Long-term Data Sharing under Exclusivity Attacks

Yotam Gafni & Moshe Tennenholtz, Technion

High level summary

- Learning improves with scale & diversity of data
- Firms are hesitant to share data. They fear *Exclusivity Attacks*: Learn best model but mislead others
- We study different protocols, under strong/weak identity (sybil attacks), for clustering (k-center) and regression (d-LR) algorithms

Simple example: Sum

- N agents want to know the **sum** of their inputs, while misleading others.
- Attack: An agent shares $i' \neq i$, then subtracts $i' - i$

Attack fail: Max

- N agents want to know the **max** of their inputs, while misleading others.
- Attack: An agent shares M > m, and the computation result is M. The agent doesn't know true max

Protocols:

- **One shot** (the sum and max examples shown above)
- **Continuous**: Agents update at will, each update causes model re-evaluation shared with all
- **Periodic**: Agents update at constant times, at each period a model re-evaluation shared with all

Vulnerability

A strategy s_j of agent j is a successful exclusivity attack if:

- 1. There is a protocol run with last algorithm output different than under $truth_j$
- 2. Any two protocol runs with different observed histories under $truth_j$ have different observed histories under s_j

A stronger vulnerability* notion is if condition 1 holds **for every** protocol run.

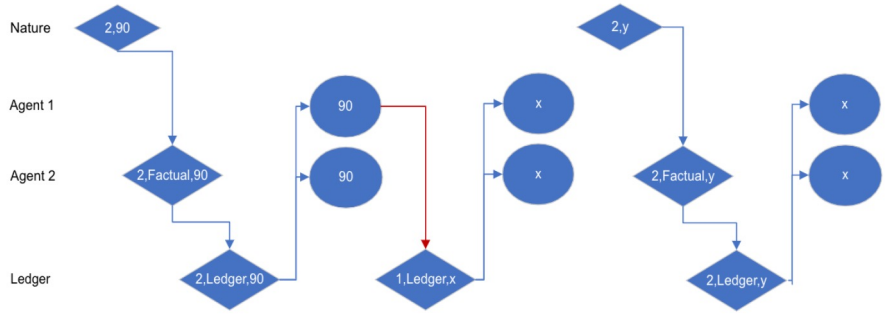
Algorithm Test Cases

	Vulnerable	Vulnerable*
d-LinearRegression	Yes, for any $\ell \geq 1$	Yes $\ell \geq d+2$; No $\ell \leq d-2$
k-Center	Yes, for any $\ell \geq 1$	No

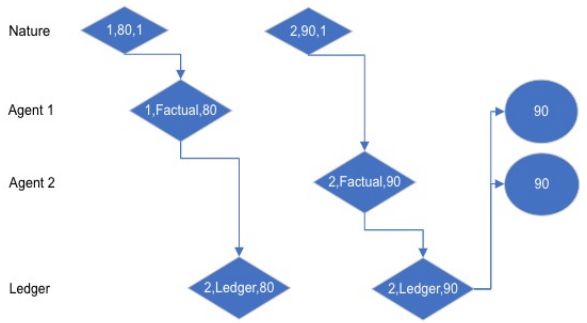
for continuous protocol, where ℓ is the number of subsequent updates by a single agent.

For the periodic protocol, both algorithms are not vulnerable.

Continuous
$(90 < y < x)$



Periodic



Acknowledgements

This research was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant No. 740435).

For more information and Research Agenda

- Mechanism Design for Data Science - mdds.net.technion.ac.il
- yotam.gafni@campus.technion.ac.il