Federated Learning with Differential Privacy: An Online Mirror Descent Approach

Olusola Odeyomi
Faculty: Gergely Záruba
Department of Electrical Engineering and Computer Science, College of Engineering

Federated learning is a machine learning paradigm that provides privacy to the local data of multiple clients communicating with a central server. Federated learning has successfully been applied in natural language processing, vehicle-to-vehicle communication, social networks, healthcare predictions through medical collaborations, wireless sensor networks etc. Although federated learning has gained much research attention in recent times, there are still some open problems. Existing research work assumes that the training data of the clients are time invariant. This assumption does not hold in real-time traffic monitoring, where events occur randomly. Thus, an online learning approach must be introduced into federated learning algorithms to capture the randomness of the clients' training data. Another open problem is improving communication and computations by removing the central server in the federated learning design. More so, the model updates at the central server may be prone to adversarial attacks. Such adversarial attacks may put the clients' local data in a potential privacy risk. Lastly, the stochastic gradient algorithms commonly used for federated learning do not fully exploit the convexity of the loss functions of the clients. This work proposes an online mirror descent learning algorithm that can handle time-varying data in a decentralized federated learning setting. To provide additional privacy, local differential privacy is introduced to the setting. The convergence of the proposed algorithm is compared to some state-of-the-art federated learning algorithms. The proposed algorithm shows to converge faster to the global model for all the clients.