Balancing Efficiency and Privacy in a Decision-Dependent Network Game

Raphaël Taisant, Mandar Datar, Hélène Le Cadre, Eitan Altman

Balancing Efficiency and Privacy in a Decision-Dependent Network Game

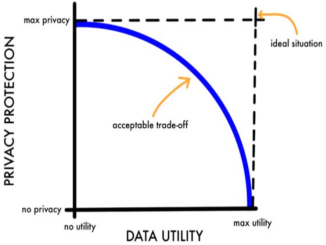
R. Taisant, M. Datar, H. Le Cadre, E. Altman

PGMO Days – November 29-30, 2022

Centre de Recherche en Informatique, Signal et Automatique de Lille

General Setting

- Trade-off between cost minimization and privacy preservation
- Strategic information might decrease the End Users (EUs)' costs while protecting their privacy
- Moral hazard (information asymmetry) and free-rider behaviors generate system inefficiencies

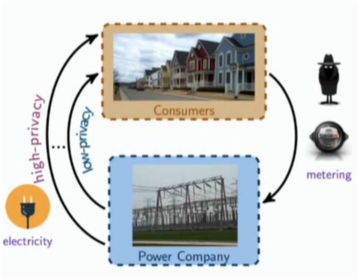


How to measure Privacy?

Privacy is captured through the minimization of information release and α indistinguishability (Dwork, 2020).

Goals

- Design contracts which incentivize the EUs to report truthfully their readings
- Capture the shift caused by the EUs' strategic information on their decisions and market performance
- Formulate the problem as a stochastic game and provide new algorithms to compute equilibria
- Quantify the trade-off between efficiency loss and privacy



Description of the Agents

- The End Users
- The Market Operator
- The Data Aggregator

The End Users

Network structure

- $\mathcal{N}$ set of N End Users (EUs) forming a directed graph $\Gamma \triangleq (\mathcal{N}, E)$
- Γ_n set of nodes EU n can interact with
- $E \subseteq \mathcal{N} \times \mathcal{N}$ set of links
- $\Gamma_0 = \mathcal{N} \setminus \{0\}$, i.e., EU 0 can communicate with any other nodes

EU n's decision variables

$\boldsymbol{x}_n \triangleq \left(D_n, G_n^c, (q_{mn})_{m\in\Gamma_n}\right) \in \mathcal{X}_n$
demand, controllable generation, bilateral trades[1]. We introduce $Q_n = \sum_{m\in\Gamma_n} q_{mn}$

G_n^{nc}: non-controllable generation of player n

EU n's strategy set

$\mathcal{C}_n(\boldsymbol{x}_{-n}) \triangleq \left\{\boldsymbol{x}_n = \left(D_n, G_n^c, (q_{mn})_{m\in\Gamma_n}\right) \in \mathcal{X}_n \mid q_{mn} = -q_{nm}, \forall m \in \Gamma_n\right\}$ with
$\mathcal{X}_n \triangleq \left\{\boldsymbol{x}_n = \left(D_n, G_n^c, (q_{mn})_{m\in\Gamma_n}\right) \in \mathbb{R}^{m_n} | \underline{D}_n \leq D_n \leq \overline{D}_n, \underline{G}_n^c \leq G_n^c \leq \overline{G}_n^c, D_n \leq G_n^c + G_n^{nc} + Q_n\right\}$

[1] $q_{mn} \geq 0$ means that n buys q_{mn} from m; while $q_{mn} < 0$ means that n sells $-q_{mn}$ to m.

