Federated Machine Learning in 6G: Opportunities and Challenges

(*half-day tutorial*)

1. Abstract

The availability of massive sensory dataset and high-performance computing and learning platforms shall make connected intelligence be a dominate feature in future 6G networks. Federated learning is a new revolutionary collaborative machine learning paradigm, which enables deep learning model training over a large volume of decentralized data residing in mobile devices without accessing clients' private data. In particular, implementing federated learning in wireless networks becomes critical for a plethora of exciting data-intensive applications in 6G, including internet of everything, autonomous vehicles, tactile internet, sustainable cities, and e-health. The aim of this tutorial is to present the recent advances in distributed optimization and wireless networking technologies for designing the wireless federated machine learning systems. Specifically, the over-the-air computation for low-latency, private and secure federated learning is presented by exploiting the waveform superposition property of a multi-access channel. The advanced wireless networking technologies, including reconfigurable intelligence surface and unmanned aerial vehicle, will be comprehensively investigated to further improve the performance and robustness of over-the-air federated learning system. The effective resource allocations strategies for single-server, hierarchical and decentralized federated learning systems shall be proposed to address the challenges including non-identical data distribution, high-dimensional model parameters, heterogeneous and limited resources. The capability of the joint learning and communication framework for making a low-latency and energy-efficient wireless federated learning system will be highlighted.

2. Intended audience

This tutorial shall provide timely materials in the field of federated learning in wireless networks. The academic researchers in the fields of machine learning, wireless communications, and signal processing, as well as the individuals from industry who concern the standardization, hardware, and software of federated edge learning, may feel strongly interested in this tutorial.

3. Objective and motivation

Federated learning becomes a key enabling technology for the paradigm shift from "connected things" to "connected intelligence" in 6G. In this tutorial, we shall introduce various communication-efficient distributed federated learning algorithms with privacy and security guarantees, including zero-order, first-order, second-order algorithms. For over-the-air federated learning systems, the convergence analysis, transceiver design and channel estimation methods will be provided to achieve the low-latency, privacy and security in the learning process. For digital communication protocols enabled federated learning, a special attention will be paid on the resource allocations under various constraints such as the stringent

computation, power, bandwidth, storage, and privacy guarantees. In particular, a novel joint learning-communication framework will be presented to minimize the latency and power consumption in the wireless federated learning system.

4. Detailed outline of the tutorial

In this tutorial, we shall introduce the system design for the over-the-air federated learning as well as the resource allocation strategies for wireless federated learning systems.

Tentative Schedule:

- ***Fundamentals of Federated Learning***
  This part first provides an overview of various types of federated learning models, followed by various communication-efficient distributed and decentralized optimization algorithms with privacy and security guarantees. Two promising types of algorithms will be presented: 1) federated averaging algorithm with convergence guarantees; 2) decentralized learning algorithm with model consensus

- ***Federated Machine Learning via Over-the-Air Computation***
  We present various federated learning algorithms with emphasizing the model aggregation components via the principles of over-the-air computation, including federated averaging, multi-task learning, differential privacy, Byzantine-resilient federated learning. The challenges and solutions will be provided, including the device scheduling, transceiver design, local computation allocation and symbol-level synchronization. The promising wireless networking technologies will be also demonstrated, e.g., reconfigurable intelligent surface and unmanned aerial vehicle.

- ***Delay Analysis and Resource Allocation in Wireless Federated Learning Systems***
  Due to the randomness of channel fading and high-dimensionality of model parameters, it is challenging to derive the overall transmission delay of federated learning over wireless fading channels. On the one hand, this part shall present a unified delay analysis framework, where both the synchronous and asynchronous downlink transmissions are considered. We shall present a novel way to analyze the empirical distribution of the overall transmission delay. On the other hand, to address the challenges including non-identical data distribution, high-dimensional model parameters, and limited resources, the problem formulations for federated learning under different network architectures with different objectives, including energy efficiency maximization, transmission delay minimization, and training loss minimization, will be presented. The challenges and solutions to these problems will be discussed, including the joint optimization of the device scheduling, transmit power, channel allocation, computation frequency, and learning accuracy. The design insights obtained from the theoretical analysis and resource optimization will be discussed.

