# Differential Privacy in Linear Distributed Control Systems: Entropy Minimizing Mechanisms and Performance Tradeoffs

Yu Wang, Zhenqi Huang, Sayan Mitra, *Senior Member, IEEE*, and Geir E. Dullerud, *Fellow, IEEE*

***Abstract*—In distributed control systems with shared resources, participating agents can improve the overall performance of the system by sharing data about their personal preferences. In this paper, we formulate and study a natural tradeoff arising in these problems between the privacy of the agent's data and the performance of the control system. We formalize privacy in terms of differential privacy of agents' preference vectors. The overall control system consists of $N$ agents with linear discrete-time coupled dynamics, each controlled to track its preference vector. Performance of the system is measured by the mean squared tracking error. We present a mechanism that achieves differential privacy by adding Laplace noise to the shared information in a way that depends on the sensitivity of the control system to the private data. We show that for stable systems the performance cost of using this type of privacy preserving mechanism grows as $O(T^3/N\varepsilon^2)$, where $T$ is the time horizon and $\varepsilon$ is the privacy parameter. For unstable systems, the cost grows exponentially with time. From an estimation point of view, we establish a lower-bound for the entropy of any unbiased estimator of the private data from any noise-adding mechanism that gives $\varepsilon$-differential privacy. We show that the mechanism achieving this lower-bound is a randomized mechanism that also uses Laplace noise.**

***Index Terms*—Communication networks, decision/estimation theory, differential privacy, distributed algorithms/control.**

## I. Introduction

AVAILABILITY of new sensors and real-time user data have heralded significant performance improvements in distributed control systems. At the same time, sharing information poses a threat to the privacy of the participating individuals. For instance, smartphones and connected vehicles can detect and report on road congestion conditions more accurately [1]–[3]; this has been used to develop crowd-sourced congestion-aware mapping and routing applications such as Google Maps and Waze. These benefits come with the risk of a loss of location-privacy. For example, researchers have shown that Waze can be used to follow a users movements [4]; and even with anonymized data such as Google Maps [5], the inherent structure of location data can lead to deanonymization [6], [7]. Similar risks and benefits arise in two-way coordination between consumers' demands and electric power utility companies: On one hand, sharing information can prevent over-provisioning through peak-shaving and reduce energy costs [8]–[10], and on the other hand, expose the consumers' personal habits.

In this article, we initiate a rigorous study of this tradeoff between privacy and performance, with a focus on idealized discrete-time, linear, distributed control systems. Consider a system with $N$ participating agents: Each agent has a *sequence private preferences* and a local controller designed to track these preferences. The preferences could be thought of as a sequence of way-points for a congestion aware navigation system. We measure the performance of the system using the mean-squared tracking error of the agents. The dynamics of each agent is influenced by the aggregate state of the system (e.g., congestion). In this setup, there is a spectrum of strategies the agents can use for achieving different levels of performance. For one, each agent could try to track its preferences without sharing any information with others. Lets call this the perfectly private strategy. At the other extreme, each agent could share its complete state information with others, and thereby, collectively infer the aggregate state and achieve a better, possibly even optimal, tracking performance. In between these two extremes are strategies that share information for improving performance without compromising on privacy of the preferences.

In order to formalize the notion of privacy in this setting, we adopt the notion of *differential privacy,* which has emerged from the literature on databases and theoretical computer science [11]–[14] and has proven to be popular and now also practical [15]. Informally, a differentially private statistical query on a database ensures that the probability distribution of the output does not change substantially with changes in the private data. Thus, an adversary cannot learn much about the participants by querying the database. Since its original development by Dwork, McSherry, Nissim, Smith, and their collaborators several variations on the formal definition of differential privacy have been proposed in [13], [16]–[19]. Our setting is about real-valued continuously changing data (modeling physical quantities like position, energy consumption, etc.), and therefore, the definition of differential privacy used here is the one from [19], which

Manuscript received October 9, 2015; revised August 14, 2016, August 16, 2016, and December 24, 2016; accepted January 8, 2017. Date of publication January 25, 2017; date of current version March 16, 2017. This work was supported by a Science of Security Lablet at the University of Illinois funded through the Maryland Procurement Office under Contract No. H98230-14-C-0141. Y. Wang and G. Dullerud are supported in part by AFOSR Grant FA9550-15-1-0059. Recommended by Associate Editor Peng Cheng and Bruno Sinopoli.