EU n's Parametrized Optimization Problem

Private Information $\theta_n \in \Theta_n \subseteq \mathbb{R}$

Utility Function $\Pi_n : \mathbb{R}^{m_n} \times \prod_m \Theta_m \to \mathbb{R}$

$$\Pi_n(\boldsymbol{x}_n, \theta_n) = \sum_{m \in \Gamma_n} c_{nm} q_{mn} - U_n(D_n, \theta_n) + C_n^G(G_n^c)$$

with

- $\boldsymbol{c}_n > \boldsymbol{0}$ EU n's preferences
- $-U_n(.) = \tilde{a}_n \Big(D_n - \theta_n\Big)^2 - \tilde{b}_n$ consumption cost, with $\tilde{a}_n, \tilde{b}_n$ positive coefficients
- $C_n^G(G_n^c) = \frac{a_n}{2} G_n^{c\,2} + b_n G_n^c + c_n$ EU n's controllable generation cost, with a_n, b_n, c_n positive coefficients

Distributed clearing as a non-cooperative game $\mathcal{G}$

$$\forall n \in \mathcal{N}, \min_{\boldsymbol{x}_n \in \mathcal{C}_n(\boldsymbol{x}_{-n})} \Pi_n(\boldsymbol{x}_n, \theta_n) \tag{1}$$

The Market Operator

Social Cost $SC(\boldsymbol{x},\boldsymbol{\theta}) \triangleq \sum_n \Pi_n(\boldsymbol{x}_n,\boldsymbol{\theta}_n)$

Centralized clearing as an optimization problem

$$\min_{\boldsymbol{x}} \; SC(\boldsymbol{x},\boldsymbol{\theta}), \tag{2a}$$

$$s.t. \;\; \boldsymbol{x} \in \mathcal{C} \triangleq \prod_n \mathcal{C}_n(\boldsymbol{x}_{-n}). \tag{2b}$$

Centralized vs Distributed Clearings (Le Cadre et al., 2020)

A subset of the solutions of problem (1) can be computed by solving the optimisation problem (2).

Variational Analysis of the Non-cooperative Game $\mathcal{G}$

Set $\boldsymbol{F}_x(\boldsymbol{x}) \triangleq \left(\nabla_{\boldsymbol{x}_n}\Pi_n(\boldsymbol{x}_n, \theta_n)\right)_n$

Definition of a Variational Equilibrium (Scutari et al., 2010)

The Variational Inequality problem $\mathrm{VI}(\boldsymbol{F}_x, \mathcal{C})$ consists in finding a vector $\boldsymbol{x}^* \in \mathcal{C}$ such that $(\boldsymbol{y} - \boldsymbol{x}^*)^T \boldsymbol{F}_x(\boldsymbol{x}^*) \geq 0, \forall \boldsymbol{y} \in \mathcal{C}$. A solution of $\mathrm{VI}(\boldsymbol{F}_x, \mathcal{C})$ is called a Variational Equilibrium (VE).

Closed Form Expression of the VE

If no energy surplus is available at node n, then at equilibrium $\boldsymbol{x}_n^* = \boldsymbol{A}_{n,n}\theta_n + \boldsymbol{A}_{n,-n}\boldsymbol{\theta}_{-n} + \left[\boldsymbol{B}_{n,n}G_n^{nc} + \boldsymbol{B}_{n,-n}\sum_{n' \neq n} G_{n'}^{nc}\right] + \boldsymbol{C}_n$, with $\boldsymbol{A}_{n,n}$, $\boldsymbol{B}_{n,n}, \boldsymbol{B}_{n,-n}, \boldsymbol{C}_n$ vectors and $\boldsymbol{A}_{n,-n}$ matrix of appropriate dimensions; otherwise $\boldsymbol{x}_n^*$ depends only on the EU n's own nominal demand, θ_n.

Problem: The coefficients of the best-responses $(\boldsymbol{x}_n^*)_n$ depend on coefficients $(\tilde{a}_n, a_n)_n$ that the other EUs might not want to share.

Assumptions 1 and 2

(1) Demand and supply balance each other at each node, i.e., $D_n = G_n^c + G_n^{nc} + Q_n, \forall n \in \mathcal{N}$.

(2) There exists at least one EU $n \in \mathcal{N}$ such that at the VE, $D_n^* \neq 0$ or $G_n^{c*} \neq 0$.

Uniqueness of the VE

Under Assumption 2, the game $\mathcal{G}$ admits a unique VE, which is in addition efficient.

