天津大學
Tianjin University

Machine Learning & Data Mining Lab

Reliable and Interpretable Personalized Federated Learning

Zixuan Qin, Liu Yang*, Qilong Wang, Yahong Han, Qinghua Hu

9336

THU-AM-375

Zixuan Qin

Jun 23, 2023

Outline

1 **Overview of work**

2 Background and significance

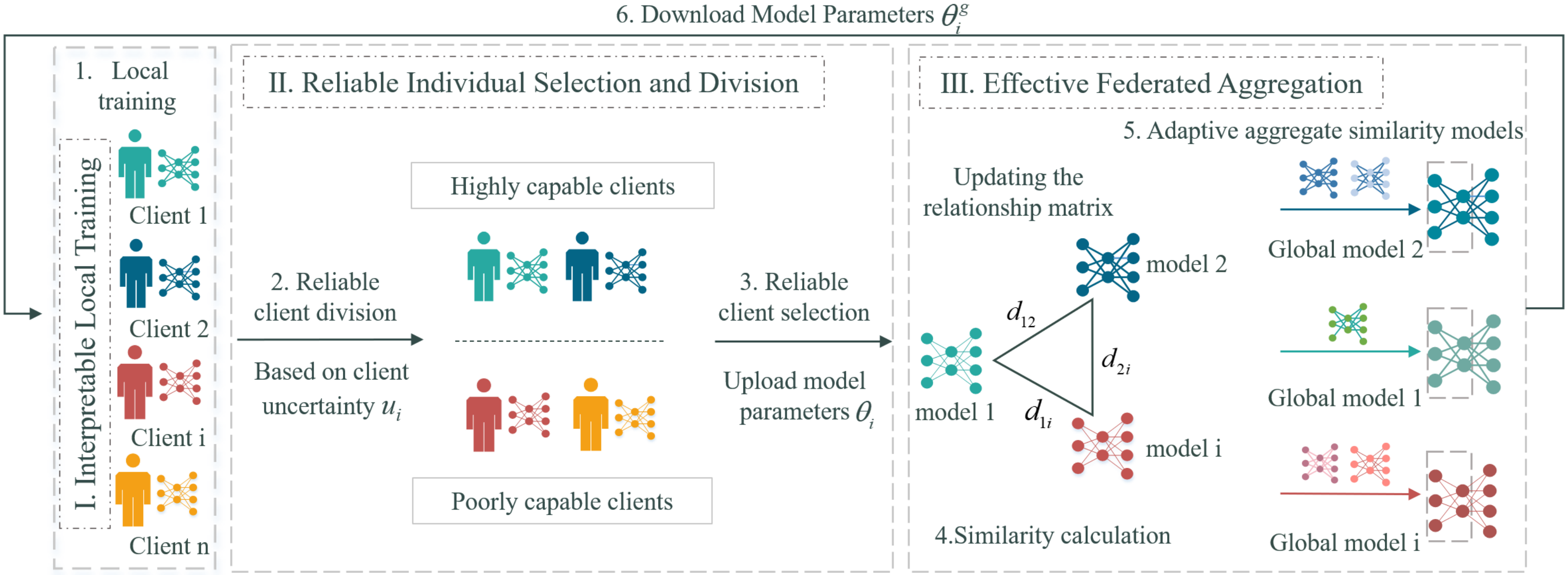
3 Reliable and interpretable federated learning

4 Experimental

5 Summary and Outlook

1. Reliable and Interpretable Personalized Federated Learning

In this paper, we propose a reliable and interpretable federated learning method (RIPFL) from a personalization perspective, which consists of interpretable local training, reliable client selection, and efficient federated aggregation.


6. Download Model Parameters θ_i^g
1. Local training
I. Interpretable Local Training
Client 1
Client 2
Client i
Client n
II. Reliable Individual Selection and Division
2. Reliable client division
Based on client uncertainty u_i
Highly capable clients
Poorly capable clients
3. Reliable client selection
Upload model parameters θ_i
III. Effective Federated Aggregation
5. Adaptive aggregate similarity models
Updating the relationship matrix
model 2
model 1
model i
d_{12}
d_{2i}
d_{1i}
4.Similarity calculation
Global model 2
Global model 1
Global model i

