Incentive Mechanism Design for Federated Learning with Unstateful Clients

Bing Luo

Assistant Professor
Electrical and Computer Engineering
Duke Kunshan University

Duke Kunshan University

- Established in 2013, as a U.S. - China Joint Venture University.
- Located in Kunshan (18 mins high-speed train from Shanghai).
- Conferred Duke University Degrees.

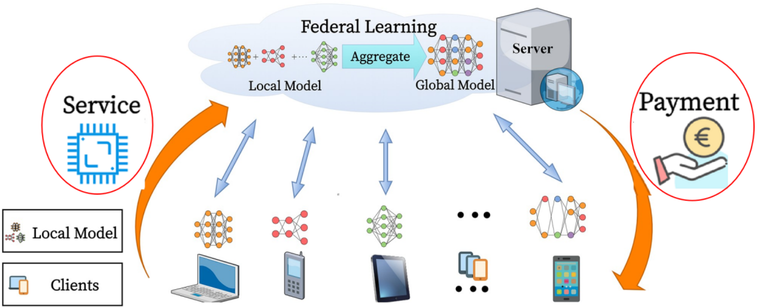
FL Research Overview

Goal: enable effective & efficient FL at the network edge

- **Mechanism Design (Game Theory) (First Half)**
  "Incentive Mechanism Design for FL with Randomized Client Participation," ***ICDCS* 2023**
  "Optimal Mechanism Design for Heterogeneous Client Sampling in FL" ***TMC* 2024**
- **Fed-Campus (Real-world System App.) (Second Half)**
  "FedCampus: A Real-world Privacy-preserving Mobile Application for Smart Campus via FL and FA," ***MobiHoc* 2024 Demo**
  "Fed-Kit: Cross-Platform FL for Android & iOS," ***INFOCOM* 2024 Demo**

Motivation: why FL needs Incentive Mechanism?

- Clients: rational individuals (not altruistic or obedient)
- Server (platform): provide reward to compensate clients' cost



Challenges in FL Incentive Mechanism

Existing mechanisms (”binary” participation) → Cost-Bias Dilemma

Challenge 1: unstable clients (diverse availability)

- Impractical to incentivize full client to participate in all rounds

Challenge 2: unbalanced and non-i.i.d. data

- Incentivize a deterministic subset of clients cause severe bias

Challenges in FL Incentive Mechanism

Existing mechanisms ("binary" participation) → Cost-Bias Dilemma

Challenge 1: unstable clients (diverse availability)

- Impractical to incentivize full client to participate in all rounds

Challenge 2: unbalanced and non-i.i.d. data

- Incentivize a deterministic subset of clients cause severe bias

Key Question 1

How to design a practical incentive mechanism for FL with unstable client availability, and ensure unbiased model convergence

Challenges in FL Incentive Mechanism

- **Challenge 3:** How to evaluate client contribution of participation on the model performance
- **Challenge 4**: Clients may have intrinsic value (internal motivation) to participate for acquiring the powerful model

Challenges in FL Incentive Mechanism

- **Challenge 3:** How to evaluate client contribution of participation on the model performance
- **Challenge 4**: Clients may have intrinsic value (internal motivation) to participate for acquiring the powerful model

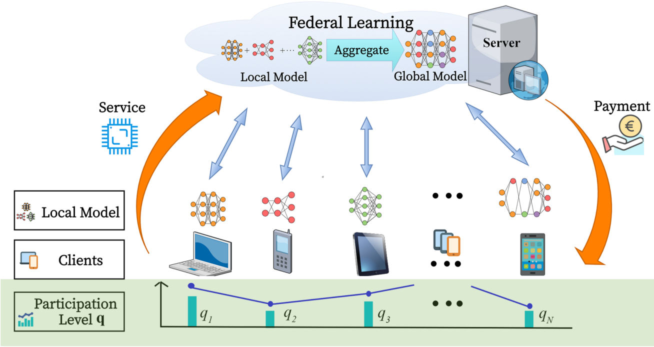
Key Question 2

How to design efficiently payment strategy, considering both clients' contribution to the model and their intrinsic value?