- ***Conclusions***

We conclude this tutorial by summarizing the insights and guidelines on applying advanced optimization and wireless networking technologies for designing the low-latency, private and secure federated learning system in 6G.

5. Speaker

Yuanming Shi, Associate Professor, ShanghaiTech University, Shanghai, China

Email: shiym@shanghaitech.edu.cn
Address: Room C-403.C, SIST Building 1, 393 Middle Huaxia Road, Pudong District, Shanghai 201210, China

Bio: Yuanming Shi received the B.S. degree in electronic engineering from Tsinghua University, Beijing, China, in 2011. He received the Ph.D. degree in electronic and computer engineering from The Hong Kong University of Science and Technology (HKUST), in 2015. Since September 2015, he has been with the School of Information Science and Technology in ShanghaiTech University, where he is currently a tenured Associate Professor. He visited University of California, Berkeley, CA, USA, from October 2016 to February 2017. Dr. Shi is a recipient of the 2016 IEEE Marconi Prize Paper Award in Wireless Communications, and the 2016 Young Author Best Paper Award by the IEEE Signal Processing Society. He is an editor of IEEE Transactions on Wireless Communications and IEEE Journal on Selected Areas in Communications. His research areas include optimization, statistics, machine learning, signal processing, and their applications to 6G, IoT, and AI.

Yong Zhou, Assistant Professor, ShanghaiTech University, Shanghai, China

Email: zhouyong@shanghaitech.edu.cn
Address: Room A-404.C, SIST Building 1, 393 Middle Huaxia Road, Pudong District, Shanghai 201210, China

Bio: Dr. Yong Zhou is currently an assistant professor at the School of Information Science and Technology at ShanghaiTech University. From 2015 to 2017, he worked as a Post-Doctoral Research Fellow in the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada. He received the PhD degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2015. He received the B.Sc. and M.Eng. degrees from the School of Information Science and Engineering, Shandong University, Jinan, China, in 2008 and 2011, respectively. His research areas include Internet of Things, federated learning, and reconfigurable intelligent surface.

6. A brief description (up to 1 page) of the technical issues that the tutorial will address, emphasizing its timeliness

This tutorial consists of three vignettes. The first involves mathematics of federated learning with emphasizing the learning models and algorithms with provable performance guarantees. We shall present various optimization algorithms to address the unique challenges in federated learning, e.g., communication bottlenecks, non-iid data, objective inconsistency, differential privacy and Byzantine attacks. The promising algorithms include federated averaging algorithm, federated split algorithm, sign gradient descent method, and decentralized federated algorithm.

The second vignette is federated learning based on the over-the-air computation. The high-dimensional model parameter of federated learning brings a unique challenge for designing the communication-efficient wireless federated learning systems. To address this challenge, we first present the principles of over-the-computation for fast model aggregation in federated learning by exploiting the waveform superposition property of a multi-access channel. The differential privacy and Byzantine-resilient over-the-air federated learning system will be also developed with convergence analysis and optimization. This is achieved by the joint design of the device scheduling, transceiver design, local computation allocation and symbol-level synchronization. The promising wireless networking technologies will be also demonstrated, e.g., reconfigurable intelligent surface and unmanned aerial vehicle, by reconfiguring the radio environments.

The third vignette is federated learning based on digital communication protocols. To theoretically analyse the convergence time of federated learning over wireless networks, including both the uplink model aggregation time and the downlink model dissemination time, is challenging due to the following reasons. First, due to the high-dimensionality of the model parameters, the transmission time of each training model in both the uplink and downlink can be much longer than the channel coherence time and thus its distribution depends on multiple random variables. Second, due to the randomness of channel fading, the uplink transmission delays of different users are not necessarily aligned. We will introduce a unified framework to analyse the approximate delay distribution of federated learning over arbitrary fading channels by utilizing tools from saddle point approximation. Moreover, address the challenges including non-identical data distribution, high-dimensional model parameters, and limited resources, it is necessary to jointly optimize the communication and computation resources. Energy-efficient and delay-aware federated learning systems need to be developed and optimized. This can be achieved by jointly optimizing the device scheduling, transmit power, channel allocation, computation frequency, and learning accuracy.