The authors are with the Coordinate Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA (e-mail: yuwang8@illinois.edu; zhuang25@illinois.edu; mitras@illinois.edu; dullerud@uiuc.edu).

Digital Object Identifier 10.1109/TCNS.2017.2658190

uses a metric on the user data. In this definition (see Definition 2), a greater degree of change in the private data of an agent permits a corresponding, but still exponentially small change in the probability distributions of the output.

We propose a mechanism for data sharing that ensures differential privacy for the participants. The idea is based on the well-known Laplace mechanism whereby each agent shares noisy versions of its state with the others. Specifically, we first derive an upper-bound on the sensitivity of the distributed system, which measures the influence of changing the private dataset on the trajectories of the agents. Then, a mechanism is designed to randomize the output by adding Laplace noise that is large enough to blur this influence in the probability sense. When noise is introduced to the system, the agents will not be able to precisely estimate the aggregate state of the system. Thus, the performance of the system will be worse than the performance under perfect state sharing. We show that this *cost of privacy* (measured by tracking error) for a time horizon $T$ of a system with $N$ agents is $O(\frac{T^3}{N\varepsilon^2})$ for stable systems and can grow exponentially with $T$ for unstable systems.

By definition, differentially private mechanisms ensure that two alternative values of the private data set cannot be distinguished by any sequence of reported states with significant probability, therefore, it obstructs accurate estimation on the private dataset for an observer. We show that there is a lower bound on the accuracy of estimation for any $\varepsilon$-differentially private randomized mechanism. Specifically, by first considering one step and then extending to the general case, we prove that, when the private dataset is protected by an $\varepsilon$-differentially private mechanism, the entropy of any unbiased estimators on them have a lower bound, which is achieved by a mechanism using Laplace noise.

The rest of the paper is organized as follows: Section II gives basic definitions and notations used throughout the paper. Section III introduces the general setup of the discrete-time linear distributed control system, together with the definitions for $\varepsilon$-differential privacy, performance measures, and estimates. Section IV provides a privacy mechanism and the related results on privacy-performance tradeoff. Section V studies the estimation problem of the private data and establishes that for any $\varepsilon$-differentially private mechanism, the (Shannon) entropy of any unbiased estimator for the private dataset has a lower bound and the mechanism that achieves the minimum is derived. Finally, the conclusions are presented in Section VI.

### A. Related Works

While there are several notions of data privacy in the computer science literature, the quantitative and statistical nature of differential privacy makes it suitable for adoption in control. The notion of differential privacy is first introduced in the context of statistical data bases where agents' private information is their participation status to the data base [11], [13]. In this context, two datasets are *adjacent* if they are different in the (binary) data corresponding to a single agent and are identical elsewhere. The definition of adjacency varies for different contexts. For example, for real-valued data bases, like the definitions presented in [20] and [21], adjacent datasets are defined as identical datasets with one agent whose values are close (as measured by a metric on its real-valued variables). This notion of differential privacy guarantees that two sets of behaviors, starting from two adjacent initial states and corresponding to any output sequence, are statistically close. Various mechanisms for achieving differential privacy have been studied in the literature [22]–[24]. The Laplace mechanism requires adding a Laplace noise to the query output and was proposed in [11].

More recently, the notion of differential privacy has been extended to dynamical systems [17], [25] and applied to various problems, such as distributed consensus protocols [17], [26]–[28], distributed optimization [29]–[32], and filtering [18], [25], [33]. In [18], [25], and [33], the authors develop a notion of differential privacy which ensures that an filter cannot precisely estimate the input to a dynamical system by looking at its output stream. Laplace and Gaussian mechanisms are presented for converting an ordinary dynamical system to a differentially private one and a Kalman filter is designed to estimate the states of a Gaussian mechanism with minimized $\ell_2$ error. The sufficient condition of the minimization problem is established in the form of linear matrix inequalities. However, the authors did not discuss whether Gaussian mechanism is the best mechanism (in terms of metric like $\ell_2$-norm or entropy) one can use. The problem studied in this paper is different from the ones introduced in these two papers in several ways. First, in the class of systems studied in Sections III-A and IV, an agent's dynamics is coupled with the environment which depends on the aggregate of all other agents' states. Second, these systems are "closed loop" and the noise added for privacy in one round affects all future states of the system. Further, in Section V we formulate an optimization problem for a general class of randomized mechanisms of minimizing the entropy of unbiased estimators, and proved that a mechanism that uses Laplace noise is the optimal.

