Collaboratively Learning Federated Models from Noisy Decentralized Data

Haoyuan Li[1][0009−0000−1237−3013], Mathias Funk[1][0000−0001−5877−2802], Nezihe Merve Gürel[2][0000−0002−4747−2406], and Aaqib Saeed[1][0000−0003−1473−0322]

[1] Eindhoven University of Technology, Eindhoven, Netherlands {h.y.li, m.funk, a.saeed}@tue.nl

[2] Delft University of Technology, Delft, Netherlands n.m.gurel@tudelft.nl

Abstract. Federated learning (FL) enables collaborative training of machine learning models using decentralized data from edge devices. However, ensuring data quality from local clients remains a critical challenge, as local data are often corrupted by noise and perturbations, compromising the aggregation process and degrading the global model. In this work, we assess client inputs in the gradient space, inspired by the disparity between gradient norm distributions from models trained on noisy versus clean data. We propose a noise-aware FL aggregation method, namely **Fed**erated **N**oise-**S**ifting (FedNS), which can be used as a plug-in approach with widely used FL strategies. Our method effortlessly integrates with existing FL strategies, enhancing the global model's performance by up to 13.68% in IID and 15.85% in non-IID settings when learning from noisy decentralized data.

Keywords: federated learning · data-centric AI · data quality.

1 Introduction

Recent advances in machine learning (ML) have led to a surge in data generated by edge devices. Federated learning (FL) is gaining traction as a distributed, privacy-preserving paradigm in decentralized ML [3, 5]. However, data quality remains a primary challenge, directly impacting ML model performance and reliability. Compromised data quality leads to data incompleteness, feature corruption, and label inconsistency [1]. Maintaining high-quality data is particularly challenging in FL due to its decentralized nature and the server's lack of access to client data, which, while addressing privacy and IP concerns, increases difficulty in ensuring data quality. Using edge devices for FL is a double-edged sword: large amounts of data can be harvested but often entail significant noise contamination. In tasks like object detection, data collected from image sensors are susceptible to visual distortions due to clients' lack of technical expertise or environmental interference [2]. In this work, we focus on the problem of noisy input data, where client features are (non-maliciously) corrupted. Our findings show that our proposed method effortlessly integrates and works well with existing

Table 1: Comparison of average accuracy across three independent runs for different datasets under clean and noisy client data scenarios. For the noisy data scenario, we consider 5 clean clients and 15 noisy clients with 100% noise level. Models are trained with FedAvg.

Data	CIFAR10		CIFAR100		PathMNIST		FMNIST		EuroSAT		Tiny-ImageNet	
	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID
Clean	90.14%	85.52%	64.79%	62.36%	87.74%	82.55%	92.34%	89.37%	94.72%	95.12%	53.26%	52.88%
Noisy	78.62%	73.51%	44.58%	42.10%	54.80%	52.14%	88.14%	84.67%	67.39%	75.06%	24.32%	22.90%

Table 2: Comparison of top-1 accuracy across datasets in IID and Non-IID settings. We evaluate the performance of FedNS with various federated aggregation methods for learning under the noisy environment.

Methods	CIFAR-10		CIFAR-100		PathMNIST		FMNIST		EuroSAT		Tiny-ImageNet	
	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID	IID	Non-IID
FedAvg[5]	78.62%	73.51%	44.58%	42.10%	54.80%	52.14%	88.14%	84.67%	67.39%	75.06%	24.32%	22.90%
+ NS (Ours)	**81.67%**	**78.44%**	**48.14%**	**45.94%**	**63.89%**	**62.92%**	**89.61%**	**88.53%**	**78.22%**	**80.12%**	**27.85%**	**25.93%**
FedProx[4]	79.89%	78.13%	46.75%	45.17%	57.28%	56.27%	87.15%	86.96%	70.83%	76.64%	24.90%	23.76%
+ NS (Ours)	**82.31%**	**81.18%**	**48.27%**	**46.80%**	**60.18%**	**63.11%**	**89.12%**	**87.48%**	**76.94%**	**81.20%**	**26.48%**	**25.98%**
FedTrimmedAvg[7]	78.92%	77.24%	41.81%	41.25%	56.34%	54.50%	90.09%	89.95%	68.30%	74.39%	16.97%	15.48%
+ NS (Ours)	**82.63%**	**82.47%**	**49.11%**	**48.32%**	**64.27%**	**63.04%**	**90.29%**	**91.57%**	**83.81%**	**80.50%**	**29.43%**	**27.46%**
FedNova[6]	81.45%	82.16%	49.48%	48.24%	55.36%	51.04%	**90.65%**	89.68%	73.54%	66.29%	28.62%	27.24%
+ NS (Ours)	**88.65%**	**88.34%**	**59.19%**	**59.17%**	**80.82%**	**81.89%**	90.57%	**91.50%**	**93.31%**	**92.70%**	**48.50%**	**46.16%**

FL aggregation strategies, such as FedAvg [5], FedProx [4], FedTrimmedAvg [7], and FedNova [6], which makes it widely applicable.

2 Experiment

Participation of noisy clients deteriorates the performance of the global model. We first conduct an experiment for model training with clean and noisy input across all the datasets and utilize the same noise configuration. With this, we aim to evaluate the upper-bound performance that can be achieved when learning from a mixture of noisy and clean clients. Table 1 presents the comparative results of average accuracy for all considered datasets. We focus on distortions due to their significant impact on degrading the model's generalization capability. We see the participation of noisy clients leads to a significant degradation in the model's generalization capability across all tasks, indicating the detrimental impact of noisy data in the FL environment.

FedNS significantly improves standard federated aggregation methods. We investigate the robustness of our proposed method by applying `FedNS` on six image datasets with different settings under the noisy scenario. As shown in Table 2, the performance of all aggregation methods exhibits a general trend of improvement by simply plugging FedNS into the considered strategies. In particular, we consider the worst-case with heterogeneous data setting in Table 2, where 15 out of 20 noisy clients participate in the federated training with high noise severity and 100% noise level. Adding `FedNS` to FL strategies yields better overall performance among all the datasets, especially for some vulnerable datasets (e.g., Path-MNIST) that are sensitive to data corruption.

References

1. Budach, L., Feuerpfeil, M., Ihde, N., Nathansen, A., Noack, N., Patzlaff, H., Naumann, F., Harmouch, H.: The effects of data quality on machine learning performance. arXiv preprint arXiv:2207.14529 (2022)
2. Dodge, S., Karam, L.: A study and comparison of human and deep learning recognition performance under visual distortions. In: 2017 26th international conference on computer communication and networks (ICCCN). IEEE (2017)
3. Konečnỳ, J., McMahan, H.B., Yu, F.X., Richtárik, P., Suresh, A.T., Bacon, D.: Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492 (2016)
4. Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A., Smith, V.: Federated optimization in heterogeneous networks. Proceedings of Machine learning and systems (2020)
5. McMahan, B., Moore, E., Ramage, D., Hampson, S., y Arcas, B.A.: Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics. PMLR (2017)
6. Wang, J., Liu, Q., Liang, H., Joshi, G., Poor, H.V.: Tackling the objective inconsistency problem in heterogeneous federated optimization. Advances in neural information processing systems (2020)
7. Yin, D., Chen, Y., Kannan, R., Bartlett, P.: Byzantine-robust distributed learning: Towards optimal statistical rates. In: International Conference on Machine Learning. Pmlr (2018)