Updates on Research and Collaborations

Matthew Hale
Department of Mechanical and Aerospace Engineering
University of Florida

Center of Excellence for Assured Autonomy in Contested Environments
Fall 2022 Review
October 12th, 2022

UF | Department of Mechanical & Aerospace Engineering
UNIVERSITY *of* FLORIDA

UF | UNIVERSITY *of* FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Personnel & Collaborations with CoE PIs

- New lab alumni:

Dr. Kasra Yazdani
Now at Samsung

Dr. Katherine Hendrickson
Now at EpiSci

- Ongoing collaboration with Dawn Hustig-Schultz and Ricardo Sanfelice (UCSC)
  - Developed hybrid model of decentralized non-convex optimization
  - Paper at CDC ’21
  - One under review at ACC ‘23
  - Journal paper in preparation

- Ongoing collaboration with Ufuk Topcu (UT-Austin)
  - Looking at privacy in symbolic systems
  - Combining our privacy mechanisms with their multi-agent algorithms

Collaborations with Air Force Colleagues

- Applied optimization work to weapon-target assignment (WTA) problems
  - K. Hendrickson, P. Ganesh, K. Volle, P. Buzaud, K. Brink, and M.T. Hale, "Decentralized Weapon-Target Assignment under Asynchronous Communications".
  - **Accepted to Journal of Guidance, Control, and Dynamics**
  - Ongoing collaboration with Kevin Brink (RW) on discrete optimization
- Joint paper at AIAA SciTech with USAFA based on senior capstone
  - A. Broshkevitch, A. Hancock, A. Peters, M. Kim, M. Anderson, et al., "An Autonomous System for the Rapid Airfield Damage Repair Mission"

- Working with Zach Bell (RW) on feedback optimization
- Working with Ben Robinson (RY) on anomaly detection in multi-armed bandits
- Collaborating on MPC with Sean Phillips and Alex Soderlund (RV)
  - Currently focused on satellite docking
  - IFAC World Congress paper in preparation

- Engaging with AFRL every summer
  - William Warke went to RW for summer 2022 with Kevin Brink
  - Gabriel Behrendt went to RV for summer 2022 with Sean Phillips
  - Alexander Benvenuti went to RW for summer 2022 with Scott Nivison

Differential Privacy for Network Design and Analysis

Calvin Hawkins & Matthew Hale

Department of Mechanical and Aerospace Engineering University of Florida

1. "Differentially Private Formation Control: Privacy and Network Co-Design" Under review. https://arxiv.org/abs/2205.13406
2. "Node and Edge Differential Privacy for Graph Laplacian Spectra: Mechanisms and Scaling Laws" Under review. https://arxiv.org/abs/2104.00654

Motivation

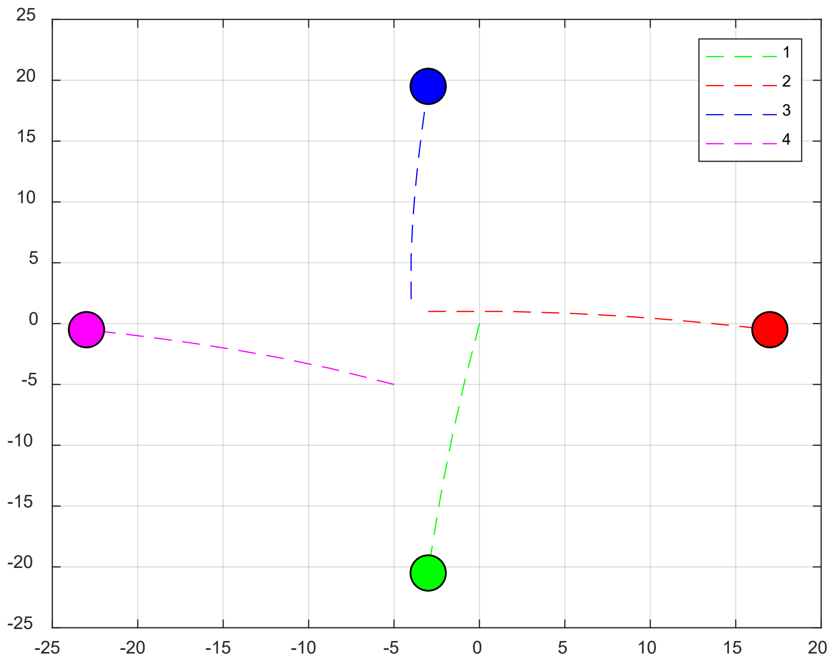
- Allow agents to collaborate while protecting their sensitive information.
- Examples:
  - Autonomous vehicles sharing location data
  - Social Networks sharing personal information
  - Data-driven control sharing sensitive state information
- Graph analyses may reveal sensitive information about individuals.

Two goals:
1. Develop tools to design networks sharing private information. (Part 1)
2. Develop tools for the private analysis of networks. (Part 2)

Part 1:
Privacy and Network Co-Design

Formation Control Background

- In this talk, formation control.
- Consider N agents where agent i has state $x_i(k) \in \mathbb{R}^d$.
- Network is modeled by a weighted, undirected graph G.
- If agents i and j communicate, maintain a distance of $\Delta_{ij} \in \mathbb{R}^d$.
- Without privacy, this is achieved by the formation control protocol.

