Abstract for Presentation

Title: Byzantine Attacks and Defenses in Federated Learning

Presenter: Shenghui Li

Abstract:
Federated learning (FL) enables distributed training across a set of clients, without requiring any of the participants to reveal their private training data to a centralized entity or each other. Due to decentralized execution, federated learning is vulnerable to attacks from adversarial (Byzantine) clients by modifying the local updates to their desires. Therefore, it is essential to develop robust federated learning algorithms that can defend Byzantine clients without losing model convergence and performance. In this presentation, we provide an overview of Byzantine attack and defense techniques during federated optimization, discussing both the existing defenses and their limitations. Additionally, we explore some factors that may impact the effectiveness of these attacks and defenses, highlighting open research challenges in this field.