Definition of Variational Stability (Mertikopoulos et al., 2017)

An equilibrium point $\boldsymbol{x}^* \in \mathcal{C}$ is said to be variationally stable (or simply stable) if there exists a neighborhood $\mathcal{U}$ of $\boldsymbol{x}^*$ such that $(\boldsymbol{y} - \boldsymbol{x}^*)^T \boldsymbol{F}_x(\boldsymbol{y}) \geq 0$ for all $\boldsymbol{y} \in \mathcal{U}$. In particular, if this property holds for all $\boldsymbol{y} \in \mathcal{C}$, we say that $\boldsymbol{x}^*$ is globally stable.

Stability of the VE

The VE solution of $\mathcal{G}$ is globally stable.

Assumption 3

(3) EUs' preferences for trading are uniform and normalized, i.e., $c_{nm} = 1, \forall n, m \in \mathcal{N}, n \neq m$.

Under Assumptions 1 and 3, controlling $\boldsymbol{D}, \boldsymbol{G}^c$ allows to control $\boldsymbol{Q}$.

The Data Aggregator

Objective Design contracts to incentivize the EUs to report truthful readings that can be later monetized.

With the introduction of the DA, the private information of each EU becomes an important asset in our model.

> **“Personal data is the new oil of the internet & the new currency of the digital world.”**
>
> MEGLENA KUNEVA, European Consumer Commissioner

Balancing Cost and Privacy

Reading sent by EU n to the data aggregator

$$\widetilde{\theta}_n = \underbrace{\widehat{\theta}_n}_{\text{deterministic bias}} + \underbrace{\varepsilon_n}_{\text{noise}}$$

Assumption 4

For each EU $n \in \mathcal{N}$, ε_n follows a centered Gaussian distribution with variance V_n. Furthermore, the random variables $(\varepsilon_n)_{n\in\mathcal{N}}$ are independent.

Contract payment to EU n

$$p_n^a(\boldsymbol{x}_n, \boldsymbol{x}_n^a, \widetilde{\boldsymbol{\theta}}) = \gamma_n - \beta_n\Big((D_n - D_n^a)^2 + (G_n^c - G_n^{c\ a})^2\Big) \quad (3)$$

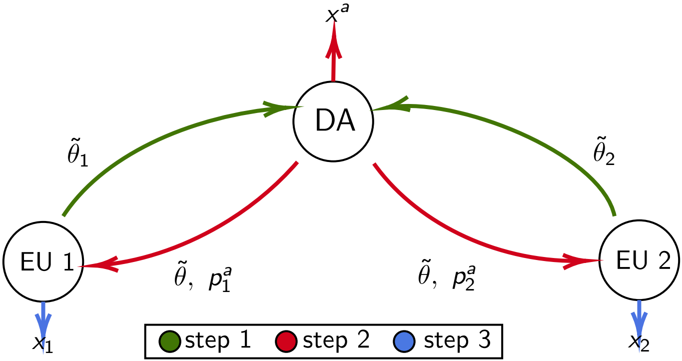
with

- γ_n,β_n non-negative parameters
- $\boldsymbol{x}_n^a = \boldsymbol{A}_n^a\widetilde{\boldsymbol{\theta}} + \boldsymbol{B}_n^a\boldsymbol{G}^{nc} + \boldsymbol{C}_n^a$ where $\boldsymbol{x}_n^a \triangleq (D_n^a, G_n^{c\ a})$ estimate built by the data aggregator

Game between DA and EUs

The DA:

- Receives readings $(\widetilde{\theta}_n)_n$
- Broadcast the readings to all the EUs
- Builds an estimate $\boldsymbol{x}^a$ of $\boldsymbol{x}$ at equilibrium
- Builds contract $p_n^a(.)$ with EU n, increasing in the accuracy of $\boldsymbol{x}_n^a$ with respect to $\boldsymbol{x}_n$