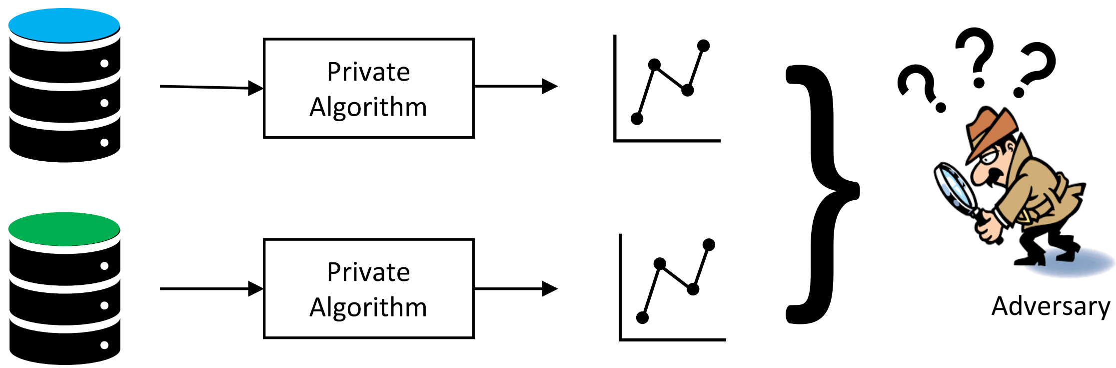


$$x_i(k+1) = x_i(k) + \gamma \sum_{j \in N(i)} w_{ij}\left(x_j(k) - x_i(k) - \Delta_{ij}\right)$$

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

Differential Privacy Background

- Statistical notion of privacy that originated in the computer science literature.

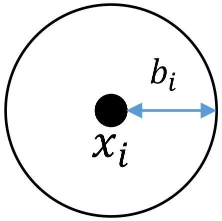


- Immune to post processing and robust to side information.
- Used by Apple, Google, Uber, and the 2020 Census.
- Agents can share trajectory data while protecting itself from other agents and eavesdroppers.

Differential Privacy Masks Differences

- Goal of Differential Privacy: Make "similar" pieces of data appear "approximately indistinguishable."
- Adjacency defines when pieces of data are similar.
  - For trajectories $x_i, x_i' \in \ell_p$

$$Adj(x_i, x_i') = \begin{cases} 1, & \|x_i - x_i{}'\|_{\ell_p} \leq b_i \\ 0, & otherwise \end{cases}$$



Definition (Differential Privacy): Let $\epsilon_i > 0$ and $\delta_i \in \left[0, \frac{1}{2}\right)$. A randomized mechanism M is (ϵ_i, δ_i) −differentially private for agent i if, for all adjacent x_i, x_i', we have

$$P[M(x_i) \in S] \leq e^{\epsilon_i} P[M(x_i') \in S] + \delta_i.$$

Sensitive data → Privacy mechanism tuned by ϵ_i, δ_i → Private data

Typical values:
$\epsilon_i \leq 3, \delta_i \leq 0.05$

Implementing Privacy

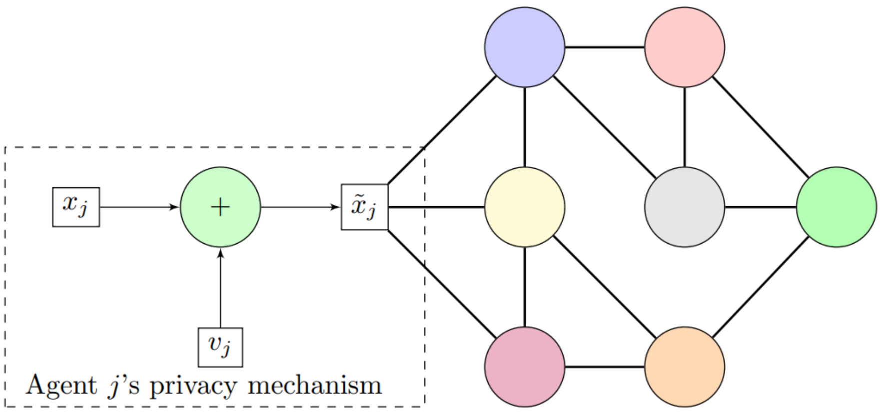
- Agent i must send $x_i(k)$ to its neighborhood $N(i)$ at each k.
- Instead, agent i will send a private version of its state to $N(i)$; $\tilde{x}_i(k)$.
- Differential privacy is implemented with the Gaussian Mechanism:

$$\tilde{x}_j(k) = x_j(k) + v_j(k),$$
$$v_j(k) \sim \mathcal{N}\left(0, \sigma_j^2 I_d\right).$$

Lemma: The Gaussian mechanism is (ϵ_i, δ_i) −differentially private for agent i if $\sigma_i \geq \kappa(\epsilon_i, \delta_i) b_i$, where

$$\kappa(\delta_i, \epsilon_i) = \frac{1}{2\epsilon_i}\left(K_{\delta_i} + \sqrt{K_{\delta_i}^2 + 2\epsilon_i}\right),$$

and $K_{\delta_i} = Q^{-1}(\delta_i)$.



Quantifying Performance

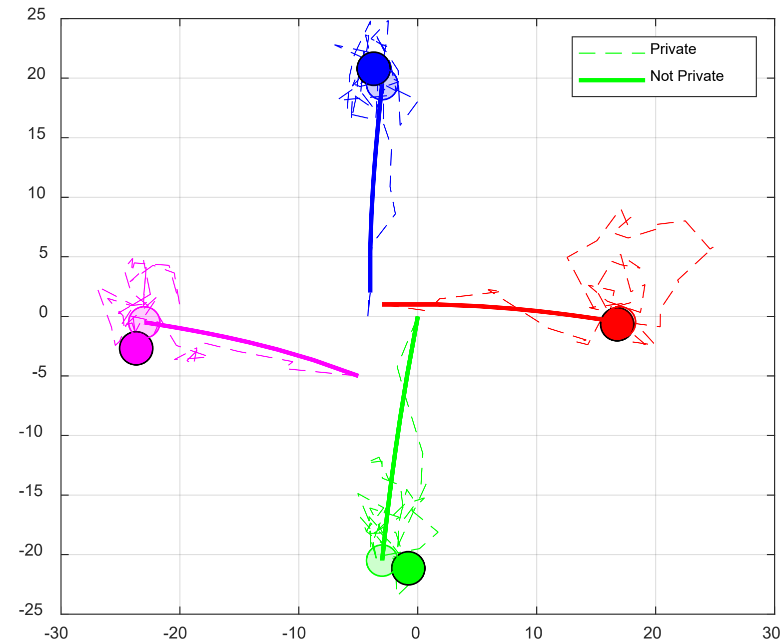
- With privacy the formation control protocol becomes

$$x_i(k+1) = x_i(k) + \gamma \sum_{j \in N(i)} w_{ij}(x_j(k) + v_j(k) - x_i(k) - \Delta_{ij}) + n_i(k).$$

- Let $e_i(k) = x_i(k) - \beta_i(k)$, where $\beta(k)$ is the state the non-private protocol converges to with initial condition $x(k)$.