Proposed Partial Participation Mechanism

Incentivize client participation level (probability) q

- **Server:** incentivize clients to join with different participation levels
- **Client:** choose best participation level to maximize own profit.



Proposed Partial Participation Mechanism

- **Server's Goal**: minimize expected FL loss under a budget.
  - **Strategy**: Design customized pricing $\boldsymbol{P} = \{P_1, \ldots, P_N\}$ to incentivize N clients' participation level $\boldsymbol{q} = \{q_1, \ldots, q_N\}$

Server's decision problem P1

$$\begin{array}{ll} \textbf{P1:} \ \min_{\boldsymbol{P}} & U_s(\boldsymbol{P}, \boldsymbol{q}) := \mathbb{E}\left[F\left(\boldsymbol{w}^R(\boldsymbol{q})\right)\right], \\ \text{s.t.} & \sum_{n=1}^{N} P_n q_n \leq B. \end{array}$$

Proposed Partial Participation Mechanism

Client's Goal: seen price P_n, choose q_n to maximize own profit

Client n's decision problem P2

$$\begin{aligned} \textbf{P2}: \max_{q_n} \quad & U_n(\boldsymbol{q}, P_n) := P_n q_n - C_n + V_n \\ \text{s.t.} \quad & 0 \le q_n \le q_{n,\max}. \end{aligned}$$

Note: It is possible for $P_n < 0$, when the value of V_n is large.

- **Local cost model**: increasing marginal cost in economic models when decision variable q_n is constrained

$$C_n = c_n q_n^{\tau}, \ \tau > 1, \text{(we let } \tau = 2 \text{ for analysis)}$$

- **Intrinsic value model**: model performance gain if participate

$$V_n := v_n \left(F(\boldsymbol{w}_n^*) - \mathbb{E}\left[F\left(\boldsymbol{w}^R(\boldsymbol{q}) \right) \right] \right), (v_n : \text{preference level})$$

Model as a Stackelberg Game

Stackelberg Game: sequential decision-making for server/clients.

Stackelberg Game

- **Server (buyer/leader)**: decides pricing strategy $\boldsymbol{P} = \{P_1, \ldots, P_N\}$ to maximize its utility in Stage I;
- **Client (seller/follower)**: given server's pricing strategy $\boldsymbol{P}$, chooses its reactive q_n to maximize its utility in Stage II.

Solution Concept of Stackelberg Game

Solution Concept: Stackelberg equilibrium (SE)

The SE of the proposed game is a set of decisions $\{\boldsymbol{P}^{\text{SE}}, \boldsymbol{q}^{\text{SE}}\}$ satisfying

$$q_n^{\text{SE}}(\boldsymbol{P}) = \arg\max_{q_n(\boldsymbol{P})} U_n\left(q_n(\boldsymbol{P})\right), \forall n \in \mathcal{N},$$

$$\mathbf{P}^{\text{SE}} = \arg\min_{\boldsymbol{P}} U_s\left(\boldsymbol{P}, \boldsymbol{q}^{\text{SE}}(\boldsymbol{P})\right).$$

At SE, neither clients or server has incentive to deviate for better choice of improving utility

Solution Concept: Stackelberg Equilibrium

Backward Induction (methodology to solve SE)

- First, solve clients' $\boldsymbol{q}(\boldsymbol{P})$ given server's pricing $\boldsymbol{P}$ in Stage II;
- Then, move back to determine server's pricing $\boldsymbol{P}$ in Stage I.

Server (leader) | Stage I: Server determines B and $\mathbf{P} = \{P_1, \ldots, P_N\}$

$\Downarrow$

Clients (followers) | Stage II: Clients determines q_n , $n \in \mathcal{N}$, given P

Challenge in Solving Stackelberg Equilibrium

Lemma 1: ensure model unbiased for arbitrary q

Lemma: adaptive aggregation for arbitrary participation q

For arbitrary $\boldsymbol{q}$, aggregate participants' local updates as

$$\mathbf{w}^{r+1} \leftarrow \mathbf{w}^{r} + \sum_{n \in \mathcal{S}(\boldsymbol{q})^{r}} \frac{1}{q_n} \left(\mathbf{w}_n^{r+1} - \mathbf{w}^{r} \right)$$

In expectation, $\mathbf{w}^{r+1}$ is unbiased towards full client participation.

