Privacy-preserving Stable Crowdsensing Data Trading for Unknown Market

IEEE INFOCOM 2023

May 17, 2023

He Sun[1] , Mingjun Xiao[1], Yin Xu[1], Guoju Gao[2], Shu Zhang[1]

1 School of Computer Science and Technology & Suzhou Institute for Advanced Study, University of Science and Technology of China

2 School of Computer Science and Technology, Soochow University

CONTENTS

CONTENTS

Introduction

Crowdsensing Data Trading (CDT)

Concept of CDT

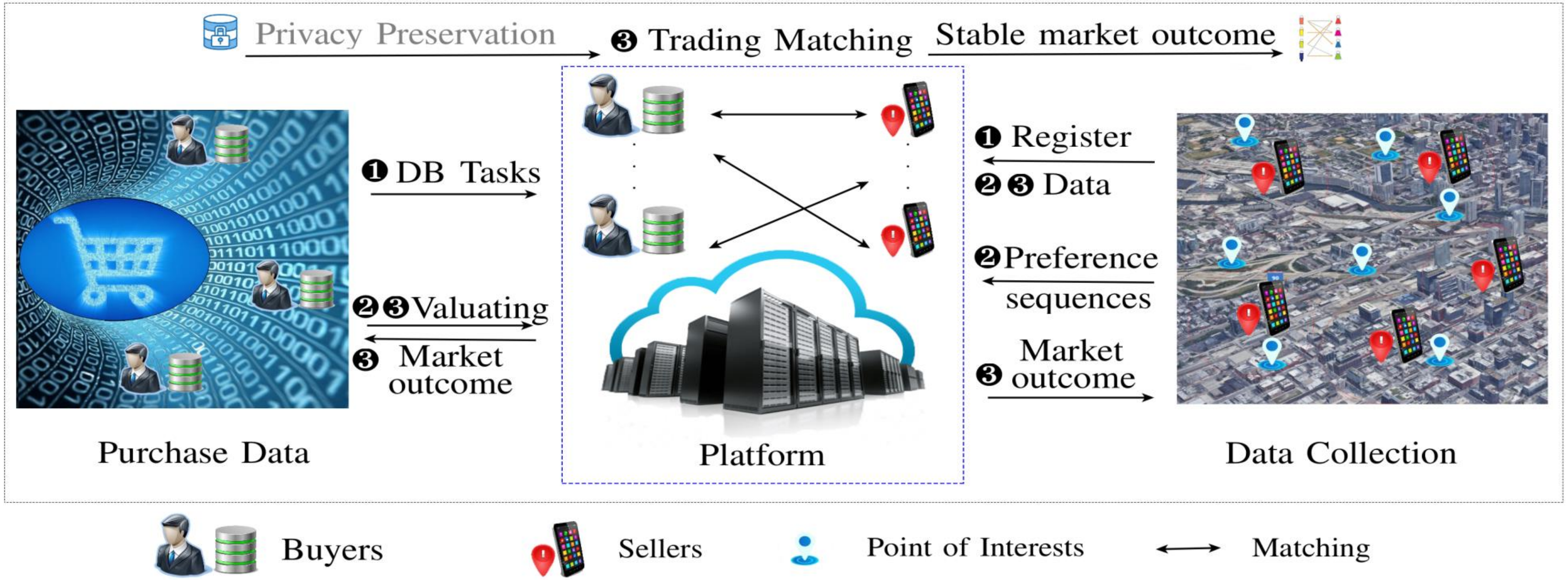
A new data trading paradigm where the **Mobile CrowdSensing (MCS)** technique is adopted to provide data sources, e.g., Thingful, ThingSpeak.

Concept of Matching Markets

- ✓ Both sides of the markets **can't just choose what you want** even if you can afford it.
- ✓ One of them **also have to be chosen.**
- ✓ They choose each other according to the **preferences** of each other.

Introduction

Components of CDT systems



Platform: As a broker, it provides a credible data trading service for sellers and buyers

Buyers: Propose and publish their data requirements to the platform to collect data

Sellers: A crowd of mobile users to provide data collection service to buyers.

Introduction

Existing Problems

- A few existing CDTs consider the stability of the Data Trading Market.
- The Data Trading Market is unknown in practice, i.e., the preference sequences over sellers are unknown by buyers.
- The private information of sellers needs to be preserved.