- To quantify performance at the network level, let

$$e_{ss} = \limsup_{k \to \infty} \frac{1}{N} \sum_{i=1}^{N} E[e_i(k)^2].$$



UF UNIVERSITY of FLORIDA
Duke UNIVERSITY
TEXAS The University of Texas at Austin
UC SANTA CRUZ

Quantifying Performance

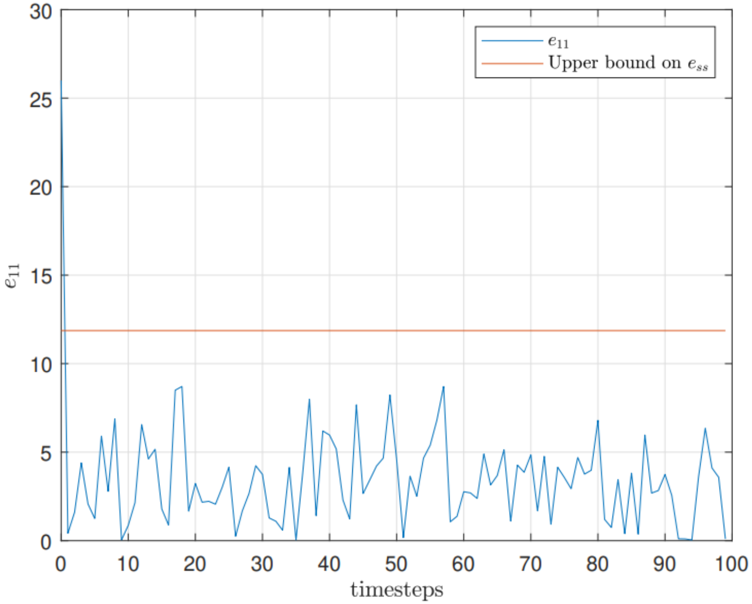
Theorem 1: Bounds on Steady-State Error

A network of N agents running the controller

$$x_i(k+1) = x_i(k) + \gamma \sum_{j \in N(i)} w_{ij}(\tilde{x}_j(k) - \tilde{x}_i(k) - \Delta_{ij})$$

is differentially private and has e_{ss} upper bounded by

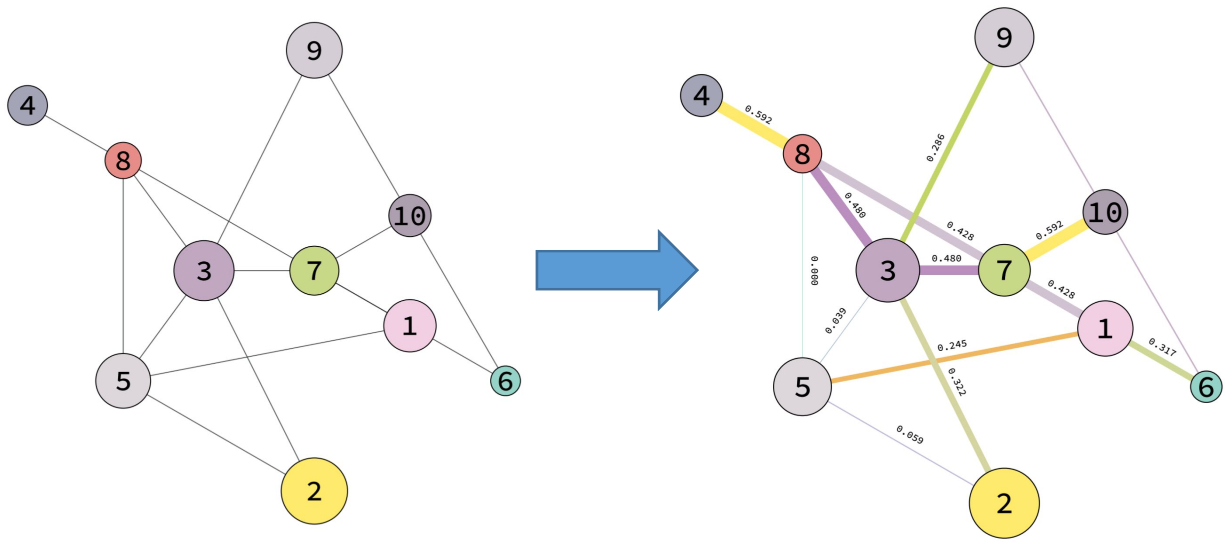
$$e_{ss} \leq \frac{\gamma d \sum_{i=1}^{N} \left(\sum_{j=1}^{N} {w_{ij}}^2 - \frac{\deg(i)^2}{N} \right) \kappa(\epsilon_i, \delta_i)^2 b_i^2}{N\, \lambda_2(G)(2 - \gamma \lambda_2(G))}$$



"Differentially Private Formation Control: Privacy and Network Co-Design" Under review. https://arxiv.org/abs/2205.13406

Privacy and Network Co-Design

- Goal: Formulate an optimization problem to design the communication topology and privacy parameters subject to constraints.
- Input: Design constraints and initial undirected, unweighted communication topology.
- Decision variables: $L(G)$, ϵ_i.



