S05-4 (02/16 10:10-10:35)

Robust Aggregation for Federated Learning

Su-Yun Huang
Institute of Statistical Science, Academia Sinica, Taipei, Taiwan

Abstract

Federated learning is a framework for multiple devices or institutions, called local clients, to collaboratively train a global model without sharing their data. For federated learning with a central server, an aggregation algorithm integrates model information sent from local clients to update the parameters for a global model. Federated average is the simplest and most commonly used aggregation method. However, it is not robust for data with outliers or under the Byzantine problem, where Byzantine clients send malicious messages to interfere with the learning process. Some robust aggregation methods were introduced in literature including marginal median, geometric median and trimmed-mean. In this talk, we propose an alternative robust aggregation method, named gamma-mean, which is the minimum divergence estimation based on a robust density power divergence. This gamma-mean aggregation mitigates the influence of Byzantine clients by assigning less weights. This weighting scheme is data-driven and controlled by a tuning parameter. Numerical examples including image classification and segmentation using deep neural networks are presented. This is a joint work with Pin-Han Huang, Cen-Jhih Li, Yi-Ting Ma and Hung Hung.

Keywords:
Byzantine Problem; Deep Learning; Federated Learning; Gamma Divergence; Robustness.