Formulation of the Stochastic Game $\mathcal{G}^{\text{stoch}}$

EU n Extended Utility $\widetilde{\Pi}_n(\boldsymbol{x}_n, \widehat{\theta}, \mathbf{V}, \boldsymbol{\varepsilon}) =$

$$\Pi_n(\boldsymbol{x}_n, \theta_n) + c_n^l \underbrace{\frac{(\widehat{\theta}_n - \theta_n)^2}{2V_n}}_{\text{Kullback-Leibler divergence}} - p_n^a(\boldsymbol{x}_n, \boldsymbol{x}_n^a, \widetilde{\boldsymbol{\theta}}) + \underbrace{\xi(\sum_{m=1}^{N} Q_m)^2}_{\text{penalty}}$$

with c_n^l, ξ non-negative parameters
Set $\mathcal{V} \triangleq \text{diag}(\mathbf{V})$. Each EU $n \in \mathcal{N}$ solves

$$\min_{\boldsymbol{x}_n, \widehat{\theta}_n, V_n} \mathbb{E}_{\boldsymbol{\varepsilon} \sim \mathcal{N}\left(\mathbf{0}, \mathcal{V}\right)} \left[\widetilde{\Pi}_n(\boldsymbol{x}_n, \widehat{\boldsymbol{\theta}}, \mathbf{V}, \boldsymbol{\varepsilon})\right], \tag{4a}$$

$$s.t.\ \underline{D}_n \le D_n \le \overline{D}_n, \tag{4b}$$

$$\underline{G}_n^c \le G_n^c \le \overline{G}_n^c, \tag{4c}$$

$$D_n = G_n^c + G_n^{nc} + Q_n, \tag{4d}$$

$$d(\widehat{\theta}_n, \theta_n) \le \alpha_n, \quad \alpha \text{ indistinguishability} \tag{4e}$$

$$\underline{V}_n \le V_n \le \overline{V}_n. \tag{4f}$$

Description of the game between the data aggregator and the EUs

Exact Penalty

If the penalty coefficient ξ in $\widetilde{\Pi}_n(.)$ is bigger than the Lagrangian multiplier of the constraint $(\sum_{m=1}^{N} Q_m)^2 = 0$, then the penalized game has the same solutions as $\mathcal{G}^{\text{stoch}}$.

Game between DA and EUs

a) Each EU n reports a reading $\widetilde{\theta}_n = \widehat{\theta}_n + \varepsilon_n$, with $\varepsilon_n \sim \mathcal{N}(0, V_n)$, to the DA by solving (4) with respect to $\widehat{\theta}_n, V_n$. The readings $\widetilde{\boldsymbol{\theta}}$ are then broadcasted to all the EUs by the DA.

b) Each EU n computes its $\boldsymbol{x}_n$ by solving (4).

Steps a) and b) can take place simultaneously or sequentially.

Nash vs Performatively Stable Equilibria

Set $\boldsymbol{y}_n \triangleq (\boldsymbol{x}_n, \widehat{\theta}_n, V_n) \in \mathcal{Y}_n$ the decision variable of EU n in $\mathcal{G}^{\text{stoch}}$.

Definition of a Nash Equilibrium (NE)

A Nash Equilibrium (NE) is a strategy profile $\boldsymbol{y}^* = (\boldsymbol{y}_n^*)_n \in \mathcal{Y}$ such that for all $n \in \mathcal{N}$:

$$\boldsymbol{y}_n^* \in \underset{\boldsymbol{y}_n \in \mathcal{Y}_n}{\operatorname{argmin}} \, \mathbb{E}_{\boldsymbol{\varepsilon} \sim \mathcal{N}\left(\mathbf{0}, \operatorname{diag}(\mathbf{V_n}, \mathbf{V^*_{-n}})\right)} \left[\widetilde{\Pi}_n(\boldsymbol{y}_n, \boldsymbol{y}^*_{-n}, \boldsymbol{\varepsilon}) \right].$$

Definition of a Performatively Stable Equilibirum (PSE) (Narang et al., 2022)