Privacy and Network Co-Design

- Objective function
  - Dense graph costs more: $\mathrm{T}r(L(G))$.
  - Agents want to be as private as possible: $\sum_{i\in[N]} \epsilon_i^2$.
  - Minimize $\Gamma\left(\{\epsilon_i\}_{i\in[N]},\ L(G)\right) = \vartheta Tr\left(L(G)\right) + \sum_{i\in[N]} \epsilon_i^2$.

Smaller ϵ_i → Stronger privacy

- Constraints
  - Performance: $e_{ss} \leq e_R \rightarrow \frac{\gamma^2 Tr(L(G)\Sigma_{\mathrm{V}}\mathrm{L(G)})}{N\ \lambda_2(G)(2-\gamma\lambda_2(G))} \leq e_R$.
  - Connectivity: $\lambda_2(G) \geq \lambda_{2_L}$.
  - Minimum level of privacy: $\epsilon_i \leq \epsilon_i^{max}$.

Privacy and Network Co-Design

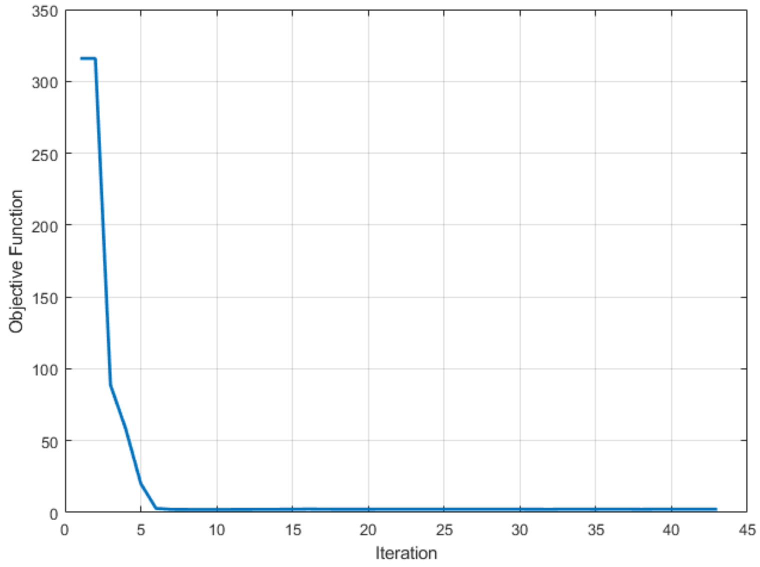
Problem 1: Privacy and Network Co-Design

$$\min_{L(\mathcal{G})\in\mathcal{L}(L_0),\{\epsilon_i\}_{i\in[N]}} \quad \vartheta \mathrm{Tr}(L(\mathcal{G})) + \sum_{i\in[N]} \epsilon_i^2$$

$$\text{subject to} \quad \frac{\gamma^2 d \mathrm{Tr}(L(G)\Sigma_v L(G))}{N\lambda_2(L)\left(2-\gamma\lambda_2(L)\right)} \leq e_R$$

$$\epsilon_i \leq \epsilon_i^{max} \quad \text{for all } i$$

$$\lambda_2(L(\mathcal{G})) \geq \lambda_{2_L}.$$

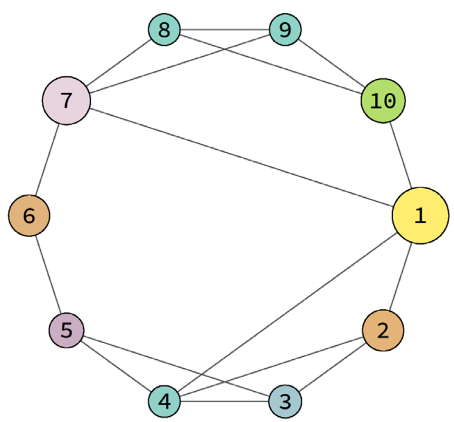


GitHub

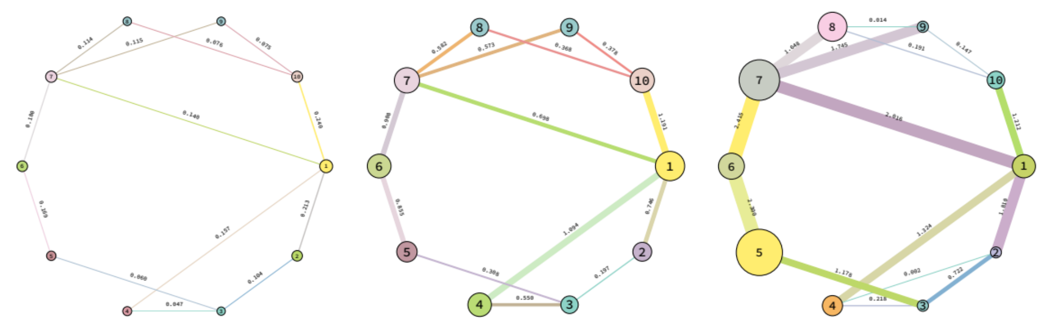
Co-Design Example

- Fix the input unweighted graph over $N = 10$ agents.
- A smaller a node is drawn, the more private it is. (Smaller epsilon)
- The thicker an edge is drawn, the more edge weight it has.
- Fix everything other than the required performance.