In [34], the authors study the optimal noise-adding mechanisms that minimizes certain $\ell_1$ cost function while keeping the query $\varepsilon$-differential privacy and derive that the optimal solution is the staircase mechanism. Our work differs from their work in three aspects. First, while they use the common definition of $\varepsilon$-differential privacy, we adopt a stronger definition of $\varepsilon$-differential privacy here as mentioned in Section I. In addition, the "cost function" we used in this work is Shannon entropy as opposed to the $\ell_1$ cost function. Finally, our problem is set upon distributed control systems where communication happens at every time instead of single query.

This work is an unification of two previous works [35], [36]. The general setup and the main results in Section IV of this paper are based on [35], in which we established a differentially private mechanism of linear distributed control system that generalize the iterative consensus mechanism studied in [17]; and studied the cost of differential privacy. In Section V, we generalized the results of [36] to this linear distributed control system, and proved that, when the private dataset is kept $\varepsilon$-differentially private there is a lower-bound on the entropy of the randomized observation. Furthermore, the lower-bound is achieved by a mechanism of adding a sequence of Laplace noise.

## II. Preliminaries

The sets of natural numbers, positive integers, positive real numbers, and real numbers are denoted respectively by $\mathbb{N}$, $\mathbb{Z}_+$

$\mathbb{R}_+$, and $\mathbb{R}$. For any $m, n \in \mathbb{N}$, the set of $n$-dimensional real vectors is $\mathbb{R}^n$ and the set of $m \times n$ real matrices is $\mathbb{R}^{m\times n}$. The positive orthant of $\mathbb{R}^n$ is denoted by $\mathbb{R}^n_+$. The set $[n] = \{1, 2, \ldots, n\}$. The absolute value of $x \in \mathbb{R}$ is denoted by $|x|$. Given a vector $x \in \mathbb{R}^n$, we denote the $i$th coordinate by $x_i$ and the $\ell_1$-norm by $\|x\|_1 = \sum_{i=1}^n |x_i|$.

The *(Shannon) entropy* of a $n$-dimensional random vector $w$ with probability distribution function $f$ is defined as

$$H(w) = -\int_{\mathbb{R}^n} f(x)\ln(f(x))\mathrm{d}x. \tag{1}$$

A scalar random variable $v$ obeys the Laplace distribution with parameter $\lambda$, written as $v \sim \mathrm{Lap}(\lambda)$, if its probability distribution function is given by

$$f_L(x) = \frac{1}{2\lambda}\exp\left(-\frac{|x|}{\lambda}\right). \tag{2}$$

The definition extends to $n$-dimensional random vectors by using the $\ell_1$-norm, namely, $w \sim \mathrm{Lap}(\lambda, n)$ if

$$f_L(x) = \left(\frac{1}{2\lambda}\right)^n \exp\left(-\frac{\|x\|_1}{\lambda}\right). \tag{3}$$

Note that the components of the Laplace random vector are independent.

## III. System Formulation

In this section, we will propose a general modeling framework for linear distributed control systems in which agents share information based on randomized mechanisms. Specifically, we will formally define the dynamics of the system in Section III-A, differential privacy in Section III-B, a metric of performance in Section III-C, and the unbiased estimators in Section III-D.

### A. Linear Distributed Systems With Randomized Communication

Let us consider a linear distributed control system with $N$ agents whose dynamics may be influenced by the *actual* states of other agents. For example, in a distributed traffic control scenario [37], one agent's speed and choice of route are influenced by the state of other agents, such as congestion in different roads. By explicitly exchanging information about their states, the agents could achieve better performance (routing delays), but at the same time, by sharing exact information about their states they may give away too much information about their private data. Thus, the agents choose to share only noisy versions of their states using a *randomized mechanism*, which we denote by $\mathcal{M}$. Specifically, at each time $t \geq 0$, the $i$th agent adds mean-zero noise $n_i(t)$ to its state and reports this noisy state $\tilde{x}_i(t)$ to the other agents

$$\tilde{x}_i(t) = x_i(t) + n_i(t). \tag{4}$$

The aggregation and dissemination of the noisy states can be performed either via a central server, as shown in Fig. 1, or in a fully distributed or peer-to-peer fashion.