- Our **goal** is to solve the above problems simultaneously

Trading Stability

Unknown Market

Privacy Concerns

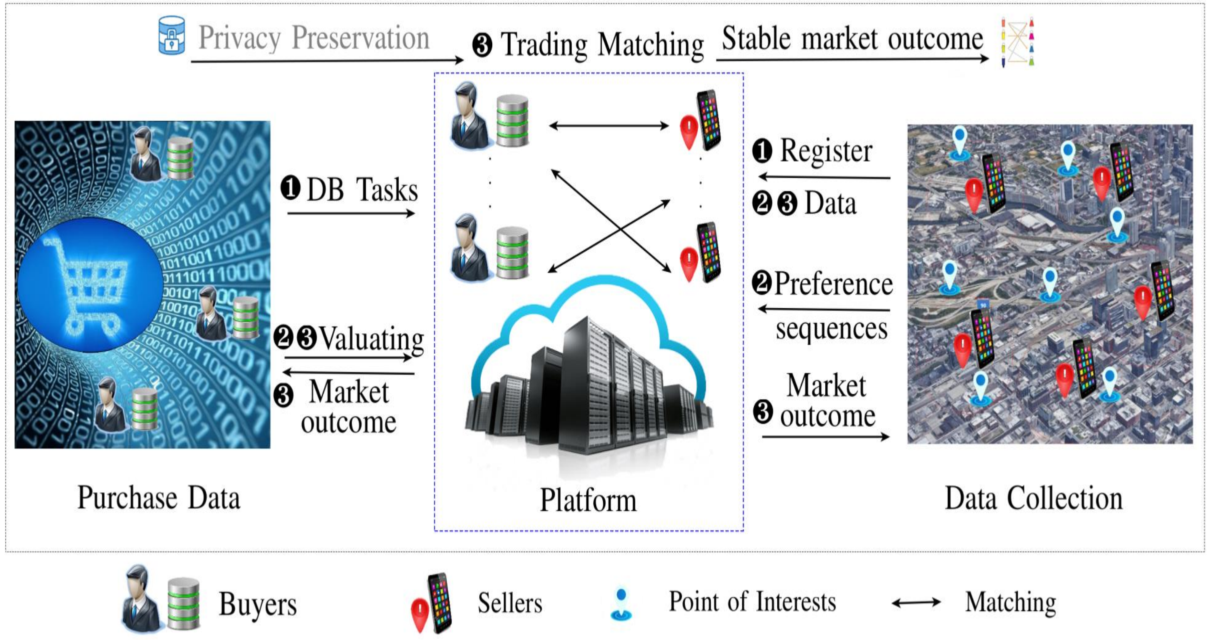
CONTENTS

System, Modeling, and Problem

Definitions in CDT systems

Buyer: They are the data consumers

- ✓ Denoted by $\boldsymbol{B} = \{1,2, \dots, B\}$.
- ✓ Focusing on the matching of tasks and sellers, the published tasks are denoted by $\boldsymbol{T} = \{1,2, \dots, T\}$.



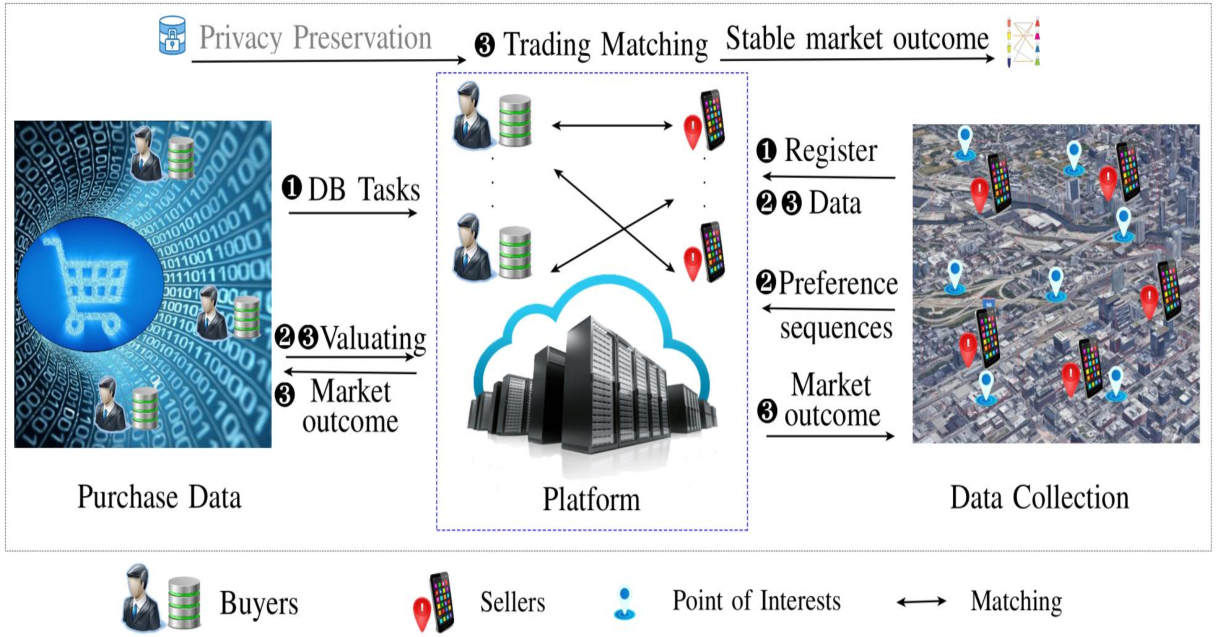
Sellers:

- ✓ Denoted by $\boldsymbol{S} = \{1,2, \dots, S\}$.
- ✓ The collected data quality of seller j for task i in l^{th} round is denoted by $q_i^l(j) \in [0,1]$.
- ✓ The mean data quality from 1st to l^{th} round is denoted by $\bar{q}_i^l(j)$. **Unknown**
- ✓ The number of sellers and tasks are unequal, thus we assuming $\boldsymbol{S} \geq \boldsymbol{T}$, W.L.O.G.