Leveraging uncertainty to guide the federated aggregation process

Outline

1 Overview of work

2 **Background and significance**

3 Reliable and interpretable federated learning

4 Experimental

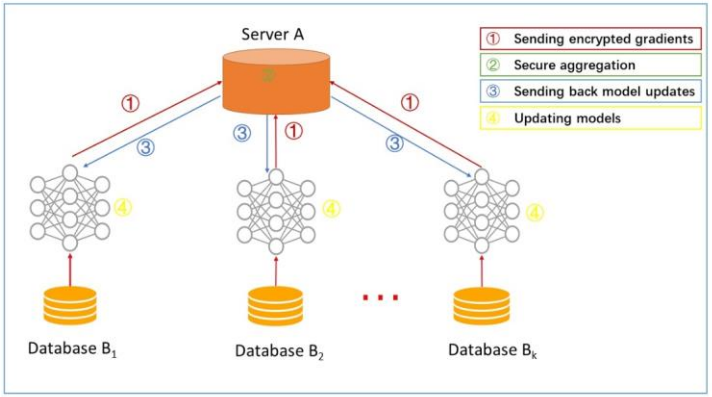
5 Summary and Outlook

2.1 Federated Learning

Data privacy

With the development of computer technology and increased awareness of privacy protection, how to learn and model data across organizations while meeting user privacy protection , data security and government regulations is a major challenge in the development of artificial intelligence

Federated Learning can be used to centralize data training by passing on information such as model parameters while protecting the privacy and security of client data.

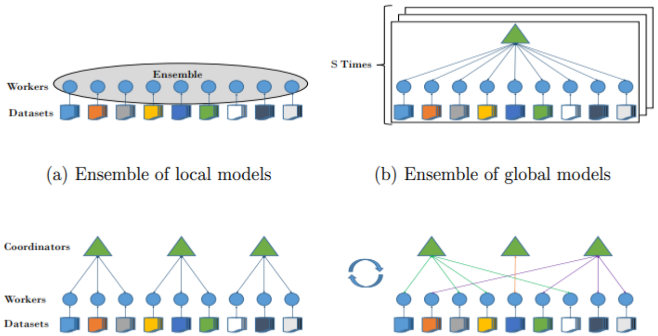


Federated learning as a distributed machine learning framework for data privacy protection

2.2 Federated Learning & Uncertainty

Quantification of Uncertainty in Federated Learning

Different clients have different data, different devices and therefore different performance, so there is a lot of uncertainty in the whole system.



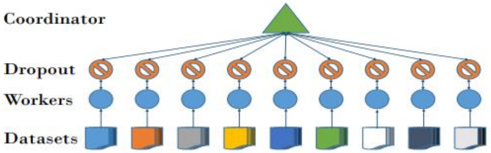
(a) Ensemble of local models

(b) Ensemble of global models

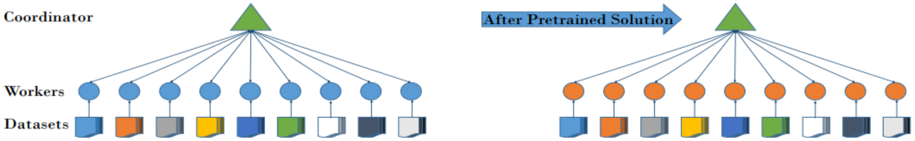
(c) mult. coord.-FA

(d) mult. coord.-RA

Ensemble learning reduces uncertainty in federated learning processes



Use Dropout to reduce uncertainty in the federated learning process



(a) Global model

(b) Federated SWAG

Use SWAG to reduce uncertainty in the federated learning process

[1] Linsner F, Adilova L, Daubener S, Kamp M, Fischer, A. Approaches to Uncertainty Quantification in Federated Deep Learning. Machine Learning and Principles and Practice of Knowledge Discovery in Databases. ECML PKDD 2021.

The quantification of uncertainty is of great significance in federated learning

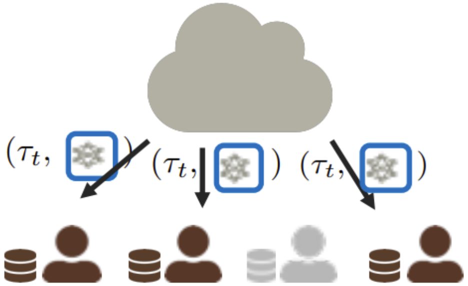
2.3 Uncertainty of client selection

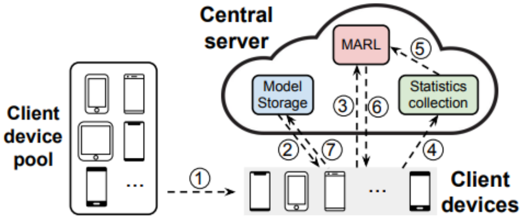
According to the performance of clients, the client selection is carried out to reduce the amount of communication, reduce the uncertainty, and improve the aggregation effect

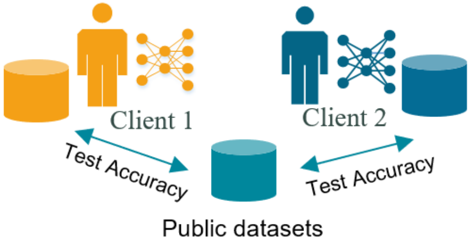
Select a client with a large amount of data and the ability to perform training quickly

Leveraging Reinforcement Learning Learn client selection strategies

Select randomly [3] or utilize the test accuracy of a public dataset for selection







Participant Selection for Scalable Federated Learning [1]

Advanced client Selection Strategy for Federated Learning [2]

Use public datasets to test effect selection

[1] T. Nishio and R. Yonetani. Client selection for federated learning with heterogeneous resources in mobile edge. *In IEEE International Conference on Communications*, 2019.

