

Free-Rider and Conflict Aware Collaboration Formation for Cross-Silo Federated Learning

Mengmeng Chen¹, Xiaohu Wu¹, Xiaoli Tang², Tiantian He³, Yew-Soon Ong^{2,3}, Qiqi Liu⁴, Qicheng Lao¹, Han Yu² ¹Beijing University of Posts and Telecommunications, ²Nanyang Technological University, 3Agency for Science, Technology and Research (A∗STAR), 4Westlake University

❑ **Background & Motivation**

❑ **Problem Description**

❑ **Solution**

❑ **Experiments**

Federated Learning

Federated Learning (FL)

 \triangleright Federated learning (FL) is a promising paradigm of distributed machine learning as it does not require sharing raw data between FL participants (FL-PTs), thereby upholding the privacy considerations.

General FL Training Process

- ➢ Multiple FL-PTs train a shared model locally with their own dataset, and upload their local model updates to a central server (CS), which then aggregates these model updates and distributes the model updates to each FL-PT.
- \triangleright This iterative interplay between the CS and FL-PTs persists until the global model achieves convergence.

Application Domains in business sector

➢ Digital banking, ridesharing, recommender systems, health care, and Electric Vehicle(EV) charging services, among others

Scenario

Two features: Self–interest, Competition

- The free-riding problem is in which some FL-PTs benefit from the contribution by others without making any contribution to the FL ecosystem.
- There is a potential conflict of interest between some two FL-PTs.

Motivating Example 1: Banks

 \triangleright Regional banks have different user groups from their respective regions and are independent, while the banks in the same region can compete for users

• An FL platform, **MELLODDY**, has been developed for drug discovery, currently comprised of 10 pharmaceutical companies, academic institutions, large industrial companies and startups, where competition exists when there are multiple organizations that are in the same market area.

- ❑ **Background & Motivation**
- ❑ **Problem Description**
- ❑ **Solution**
- ❑ **Experiments**

\Box Relationships among FL-PTs $V = \{v_1, v_2, ..., v_n\}$

Known Parameters:

- Benefit Graph $G_b = (V, E_b)$. If v_i can benefit from v_j 's data, then there is a directed edge from v_j to v_i (i.e.,(v_j , v_i) \in E_b) and the weight of this edge is $w_{j,i}$ >0.
- \triangleright Competing Graph $G_c = (V, E_c)$. For any two FL-PTs v_i and v_j , if they compete against each other, then there is an undirected edge between v_i and v_j (i.e., $(v_j, v_i) \in E_c$) and if they are independent of each other, then $(v_j, v_i) \notin E_c$.

Decision Variables $X = (x_{j,i})$:

▶ Data Usage Graph $G_u = (V, E_u)$. Let $X = (x_{j,i})$ be an n×n matrix where $x_{j,i} \in \{0,1\}$: for two different FL-PTs v_i and v_j , $x_{j,i}$ is set to one if v_j will contribute to v_i in the FL training process and $x_{j,i}$ is set to zero otherwise. \triangleright G_u will be a subgraph of the benefit graph G_b .

Collaboration Principles

Principle 1. Absence of free riders

For any FL-PT $v_i \in V$, there exists a FL-PT $v_j \in V$ that benefits v_i if and only if there exists at least one FL-PT v_k that can benefit from v_i . Each FL-PT $v_i \in S_k$ is only concerned with the contributions of other FL-PTs within the same S_k .

Coalitions: A partition $\pi = \{S_1, S_2, ..., S_K\}$ is said to be a set of coalitions if we have for any $S_k \in \pi$ with $|S_k| \ge 2$ and v_i ∈ S_k that $\sum_{v_j \in S_k - \{v_i\}} w_{i,j} > 0$ and $\sum_{v_j \in S_k - \{v_i\}} w_{j,i} > 0$

Principle 2. Avoiding conflict of interest

 \triangleright For any two competing FL-PTs v_i and v_j , v_j is unreachable to v_i in the data usage graph G_u .

Problem to Be Solved

- \triangleright The problem of this paper is to find a partition π of FL-PTs such that
- ⚫ Principles 1 and 2 are satisfied.
- Subject to Principles 1 and 2, no coalitions of π (i.e., no subset π' of π) can collaborate together and be merged into a larger coalition $S' = \bigcup_{S_k \in \pi'} S_k$ with a higher utility $u(S')$. Formally, let

 $\Pi = \{\pi' \subseteq \pi \mid \sum_{s_k \in \pi'} u(S_k) < u(S'), \text{Principles 1 and 2 are satisfied by S'}\}.$ Then $\Pi = \emptyset$.