System, Modeling, and Problem

The workflow of CDT systems

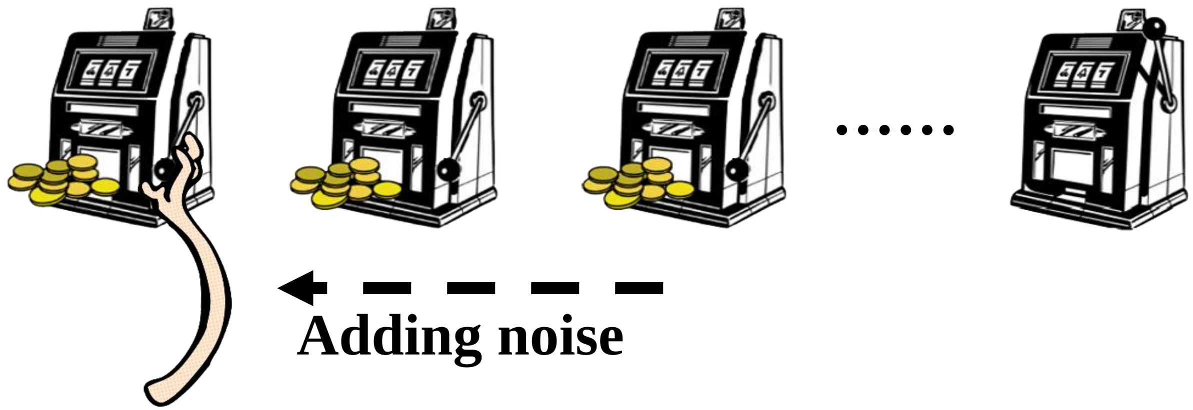
- ✓ **Buyers** publish tasks and sellers register on the platform.
- ✓ **Sellers** transfer the collected data and buyers give the data evaluation to the platform as matching feedback.
- ✓ The **platform** builds the initial perturbed preference sequences after adding some noise.



- ✓ Meanwhile, each **seller** gives their preference sequences to the platform.
- ✓ The **platform** makes matching and gets a matching result by G-S algorithm in each round.

System, Modeling, and Problem

ϵ-Differentially private bandit model



$$j^* = \Phi_i^l(q_i^{1:l-1})$$

Return the selected arm

$$\mathbb{P}\{\Phi_i(q_i^{1:l-1}) \in \mathcal{X}\} \leq e^{\epsilon} \cdot \mathbb{P}\{\Phi_i(q_i^{1:l-1'}) \in \mathcal{X}\} \quad (1)$$

- ✓ where $\epsilon > 0$ is a small constant that the policy provides, indicating the privacy-preserving level.

Platform	Game players
Sellers	Arms
Select a seller	Pull an arm
Data quality	Reward
Protected Data quality	Perturbed reward

- ✓ A bandit policy Φ_i of play i is a sequence of arm-pulling decisions.
- ✓ $\Phi_i = \{\Phi_i^1, \ldots, \Phi_i^l, \ldots\}$
- ✓ $q_i^{1:l} = \{q_i^1, \ldots, q_i^l\}$
- ✓ $q_i^{1:l-1'}$ is its adjacent sequence

System, Modeling, and Problem

δ-Stable Matching Model

Definition of preference

Unknown preference sequences of the buyer

- ✓ Denoted by $\pi_k^{l'} = \{\dots, \pi_i^l, \dots\}$, $\pi_i^l = \{\dots, j, j', \dots\}$.
- ✓ $\pi_i^l(j)$ denotes the rank of seller j in π_i^l.
- ✓ $v_i = \{\dots, v_i^l(j), \dots\}$ denotes the value. (Unknown)

Preference sequence of the seller

- ✓ Denoted by $\pi_\mathrm{j} = \{\dots, i, i', \dots\}$.
- ✓ $\pi_j(i)$ denotes the rank of task i in π_j.