- Intuition: inverse probability weighting (Horvitz-Thompson Estimator) client n's gradient in aggregation (i.e., $\frac{1}{q_n}$)

Challenge in Solving Stackelberg Equilibrium

Challenge: how to analytically characterize q in $\mathbb{E}[F(\mathbf{w}^R(\mathbf{q}))]$

Server's decision problem P1

$$\begin{array}{ll} \textbf{P1:}\ \min_{\boldsymbol{P}} & U_s(\boldsymbol{P}, \boldsymbol{q}) := \mathbb{E}\left[F\left(\boldsymbol{w}^R(\boldsymbol{q})\right)\right], \\ \text{s.t.} & \sum_{n=1}^{N} P_n q_n \leq B. \end{array}$$

Client n's decision problem P2

$$\begin{array}{ll} \textbf{P2}:\ \max_{q_n} & U_n(\boldsymbol{q}, P_n) := P_n q_n - c_n q_n^2 + v_n\left(F(w_n^*) - \mathbb{E}\left[F(\boldsymbol{w}^R(\boldsymbol{q}))\right]\right) \\ \text{s.t.} & 0 \leq q_n \leq q_{n,\max}. \end{array}$$

Challenge in Solving Stackelberg Equilibrium

Theorem: convergence bound for arbitrary participation level q

$$\mathbb{E}[F\left(\mathbf{w}^R(\mathbf{q})\right)] - F^* \leq \frac{1}{R}\left(\alpha \sum_{i=1}^{N} \frac{(1-q_n)}{q_n} + \beta\right)$$

where $\alpha = \frac{8LE}{\mu^2}$, $\beta = \frac{2L}{\mu^2 E}\left(\sum_{n=1}^{N} \frac{\sigma_n^2}{N^2} + 8\sum_{n=1}^{N} \frac{G_n^2(E-1)^2)}{N}\right) + \frac{12L^2}{\mu^2 E}\left(F^* - \sum_{n=1}^{N} \frac{F_n^*}{N}\right) + \frac{4L^2}{\mu E}\|\boldsymbol{w}_0 - \boldsymbol{w}^*\|^2$

Note: for non-convex loss function, we still have similar variance term with $\boldsymbol{q}$.

Insights:

- Indicate how partial client participation ($q_n < 1$) affect the convergence rate compared to full participation ($q_n = 1$).
- Indicate incentive only a deterministic subset of clients may never converge to the optimal (e.g., $q_n \to 0$, $R \to \infty$);

Challenge in Solving Stackelberg Equilibrium

With the bound, P1 can be analytically approximated as P1′:

$$\mathbf{P1}' : \min_{\boldsymbol{q}} \sum_{n=1}^{N} \frac{(1-q_n)}{q_n}$$

$$\text{s.t.} \sum_{n=1}^{N} \left(2c_n q_n - \frac{v_n}{q_n^2} \right) q_n \leq B$$

Challenge in Solving Stackelberg Equilibrium

With the bound, P1 can be analytically approximated as P1′:

$$\mathbf{P1}': \min_{\boldsymbol{q}} \sum_{n=1}^{N} \frac{(1-q_n)}{q_n}$$

$$\text{s.t.} \sum_{n=1}^{N} \left(2c_n q_n - \frac{v_n}{q_n^2}\right) q_n \leq B$$

- **P1′** is non-convex in $\boldsymbol{q}$, and can be efficiently solved by a "liner search + convex optimization".