- ❑ **Background & Motivation**
- ❑ **Problem Description**
- ❑ **Solution**
- ❑ **Experiments**

Main Idea

- \triangleright We find a partition $\hat{\pi} = {\hat{S}_1, \hat{S}_2, ..., \hat{S}_H}$ of all FL-PTs V such that the FL-PTs of each subset $\hat{S}_h \in \hat{\pi}$ are independent of each other.
- \triangleright $\hat{S}_h \in \hat{\pi}$ is further partitioned into several subsets/coalitions, denoted as $SCC_h = {\hat{S}_{h,1}, \hat{S}_{h,2}, ..., \hat{S}_{h,y_h}}$ such that for all $l \in [1, y_h]$, $G_b(\hat{S}_{h,l})$ is a strongly connected component of $G_b(\hat{S}_h)$.
- ≻ For any coalitions of $\bigcup_{h=1}^{H} SCC_h$, we merge these coalitions into a larger one if doing so achieves a higher coalition utility without violating Principles 1 and 2.

\Box New Graph: Z_b and Z_c \Box Merge Operation

- \triangleright In the graph Z_b , there is a directed edge from \hat{v}_l to $\hat{v}_{l'}$ if and only if there exist two nodes $v_i \in \hat{v}_l$ and $v_j \in \hat{v}_{l'}$ such that (v_i, \cdot) v_j) is a directed edge in the benefit graph G_h .
- \triangleright In the graph Z_c , there is an undirected edge between \hat{v}_l and $\hat{v}_{l'}$ if and only if there exist two nodes $v_i \in \hat{v}_l$ and $v_j \in \hat{v}_{l'}$ such that (v_i, v_j) is an undirected edge in the competing graph G_c .

Algorithm 3: Merge $(\mathcal{X}, \pi, \mathcal{Z}_b, \mathcal{Z}_c, y)$

 $\overline{1 \hat{v}_y \leftarrow \bigcup_{\hat{v}_j \in \mathcal{X}} \hat{v}_j, y \leftarrow y+1, \pi \leftarrow \pi - \mathcal{X}, \text{ and } \pi \leftarrow \pi \cup \{\hat{v}_y\};$

- 2 Add \hat{v}_v into \mathcal{Z}_b as a new node, and all the edges in the graph \mathcal{Z}_b that point to (resp. point from) the nodes of X change to point to (resp. point from) \hat{v}_u ;
- 3 Add \hat{v}_v into \mathcal{Z}_c as a new node, and all the edges in the graph \mathcal{Z}_c whose endpoints are the nodes of X change to become the edges whose endpoints are \hat{v}_u ;
- 4 Remove the nodes of X from both \mathcal{Z}_b and \mathcal{Z}_c ;
- 5 **Return** $(\hat{v}_y, \pi, \mathcal{Z}_b, \mathcal{Z}_c, y)$;

Definition 2. In the graph Z_b , there is a directed edge from \hat{v}_l to $\hat{v}_{l'}$ if and only if there exist two nodes $v_i \in \hat{v}_l$ and $v_j \in \hat{v}_{l'}$ such that (v_i, v_j) is a directed edge in the benefit graph \mathcal{G}_b . In the graph \mathcal{Z}_c , there is an undirected edge between \hat{v}_l and $\hat{v}_{l'}$ if and only if there exist two nodes $v_i \in \hat{v}_l$ and $v_i \in \hat{v}_l$ such that (v_i, v_j) is an undirected edge in the competing graph \mathcal{G}_c . For any two coalitions \hat{v}_l and $\hat{v}_{l'}$ of π , \hat{v}_l is said to benefit (resp. benefit from) $\hat{v}_{l'}$ if there is a directed edge $(\hat{v}_l, \hat{v}_{l'})$ (resp. (\hat{v}_l, \hat{v}_l)) in the graph \mathcal{Z}_b ; \hat{v}_l and $\hat{v}_{l'}$ are said to be competitive if there is an undirected edge $(\hat{v}_l, \hat{v}_{l'})$ in the graph Z_c and independent of each other otherwise.

 \triangleright MergeCycle: While there is a node \hat{v}_{y_i} of Z_b with $|\hat{v}_{y_i}| = 1$ such that (i) there is a cycle $(\hat{v}_{y_1}, \hat{v}_{y_2}, \dots, \hat{v}_{y_\theta}, \hat{v}_{y_1})$ in the graph Z_b that contains \hat{v}_{y_i} and (ii) the nodes $\hat{v}_{y_1}, \hat{v}_{y_2},..., \hat{v}_{y_\theta}$ of this cycle are independent of each other do Merge Operation.