Adding noise ➡ Matching is not truly stable

Definition of δ-stable: We say a market outcome M^l is δ-stable with a probability less equal than $1-\delta$ that a preference sequence is invalid, i.e., there exists two matching pairs $\langle i, j\rangle$ and $\langle i, j^*\rangle, \forall i \in T, \forall j, j^* \in S$, satisfies $\pi_i^l(j) \prec_i \pi_i^l(j^*)$, $\hat{\pi}_i^l(j) \prec_i \hat{\pi}_i^l(j^*)$ and $\hat{v}_i^l(j) - \hat{v}_i^l(j^*) > \xi_0'$, denoted by $\widehat{M}^k$. ξ_0' is a perturbed care bound and δ is a constant less than but close to 1.

$\pi_i^l(j) \prec_i \pi_i^l(j^*)$: task i prefers seller j to j^* in l^{th} round.

System, Modeling, and Problem

Problem formulation

Our goal is to make the optimal matching in each round according to the built perturbed preference sequences, i.e., to maximize the expected accumulative reward for each task, assuring the ϵ-differential privacy and δ-stable of market outcomes in each rounds.

$$Maximize: \sum_{l} q_i^l(m^l(i))$$

Expected accumulative reward for task i.

$$Subject\ to: Eq.\ (1)\ holds$$

Each bandit policy of the task needs to satisfy ϵ-differential privacy.

$$\mathcal{M}^l\ is\ \delta\text{-}stable$$

The market outcome in each round needs to be δ-stable.

CONTENTS

The DPS-CB Data Trading Mechanism

Basic Idea of DPS-CB Mechanism

✓ Traditional UCB index

✓ Traditional Gale and Shapley

The hybrid ϵ- differential privacy mechanism → **The Differentially Private Upper Confidence Bound(DP-UCB) index** → **DPS-CB Mechanism**

- ✓ Preserving the privacy of sellers
- ✓ Theoretical guarantee

- ✓ Unknown market
- ✓ Balance exploration & exploitation
- ✓ Maximize the accumulative reward

- ✓ Since the added noise, we first define the δ-Stable
- ✓ Assuring the δ-Stability of the market outcome theoretically

The DPS-CB Data Trading Mechanism

DPS-CB Mechanism

- **Hybrid ϵ-differential privacy**

- ✓ $c_2(l)$ is a function that counts the number of 1 in the binary expression of l

$$\mathcal{H}(q_i^{1:l}(j)) = \boxed{\sum_l q_i^l(j)} + \boxed{Lap(\frac{2TS}{\epsilon}) + \boxed{c_2(l)} Lap(\frac{2TSlogl}{\epsilon})}$$

- ✓ Adding the hybrid noise to a data quality sequence

- ✓ $Lap()$ denotes Laplace distribution whose probability is $f(x)|_{Lap(\gamma)} = \frac{1}{2\gamma}\exp\left(\frac{-|x|}{\gamma}\right)$.
- ✓ The $c_2(l)+1$ Laplace noises will be added in l^{th} round.

The DPS-CB Data Trading Mechanism

DPS-CB Mechanism

➢ DP-UCB index

- ✓ The DP-UCB indexes are computed by the perturbed average data quality and upper confidence bound.
- ✓ It can well tackle the e-e dilemma and preserve the privacy

$$I_i^l(j) = \begin{cases} -1 & \text{if } n_i^l(j) = 0, \\ \boxed{\hat{q}_i^l(j)} + \boxed{\sqrt{\frac{7log(l)}{4n_i^l(j)}}} & \text{otherwise.} \end{cases}$$

$$\text{where} \quad \hat{q}_i^l(j) = \frac{1}{n_i^l(j)} \hat{Q}_i^l, \quad \hat{Q}_i^l = \mathcal{H}(q_i^{1:l}(j))$$

- ✓ The perturbed average data quality of seller j for task i in l^{th} round.
- ✓ $n_i^l(j)$ is the number of times that task i matches seller j until l^{th} round

- ✓ The upper confidence bound is a way to balance the exploration and exploitation (e-e dilemma).
- ✓ When the $n_i^l(j)$ increases (exploitation), the probability of other new matching pairs matched will increase (exploration).

The DPS-CB Data Trading Mechanism

DPS-CB Mechanism

$l \leq T$

$$\hat{\pi}_i^T = \{\cdots, j, j', \ldots\} \xleftarrow{\textbf{Sorted}} \hat{v}_i^T = \{\cdots, I_i^T(j), \ldots\}$$

Perturbed preference sequences of task

Perturbed preference value sequences

- ✓ The DP-UCB indexes of sellers for different tasks are learned and sorted in descending order in first T rounds
- ✓ It forms the initial perturbed preference sequences of tasks for initial exploration.

$$\pi_j = \{\cdots, i, i', \ldots\}$$

Perturbed preference value sequences of seller

The DPS-CB Data Trading Mechanism

DPS-CB Mechanism

$l > T$

$$\hat{\pi}_i^l = \{\cdots, j, j', \ldots\}, \xleftarrow{\textbf{Updated}} \hat{v}_i^l = \{\cdots, I_i^l(j), \ldots\}$$