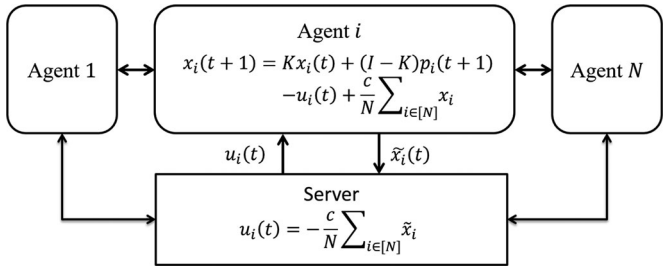



Fig. 1. Diagram of a distributed control system.

The state $x_i \in \mathbb{R}^n$ of agent $i$ evolves as a discrete-time dynamical system

$$x_i(t+1) = Ax_i(t) + v_i(t) + \frac{c}{N}\sum_{j\in[N]} x_j(t) \tag{5}$$

where 1) $x_i(t) \in \mathbb{R}^n$ is the state of agent $i$ at time $t < T$; 2) $v_i(t) \in \mathbb{R}^n$ is the local control input; and 3) $c \in \mathbb{R}$ is a coupling coefficient capturing the aggregate influence of the other agents. This model of coupling via average states is adopted for the sake of simplicity.

Each agent $i$ is also associated with a sequence $p_i(t)$ of (possibly constant) preferences or waypoints that it aims to track. To achieve this, the simplest approach is a feedback control $v_i(t)$ based on the information of *average state* $u'(t) = -\frac{c}{N}\sum_{j\in[N]}\tilde{x}_j$ received from the server and adopts the linear feedback control law

$$v_i(t) = K'(x_i(t) - p_i(t+1)) + (I-A)p_i(t+1) - u'(t) \tag{6}$$

where the $K'(x_i(t) - p_i(t+1))$ is a linear feedback term of the tracking error, $(I-A)p_i(t+1)$ is an additive term to move the equilibrium of $x_i(t)$ to $p_i(t+1)$, and $-u'(t)$ tries to cancel the effect of the aggregate state. Thus, we have

$$\tilde{x}_i(t) = x_i(t) + n_i(t) \tag{7}$$

$$u'(t) = \frac{c}{N}\sum_{j\in[N]}\tilde{x}_j \tag{8}$$

$$x_i(t+1) = Kx_i(t) + (I-K)p_i(t+1) - u'(t) + \frac{c}{N}\sum_{j\in[N]} x_j(t) \tag{9}$$

where $K = K' + A \in \mathbb{R}^{n\times n}$ is the closed loop dynamics matrix.

Fixing a time horizon $T$, we refer to the combination of the initial state and the sequence of preferences $d_i = (x_i(0), p_i(1), \ldots, p_i(T-1))$ of an individual agent as the *private data* of this agent. The *private dataset* of the system is the ordered collection $D = \{d_i\}_{i\in[N]}$ of $N$ elements. The set of all possible private dataset is denoted by $\mathcal{D}$. Given a private dataset $D \in \mathcal{D}$, we refer to 1) the sequence of aggregated states $\{x(t)\}_{t<T}$ generated by the system as the *trajectory* of the system and 2) the sequence of aggregated reported states $O = \{\tilde{x}(t)\}_{t<T} \in \mathbb{R}^{\mathrm{nNT}}$ generated by the system as the *observation* of the system.

Combining (7)–(9), the closed loop dynamics of agent $i$ is

$$x_i(t+1) = Kx_i(t) + (I-K)p_i(t+1) - \frac{c}{N}\sum_{j\in[N]} n_j(t). \tag{10}$$

The state of the $i$th agent at time $t+1$ can be written as a function of its preference sequence $\{p_i(s)\}_{s\le t}$ and the sequence $\{n_i(s)|i\in[N], s\le t\}$ of noise vectors added in all previous rounds.

### B. Differential Privacy of Distributed Control Systems

To apply the concept of *differential privacy* in the context of dynamical systems, we first define a metric on the space of private datasets.

*Definition 1:* For two private datasets $D=\{d_i\}_{i\in[N]}$ and $D'=\{d_i'\}_{i\in[N]}$, the *distance* between them is defined by $\|D-D'\|_1 = \sum_{i\in[N]}\|d_i-d_i'\|_1$.