A Performatively Stable Equilibrium (PSE) is a strategy profile $\boldsymbol{y}^s = (\boldsymbol{y}_n^s)_n \in \mathcal{Y}$ such that for all $n \in \mathcal{N}$:

$$\boldsymbol{y}_n^s \in \underset{\boldsymbol{y}_n \in \mathcal{Y}_n}{\operatorname{argmin}} \, \mathbb{E}_{\boldsymbol{\varepsilon} \sim \mathcal{N}\left(\mathbf{0}, \mathcal{V}^s\right)} \left[\widetilde{\Pi}_n(\boldsymbol{y}_n, \boldsymbol{y}^s_{-n}, \boldsymbol{\varepsilon}) \right]. \tag{5}$$

Main Results

Strong Convexity

The utility function $\mathbb{E}_{\varepsilon}\left[\widetilde{\Pi}_n(\boldsymbol{y}_n, \boldsymbol{y}_{-n}, \varepsilon)\right]$ is strongly convex in $\boldsymbol{y}_n$, $\forall n$.

Let $\mathrm{SOL}(\mathcal{G})$ be the set of solutions of $\mathcal{G}$

Uniqueness and Efficiency of the NE

- There exists a unique NE solution of $\mathcal{G}^{\mathrm{stoch}}$.
- If the DA's estimate $\boldsymbol{x}^a$ is perfect for the game $\mathcal{G}$, i.e., $\boldsymbol{x}^a(\boldsymbol{\theta}, \boldsymbol{G}^{nc}) = \boldsymbol{x}^{\mathcal{G}}$ with $\boldsymbol{x}^{\mathcal{G}} \in \mathrm{SOL}(\mathcal{G})$, then the NE solution of $\mathcal{G}^{\mathrm{stoch}}$ is efficient.

Uniqueness of the PSE

There exists a unique PSE solution of $\mathcal{G}^{\text{stoch}}$.

Set $\Pi_n^\sharp(\boldsymbol{x}_n, \widehat{\boldsymbol{\theta}}, \boldsymbol{V}, \boldsymbol{\varepsilon}) = \Pi_n(\boldsymbol{x}_n, \theta_n) + c_n^I \frac{(\widehat{\theta}_n - \theta_n)^2}{2V_n} - p_n^a(\boldsymbol{x}_n, \boldsymbol{x}_n^a, \widetilde{\theta})$, and define the non-cooperative game without penalty $\mathcal{G}^\sharp(\widehat{\boldsymbol{\theta}}, \boldsymbol{V})$, where each EU $n \in \mathcal{N}$ solves:

$$\min_{\boldsymbol{x}_n} \mathbb{E}_{\boldsymbol{\varepsilon} \sim \mathcal{N}\left(\mathbf{0}, \mathcal{V}\right)} \left[\Pi_n^\sharp(\boldsymbol{x}_n, \widehat{\boldsymbol{\theta}}, \boldsymbol{V}, \boldsymbol{\varepsilon})\right], \tag{6a}$$

$$s.t. \quad \underline{D}_n \leq D_n \leq \overline{D}_n, \tag{6b}$$

$$\underline{G}_n^c \leq G_n^c \leq \overline{G}_n^c, \tag{6c}$$

$$D_n = G_n^c + G_n^{nc} + Q_n, \tag{6d}$$

$$\sum Q_m = 0. \tag{6e}$$

$\mathcal{G}^\sharp$ as a Potential Game

$\mathcal{G}^\sharp(\widehat{\boldsymbol{\theta}}, \boldsymbol{V})$ is a generalized potential game, $\forall \widehat{\boldsymbol{\theta}}, \boldsymbol{V}$.

$\rightarrow$ $\mathcal{G}^\sharp$ can be reformulated as an optimization problem.

Algorithms Description

NE and Social Optimum are obtained with a gradient descent method.