Input:



Sample output:

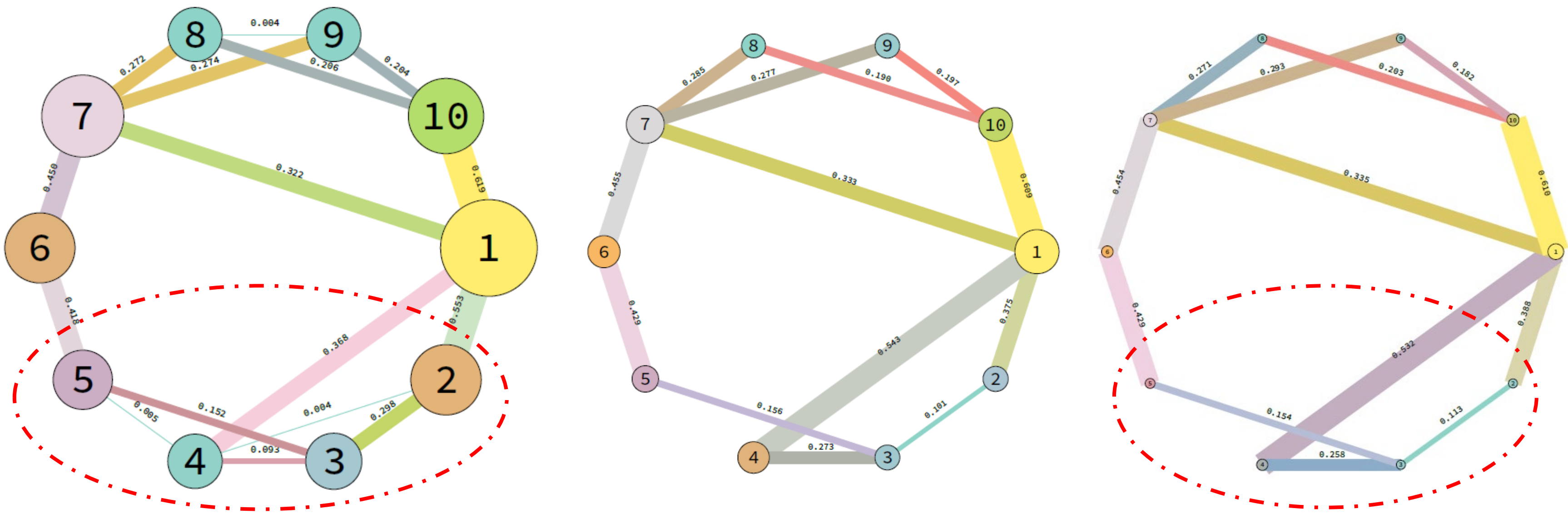


(a) $\lambda_{2L} = 0.1$ (b) $\lambda_{2L} = 0.5$ (c) $\lambda_{2L} = 1.0$

Co-Design Example: Tuning Performance

Fix $\gamma = \frac{1}{2n}, \vartheta = 10, \lambda_{2L} = 0.2, \delta_i = 0.05, b_i = 1.$

- $\epsilon_{max} = [0.4, 0.9, 0.55, 0.35, 0.8, 0.45, 0.7, 0.5, 0.52, 0.58].$
- Let $e_R \in \{2, 8, 64\}$.



$e_R = 2$ $\quad$ $e_R = 8$ $\quad$ $e_R = 64$

Performance requirements weaken.

1. C. Hawkins and M. Hale "Differentially Private Formation Control: Privacy and Network Co-Design," Under review: https://arxiv.org/pdf/2205.13406.pdf

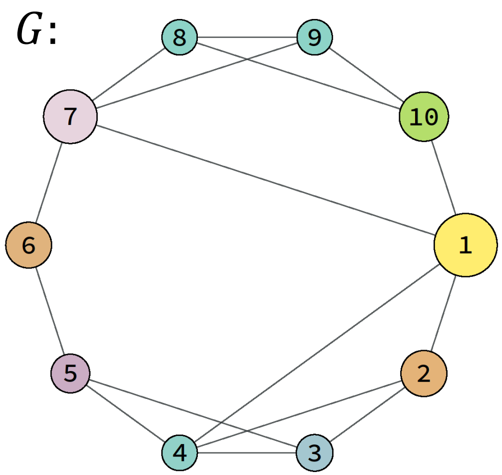
Part 2:
Private Network Analysis

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

Background

- Graph analyses may reveal sensitive information about individuals.
- Numerous scalar-valued graph properties pose known privacy threats.
  - Counts of triangles.
  - Counts of subgraphs.
  - Lots more.
- In this talk, we will focus on the privacy of the spectrum of the graph Laplacian.

G:



Need privacy in these calculations!

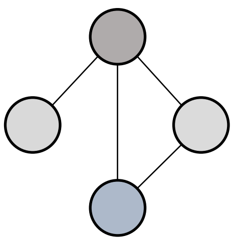
$$\lambda_1(L(G)), \ldots, \lambda_n(L(G))$$

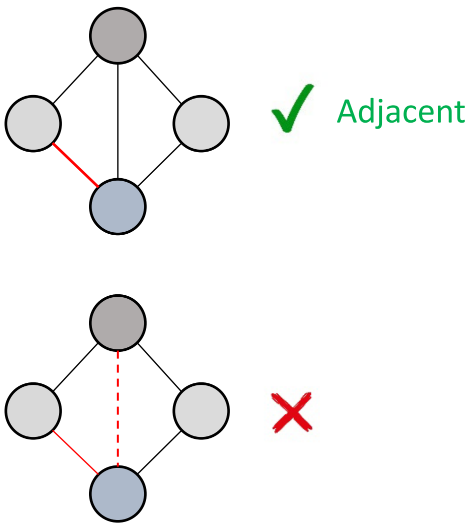
Implementing Privacy (Adjacency)

- "Similar" pieces of data appear "approximately indistinguishable."
- Similarity is defined over the edge set. Adjacency parameter A.

$$Adj(G,G') = \begin{cases} 1, & |E(G)\Delta E(G')| \leq A \\ 0, & otherwise \end{cases}$$

Edge Privacy:
$A = 1$





Definition (Edge Privacy):

Let $\epsilon > 0$ and $\delta \in \left[0, \frac{1}{2}\right)$. A randomized mechanism M is (ϵ, δ) −differentially private for agent i if, for all adjacent G, G', we have

$$P[M(G) \in S] \leq e^{\epsilon} P[M(G') \in S] + \delta$$

- Each eigenvalue is bounded on $[0, n]$.
- We use the bounded Laplace mechanism[1].