- \triangleright **MergePath**: While there is a node \hat{v}_{y_i} of Z_b with $|\hat{v}_{y_i}| = 1$ such that (i) there is a simple path $(\hat{v}_{y_1},...,\hat{v}_{y_i},...,\hat{v}_{y_\theta})$ with $\hat{v}_{y_1} \ge$ 2 and $\hat{v}_{y_\theta} \ge 2$ and (ii) the nodes $\hat{v}_{y_1}, \hat{v}_{y_2},..., \hat{v}_{y_\theta}$ of this cycle are independent of each other do Merge and MergeCycle Operation.
- \triangleright **MergeNeighbors**: While there is an edge $(\hat{v}_l, \hat{v}_{l'})$ of Z_b with $|\hat{v}_l| \ge 2$ and $|\hat{v}_{l'}| \ge 2$ such that \hat{v}_l and $\hat{v}_{l'}$ are independent of each other do Merge, MergeCycle and MergePath Operation.

- ❑ **Background & Motivation**
- ❑ **Problem Description**
- ❑ **Solution**
- ❑ **Experiments**

Experimental Settings

A Naive Pre-Processing Procedure

- **NEURAL INFORMATION** PROCESSING SYSTEMS
- ≻ We use the operations in lines 1-4 of Algorithm 1 to generate a set of coalitions, denoted as $\cup_{h=1}^H SCC_h$, where SCC_h = ${\{\hat{S}_{h,1}, \hat{S}_{h,2}, ..., \hat{S}_{h,y_h}\}.$ This makes the previous FL approaches applicable to the scenario of this paper.

Datasets

- ➢ **Synthetic data:** A randomly generated dataset for regression tasks, which is generated in a similar way that has been used in literature.
- ➢ **CIFAR-10 and CIFAR-100:** Both the CIFAR-10 and CIFAR-100 datasets contain 60,000 color images for image classification tasks but have different levels of complexity. CIFAR-10 images have 10 classes with 6,000 images per class, while CIFAR-100 is more complex and has 100 classes with only 600 images per class.
- ➢ **eICU:** A dataset collecting electronic health records (EHRs) from many hospitals across the United States admitted to the intensive care unit(ICU). The task is to predict mortality during hospitalization.

Baselines

- ➢ **FedAvg**: A vanilla FL algorithm.
- ➢ **FedProx and SCAFFOLD**: Represent two typical approaches that make the aggregated model at the CS.
- ➢ **pFedHN and pFedMe**: Two approaches based on hypernetworks and meta-learning respectively.
- ➢ **FedDisco and pFedGraph**: Based on data complementarity.
- ➢ **FedOra**: Assesses if a FL-PT generalization performance can benefit from knowledge transferred from others and maximizes it.
- ➢ **Local**: Each FL-PT simply takes local ML training without collaboration.

Experimental Results under Synthetic Data

Two settings are considered:

- ➢ **Weakly Non-IID setting**: There exists a quantity skew, i.e., a significant difference in the sample quantities of FL-PTs.
- ➢ **Strongly Non-IID setting**: Conflicting learning tasks are generated by flipping over the labels of some FL-PTs.

Table 1: Experiments with synthetic data (Weakly Non-IID, MSE) under fixed competing graphs

	v_1	$\scriptstyle v_2$	v_3	$\boldsymbol{v_4}$	v_{5}	v_{6}	v_{7}	v_{8}
LOCAL.							0.32 ± 0.05 0.28 ± 0.00 1.00 ± 0.07 0.69 ± 0.08 0.28 ± 0.02 0.28 ± 0.01 0.72 ± 0.06 0.90 ± 0.11	
FEDAVE							0.25 ± 0.01 0.25 ± 0.01 0.79 ± 0.05 0.55 ± 0.05 0.23 ± 0.01 0.23 ± 0.00 0.61 ± 0.04 0.74 ± 0.07	
FEDPROX							0.26 ± 0.01 0.27 ± 0.01 0.90 ± 0.10 0.67 ± 0.06 0.26 ± 0.01 0.26 ± 0.01 0.76 ± 0.11 1.02 ± 0.17	
SCAFFOLD							0.27 ± 0.01 0.28 ± 0.00 0.90 ± 0.03 0.67 ± 0.06 0.25 ± 0.01 0.26 ± 0.01 0.72 ± 0.09 0.92 ± 0.10	
PFEDME							0.28 ± 0.02 0.29 ± 0.03 1.13 ± 0.55 0.86 ± 0.58 0.33 ± 0.13 0.33 ± 0.12 0.74 ± 0.02 0.82 ± 0.04	
PFEDHN							0.35 ± 0.07 0.31 ± 0.05 0.91 ± 0.07 0.61 ± 0.06 0.33 ± 0.04 0.31 ± 0.05 0.70 ± 0.09 0.90 ± 0.18	
							PFEDGRAPH 0.26 ± 0.01 0.27 ± 0.01 0.90 ± 0.04 0.67 ± 0.08 0.26 ± 0.01 0.26 ± 0.00 0.74 ± 0.08 0.99 ± 0.05	
							FEDEGOISTS 0.23 ± 0.01 0.24 ± 0.00 0.24 ± 0.01 0.22 ± 0.02 0.22 ± 0.00 0.23 ± 0.01 0.25 ± 0.01 0.25 ± 0.02	