[2] Sai Qian Zhang and Jieyu Lin and Qi Zhang. Learning Advanced Client Selection Strategy for Federated Learning. *In Proceedings of the AAAI Conference on Artificial Intelligence*, 2022.

[3] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. *In Proceedings of the International Conference on Artificial Intelligence and Statistics*, 2017.

Select the appropriate client model for uploading, thereby reducing the uncertainty

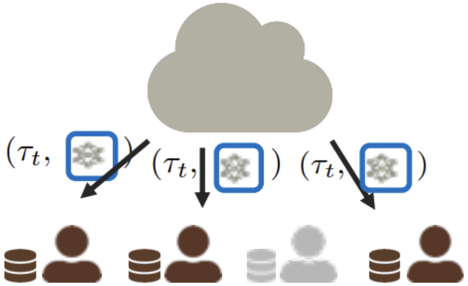
2.3 Uncertainty of client selection

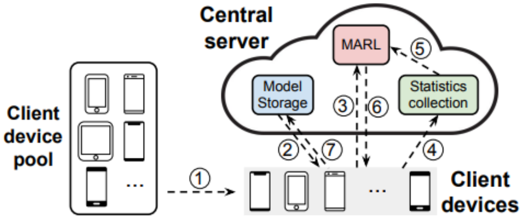
According to the performance of clients, the client selection is carried out to reduce the amount of communication, reduce the uncertainty, and improve the aggregation effect

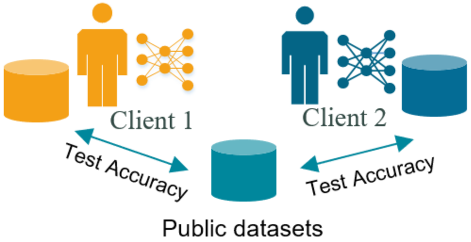
Select a client with a large amount of data and the ability to perform training quickly

Leveraging Reinforcement Learning Learn client selection strategies

Select randomly [3] or utilize the test accuracy of a public dataset for selection







Participant Selection for Scalable Federated Learning [1]

Advanced client Selection Strategy for Federated Learning [2]

Use public datasets to test effect selection

Clients with large amount of data and high training speed may not provide the knowledge needed by other clients

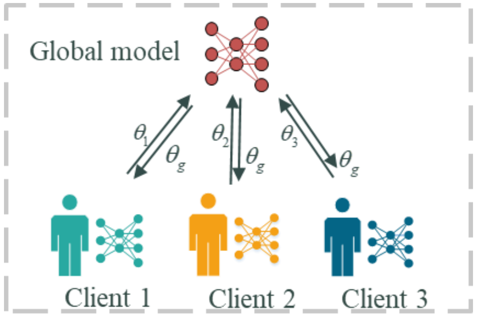
Training costs are high, and uncertainty in client performance cannot be measured

Random selection lacks interpretability, and accuracy cannot reliably measure client uncertainty

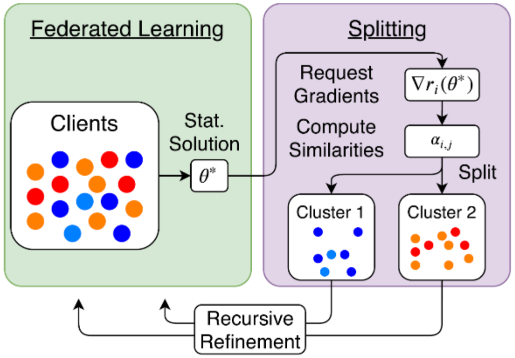
Uncertainty is not considered in client selection process

2.4 Uncertainty of Federated Aggregation

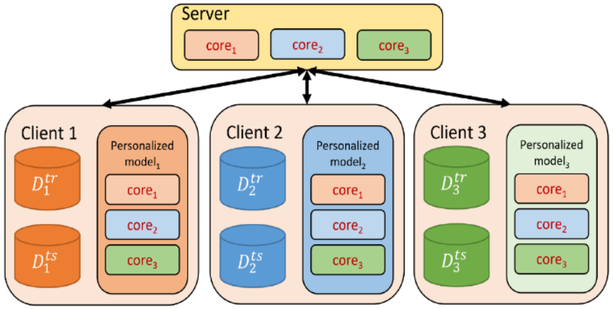
Aggregation of client models is the core step of federated learning. Efficient aggregation can speed up global convergence and improve client performance at the same time



Federated averaging algorithm [1]



Clustering-based Federated Learning Algorithm [2]



Adaptive personalized federated aggregation [3]

Weighted average of all clients participating in the aggregation

Each cluster center is generated A global model

Each client chooses to aggregate the client models that it helps larger

[1] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. *In Proceedings of the International Conference on Artificial Intelligence and Statistics*, 2017.

