Towards Fault-Tolerant Federated and Distributed Machine Learning

Sanmi Koyejo

Stanford University
sanmi@cs.stanford.edu

Abstract

Machine learning (ML) models are routinely trained and deployed among distributed devices, e.g., learning with geo-distributed data centers and federated learning with mobile devices. Such shared computing platforms are susceptible to hardware, software, communication errors, and security concerns. This talk will outline some of the threat models in distributed learning, along with robust learning methods proposed to augment the fault tolerance of distributed machine learning, showing both theoretical and empirical evidence of robustness to benign and adversarial attacks.

Copyright © 2024, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.