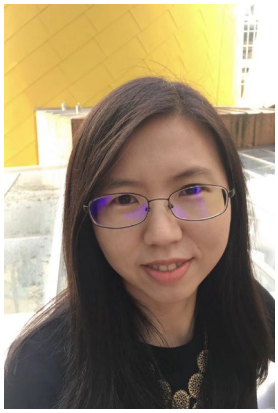
ELECTRICAL AND COMPUTER ENGINEERING SEMINAR



Lili Su
MIT

Learning with Distributed Systems: Adversary-Resilience and Neural Networks

Wednesday, February 26th

ISEC 138

11:00am- 12:00pm

Abstract: In this talk, Su will first talk about how to secure Federated Learning (FL) against adversarial faults.
FL is a new distributed learning paradigm proposed by Google. The goal of FL is to enable the cloud (i.e., the learner) to train a model without collecting the training data from users' mobile devices. Compared with traditional learning, FL suffers serious security issues and several practical constraints call for new security strategies. Towards quantitative and systematic insights into the impacts of those security issues, Su and her team formulated and studied the problem of Byzantine-resilient Federated Learning. Su proposed two robust learning rules that secure gradient descent against Byzantine faults. The estimation error achieved under our more recently proposed rule is order-optimal in the minimax sense. Then, she will briefly talk about her recent results on neural networks, including both biological and artificial neural networks. Notably, her results on the artificial neural networks (i.e., training over-parameterized 2-layer neural networks) improved the state-of-the-art. In particular, they showed that nearly-linear network over-parameterization is sufficient for the global convergence of gradient descent.

Bio:

Lili Su is a postdoc in the Computer Science and Artificial Intelligence Laboratory (CSAIL) at MIT, hosted by Professor Nancy Lynch. She received a Ph.D. in Electrical and Computer Engineering from the University of Illinois at Urbana-Champaign in 2017, supervised by Professor Nitin H. Vaidya. Her research intersects distributed systems, learning, security, and brain computing. She was the runner-up for the Best Student Paper Award at DISC 2016, and she received the 2015 Best Student Paper Award at SSS 2015. She received UIUC's Sundaram Seshu International Student Fellowship for 2016, and was invited to participate in Rising Stars in EECS (2018). She has served on TPC for several conferences including ICDCS and ICDCN