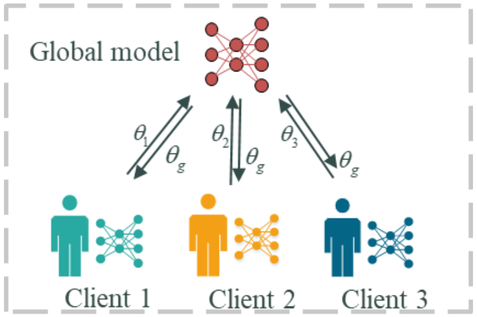
[2] Felix Sattler, Klaus-Robert Müller, and Wojciech Samek. Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints. *In IEEE Transactions on Neural Networks and Learning Systems*,2021.

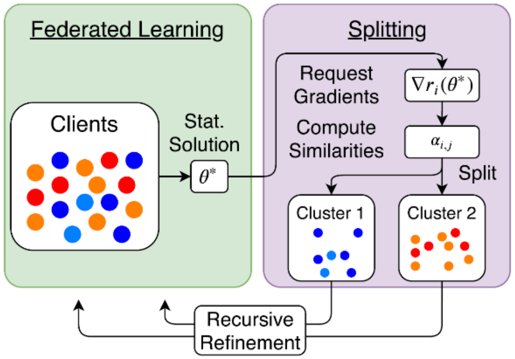
[3] Jun Luo and Shandong Wu. Adapt to adaptation: Learning personalization for cross-silo federated learning. *In Proceedings of the International Joint Conference on Artificial Intelligence*, 2022.

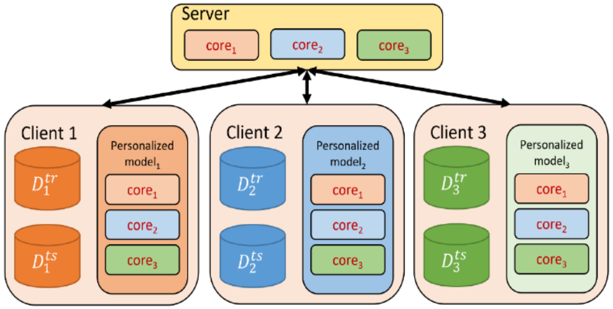
Clients need to assimilate the knowledge of other clients through model aggregation

2.4 Uncertainty of Federated Aggregation

Aggregation of client models is the core step of federated learning. Efficient aggregation can speed up global convergence and improve client performance at the same time







Federated averaging algorithm [1]

Simple weighted averaging is not the best solution when the client data is very different

Clustering-based Federated Learning Algorithm [2]

When the client data is very different, more clustering centers are needed, and the clustering division is difficult

Adaptive personalized federated aggregation [3]

When the number of clients is large, the number of models to be aggregated for each client cannot be reliably evaluated

When there are differences between clients data and models, simple weighted aggregation is not applicable, and clients cannot adaptively aggregate to generate a global model that is beneficial to them according to the uncertainty of individual models.

Trusted and effective knowledge exchange and fusion cannot be carried out between clients

Outline

1 Overview of work

2 Background and significance

3 **Reliable and interpretable federated learning**

4 Experimental

5 Summary and Outlook

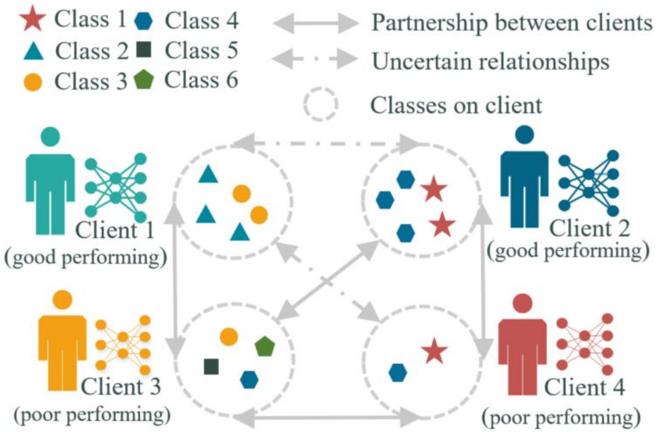
3.1 Reliable and Interpretable client Selection Strategy (RIPFL)

- **Client selection and training are often unreliable and unexplainable**
- **Uncertainty in the training process cannot be quantified**
- **When the number of clients is large and the data distribution is very different, the synergies between clients are often ignored due to unexplained random client selection**
- **Collective intelligence is underutilized**

client local training uncertainty is not quantified

The selection of clients participating in the aggregation cannot be explained

A uniform global model does not work for all clients



[1] Zixuan Qin, Liu Yang , Qilong Wang, Yahong Han, Qinghua Hu. Reliable and interpretable personalized federated learning. International Conference on Computer Vision and Pattern Recognition, 2023.