Table 2: Experiments with synthetic data (Strongly Non-IID, MSE) under fixed competing graphs v_1 v_2 v_4 v_3 v_5 v_6 v_7 v_{8} 0.29 ± 0.03 0.29 ± 0.02 0.26 ± 0.00 0.29 ± 0.04 0.27 ± 0.01 0.27 ± 0.04 0.27 ± 0.02 0.27 ± 0.01 **LOCAL** 0.25 ± 0.00 0.25 ± 0.01 0.23 ± 0.01 0.23 ± 0.01 0.23 ± 0.01 0.22 ± 0.00 0.23 ± 0.02 0.24 ± 0.02 **FEDAVE** 0.27 ± 0.02 0.26 ± 0.01 0.26 ± 0.01 0.26 ± 0.01 0.24 ± 0.01 0.24 ± 0.01 0.25 ± 0.01 0.25 ± 0.01 **FEDPROX** 0.26 ± 0.01 0.26 ± 0.01 0.26 ± 0.01 0.26 ± 0.01 0.24 ± 0.01 0.24 ± 0.01 0.25 ± 0.01 0.25 ± 0.01 **SCAFFOLD PFEDME** 0.36 ± 0.12 0.37 ± 0.12 0.25 ± 0.00 0.25 ± 0.01 0.28 ± 0.02 0.27 ± 0.01 0.27 ± 0.01 0.28 ± 0.01 0.33 ± 0.05 0.34 ± 0.03 0.32 ± 0.05 0.28 ± 0.03 0.34 ± 0.03 0.29 ± 0.03 0.29 ± 0.05 0.29 ± 0.06 **PFEDHN** 0.26 ± 0.01 0.27 ± 0.01 0.26 ± 0.02 0.26 ± 0.02 0.24 ± 0.01 0.24 ± 0.01 0.25 ± 0.01 0.25 ± 0.01 PFEDGRAPH FEDEGOISTS 0.24 ± 0.00 0.27 ± 0.05 0.24 ± 0.03 0.22 ± 0.01 0.22 ± 0.00 0.22 ± 0.00 0.22 ± 0.01 0.22 ± 0.01

Results: FedEgoists has the best performance compared with baselines.

Experimental Results under CIFAR-10 and CIFAR-100

CIFAR10:

Table 3: Accuracy comparisons (MTA) under different α on CIFAR10.

