Statistics Seminar

Department of Mathematical Sciences

DATE:	Thursday, March 28, 2019
TIME:	1:15pm – 2:15pm
LOCATION:	WH 100E
SPEAKER:	Waheed U. Bajwa, Rutgers University
TITLE:	Adversarially resilient machine learning in fully distributed environments

Abstract

Distributed machine learning algorithms enable processing of datasets that are distributed over a network without gathering the data at a centralized location. While efficient distributed algorithms have been developed under the assumption of faultless networks, failures that can render these algorithms nonfunctional indeed happen in the real world. In this talk, we focus on the problem of Byzantine failures, which are the hardest to safeguard against in distributed algorithms. While Byzantine fault tolerance has a rich history, existing work does not translate into efficient and practical algorithms for high-dimensional distributed learning tasks. In this talk, we discuss the theoretical characteristics and experimental performance of a few Byzantine-resilient algorithms that have been developed in our lab for high-dimensional distributed machine learning in fault-prone networks. In particular, we show that a single Byzantine node in the network can lead to failures of most state-of-the-art distributed learning algorithms; in contrast, our developed algorithms are capable of handling multiple Byzantine failures in the network without noticeable reduction in performance.