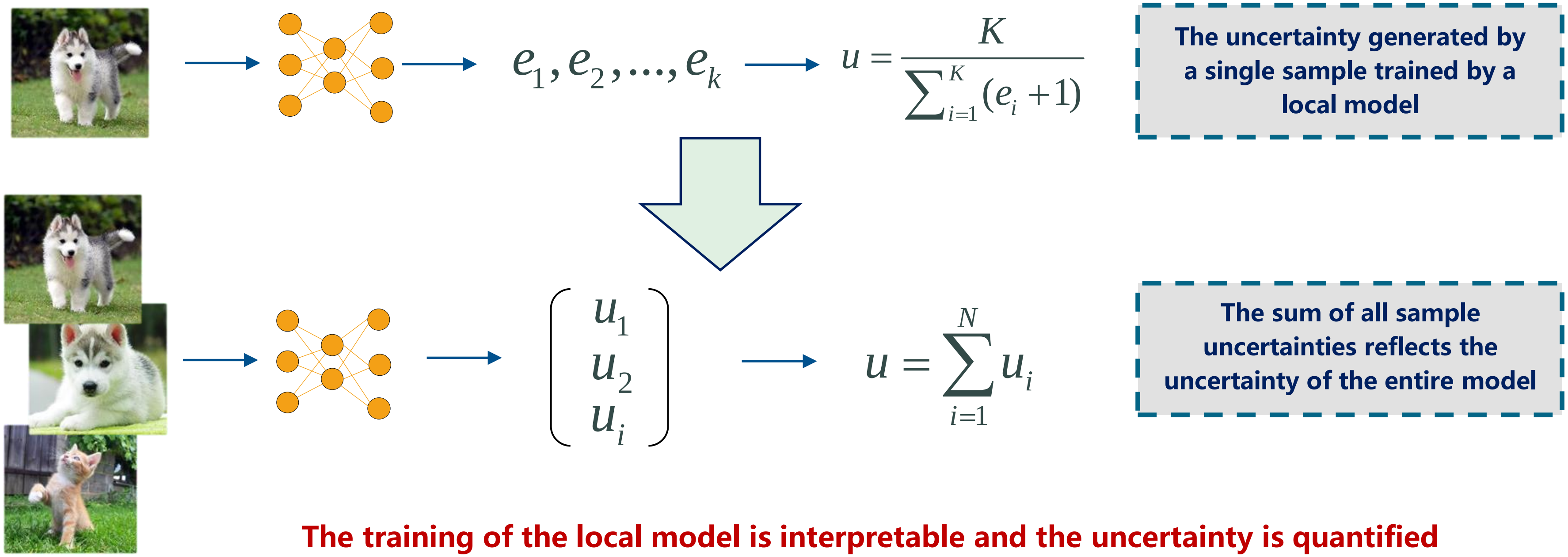
There is a need for an interpretable federated learning framework that can quantify client uncertainty

3.2 Uncertainty of local training

1. Quantification of uncertainty in the client's local training process

Dempster-Shafer evidence theory (DST) is a generalization of subjective probability from Bayesian theory and has been applied to reliably quantify uncertainty [1, 2].

Each class holds a certain belief mass, which is computed using the class evidence



$$e_1, e_2, \ldots, e_k$$

$$u = \frac{K}{\sum_{i=1}^{K}(e_i + 1)}$$

The uncertainty generated by a single sample trained by a local model

$$\begin{pmatrix} u_1 \\ u_2 \\ u_i \end{pmatrix}$$

$$u = \sum_{i=1}^{N} u_i$$

The sum of all sample uncertainties reflects the uncertainty of the entire model

The training of the local model is interpretable and the uncertainty is quantified

[1] Murat Sensoy, Lance Kaplan, and Melih Kandemir. Evidential deep learning to quantify classification uncertainty. In Proceedings of the International Conference on Neural Information Processing Systems, 2018.

