Sun Jingwei

jingwei.sun@duke.edu
(919)-536-8835

EDUCATION

PhD student, Electrical and Computer Engineering, Duke University 2021-2025(estimated)
Advisor: Prof. Yiran Chen and Prof. Hai Li
Overall GPA: 4.0/4.0

MS, Electrical and Computer Engineering, Duke University 2019-2021
Overall GPA: 4.0/4.0

BE, Electronic Engineering, Wuhan University 2015-2019
Overall GPA: 3.7/4.0 In-major GPA: 3.8/4.0 In-major average grade: 90.01

RESEARCH INTERESTS

- Privacy-preserving and robust federated learning.
- Efficient federated learning.

SELECTED PUBLICATIONS

- **Sun, J.**, Li, A., Duan, L., Alam, S., Deng, X., Guo, X., Wang, H., Gorlatova, M., Zhang, M., Li, H., & Chen, Y. (2022). FedSEA: A Semi-Asynchronous Federated Learning Framework for Extremely Heterogeneous Devices. *ACM Conference on Embedded Networked Sensor Systems (SenSys2022).*
- Tang, M., Ning, X., Wang, Y., **Sun, J.**, Wang, Y., Li, H., & Chen, Y. (2022). FedCor: Correlation-Based Active Client Selection Strategy for Heterogeneous Federated Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR2022).*
- **Sun, J.**, Li, A., DiValentin, L., Hassanzadeh, A., Chen, Y., & Li, H. (2021). FL-WBC: Enhancing Robustness against Model Poisoning Attacks in Federated Learning from a Client Perspective. In *Advances in neural information processing systems (NeurIPS2021).*
- **Sun, J.**, Li, A., Wang, B., Yang, H., Li, H., & Chen, Y. (2021). Soteria: Provable Defense Against Privacy Leakage in Federated Learning From Representation Perspective. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR2021).*
- Li, A., **Sun, J.**, Li, P., Pu, Y., Li, H., & Chen, Y. (2021). Hermes: an efficient federated learning framework for heterogeneous mobile clients. *International Conference on Mobile Computing and Networking (MobiCom2021).*
- Li, A., **Sun, J.**, Zeng, X., Zhang, M., Li, H., & Chen, Y. (2021). FedMask: Joint Computation and Communication-Efficient Personalized Federated Learning via Heterogeneous Masking. *ACM Conference on Embedded Networked Sensor Systems (SenSys2021).*
- Li, A., **Sun, J.**, Wang, B., Lin, D., Li, S., Chen, Y., & Li, H. (2021). LotteryFL: Empower Edge Intelligence with Personalized and Communication-Efficient Federated Learning. *ACM/IEEE Symposium on Edge Computing (SEC2021).*

HONORS & AWARDS

- **Second Prize**, *China Undergraduate Mathematical Contest in Modeling, National Contest District*
- **Meritorious Winner** of Mathematical Contest in Modeling
- Outstanding Student of Wuhan University, academic year 2015 - 2016, 2016 – 2017, 2017-2018

SELECTED RESEARCH PROJECTS

Research on Privacy-preserving Federated Learning Systems
Supervised by Prof. Yiran Chen, Duke University

- Explicitly show the representation leakage from local updates uploaded by edge devices.
- Reveal that representation leakage is the essential cause of privacy leakage in FL.
- Propose a representation-based defense against model inversion attacks and provide a certified robustness guarantee.
- Paper published on CVPR2021.

Research on Robust Federated Learning Systems
Supervised by Prof. Hai Li, Duke University

- Show that strong model poisoning attacks cannot be defended by server-based defenses and will be long-lasting in the global model.
- Propose a quantitative estimator of poisoning attack effect on model parameters.
- Theoretically and experimentally show that the long-lasting attack effect reside in the kernels of Hessian metrices of local training.
- Propose a client-based defense called FL-WBC (White Blood Cells for Federated Learning) to mitigate the long-lasting attack effect in the global model by perturbing the kernels of Hessian metrices during local training.
- Paper to be appeared on NeurIPS2021.

Research on Computation & Communication-efficient Federated Learning Systems
Cooperating with Ang Li, Supervised by Prof. Yiran Chen, Duke University

- Improve the computation and communication efficiency of FL by assigning personalized subnetworks to clients through Lottery-Ticket-Hypothesis and structural pruning.
- Significantly improve the communication efficiency of FL further by applying trainable binary masks to fixed weights (theoretically 32 times of communicational cost reduction).
- Papers published on MobiCom2021, SenSys2021 and SEC2021.

PROFESSIONAL SKILLS

- Programming Language: Python, MATLAB, C/C++, JAVA, Verilog HDL
- Deep/machine learning framework: Pytorch, Keras, sklearn,Tensorflow
- Microprocessor IDE: Code Composer Studio, Keil, Quartus II