Secure Aggregation Meets Sparsification in Decentralized Learning

Sayan Biswas, Anne-Marie Kermarrec, Rafael Pires, Rishi Sharma, Milos Vujasinovic

Motivation

Secure aggregation [1]:

- Adds communication overhead
- Makes compression hard
- Is not compatible with sparsification out of box

Privacy at the cost of communication overhead

Pairwise additive masking

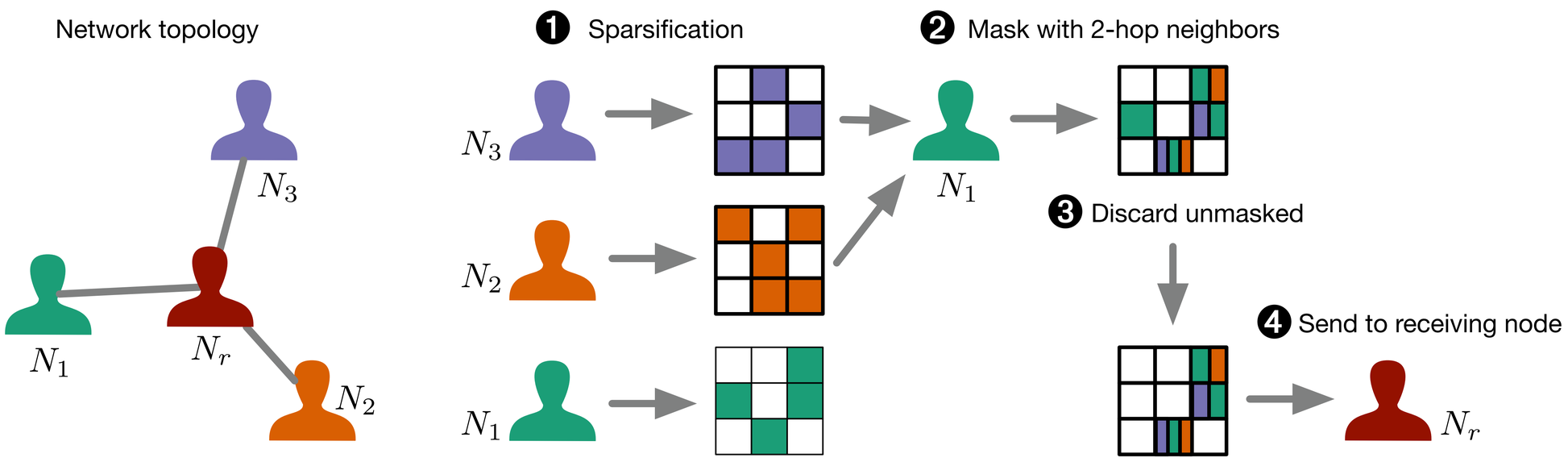
For $\forall a, b \in \mathbb{R}$ and $\forall c \in \mathbb{R}$:

$$a + b = (a + c) + (b - c)$$

Adding and subtracting a randomly selected number from a sum does not change its value