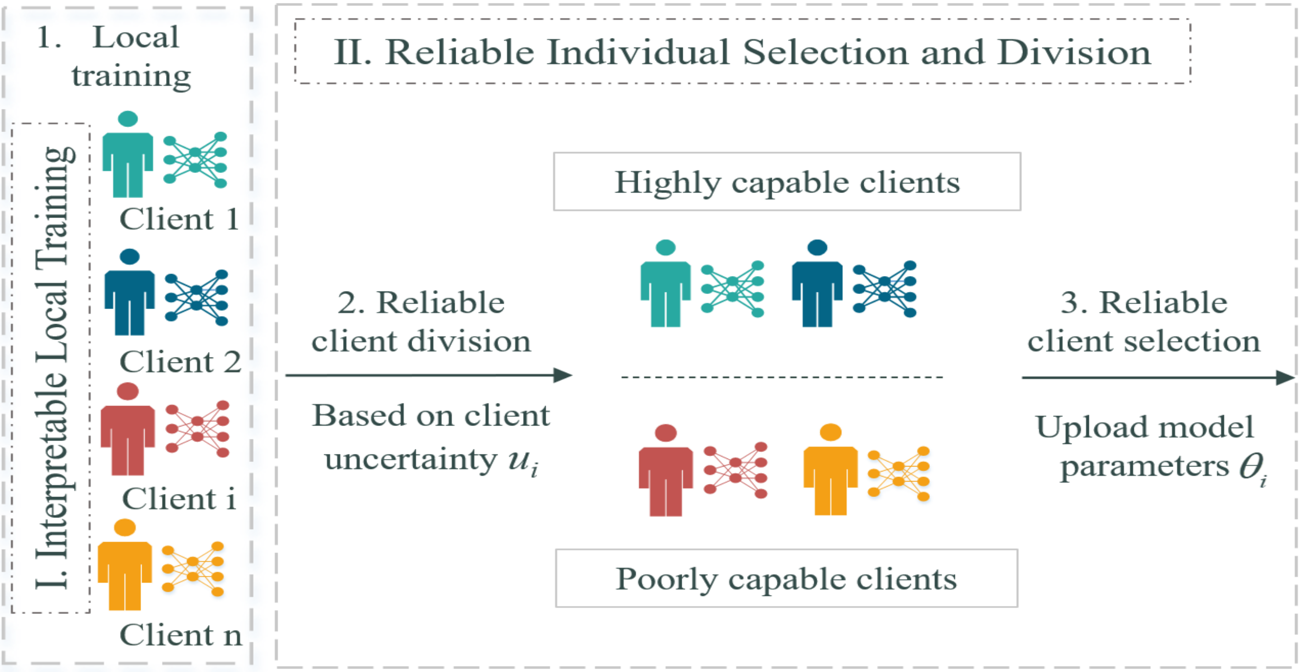
[2] Zongbo Han, Changqing Zhang, Huazhu Fu, and Joey Tianyi Zhou. Trusted multi-view classification. In Proceedings of the International Conference on Learning Representations, 2021.

The explainability of local models provides a foundation for client selection based on uncertainty

3.3 Reliable and interpretable client selection strategies

Divide and select clients based on individual uncertainty

Based on the calculation of individual uncertainty, the uncertainty is used as a guide to divide the client group according to performance, so as to ensure that the clients with low uncertainty account for a large proportion of the clients participating in the aggregation, so as to generate a high-value global model



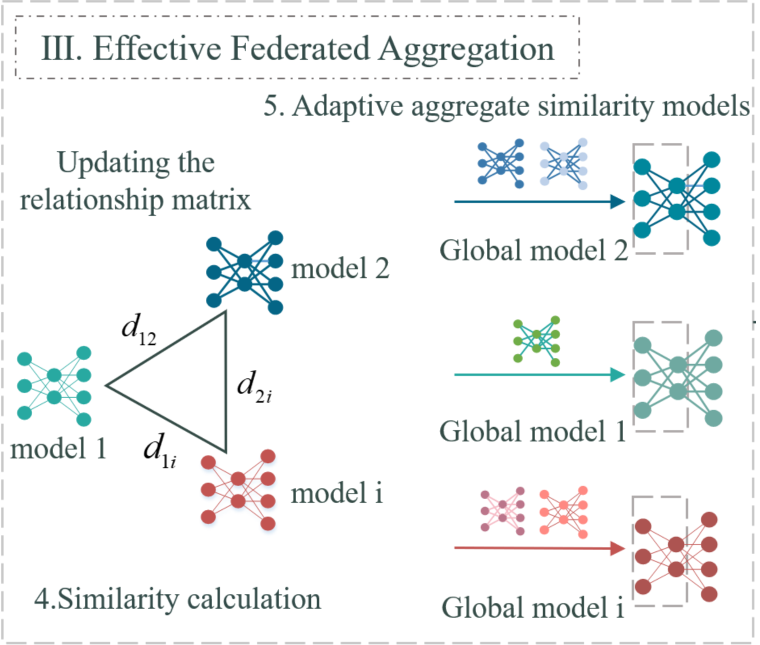
1. Local training
I. Interpretable Local Training
Client 1
Client 2
Client i
Client n
II. Reliable Individual Selection and Division
2. Reliable client division
Based on client uncertainty u_i
Highly capable clients
Poorly capable clients
3. Reliable client selection
Upload model parameters θ_i

All the clients with low uncertainty are reliably selected, which ensures that the poor performing clients will receive the help of as many better performing clients as possible

The selection of clients to participate in federated aggregation is reliably explained

3.4 Efficient personalized aggregation

When there are differences in individual knowledge, it is obviously unreasonable to perform a simple and general average, and a uniform global model will not be applicable to all clients.



