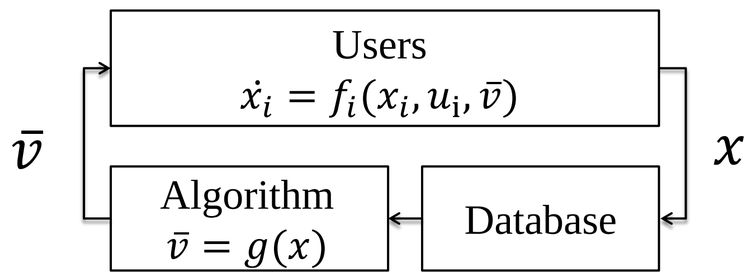
Privacy and Security in Distributed Control: Differentially Private Consensus

Zhenqi Huang, Sayan Mitra, Geir Dullerud

University of Illinois at Urbana-Champaign

What are the costs and limits of privacy (and security) in database-driven control systems?

Motivating Problem



- u_i: Private data or preferences (e.g., destination)
- x_i: Individual's state (e.g., position)
- $\bar{v}$: Aggregate information for better decision making (e.g., average delay on routes)
- m: A metric for performance (e.g., average user delay)
- What is the best achievable m for a given level of privacy of u_i ?

Consensus

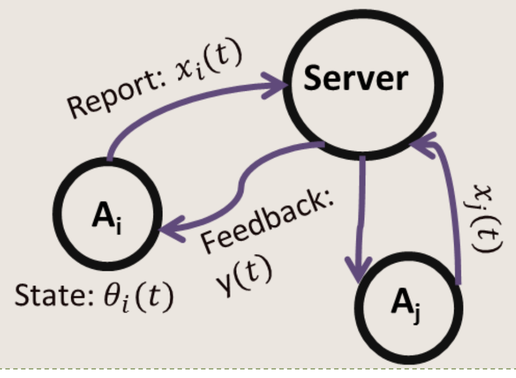
- **Iterative consensus**: a building block in distributed control (e.g., load balancing, sensor fusion, and flocking).
- **Adversary**: intercept messages from agents and server state
- Is it possible to possible to achieve consensus accurately while **preserving privacy** of individual agents (here initial values) ?

Properties

- **ε-Differential Privacy**: let s, s' be two initial states that differ in one user's initial local value by a unit, Obs be any message stream produced.

$$\frac{\Pr[s \text{ produces } Obs]}{\Pr[s' \text{produce } Obs]} \leq e^{\varepsilon}$$

- **Convergence**: all the local values converge to a common value in m.s.
- ***r*-Accuracy**: with high probability, the convergent point is in the r -ball of the initial average.



- Add the noise to the actual local value:

$$x_i(t) = \theta_i(t) + \eta_i(t)$$

- Server computes the average and sends feedback:

$$y(t) = \frac{1}{N}\sum x_i(t)$$

- Agents update local value using feedback:

$$\theta_i(t+1) = (1-\sigma)\,\theta_i(t) + \sigma y(t)$$

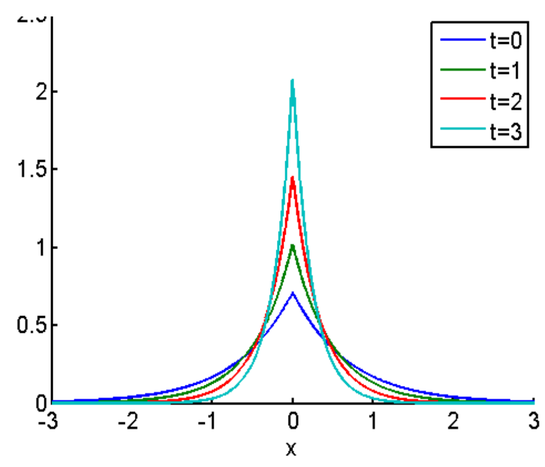
Fully distributed (see paper) algorithm allows some of the participants to leak information

Mechanism

Idea: Decaying noise cover dynamics

- Each round, user i samples a **decaying Laplace noise** $\eta_i(t) \sim Lap(q^t)$

PDF: $f(x) = \frac{1}{2q^t} e^{-\frac{|x|}{q^t}}$



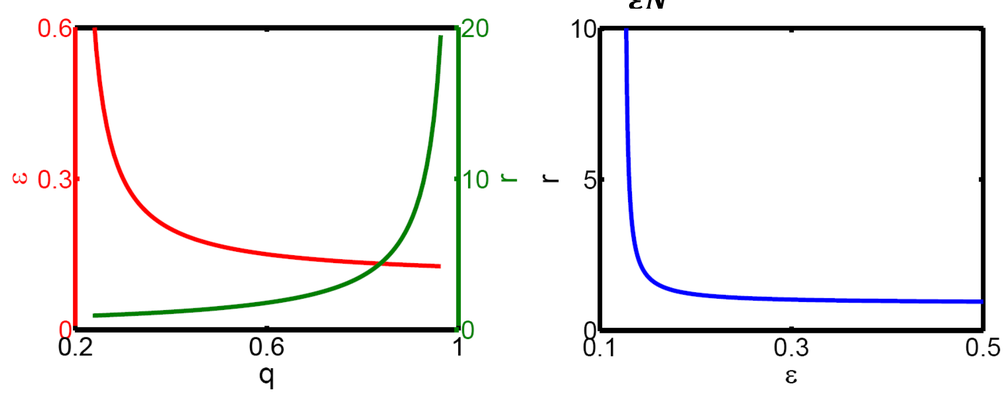
- **Parameters**

$q \in (0,1)$ *noise decay*

$\sigma \in (0,1)$ *feedback weight*

Summary

- A server-based & fully distributed mechanisms for iterative consensus
- Convergence, $\boldsymbol{\varepsilon}$-differential privacy and $\boldsymbol{O}\left(\frac{1}{\varepsilon\sqrt{bN}}\right)$-accuracy. Tradeoff shown in fig.
- A lower bound of accuracy: $\Omega(\frac{1}{\varepsilon N})$



Differentially Private Iterative Synchronous Consensus, Zhenqi Huang, Sayan Mitra, and Geir Dullerud. *In Proceedings of the WPES in conjunction with the ACM CCS conference 2012*

2012 Science of Security Community Meeting
Nov. 29-30, 2012
National Harbor, MD
http://cps-vo.org/group/sosmtg

Vote Here