Then we wanted to use an existing algorithm (Narang, 2022) as a benchmark. It requires to adapt the objective function as follow:

$$\mathbb{E}_{\boldsymbol{\varepsilon}\sim\mathcal{N}\left(\mathbf{0},\mathcal{V}\right)}\left[\widetilde{\Pi}_n(\boldsymbol{x}_n,\widehat{\boldsymbol{\theta}},\boldsymbol{V},\boldsymbol{\varepsilon})\right]=\mathbb{E}_{\varepsilon_n\sim\mathcal{N}(0,V_n)}\left[\overline{\Pi}_n(\boldsymbol{x}_n,\widehat{\boldsymbol{\theta}},\boldsymbol{V},\varepsilon_n)\right], \quad (7)$$

At each iteration t of the algorithm:

- each EU sample its ε_n^t.
- each EU update its decision variable using:

$$\boldsymbol{y}_n^{t+1}=\mathrm{proj}_{\mathcal{Y}_n}\left(\boldsymbol{y}_n^t-\eta\nabla_n\overline{\Pi}_n(\boldsymbol{x}_n,\widehat{\boldsymbol{\theta}},\boldsymbol{V},\varepsilon_n)\right). \quad (8)$$

Problem: those algorithms require that each player have a total access to $\widehat{\boldsymbol{\theta}}$.

Algorithms Description

In our game: $\widetilde{\Pi}_n(\boldsymbol{y}^t, \boldsymbol{\varepsilon}^t) \equiv \widetilde{\Pi}_n(\boldsymbol{x}_n^t, \widehat{\theta}_n^t, V_n^t, \widetilde{\boldsymbol{\theta}}^t)$

To avoid the previous problem, we adapted the Repeated Stochastic Gradient Method (Narang, 2022) and created the Coupled Privacy Repeated Stochastic Gradient Method (CP-RSGM):
at each iteration t:

- each EU sample its ε_n^t and shares its $\widetilde{\theta}_n^t$ with the DA.
- the DA broadcasts the $\widetilde{\theta}_n^t$.
- each EU update its decision variable using:

$$\boldsymbol{y}_n^{t+1} = \mathrm{proj}_{\mathcal{Y}_n}\big(\boldsymbol{y}_n^t - \eta \nabla_n \widetilde{\Pi}_n(\boldsymbol{y}^t, \boldsymbol{\varepsilon}^t)\big). \tag{9}$$

Algorithms Description

If we update sequentially the information variables and the energy variables, we use the Privacy Split Repeated Stochastic Gradient Method (PS-RSGM).

Algorithm Privacy Split Repeated Stochastic Gradient Method (PS-RSGM)

1: Find $\boldsymbol{x}^{\mathcal{G}} \in \mathrm{SOL}(\mathcal{G})$.

2: Find $\widehat{\theta}_n^{\sharp}, V_n^{\sharp} = \text{argmin}_{\widehat{\theta}_n, V_n} \mathbb{E}_{\boldsymbol{\varepsilon}} \left[\widetilde{\Pi}_n(\boldsymbol{x}_n^{\mathcal{G}}, \widehat{\boldsymbol{\theta}}, \boldsymbol{V}, \varepsilon) \right]$ under constraints (4e), (4f) $\forall n$.
The solution is found by applying a CP-RSGM with $\boldsymbol{x} = \boldsymbol{x}^{\mathcal{G}}$ fixes.

3: Find $\boldsymbol{x}_n^{\sharp} \, \forall n \in \mathcal{N}$ by solving $\mathcal{G}^{\sharp}(\widehat{\boldsymbol{\theta}}^{\sharp}, V^{\sharp})$.

Efficiency Loss

For an equilibrium $\boldsymbol{y}$: $\text{efficiency gap}(\boldsymbol{y}) = SC(\boldsymbol{y}) - SC(\boldsymbol{y}^{\text{so}})$

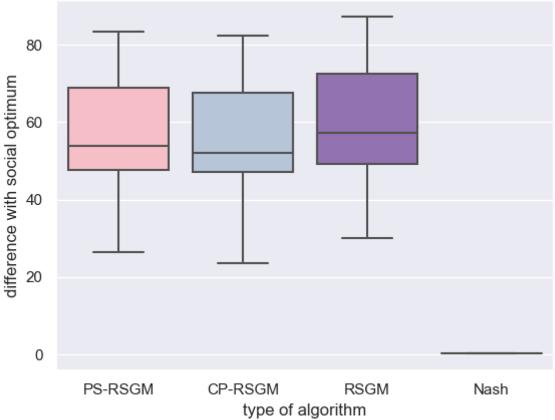


Figure: Box plots of the efficiency gaps for each algorithm.