Perturbed preference sequences of task

Perturbed preference value sequences

- ✓ The platform will make a matching in the Gale-Shapley way in each round until all tasks are matched.
- ✓ *Note: the market outcome returned by GS algorithm is always optimal for the proposing side (i.e., tasks).

$$\pi_j = \{\cdots, i, i', \ldots\}$$

Perturbed preference value sequences of seller

D. E. Knuth, *Stable marriage and its relation to other combinatorial problems: An introduction to the mathematical analysis of algorithms*. American Mathematical Soc., 1997, vol. 10

The DPS-CB Data Trading Mechanism

Algorithm 1: DPS-CB mechanism

Input: the total time T, the preference sequences set $\{\pi_j | \forall j \in \mathcal{S}\}$ of sellers.

Output: $\{\mathcal{M}^l | l = 1, 2, ...\}$

1 **for** $l = 1, ..., N$ **do**

2   **if** $l \leq T$ **then**

3         $m^l(l) \leftarrow j, \ \forall\ j \in \mathcal{S}$

4   Get $\hat{q}_l^l(j)$ as the corresponding reward according to Eqs. (6-8) while using ϵ as the privacy budget the under hybrid differentially private mechanism.

5   **else if** $l = T + 1$ **then**

6   Compute the DP-UCB indexes $I_i^l(j)$, $\forall i \in \mathcal{T}$, $\forall j \in \mathcal{S}$ according to Eq. (9).

7   Sort the sellers by the DP-UCB index to build the initial perturbed preference sequence $\hat{\pi}_i^l$ of each task over sellers.

8   Compute stable matching to get the market outcome $\mathcal{M}^l$ according to $\{\pi_j | \forall j \in \mathcal{S}\}$ and $\{\hat{\pi}_i^l | \forall i \in \mathcal{T}\}$ using G-S algorithm.

9   **else**

10   Update $I_i^l(j)$, $\forall i \in \mathcal{T}$, $\forall j \in \mathcal{S}$ and $\{\hat{\pi}_i^l | \forall i \in \mathcal{T}\}$ according to Eqs. (6-9).

11   Compute stable matching to get the market outcome $\mathcal{M}^l$ in the way of Step 8.

12   **end**

13 **end**

Lines 1- 4:
Initial exploration: quality learning

Lines 5- 8:
Compute the DP-UCB indexes and build the perturbed preference sequences

Lines 9- 12:
Exploitation: Make matching according to the learned preferences and update the DP-UCB indexes and preferences

The DPS-CB Data Trading Mechanism

Theoretical Analysis

- ✓ **Theorem 1.** The DP-SCB mechanism satisfies ϵ-differential privacy.

$$\frac{\mathbb{P}\{\mathcal{H}(q_i^{1:l}(j)) = r_0\}}{\mathbb{P}\{\mathcal{H}(q_i^{1:l}(j)') = q_0\}} \leq e^{\frac{\epsilon \Delta_q}{TS}} \leq e^{\frac{\epsilon}{TS}}$$

- ✓ **Theorem 2.** The market outcome computed by DP-SCB mechanism is δ-stable.

$$\epsilon \geq \frac{ln\delta}{(\zeta_{min} - \zeta_{max})l}$$

- ✓ **Theorem 3.** The DPS-CB mechanism can achieve $O(log(N))$ pessimal stable regret

$$Reg_i'(N) \leq S\Delta' + \sum_{j':\Delta'_{i,j'}>0} \Delta'_{i,j'} e^{-\frac{1}{\epsilon(\zeta_{min}-\zeta_{max})N}}$$

$$\cdot \left[\min_{G \in \mathcal{F}(M')} \sum_{\langle i,j^*,j \rangle \in G} \left(5 + \frac{7log(N)}{\Delta^2_{i,j^*,j}}\right)\right]$$