Define $M := \sum_{n=1}^{N} c_n q_n^2$, linear search bounded M and solve convex P1″

$$\mathbf{P1}'': \min_{\boldsymbol{q}, M} g(\boldsymbol{q}, M) := \sum_{i=1}^{N} \frac{(1-q_n)}{q_n}$$

$$\text{s.t.} \quad 2M - \sum_{n=1}^{N} \frac{v_n}{q_n} \leq B,$$

Insights of the Equilibrium (KKT conditions)

Insights for clients' participation level q_n^{SE}

- **(Local cost).** Clients with larger c_n have lower q_n^{SE}, given similar v_n among others.
- **(Intrinsic value).** It is counter-intuitive that clients with larger v_n have lower q_n^{SE}, given similar c_n among others.
  - This is because the server tends to set a lower price P_n for clients whose v_n is large, which yields a smaller payment $P_n q_n$.

Insights of the Equilibrium (KKT conditions)

Insights for Pricing Design P^{SE}:

- **(Local cost).** Counter-intuitively, clients with larger local cost c_n have higher price P_n^{SE} (to ensure the model unbiasedness.)
- **(Intrinsic value).** Bi-direction payment between the server and clients: there exists a threshold v^{t}, such that $P_n^{SE} > 0$, if $v_n \leq v^{\mathrm{t}}$, and $P_n^{SE} < 0$ otherwise

Experimental Setup

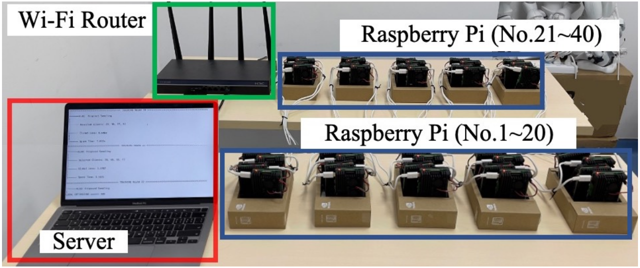
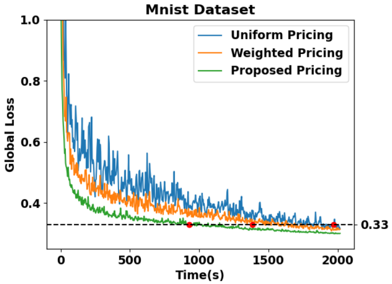


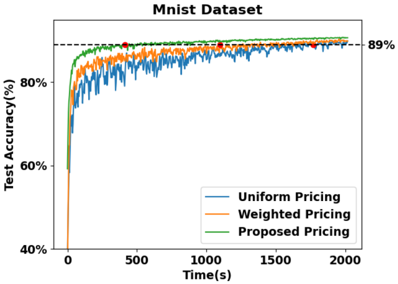
Figure. Hardware testbed

- **Prototype Setup:**
  - 40 Raspberry Pis (clients) and a laptop (server)
  - logistic regression and MNIST dataset (randomly subsample 14, 463 data, distributed in unbalanced and non-iid)
  - Budget $B = 40$;
  - Mean local cost $\bar{c} = 20$ with exponential distribution;
  - Mean intrinsic value $\bar{v} = 30,000$ with exponential distribution.

Experimental Result

- Performances of Training Loss and test accuracy with different pricing schemes for MNIST dataset.





Benchmarks:

- Uniform pricing: same price for all devices
- Weighted pricing: price based on their datasize

Platform's Practical Concerns

Previous mechanism works for complete information, but...

Platform's Practical Concerns

Previous mechanism works for complete information, but...

- **Information Asymmetry**: client's cost valuation c_n is **unknown to the platform**
- **Client strategic behavior**: may manipulate by **misreporting its cost information** to its own advantage

Platform's Practical Concerns

Previous mechanism works for complete information, but...