Convergence Rates

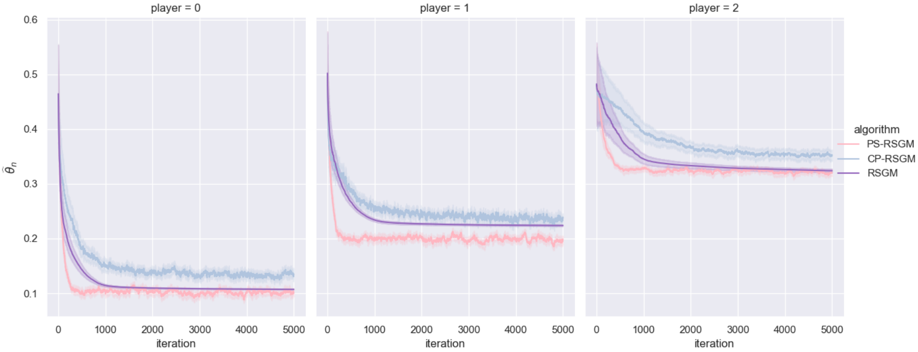


Figure: 95% confidence interval for $\widehat{\boldsymbol{\theta}}$ while learning the PSE

Balancing Efficiency and Privacy

Total information released: sum of the Kullback-Leibler divergence of every player.

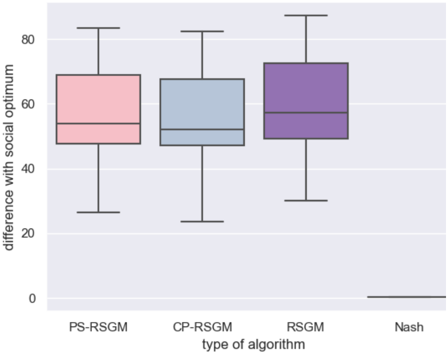


Figure: Box plots of the efficiency gaps for each algorithm.

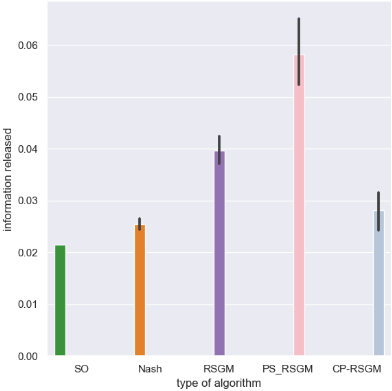


Figure: Total information released by the EUs for each algorithm.

Conclusion

Take-Aways

- We have modeled the shift caused by the EUs' strategic information on their decisions and market performance as a decision-dependent game
- We have analyzed its outcome relying on Nash Equilibrium and Performatively Stable Equilibrium (PSE)
- We have proposed two new algorithms to compute the PSE
  - * CP-RSGM outperforms RSGM
  - * PS-RSGM achieves faster convergence rates than CP-RSGM but requires more information release
- The balance between efficiency and privacy is evaluated numerically

Next Steps

- Prove the algorithm convergence relying on two-time scale stochastic approximation theory
- Formulate the DA's problem as a Stackelberg game and solve it

Thank You!

Bibliography

A. Narang, E. Faulkner, D. Drusvyatskiy, M. Fazel, and L. ratliff, Mutliplayer Performative Prediction Learning in Decision-Dependent Games, AISTATS 2022.

T. Westenbroek, R. Dong, L. J. Ratliff, and S. Shankar Sastry, Competitive Statistical Estimation with Strategic Data Sources, IEEE TAC, vol. 65, pp. 1537-1551, 2019.

I. Shilov, H. Le Cadre, A. Busic, Privacy Impact on Generalized Nash Equilibrium in Peer-to-Peer Electricity Market, Operations Research Letters, vol. 49, no. 5, pp. 759–766, 2021.

R. Taisant, M. Datar, H. Le Cadre, E. Altman, Balancing Efficiency and Privacy in a Decision-Dependent Network Game, HAL Preprint `https://hal.inria.fr/hal-03816949/document`