CESAR

Overview



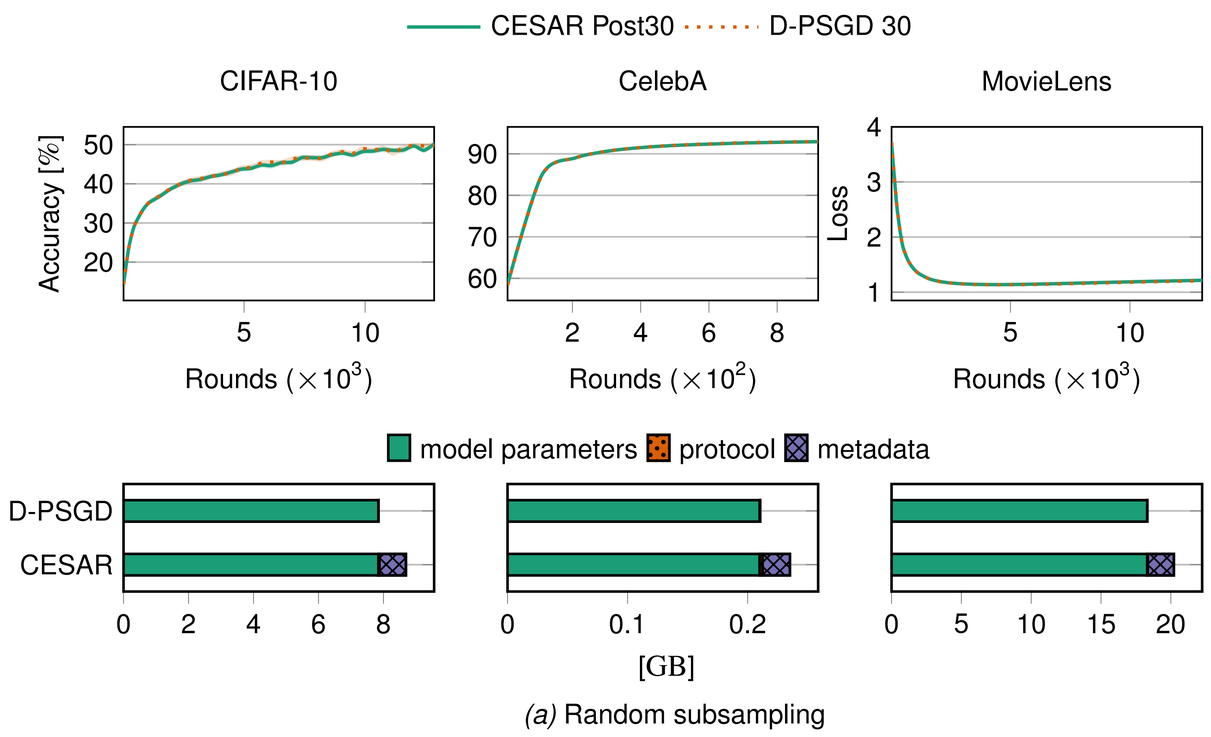
Algorithm

- Performed after sparsification
- Performed in two stages:
  - **Prestep**: Second degree neighbours coordinate to mask mutually selected indices before sending them to the common neighbor
  - **Model exchange and aggregation**: Indices with less than s masks applied are discarded before transmitting the model (s called *masking requirement*)
- Masks cancel out upon plain averaging

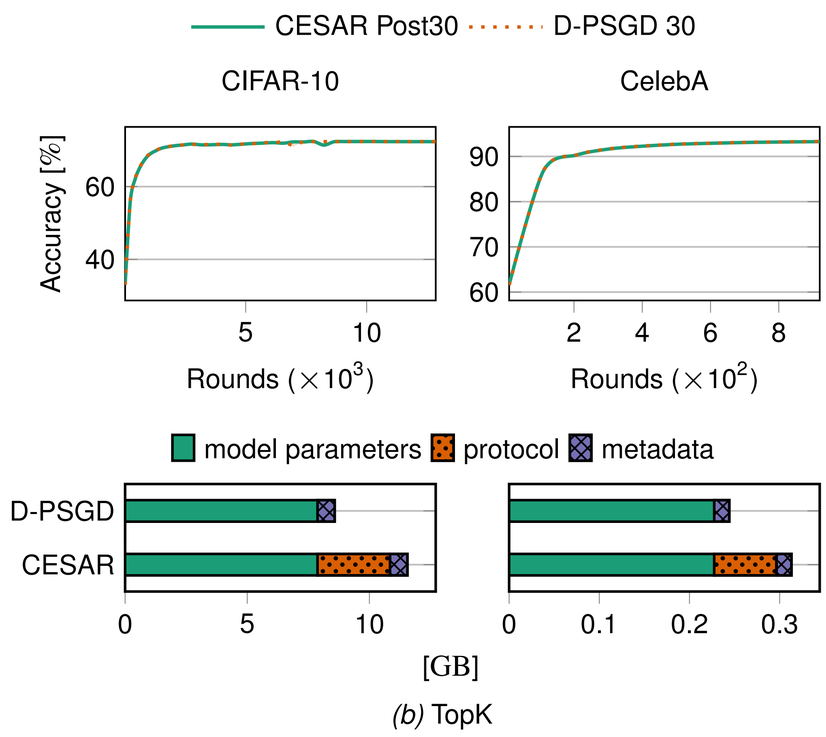
Properties

1. **Privacy guarantees**:
   - CESAR is resilient against **honest-but-curious adversaries**
   - CESAR is resilient against **collusion**
2. **Communication overhead**:
   - Prestep (protocol overhead): $O(\alpha d \delta_{\text{max}}^2)$ (α - percentage of selected parameters; d - total number of parameters; δ_{max} - maximum degree in the network)

Evaluation



(a) Random subsampling



(b) TopK

Evaluation setting

- Datasets: CIFAR, CelebA, MovieLens
- Baseline: D-PSGD [2]
- Masking requirement (s): 1
- Data distribution: IID with TopK, NIID with random subsampling
- Network size: 96 nodes
- Topology: 6-regular

[1] Keith Bonawitz et al. "Practical secure aggregation for privacy-preserving machine learning". In: *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 1175–1191.

[2] Lin Xiao and Stephen Boyd. "Fast linear iterations for distributed averaging". In: *Systems & Control Letters* 53.1 (2004), pp. 65–78. ISSN: 0167-6911. DOI: 10.1016/j.sysconle.2004.02.022.