CONTENTS

Experimental Evaluation

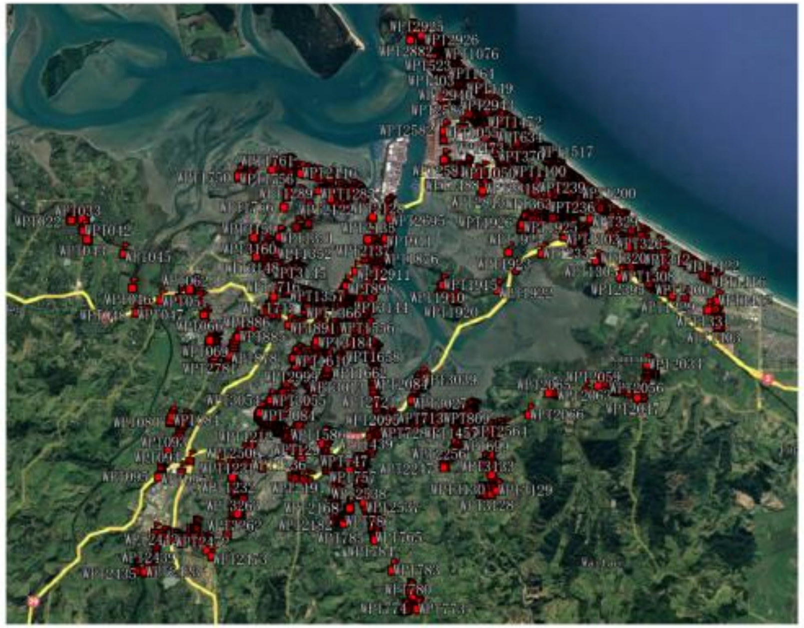
Evaluation Setup

Parameter Name	Range
number of rounds N	$1,2,3\ldots,10$ $(\times 10^3)$
number of sellers $\boldsymbol{S}$	50
number of tasks $\boldsymbol{T}$	50
Data quality $q_i(j)$	(0,1]
Privacy parameter ϵ	2.0, 1.6, 1.2, 0.8
Corporation algorithm ϵ_0-first	0.1, 0.2

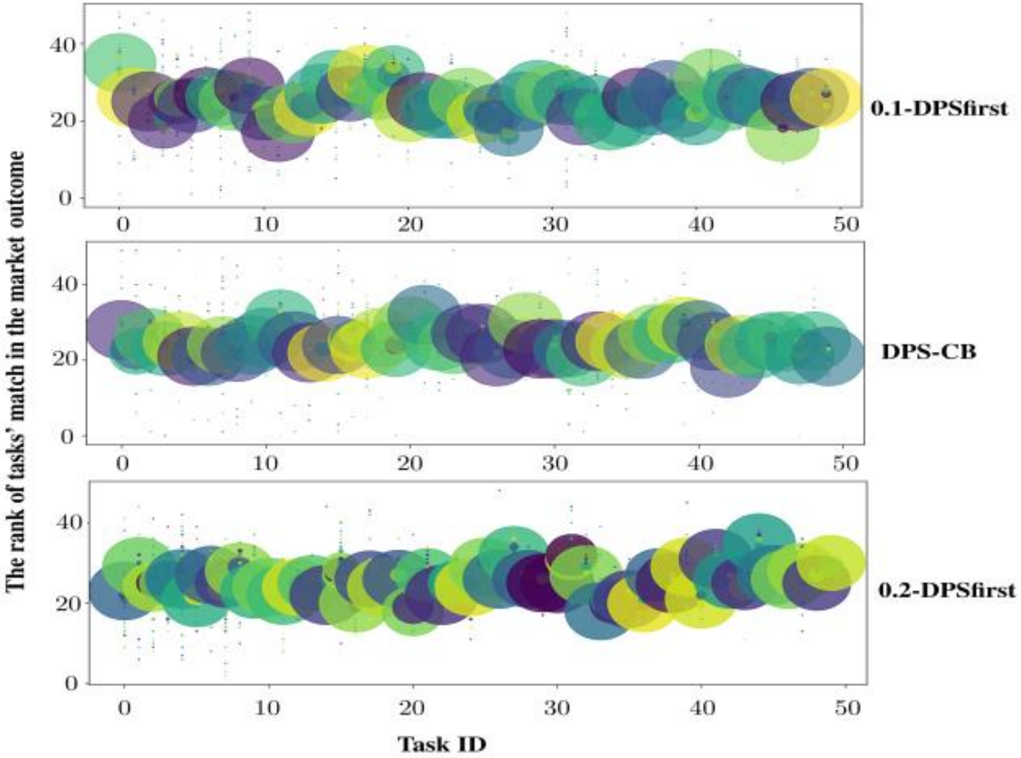
- ✓ **Dataset:**
  A real-world driving records analysis dataset of Uber drivers in New Zealand[31]
- ✓ **Compared Algorithms:**
  ϵ_0-DPSfirst [2][32][33] (ϵ_0 = 0.1, 0.2), and DPS-random