LOCAL FEDPROX SCAFFOLD **PFEDME PFEDHN** FEDDISCO PFEDGRAPH FEDORA **FEDEGOISTS FEDAVG** α 0.05 PAT 80.47 \pm 2.06 36.86 \pm 3.00 36.62 \pm 6.17 36.61 \pm 6.18 48.66 \pm 6.38 66.53 \pm 2.00 36.61 \pm 6.18 52.04 \pm 8.66 69.73 \pm 1.62 81.35 \pm 0.30 Dir $|61.59 \pm 0.53\ 44.98 \pm 1.91\ 46.94 \pm 2.12\ 46.76 \pm 2.92\ 44.64 \pm 2.61\ 55.61 \pm 0.45\ 46.74 \pm 2.99\ 46.56 \pm 2.55\ 55.28 \pm 0.75\ 63.06 \pm 0.64$ 0.05 PAT $|80.47 \pm 2.06|49.40 \pm 5.50|48.19 \pm 5.17|48.18 \pm 5.16|56.56 \pm 1.66|66.61 \pm 1.62|48.19 \pm 5.17|55.35 \pm 4.51|68.65 \pm 2.02|80.73 \pm 1.35|48.65 \pm 2.02|80.73 \pm 1.35|48.65 \pm 2.02|48.65 \pm 2.02|48.65 \pm 2.02|48.65 \pm 2.02|48.65 \pm$ 0.1 Dir $\left| 61.59 \pm 0.53 \right.$ 46.77 \pm 1.96 48.71 \pm 1.97 48.61 \pm 2.02 46.65 \pm 2.74 54.21 \pm 0.83 48.56 \pm 1.99 49.10 \pm 3.19 55.97 \pm 0.22 62.74 \pm 1.09 0.1 PAT $|80.47 \pm 2.06\,63.67 \pm 2.10\,57.26 \pm 1.48\,57.24 \pm 2.34\,79.27 \pm 1.35\,76.08 \pm 2.20\,57.25 \pm 2.15\,60.27 \pm 2.33\,72.74 \pm 1.91\,81.30 \pm 1.46$ 0.2 Dir $\left| 61.59 \pm 0.53\right.$ 55.69 \pm 1.90 53.79 \pm 1.07 54.16 \pm 0.79 53.64 \pm 0.79 61.31 \pm 0.56 54.08 \pm 1.43 53.85 \pm 1.07 55.67 \pm 0.96 66.62 \pm 1.23 0.2 PAT $|80.47 \pm 2.06\; 57.95 \pm 2.37\; 59.82 \pm 4.88\; 59.83 \pm 4.87\; 63.09 \pm 3.26\; 65.11 \pm 2.4\; 59.82 \pm 4.88\; 62.12 \pm 4.51\; 71.51 \pm 2.40\; 81.37 \pm 1.41$ 0.3 Dir $\left| 61.59 \pm 0.53\right.$ 50.48 \pm 0.87 49.99 \pm 1.15 50.09 \pm 1.29 49.33 \pm 1.94 53.21 \pm 0.49 50.17 \pm 1.29 50.66 \pm 1.59 55.9 \pm 1.01 63.39 \pm 0.89 0.3 PAT $|80.47 \pm 2.06$ 58.47 \pm 5.87 63.28 \pm 4.54 63.27 \pm 4.54 66.36 \pm 3.88 67.51 \pm 3.04 63.28 \pm 4.55 63.30 \pm 4.61 72.89 \pm 1.67 82.54 \pm 0.30 0.4 Dir $\left| 61.59 \pm 0.53 \right.$ 50.14 \pm 2.2 51.20 \pm 2.16 51.23 \pm 2.09 51.00 \pm 0.94 53.04 \pm 0.80 51.14 \pm 2.09 51.14 \pm 2.16 57.26 \pm 0.32 62.81 \pm 0.88 0.4

Setting: We show the performance of the proposed approach when α takes different values in {0.05,0.1,0.2,0.3,0.4}, representing different levels of competing intensity between FL-PTs.

CIFAR100:

Table 4: Accuracy comparisons (MTA) under different α on CIFAR100.

FedEgoists has the best ance compared with the elines.

New Metric

- \triangleright r_{α,l,p} : The performance of the proposed approach.
- \triangleright r_{α,l,i}: The performance of the i-th baseline approach. i $\in \{1,2,..., 9\}$
- \triangleright l^{*}: l^{*} = argmax_{l∈[1,5]}(max_{i∈[1,9]}r_{α,l,i} r_{α,l,p}) where max_{i∈[1,9]}r_{α,l,i} is the best performance of all the baseline approaches in the l^{*}-th trial and max_{i∈[1,9]}r_{α,l,i} – r_{α,l,p} is their performance improvement (or the difference) to the proposed approach, which may be negative if the proposed approach achieves a better performance.

Table 5: The worst-case performance of the proposed approach compared with the baseline approaches.

	0.05								0.4	
	PAT	Dir	PAT	Dir	PAT	Dir	PAT	Dir	PAT	Dir
CIFAR10						$\mid 0.011000 \mid$ -0.002903 $\mid 0.022900 \mid$ -0.000624 $\mid 0.025800 \mid$ -0.0006030 $\mid 0.028800 \mid$ -0.005725 \mid -0.002399 \mid -0.000100				
						$CIFAR100$ -0.000999 \vert 0.076002 \vert 0.011400 \vert -0.000008 \vert -0.000636 \vert -0.0009356 \vert -0.000020 \vert -0.032153 \vert -0.000699 \vert -0.027078				

Experimental Results under eICU

Settings:

- Find the There are ten hospitals in total, with $\{v_i\}_{i=0}^4$ as large hospitals and $\{v_i\}_{i=5}^9$ as small hospitals.
- ➢ Due to the extreme imbalance of data labels, where over 90% are negative labels, we use the AUC scores to evaluate the performance of the trained model

Table 6: eICU

Figure 6: Real-world Collaboration Example

Results: Extensive experiments over real-world datasets have demonstrated the effectiveness of the proposed solution compared to nine baseline methods, and its ability to establish efficient collaborative networks in cross-silos FL with FL-PTs that engage in business activities.

Thank you for your listening!

Any questions?