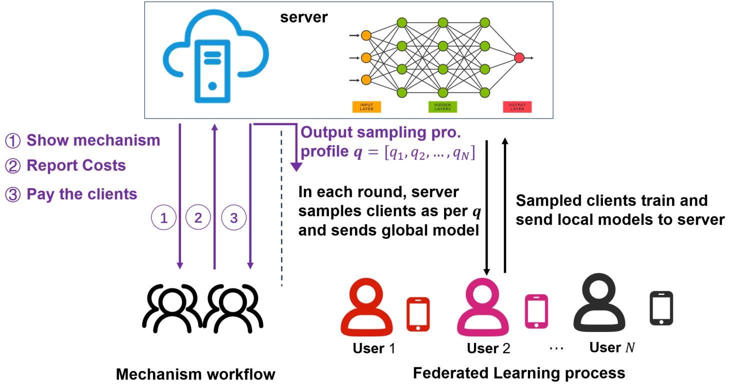
- **Information Asymmetry**: client's cost valuation c_n is **unknown to the platform**
- **Client strategic behavior**: may manipulate by **misreporting its cost information** to its own advantage

Key Question

How should the platform design a practical mechanism to address information asymmetry and client strategicness?

Proposed Auction-based Mechanism Design

We design an auction-based mechanism $m = (P, q)$: payment $P(\cdot)$ and participation $q(\cdot)$ are functions of client reported cost $\tilde{c}_n$ (true cost c_n).



Desirable Economic Properties

Desirable economic properties $m = (P, q)$ should satisfy:

Incentive Compatibility (IC)

IC ensures any client n (with true cost c_n) can maximize its utility if truthfully reports its cost:

$$u(c_n; c_n) \geq u(\tilde{c}_n; c_n), \quad \forall \tilde{c}_n \neq c_n$$

Individual Rationality (IR)

IR ensures that any client's utility is non-negativity:

$$\max_{\tilde{c}_n} \; u(\tilde{c}_n; c_n) \geq 0$$

Budget Feasibility

$$\mathbb{E}_{\boldsymbol{c}} \left[\sum_{n \in \mathcal{N}} q(c_n) \cdot r(c_n) \right] \leq B.$$

Mechanism Design Problem

Mechanism Design Problem P1

$$
\begin{aligned}
\mathrm{P1}: \min_{P(\cdot),q(\cdot)} \quad & \mathbb{E}_{\boldsymbol{c}}\left[F\left(\boldsymbol{w}^{R}(q(c_n))\right)\right] \\
\text{s.t.} \quad & \text{Incentive compatibility (IC)} \\
& \text{Individual rationality (IR)} \\
& \text{Budget feasibility} .
\end{aligned}
$$

Optimal Mechanism Design for IC and IR

Theorem 2. (Myerson's Lemma)

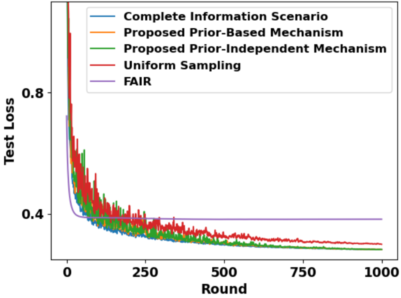
A mechanism $m = (P, q)$ is IC and IR iff:

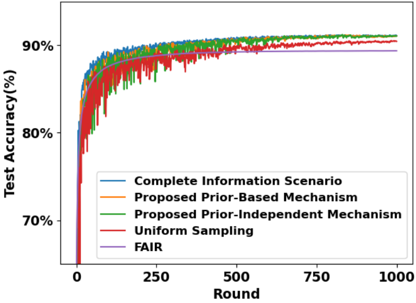
- Participation $q(\tilde{c})$ is non-increasing in the report $\tilde{c}$;
- Payment function $P(\tilde{c})$ has the following form:

$$P(\tilde{c}) = \tilde{c} + \frac{1}{q(\tilde{c})} \int_{\tilde{c}}^{c_{\max}} q(z)dz.$$

Experimental Result

Performances of Loss and accuracy with different sampling strategies for MNIST dataset, with exponential distribution cost.





Observation: Similar to complete information upper bound

Summary

- We firstly design a practical mechanism for FL with unstable client availability, which guarantees the obtained model is unbiased to converge.
- We derived tractable convergence bound that analytically characterizes the impact of clients' participation levels on the model performance, yielding a customized pricing scheme.
- We introduced a new intrinsic value in clients' utilities, which allows an interesting possibility of bidirectional payment.
- To address the challenge of unknown prior information, we further designed a prior-independent mechanism that leverages incentive compatibility.

Thanks !!