1. Holohan, Naoise, et al. "The bounded laplace mechanism in differential privacy." *arXiv preprint arXiv:1808.10410* (2018).

Privacy Mechanism

Definition (Bounded Laplace mechanism for λ_i[1]). Let $b > 0$ and $D = [0, n]$. Then the bounded Laplace mechanism W_{λ_i} is given by its probability density function $f_{W_{\lambda_i}}$ as

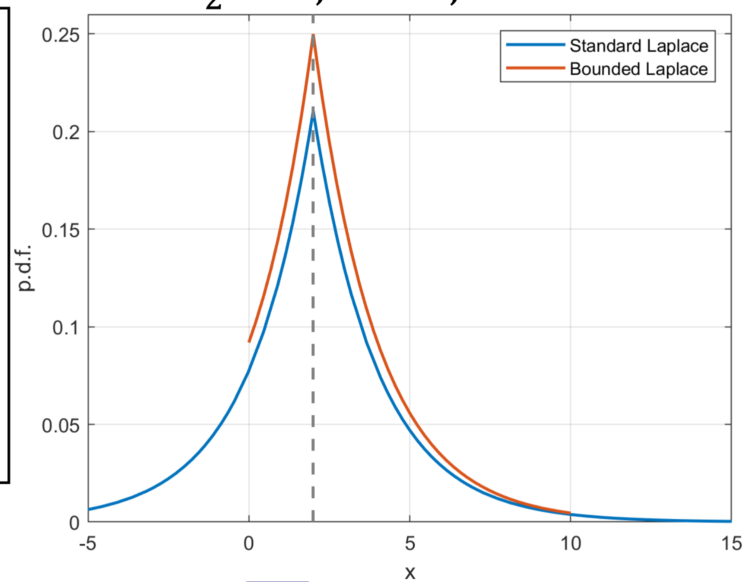
$$f_{W_{\lambda_i}}(x) = \begin{cases} 0, & x \notin D \\ \dfrac{1}{C(\lambda_i, b)} \dfrac{1}{2b} e^{-\frac{|x-\lambda_i|}{b}}, & x \in D \end{cases}$$

Where $C(\lambda_i, b)$ is a normalizing term.

Theorem 2: Let $\varepsilon > 0$, $\delta \in (0,1)$ and adjacency parameter A. The bounded Laplace mechanism is (ε, δ)-differentially private if

$$b \geq \frac{2A}{\varepsilon - \log\left(\dfrac{1 - \frac{1}{2} e^{-\frac{2A}{b}}\left(1 + e^{-\frac{n}{b}-1}\right)}{1 - \frac{1}{2}\left(1 + e^{-\frac{n}{b}}\right)}\right) - \log(1 - \delta)}$$

$\lambda_2 = 2, b = 2, n = 10$

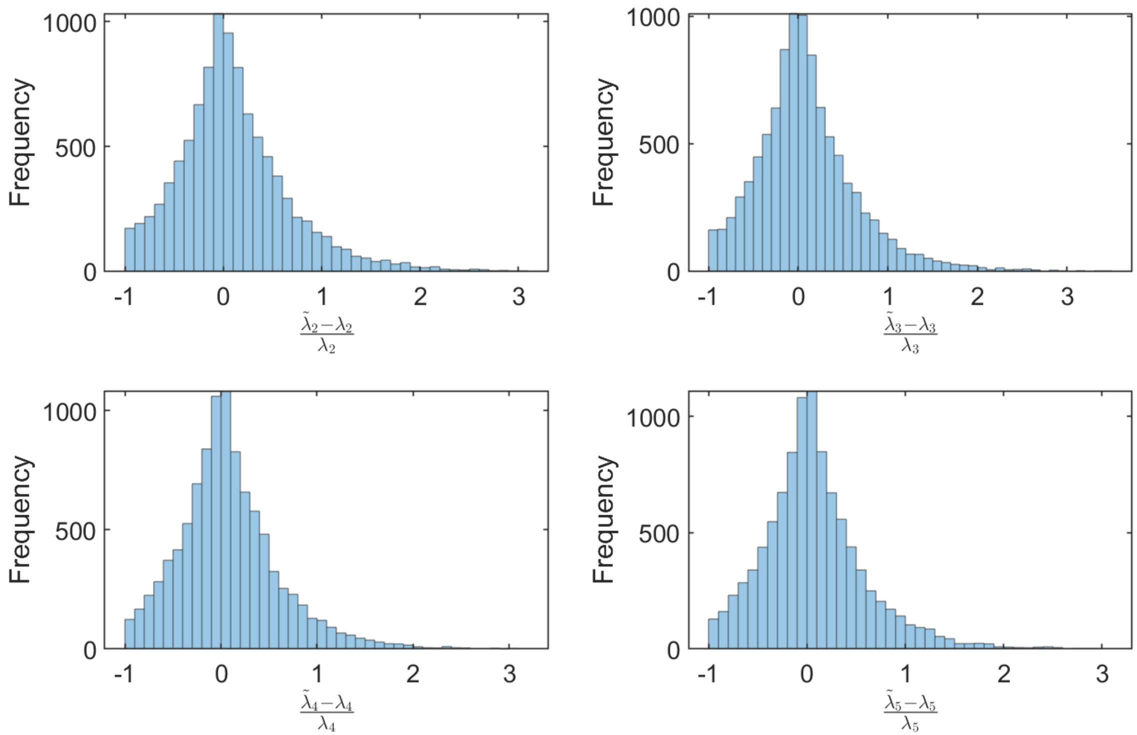


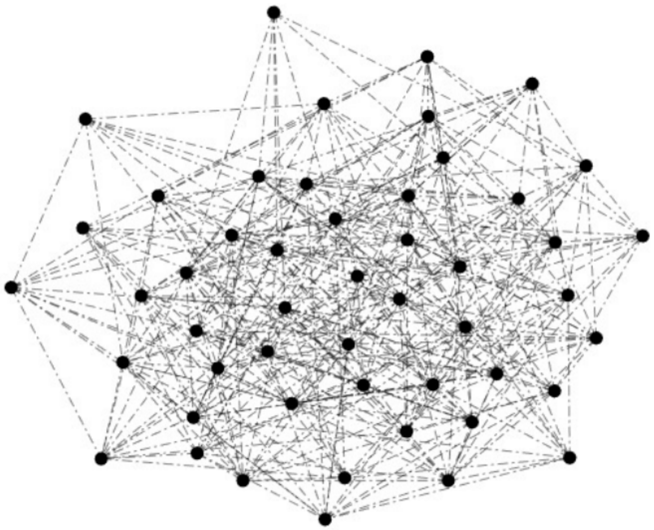
Private Analysis: Accuracy

Theorem 3:

$$E[\tilde{\lambda}_i - \lambda_i] = \frac{1}{2C(\lambda_i, b)}\left(2\lambda_i + be^{-\frac{\lambda_i}{b}} - (n+b)e^{-\frac{n-\lambda_i}{b}}\right) - \lambda_i$$

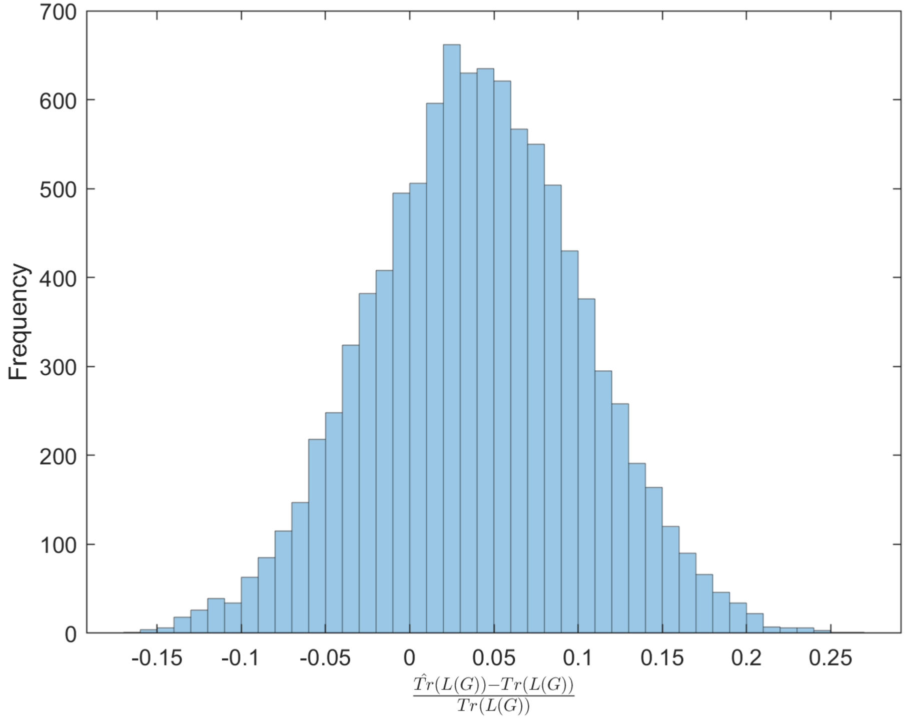
- Fix a graph G on 50 nodes, $\epsilon = 0.6, \delta = 0.05, A = 2$.
- Generate 10^4 private $\tilde{\lambda}_i$ for $i \in \{2, \ldots, 5\}$.

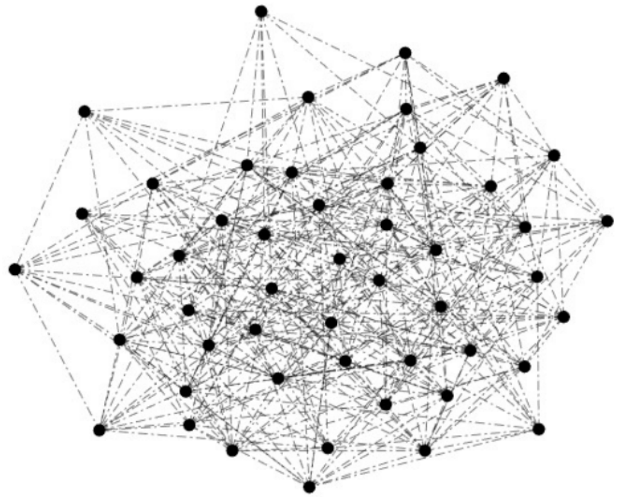




Private Analysis: Trace

- $Tr(L(G)) = \sum_{i=1}^{n} \lambda_i(L(G))$.
- Fix a graph G, $\epsilon = 0.4, \delta = 0.05, A = 2$.
- Generate 10^4 private spectra $\{\tilde{\lambda}_i\}_{i=1}^{n}$.
- Estimate the trace as $\widehat{Tr}(L(G)) = \sum_{i=1}^{n} \tilde{\lambda}_i(L(G))$

