Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

Resilient Over-the-Air Computation with Applications in Federated Learning

Novel use cases for mobile communication networks include the aggregation of large amounts of data, which is stored in a distributed manner across network users. For instance, Federated Learning requires the aggregation of machine learning model updates from contributing users.

Over-the-Air (OtA) computation is an approach with the potential to drastically reduce the communication overhead of wireless distributed data-processing systems (e.g. Federated Learning). It exploits the multiple-access property and linearity of the wireless channel to compute sums of pre-processed data by the channel. This important property at the same time opens great opportunities for adversaries to corrupt the computation process. Therefore, Increasing the resiliency of OtA computation systems against adversaries is important.

Several solutions [1-4] have been proposed to tackle this problem, which make different assumptions and impose different constraints on the system. These solutions shall be evaluated and compared, theoretically as well as empirically by a simple Federated Learning implementation.

[1] X. Fan, Y. Wang, Y. Huo, and Z. Tian, “BEV-SGD: Best Effort Voting SGD Against Byzantine Attacks for Analog-Aggregation-Based Federated Learning Over the Air,” IEEE Internet of Things Journal, vol. 9, no. 19, pp. 18946–18959, Oct. 2022.

[2] S. Park and W. Choi, “Byzantine Fault Tolerant Distributed Stochastic Gradient Descent Based on Over-the-Air Computation,” IEEE Transactions on Communications, vol. 70, no. 5, pp. 3204–3219, May 2022,

[3] S. Huang, Y. Zhou, T. Wang, and Y. Shi, “Byzantine-Resilient Federated Machine Learning via Over-the-Air Computation,” arXiv:2105.10883 [cs, math], May 2021, Accessed: Dec. 21, 2021

[4] H. Sifaou and G. Y. Li, “Robust Federated Learning via Over-the-Air Computation,” in 2022 IEEE 32nd International Workshop on Machine Learning for Signal Processing (MLSP), Aug. 2022.

Prerequisites

- knowledge in statistics and estimation theory
- basic knowledge of machine learning with Tensorflow

Advisors

Luis Maßny