On Differential Privacy of Distributed Control System

Zhenqi Huang, Yu Wang, Sayan Mitra and Geir Dullerud
Coordinate Science Lab
University of Illinois at Urbana Champaign
General Question

• For distributed control systems, how expensive is it to preserve privacy?

• Navigation
  – Routing delays vs location privacy

• Smart Grid
  – Peak demand vs schedule privacy
Differential Privacy (DP)

• Introduced in [1]: a private mechanism should not provide substantially different outputs if one user's data changes

• In [2]: minimization of estimation error for open-loop dynamical systems with differential privacy

• [3] discuss cost of privacy for consensus algorithms

Differential Privacy (DP)

- **Def. DP**: \( M \) is a mechanism that gives \( \epsilon \)-differential privacy with \( \epsilon > 0 \), if for all datasets \( D \) and \( D' \) that differ in one user’s data, for all subset of observations \( S \subseteq Range(M) \),
  \[
  \Pr[M(D) \in S] \leq e^{\epsilon} \Pr[M(D') \in S]
  \]
A Simple Example of DP Algorithm

- Weight watchers example
  - Multiple people diet together. Each people participated has a weight value in the range \([a, b]\). They want to compute the average weight without reporting their exact weight.
  - Each participant will add a carefully chosen noise to his own weight and report it to the server.
  - The server can then publish the average without bleaching the individuals’ privacy

- Laplace noise
  - Noise \(\sim Lap(\epsilon(b-a))\)
  - \(f(x) = \frac{1}{2\epsilon(b-a)} e^{\epsilon(b-a)}\)
Distributed Control System

\[ z = h(x_1, x_2, \ldots, x_N) \]

Agent \( i \) (\( p_i \))

\[ x_i' = f(x_i, u_i, z) \]

Controller

\[ u_i = g(x_i, \tilde{z}, p_i) \]

Plant

\[ \tilde{z} = h(\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_N) \]

Server

Observables: \( \tilde{x}_i, \tilde{z} \)

Valuable information: \( p_i \)
Example: Navigation

- Routing of N agents on a 2-D plan:
  - The agent i's state $x_i \in \mathbb{R}^2$
  - Preference of agent $i$ is a path with length $T$: $p_i \in \mathbb{R}^{2T}$
  - The environment state, center of mass: $z = \frac{1}{N} \sum_i x_i$
  - The update law of the individual agent's state at time $t$:
    $$x_i(t + 1) = x_i(t) + c(z(t) - x_i(t)) + u_i(t)$$
  - The control law:
    $$u_i(t) = -cz_i(t) + 0.8(p_i(t) - x_i(t))$$

- To design: the report strategy:
  $$\tilde{x}_i(t) = r(t, x_i(t))$$
DP for Distributed Control System

- The sensitive data of the system $p = \{p_1, p_2, ..., p_N\}$
  - $p_i$ is the desired trajectory of agent $i$:
    $p_i = [p_i(0), p_i(1), ..., p_i(T)]$
  Unbounded change in $p_i$ results in unbounded change in system's behavior

- **Def. DP:** Let $Obs$ be any observation stream of bounded time $T$ and $p, p'$ be different in agent $i$’s preferences. The DCS is $\epsilon$-DP if:
  $$\Pr[p \text{ leads to } Obs] \leq e^{\epsilon \cdot |p - p'|} \Pr[p' \text{ leads to } Obs]$$
Cost of Privacy for Distributed Control System

• **Average Cost:** \( \frac{1}{N} \sum_{t=0}^{T} \sum_{i} |x_{i}(t) - p_{i}(t)|^{2} \)
  - Fixed a DCS, depends only on the preferences \( p \)

• **Baseline Mechanism** \( M' : \tilde{x}_{i}(t) = x_{i}(t) \)

• The **Cost of Privacy** of a DP mechanism \( M \) is:
  \[
  CoP = \sup_{p} E[C_{M,p} - C_{M',p}]
  \]
Sensitivity

- The sources of uncertainty of the system
  - The preferences of agents
  - The randomized report function
- Fixed a sequence of observation \((Obs)\) and the agents’ preferences \((p)\), the trajectories of all the agents are fully specified: \(x(Obs, p, t)\)

- **Def. Sensitivity:** difference in the system’s states resulting from change in individual’s \(p_i\)

\[
\Delta(t) = \sup_{Obs, adj(p, p')} \frac{|x(Obs, p, t) - x(Obs, p', t)|}{|p_i - p'_i|}
\]
A DP Algorithm

• Theorem: The following distributed control system is $\epsilon$-differentially private:
  - At each time $t$ each agent adds an vector of independent Laplace noise $Lap\left(\frac{\Delta(t)T}{\epsilon}\right)$ to its actual state:
    \[
    \tilde{x}_i(t) = x_i(t) + Lap\left(\frac{\Delta(t)T}{\epsilon}\right)
    \]

• Sensitivity and Cost of Privacy are properties of the dynamics of the system.
Linear Distributed Control Systems

• Linear distributed control system:

\[ z_i(t) = \frac{1}{N} \sum_i x_i \]

\[ x_i(t + 1) = Ax_i(t) + cz(t) + u_i(t) \]

\[ u_i(t) = -c\bar{z}(t) + K(x_i(t) - p_i(t)) \]

• We will design an \( \epsilon \)-differentially private mechanism for this system and reason about cost of privacy.
Sensitivity of Linear Distributed Control Systems

• **Sensitivity:**
  \[ \Delta(t) = |(cI + K)^t| + |\sum_{s=0}^{t} (cI + K)^s (I - K)| \]
  - Independent to the number of agents.
  - Converges to a constant if the closed-loop dynamics is stable.
  - Diverges exponentially otherwise.

• **DP Mechanism:**
  \[ \tilde{x}_i(t) = x_i(t) + Lap\left(\frac{\Delta(t)T}{\epsilon}\right) \]
CoP of Linear Distributed Control system

- **Cost of Privacy**: $O\left(\frac{T^3}{N^2\epsilon^2}\right)$

- The strategy works for systems with many short-lived agents.
- The cost of privacy is low for systems with large number of agents.

- Improvement: protecting several waypoint instead of the whole desired trajectory $CoP \sim O\left(\frac{k^3}{N^2\epsilon^2}\right)$
Cost of Privacy

Cost v.s. (Decreasing) Privacy

Cost v.s. (Increasing) Number of agents
Conclusion

• A framework for studying the cost of differential privacy for distributed control systems.

• A communication strategy to guarantee differential privacy.

• A linear system with quadratic cost is specified

• Cost of privacy has the order $O\left(\frac{T^3}{N^2\epsilon^2}\right)$ for stable dynamics, and grows exponentially otherwise.