7. Prior history of the tutorial presentations

The speaker has been working on large-scale and distributed optimization for more than 8 years, with published results covering various aspects, including different problem models, algorithm design, and theoretical analysis for wireless communications and machine learning. In particular, the speaker gave tutorials on sparse and low-rank optimization with applications in dense wireless networks at Globecom 2017 titled “Sparse and Low-Rank Optimization for Dense Wireless Networks: Models, Algorithms, and Theory”, and at ICCC 2018 titled “Generalized Sparse and Low-Rank Optimization for Ultra-Dense Networks: Models,

Algorithms and Theory". The speaker will also give the tutorial titled "Mobile Edge Artificial Intelligence: Opportunities and Challenges" at Globecom 2019.

This tutorial instead focuses on novel applications on large-scale and distributed optimization techniques for designing federated machine learning in wireless networks, with emphasizing on novel system models, performance metrics, optimization algorithms and theoretical analysis.

Representative Publications:

- K. Yang, T. Jiang, Y. Shi, and Z. Ding, "Federated learning via over-the-air computation," *IEEE Trans. Wireless Commun.,* vol. 19, no. 3, pp. 2022-2035, Mar. 2020.
- K. Yang, Y. Shi, Y. Zhou, Z. Yang, L. Fu, and W. Chen, "Federated machine learning for intelligent IoT via reconfigurable intelligent surface," *IEEE Netw.,* vol. 34, no. 5, pp. 16-22, Oct. 2020.
- Z. Wang, J. Qiu, Y. Zhou, Y. Shi, L. Fu, W. Chen, and K. B. Lataief, "Federated learning via intelligent reflecting surface," https://arxiv.org/abs/2011.05051, 2020.
- K. Yang, Y. Zhou, Z. Yang, and Y. Shi, "Communication-efficient edge AI inference over wireless networks," *ZTE Commun.,* vol. 18, no. 2, pp. 31-39, Jun. 2020.
- L. Li, L. Yang, X. Guo, Y. Shi, H. Wang, W. Chen, and K. B. Letaief, "Delay analysis of wireless federated learning based on saddle point approximation and large deviation theory," submitted to JSAC, 2021.
- Z. Wang, Y. Shi, Y. Zhou, H. Zhou, and N. Zhang, "Wireless-powered over-the-air computation in intelligent reflecting surface aided IoT networks," *IEEE Internet of Things J.*, vol. 8, no. 3, pp. 1585-1598, Feb. 2021.
- J. Dong, Y. Shi, and Z. Ding, "Blind over-the-air computation and data fusion via provable Wirtinger flow," *IEEE Trans. Signal Process.*,vol. 68, pp. 1136-1151, Feb. 2020.
- Y. Shen, Y. Shi, J. Zhang, and K. B. Letaief, "LORM: Learning to optimize for resource management in wireless networks with few training samples," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 665-679, Jan. 2020.
- Y. Yang, Y. Zhou, T. Wang, and Y. Shi, "Reconfigurable Intelligent Surface Assisted Federated Learning with Privacy Guarantee," *in Proc. IEEE ICC Workshop*, Jun. 2021.
- S. Huang, Y. Zhou, T. Wang, and Y. Shi, "Byzantine-Resilient Federated Machine Learning via Over-the-Air Computation," *in Proc. IEEE ICC Workshop*, Jun. 2021.
- S. Xia, J. Zhu, Y. Yang, Y. Zhou, Y. Shi, and W. Chen, "Fast Convergence Algorithm for Analog Federated Learning," *in Proc. IEEE ICC*, Jun. 2021.