FedTrans: Client-Transparent Utility Estimation for Robust Federated Learning

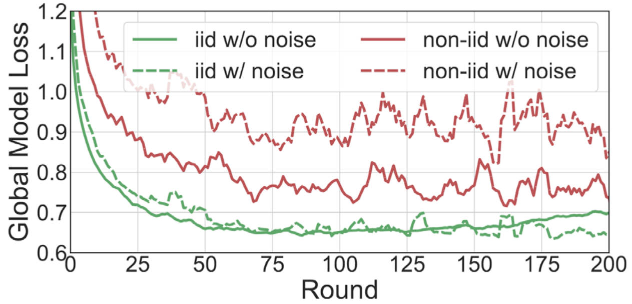
Mingkun Yang*, Ran Zhu*, Qing Wang, Jie Yang

TU Delft — Delft University of Technology · HarmonicAI

Project · Paper · ICLR

MOTIVATION

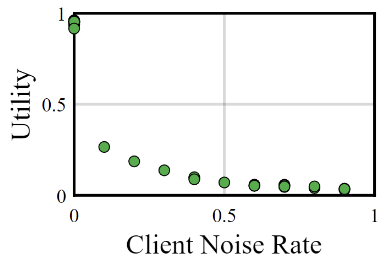
Client Utility The **quality of local labels/data** has significant impacts on the performance of global model. We define such impacts as client utility.



Client-Transparent Estimation

Ideally, inference of client utility should be

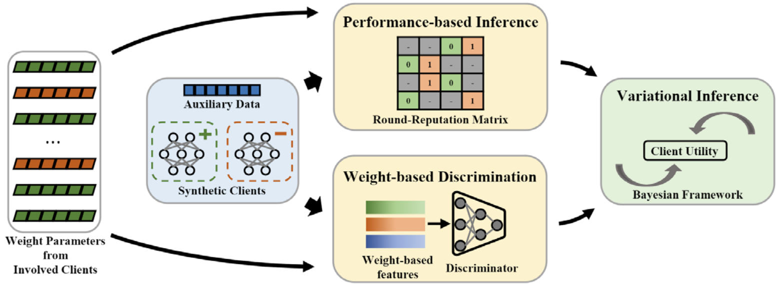
- **Transparent:** no additional client-side operations;
- **Indicative:** inversely proportional to the actual noise level.



FedTrans allows to:

- maintain the **same level of privacy guarantee** as other SOTA frameworks;
- guide **client selection** for global model aggregation by selecting clients with optimal utilities.

METHOD

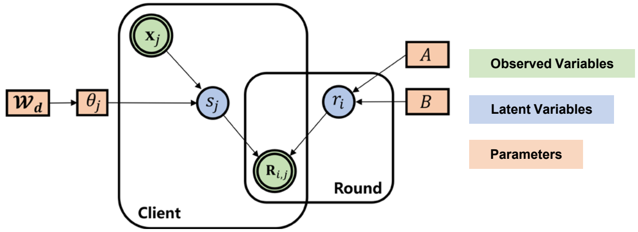


We use **auxiliary data (at the central server)** to infer client utility by fusing two kinds of information: local model performance and weights.

Intuition	Approach	Challenges
Performance-based	Round-reputation Matrix	Not fully reliable
Weight-based	Discriminator	Lack of labels

Bayesian Inference

We proposed a unified **Bayesian framework** and apply a **Variational Inference** algorithm to update the parameters.



Discriminator

$$s_j \sim Ber(\theta_j) = Ber(f^{w_d}(x_j))$$

Round Informativeness

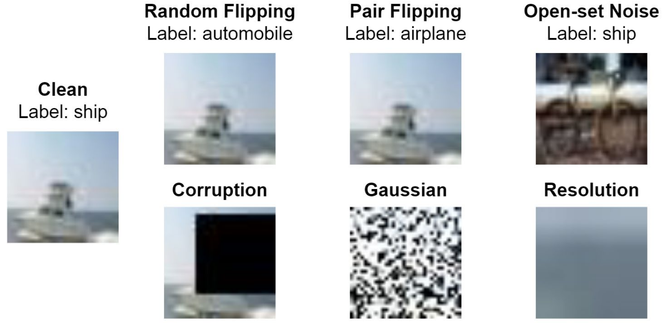
$$r_j \sim Beta(\alpha_j, \beta_j)$$

Round-Reputation Matrix

$$p(\boldsymbol{R}_{i,j}|s_j, r_j) = r_j^{\mathbb{1}(s_j=\boldsymbol{R}_{i,j})} + (1-r_j)^{\mathbb{1}(s_j\neq\boldsymbol{R}_{i,j})}$$

EVALUATION

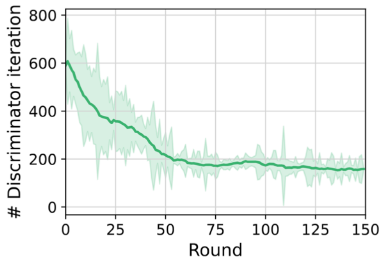
We construct the local noise in both **label** and **feature** space.



Setup CIFAR10 in Dirichlet distribution with 30% noisy clients; auxiliary dataset contains **200 samples** randomly selected from test set.

	Hybrid (*intra-*)	**Label** (*intra-*)	**Image** (*intra-*)
FedAvg (McMahan et al., 2017)	68.3% ± 0.6%	66.4% ± 0.3%	69.2% ± 2.4%
FLDebugger (Li et al., 2021)	64.3% ± 0.3%	61.2% ± 0.4%	66.1% ± 0.5%
Oort (Lai et al., 2021)	56.2% ± 0.3%	56.8% ± 0.8%	65.8% ± 0.0%
Robust-FL (Yang et al., 2022b)	70.6% ± 0.8%	73.4% ± 0.4%	70.8% ± 0.1%
RHFL (Fang & Ye, 2022)	70.1% ± 0.1%	68.8% ± 0.4%	73.0% ± 0.1%
DivFL (Balakrishnan et al., 2022)	70.1% ± 1.0%	70.7% ± 0.3%	72.7% ± 0.6%
FedCorr (Xu et al., 2022)	73.7% ± 0.4%	**75.7% ± 0.1%**	73.7% ± 0.6%
Fine-tuned DivFL	70.6% ± 0.4%	68.7% ± 0.2%	70.0% ± 0.4%
Fine-tuned FedCorr	68.2% ± 0.2%	69.2% ± 0.3%	67.0% ± 0.2%
FedTrans	**76.9% ± 0.3%**	**75.7% ± 0.4%**	**77.0% ± 0.2%**

- ***Top-1* accuracy:** global model of FedTrans consistently outperforms other baselines in all noise settings.
- **Auxiliary data efficiency:** FedTrans exploits it in a more efficient way than simply fine-tuning the global model.



Overheads

The overall optimization time **significantly decreases** as FL proceeds with diminishing discriminator iterations.