1. Each individual chooses models similar to its own to aggregate

2. The number of other models chosen to aggregate is related to uncertainty and adaptively adjusted with training. In general, clients with higher uncertainty need more group knowledge to help them grow

This flexible and interpretable aggregation method is not limited by a unified global model. It ensures that each client can aggregate different amounts of group information to generate personalized global models that benefit them

Use uncertainty to guide the federated aggregation process

Outline

1 Overview of work

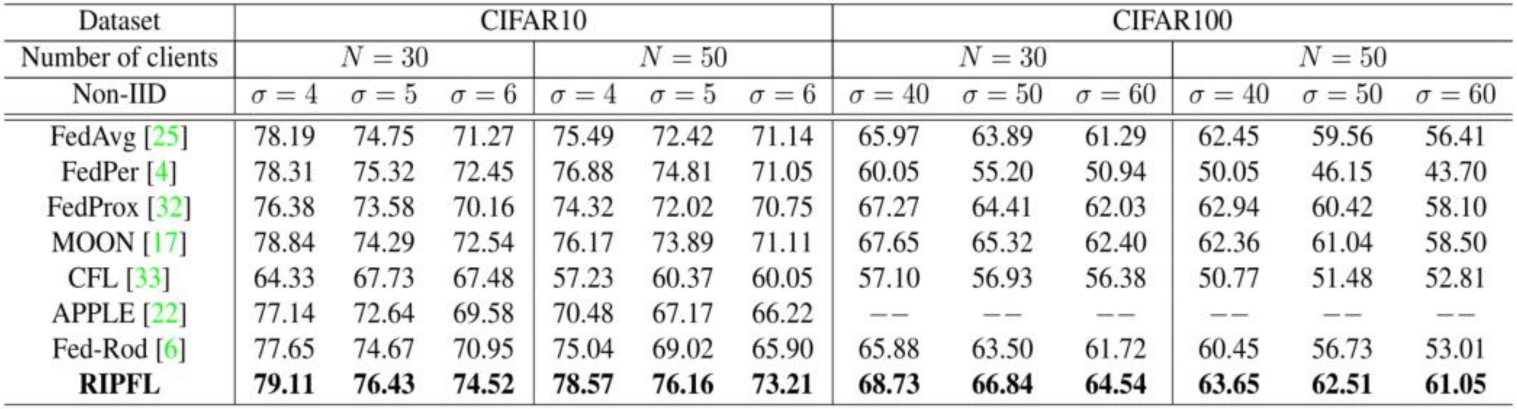
2 Background and significance

3 Reliable and interpretable federated learning

4 **Experimental**

5 Summary and Outlook

4.1 Experimental results and analysis

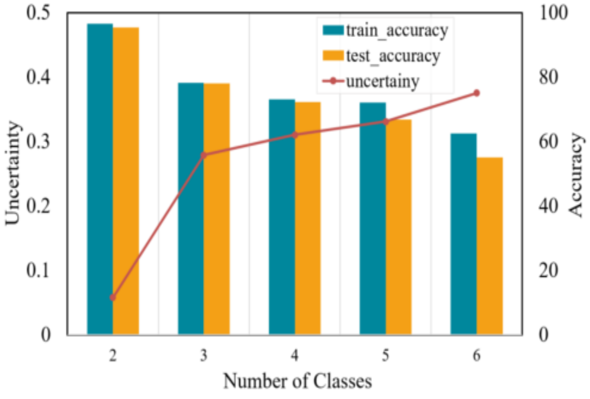


Dataset	CIFAR10						CIFAR100					
Number of clients	$N = 30$			$N = 50$			$N = 30$			$N = 50$		
Non-IID	$\sigma = 4$	$\sigma = 5$	$\sigma = 6$	$\sigma = 4$	$\sigma = 5$	$\sigma = 6$	$\sigma = 40$	$\sigma = 50$	$\sigma = 60$	$\sigma = 40$	$\sigma = 50$	$\sigma = 60$
FedAvg [25]	78.19	74.75	71.27	75.49	72.42	71.14	65.97	63.89	61.29	62.45	59.56	56.41
FedPer [4]	78.31	75.32	72.45	76.88	74.81	71.05	60.05	55.20	50.94	50.05	46.15	43.70
FedProx [32]	76.38	73.58	70.16	74.32	72.02	70.75	67.27	64.41	62.03	62.94	60.42	58.10
MOON [17]	78.84	74.29	72.54	76.17	73.89	71.11	67.65	65.32	62.40	62.36	61.04	58.50
CFL [33]	64.33	67.73	67.48	57.23	60.37	60.05	57.10	56.93	56.38	50.77	51.48	52.81
APPLE [22]	77.14	72.64	69.58	70.48	67.17	66.22	−−	−−	−−	−−	−−	−−
Fed-Rod [6]	77.65	74.67	70.95	75.04	69.02	65.90	65.88	63.50	61.72	60.45	56.73	53.01
RIPFL	**79.11**	**76.43**	**74.52**	**78.57**	**76.16**	**73.21**	**68.73**	**66.84**	**64.54**	**63.65**	**62.51**	**61.05**