Experimental Evaluation

Drivers and rank distribution



(a) Uber drivers' distribution

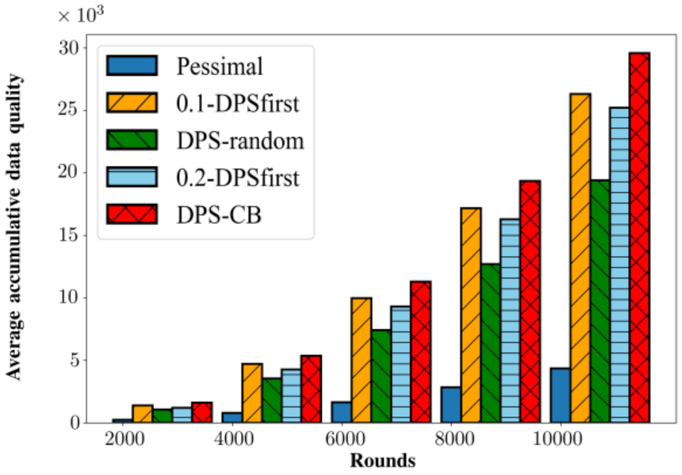


(b) The rank distribution of DPS-CB and compared algorithms, $\epsilon = 2.0$

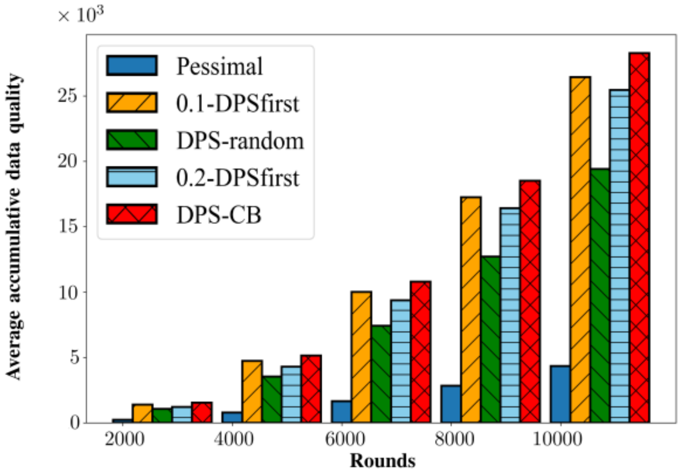
Experimental Evaluation

Accumulative reward

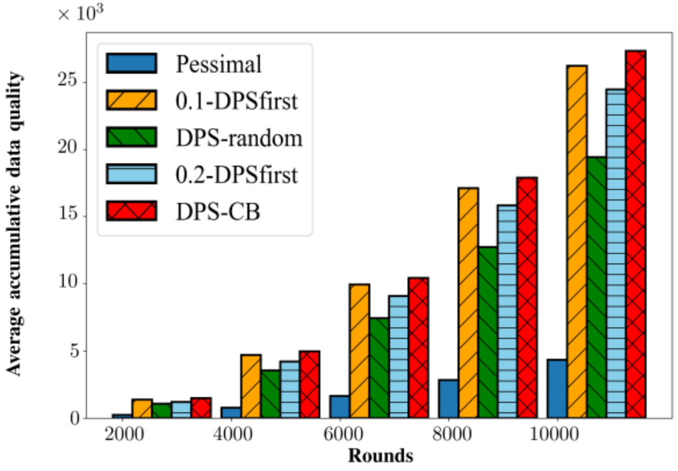
- ✓ The average accumulative data quality
- ✓ ϵ_0 -DPSfirst, DPS-random, Pessimal and DPS-CB
- ✓ Different privacy budgets, $\epsilon = 2.0, 1.6, 1.2, 0.8$
- ✓ S, T = 50, N = 10000



