am committed to improving distributed/federated training algorithms that can seamlessly scale to a large number of computing nodes in realistic scenarios in terms of byzantine robustness, privacy preserving, communication/computation efficiency, and generalization performance.

Publication & Manuscripts

[1] **NDSS 2023,** UNDER REVIEW (passed the first round of review)**:**

Jianrong Lu; Shengshan Hu; Wei Wan; Minghui Li; Leo Yu Zhang; Xiaojing Ma; Hai Jin. ***"Shielding Federated Learning: Rectifying Direction Is All You Need"***. The Network and Distributed System Security Symposium (NDSS), 2023. Under review.

Note: This is my first paper which got one **"minor revision", three "major revisions"** and **one "rejection"** in the USENIX Security Symposium (USENIX Security).

[2] **WWW 2023,** IN PREPARATION (all experiments and parts of writings have been completed).

Jianrong Lu; Wei Wan; Shengshan Hu; Yutong Dai; Dezhong Yao; Lichao Sun; Leo Yu Zhang;

Hai Jin. ***"Rethinking the Optimization Objective in Federated Learning".*** Submitting to the Web Conference (formerly known as International World Wide Web Conference, abbreviated as WWW).

[3] **CVPR 2023,** IN PREPARATION (all experiments have been completed)**:**

Jianrong Lu; Wei Wan; Shengshan Hu; Leo Yu Zhang; Hai Jin. ***"Federated Heterogeneous Optimization without Strong Assumptions".*** Submitting to the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023.

[4] **MICCAI 2023,** IN PREPARATION (parts of experiments have been completed)**:**

Jianrong Lu; Longling Zhang, Wei Wan; Shengshan Hu; Leo Yu Zhang; Hai Jin. ***"Federated PET/CT Data Fusion and Auto-segmentation".*** Submitting to the International Conference on Medical Image Computing and Computer Assisted Intervention.

[5] **WCNC 2021,** ACCEPTED ([PDF])**:**

Wei Wan; **Jianrong Lu**; Shengshan Hu; Leo Yu Zhang; Xiaobing Pei . ***"Shielding Federated Learning: A New Attack Approach and Its Defense".*** Accepted by IEEE Wireless Communications and Networking Conference (WCNC), 2021.

[6] **IJCAI-ECAI 2022,** ACCEPTED (LONG oral presentation, acceptance rate 3% [PDF]) **:**

Wei Wan; Shengshan Hu; **Jianrong Lu**; Leo Yu Zhang. ***"Shielding Federated Learning: Robust Aggregation with Adaptive Client Selection".*** Accepted by the 31st International Joint Conference on Artificial Intelligence and the 25th European Conference on Artificial Intelligence (IJCAI-ECAI), 2022.

[7] **TrustCom 2022,** ACCEPTED ([PDF])**:**

Junyu Shi; Wei Wan; **Jianrong Lu**; Shengshan Hu; Leo Yu Zhang. ***"Challenges and Approaches for Mitigating Byzantine Attacks in Federated Learning".*** Accepted by IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2022.

[8] **MSN 2022,** UNDER REVIEW**:**

Minghui Li; Junyu Shi; Wei Wan; **Jianrong Lu**; Shengshan Hu; Leo Yu Zhang. ***"Shielding Federated Learning: Mitigating Byzantine Attacks with Less Constraints".*** International Conference on Mobility, Sensing and Networking (MSN), 2022.

[9] **AAAI 2023,** UNDER REVIEW**:**

Wei Wan; Shengshan Hu; Minghui Li; Leo Yu Zhang; **Jianrong Lu**; Yuanyuan He; Hai Jin. ***"Shielding Federated Learning: a Four-Pronged Defense against Byzantine Attacks".*** The Thirty-Seventh AAAI Conference on Artificial Intelligence (AAAI), 2023. Under review.

Miscellaneous Experience

Awards:

Second-class Academic Scholarship

Certification:

Fujian Computer Rank Examination (Level 2 C Programming Language) Excellent Certificate

Employment History:

Volunteer Teacher in Young Volunteers Association

Teaching Assistant, Teacher , and Compus Manager in iShow International English

Skills

Coding: Pytorch, Tensorflow, C, C++, Python, SQL, Markdown

Databases: Oracle

Misc.: Academic research, LATEX typesetting and publishing