EPFL-Inria
INTERNATIONAL LAB

EPFL Inria

Workshop EPFL-Inria
November 23 and 24, 2023, Lyon

Rafael Pires, EPFL

Title: « Low-cost Privacy-aware Decentralized Learning »

Abstract:
Decentralized learning represents an innovative paradigm in which distributed nodes collaborate by exchanging models, while preserving the confidentiality of their local training data. Despite offering better privacy protection compared to data sharing, models remain vulnerable to revealing sensitive information under adversarial attacks. To address this concern, solutions such as private averaging and differential privacy have been proposed. However, they incur a significant communication overhead or compromised utility.
In this paper, we introduce a novel lightweight algorithm, ZEROSUM, that employs noise addition to each model during the exchange process. This approach strategically correlates the noise injected into models sent to different nodes, leading to eventual self-cancellation. Our experimental study using threshold-based membership inference attacks indicates that ZEROSUM achieves the best trade-off between vulnerability and accuracy across distinct datasets. Furthermore, it reduces the communication cost by factors ranging from 3× to 38× compared to other methods. The effectiveness of ZEROSUM establishes it as a compelling choice for privacy-aware decentralized learning.