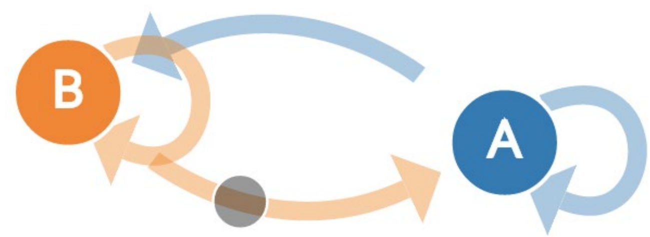




True Value: $Tr(L(G)) = 736$
Average error: 3.97%

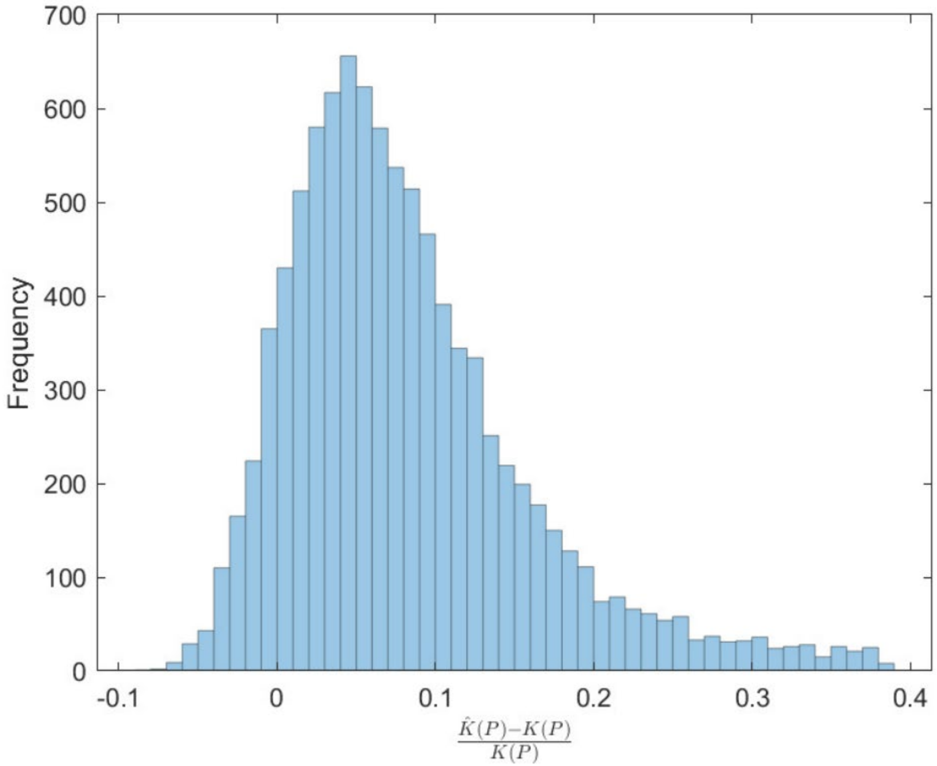
Private Analysis: Kemeny's Consant

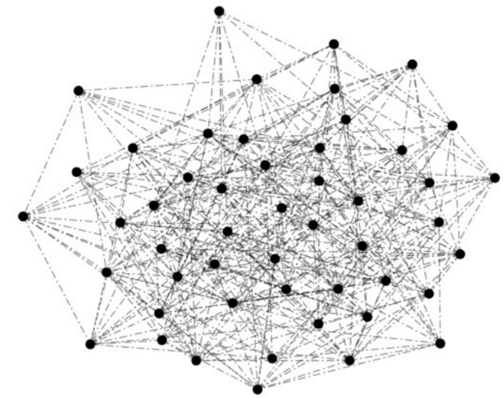
- Kemeny's constant = expected time steps from state i to a random state sampled from the stationary distribution of a Markov chain.
- In network control, discrete time consensus is governed by $P = I - \gamma L(G)$
- P can be analyzed as the transition matrix of Markov chain.
  - Error of consensus is in terms of the Kemeny constant.
- Estimate with the private spectrum $\{\tilde{\lambda}_i\}_{i=1}^{n}$.
- Kemeny's consant: $K(P) = \sum_{i=2}^{n} \frac{1}{1-\lambda_i(P)}$
  - $K(P) = \frac{1}{\gamma} \sum_{i=2}^{n} \frac{1}{\lambda_i(L(G))}$
  - Private estimate $\widehat{K}(P) = \frac{1}{\gamma} \sum_{i=2}^{n} \frac{1}{\tilde{\lambda}_i(L(G))}$



Private Analysis: Kemeny's Consant

- Fix a graph G, $\epsilon = 1.0, \delta = 0.05, A = 2, \gamma = \frac{1}{n}$.
- Generate 10^4 private spectra $\{\tilde{\lambda}_i\}_{i=1}^{n}$
- Estimate Kemeny's constant as $\widehat{K}(P) = \frac{1}{\gamma}\sum_{i=2}^{n}\frac{1}{\tilde{\lambda}_i(L(G))}$



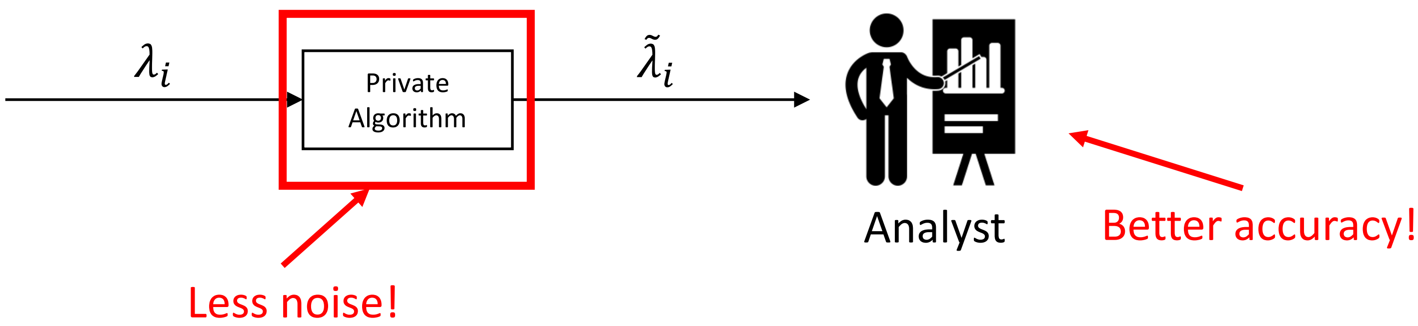


True Value: $K(P) = 102.70$
Average error: 0.55%

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ

Future Work

- The development of new privacy mechanisms for other graph properties.
- Applications to basic reproduction number of an epidemic model.
- Privacy in multi-agent MDPs and reinforcement learning.



Thank you

calvin.hawkins@ufl.edu