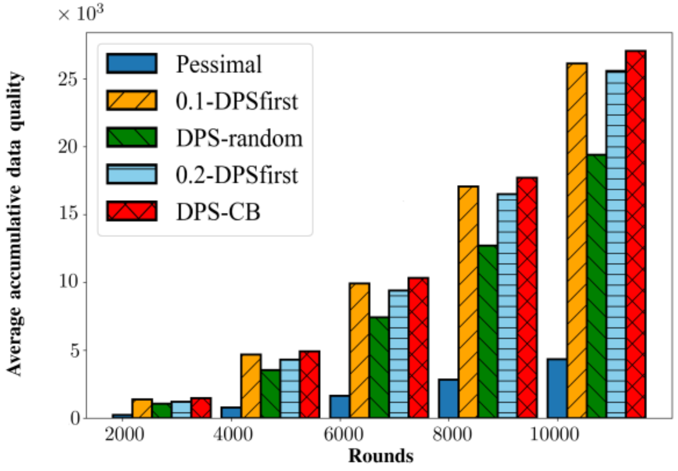
(a) $\epsilon = 2.0, N = 10000$



(b) $\epsilon = 1.6, N = 10000$



(c) $\epsilon = 1.2, N = 10000$

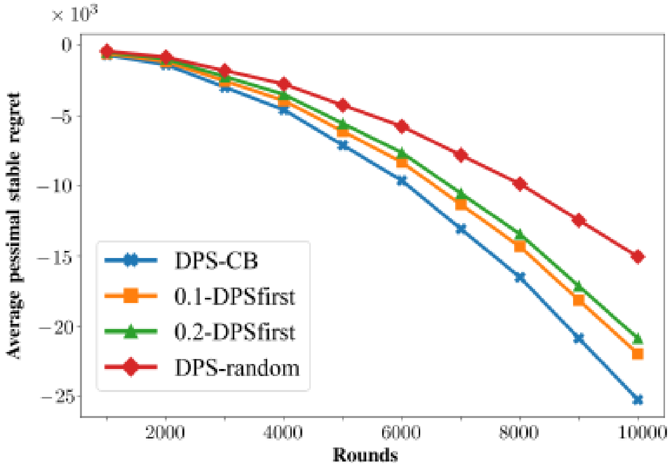


(d) $\epsilon = 0.8, N = 10000$

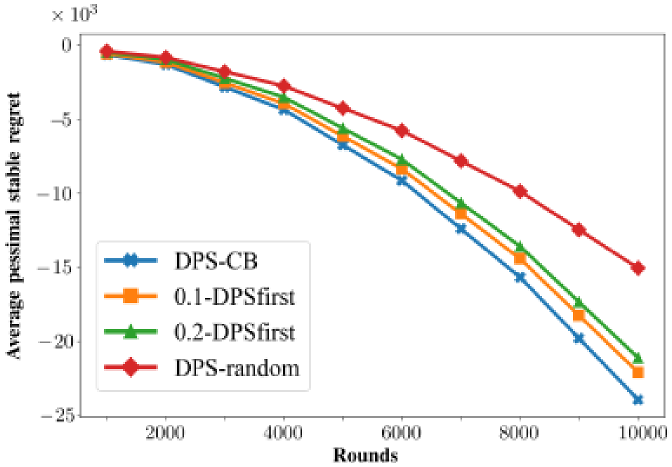
Experimental Evaluation

Pessimal stable regret

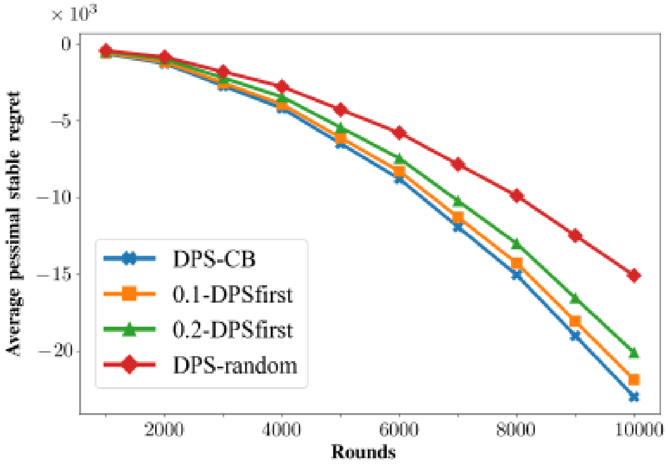
- ✓ The average pessimal stable regret
- ✓ ϵ_0 -DPSfirst, DPS-random, Pessimal and DPS-CB
- ✓ Different privacy budgets, $\epsilon = 2.0, 1.6, 1.2, 0.8$
- ✓ S, T = 50, N = 10000



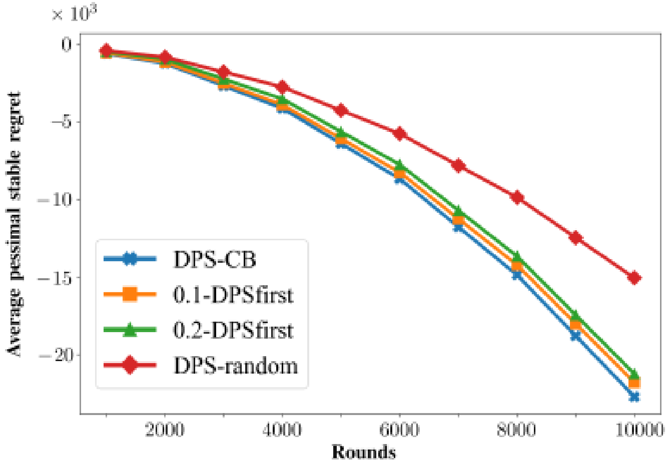
(a) $\epsilon = 2.0, N = 10000$



(b) $\epsilon = 1.6, N = 10000$



(c) $\epsilon = 1.2, N = 10000$



(d) $\epsilon = 0.8, N = 10000$

CONTENTS

Conclusion

- **Focus on privacy-preserving unknown-market stable data trading mechanism design**
- **Model the privacy-preserving stable data trading for unknown market as Differentially Private Stable Competing Bandit model**
  - Maximize the expected accumulative reward for each task
  - Assuring the ϵ-differential privacy of DPS-CB
  - Assuring δ-stable of market outcomes by DPS-CB in each rounds
- **Prove that the market outcome of DPS-CB mechanism is δ-stable.**
- **Prove that DPS-CB mechanism can achieves a tight sublinear bound on regret.**
- **The performance is demonstrated on a real-world dataset.**

Thank you for your attention!

He Sun , Mingjun Xiao , Yin Xu , Guoju Gao , Shu Zhang

hesun@mail.ustc.edu.cn