Differentially Private Average Consensus with Optimal Noise Selection

In the multi-agent average consensus problem, a group of agents seek to agree on the average of their individual values by exchanging information with their neighbors.

In many of its applications, the individual values of agents include sensitive information. Thus, guaranteeing the privacy of the individual agents is an important aspect.

We address this problem using the strong notion of differential privacy because of its rigorous formulation, resilience to post-processing and auxiliary information and independence from the model of the adversary.

**Motivation**

Consider \( n \) agents interacting over an undirected connected graph \( G \) with dynamics

\[
\theta(\cdot+i) = \theta(\cdot) - \delta x(k) + S \mathbf{y}(k),
\]

where \( \delta \) and \( x(\cdot) \) are the step size and \( x(\cdot) \) is a vector random variables on the total sample space \( \mathcal{X} = \mathcal{R}^n \).

For \( \delta \in \mathcal{R}^n \), a pair of initial states \( \theta(0) \) and \( x(0) \) are called \( \delta \)-adjacent if,

\[
\delta_{ij} = \begin{cases} 
1 & \text{if } i = j \ \\
0 & \text{if } i \neq j
\end{cases}
\]

For any fixed initial state \( x(0) \), let \( \theta'(\cdot) : \mathcal{R}^n \rightarrow \mathcal{R}^n \) be such that \( \theta'(0) = x(0) \).

**Differentially Private Average Consensus Problem**

Design the distributed dynamics (1) and the distribution of the noise sequences \( \mathbf{y} \) such that asymptotic average consensus and \( \epsilon \)-differential privacy are guaranteed. \( \epsilon \) is kept as small as possible, and the algorithm’s accuracy is maximized.

**Laplacian Dynamics: Noise Design and Analysis**

Consider the following linear distributed dynamics,

\[
\theta(\cdot+i) = \theta(\cdot) - \delta x(k) + S \mathbf{y}(k),
\]

where \( \delta \) and \( x(\cdot) \) are the step size and \( x(\cdot) \) is a vector random variables on the total sample space \( \mathcal{X} = \mathcal{R}^n \).

For \( \delta \in \mathcal{R}^n \), a pair of initial states \( \theta(0) \) and \( x(0) \) are called \( \delta \)-adjacent if,

\[
\delta_{ij} = \begin{cases} 
1 & \text{if } i = j \ \\
0 & \text{if } i \neq j
\end{cases}
\]

For any fixed initial state \( x(0) \), let \( \theta'(\cdot) : \mathcal{R}^n \rightarrow \mathcal{R}^n \) be such that \( \theta'(0) = x(0) \).

Given \( \delta, \epsilon \in \mathcal{R}^n \), the dynamics (1) is \( \epsilon \)-differentially private if for any pair of \( \delta \)-adjacent \( \theta(0) \) and \( \theta'(0) \) and any set \( C \subset \mathcal{R}^n \),

\[
P(\theta \in \mathcal{C} | x(0)) \leq e^{\epsilon}P(\theta \in \mathcal{C} | x'(0)).
\]

The variance of \( \theta_n \) around \( \theta_0 \) is a consequence of the lack of preservation of the average by (3) due to the term \( S \mathbf{y}(k) \) which in turn, helps to maintain privacy.

**Theorem: Asymptotic Convergence of the Proposed Algorithm**

Consider a network executing the distributed dynamics (3). Let \( x_0 \in (0,2) \) and \( \eta(\cdot) \) be Laplace distribution \( \mathcal{L}(\epsilon) \) with \( \eta(k) = \epsilon q_i, \eta_i \in \mathcal{R}^n, i \in \{0,1,\ldots,n\}. \)

Thus, we have each agent independently set \( (\eta_i, q_i) = (1 + \epsilon, \epsilon + c) \) with \( c \ll 1 \).

**Simulations**

We simulated (3) for \( n = 50 \) agents with random topology and initial conditions. We set \( \delta = 1, \epsilon = 0.1, (\eta_i, q_i) = (1 + \epsilon, \epsilon + c) \) with \( c = 10^{-4} \) for all \( i \in \{0,1,\ldots,n\} \).

**References**