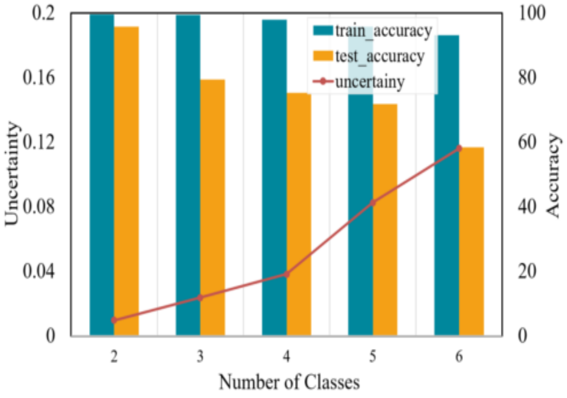
Table 1. Test accuracy (%) of different FL methods on CIFAR10 and CIFAR100, where N denotes the number of clients. APPLE with a more complex network on a larger dataset would lead to a large overhead, and experiments are only performed on CIFAR10 owing to the limitations of the experimental equipment.

Results on different task datasets and under different experimental Settings show that the proposed model (RIPFL) exhibits higher performance than state-of-the-art federated learning methods. The proposed federated learning framework is suitable for classification problems with large differences in data distribution between clients, complex client tasks, and a large number of clients.

4.2. Reliability verification



(a) Global iteration rounds of 20.



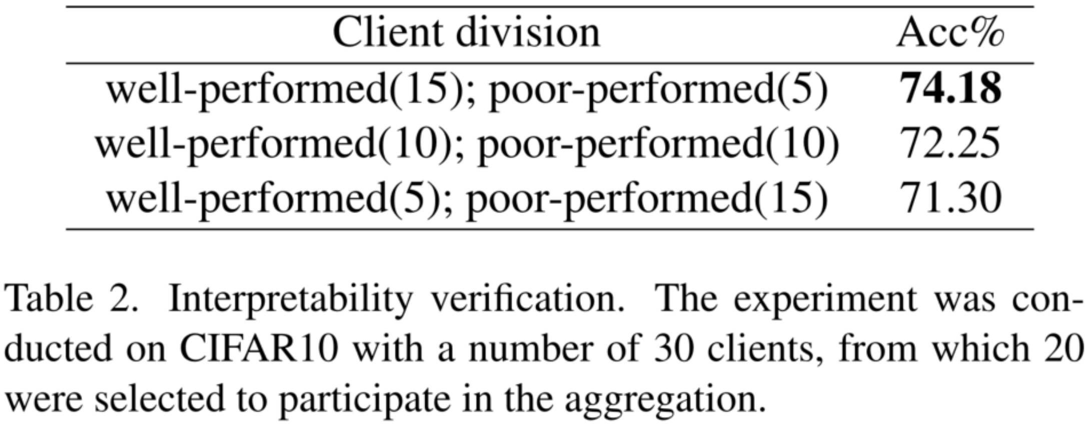
(b) Global iteration rounds of 60.

When accuracy on the training set is generally high, uncertainty can reliably distinguish how different clients perform on the test set

The larger the number of client categories, the more complex the task, and the higher the uncertainty. And the more clients you need to talk to

We experimented with RIPFL and FedAvg with attacks against client-side data. RIPFL's accuracy drops from 74.52% to 73.58% after being attacked, while FedAvg's accuracy drops from 71.27% to 68.86%. The performance degradation of RIPFL is less than that of FedAvg, which proves the reliability of RIPFL. From the aggregation point of view, the uncertainty after being attacked increases and the probability of being selected decreases. From a personalization point of view, only similar clients are selected to collaborate, which can also reduce the impact of the attack.

4.3 Interpretability verification



Client division	Acc%
well-performed(15); poor-performed(5)	**74.18**
well-performed(10); poor-performed(10)	72.25
well-performed(5); poor-performed(15)	71.30

Table 2. Interpretability verification. The experiment was conducted on CIFAR10 with a number of 30 clients, from which 20 were selected to participate in the aggregation.

As can be seen, the accuracy rate is higher when more high-performing clients are selected. The higher accuracy indicates that high performing clients are more capable of helping other clients improve their performance, while poor performing clients may degrade the performance of the global model, which clearly supports our interpretable selection approach.

Outline

1 Overview of work

2 Background and significance

3 Reliable and interpretable federated learning

4 Experimental

5 **Summary and Outlook**

5. Summary and Outlook

Research on uncertainty of Federated Learning

- This paper combines the federated learning framework with the quantification of local client uncertainty, using uncertainty to guide the entire process of local training, client selection and federated aggregation of clients involved in federated learning
- Expand to multi-intelligent machine learning to dig deeper into the hidden and group machine learning related knowledge behind social learning

Reliable and Interpretable Personalized Federated Learning

Zixuan Qin

Jun 23, 2023