Mathematically, the randomized mechanism $\mathcal{M}$ is a stochastic map from the private dataset $D$ to the observation $O$. By applying the metric version of differential privacy used in [19], we derive a definition of $\varepsilon$-differential privacy for the randomized mechanism $\mathcal{M}$.

*Definition 2:* Given a time horizon $T>0$ and a parameter $\varepsilon>0$, a randomized mechanism $\mathcal{M}: D\to O$ is $\varepsilon$-differentially private up to time $T-1$, if

$$\mathbb{P}\left[M(D)\in\mathcal{O}\right] \le e^{\varepsilon\|D-D'\|_1}\,\mathbb{P}\left[M(D')\in\mathcal{O}\right] \tag{11}$$

for any subset $\mathcal{O}\subseteq\mathbb{R}^{\mathrm{nNT}}$ and any two datasets $D, D'$.

*Remark 1:* If the system is $\varepsilon$-differentially private up to time $T-1$, then it is $\varepsilon$-differentially private up to any time $S<T$.

Roughly speaking, the definition above requires that the probabilities of getting the same observation are close depending on the distance between the two datasets. In other words, the probability that a small change in the private dataset is detected from the observation is very low.

The privacy of the system increases as $\varepsilon$ decreases. For $\varepsilon\to\infty$, all randomized mechanisms are $\varepsilon$-differentially private; for $\varepsilon=0$, only the mechanisms that generate identical observations will be $\varepsilon$-differentially private.

### C. Measuring Cost of Privacy

We define a cost function to evaluate the quality of the control with respect to the noisy mechanism. It measures the distance between the target waypoints (given by the preference $p_i(t)$), and the real trajectory using the second moment.

For a $\varepsilon$-differentially private mechanism $\mathcal{M}$ and a private dataset $D$ as discussed in Section III-A, we can use the second moment of the tracking error to define a cost function for agent $i$ up to time $T-1$

$$\mathrm{cost}_{\varepsilon,D,i} = \mathbb{E}\left[\sum_{t=1}^{T-1}\|x_i(t)-p_i(t)\|_2^2\right]. \tag{12}$$

Obviously, the cost functions increase with time $T$. Let $\{\overline{x}(0),\ldots,\overline{x}(T-1)\}$ be the aggregate trajectory of the system with dataset $D$ and no noise (i.e., $n_i(t)=0$ for all $t$). We define

$$\overline{\mathrm{cost}}_{D,i} = \sum_{t=1}^{T-1}\|\overline{x}_i(t)-p_i(t)\|_2^2 \tag{13}$$

to be the cost associated with agent $i$ under the nonprivate communication mechanism that shares perfect state information. The *cost of privacy* of mechanism $\mathcal{M}$ is defined as the supremum in the change of single agent's cost over all datasets relative to the nonprivate mechanism

$$\Delta(\varepsilon,T) = \sup_{i\in[N],D\in\mathcal{D}}(\mathrm{cost}_{\varepsilon,D,i} - \overline{\mathrm{cost}}_{D,i}). \tag{14}$$

The cost of privacy $\Delta(\varepsilon,T)$ will be greater with more noisy communication.

### D. Accuracy of Unbiased Estimators

When the agents coordinate by sharing information via the central server, the more accurate an agent can estimate the states of others, the more efficient the coordination can be. In Section V, we will study, when measured by entropy, how well the estimation of the state can be, for a distributed control system which is using a privacy preserving mechanism. Consider any unbiased estimator

$$\hat{D} = \{(\hat{x}_i(0),\hat{p}_i(1),\ldots,\hat{p}_i(T-1))|i\in[N]\} \tag{15}$$

of the private dataset from a sequence of reported states $O$. Since the property of differential privacy is immune to postprocessing, and the estimator $\hat{D}$ is a function of the observation, the probability distribution function $f(D,\theta)$ of the estimator $\hat{D}$ on the private dataset $D$ satisfies that

$$f(D,\theta) \le e^{\varepsilon\|D-D'\|_1} f(D',\theta) \tag{16}$$

for any possible value of the estimator $\theta\in\mathbb{R}^{\mathrm{nNT}}$ and any private datasets $D$ and $D'$.

There are multiple ways to measure the accuracy of the estimator $\hat{D}$, including variance, high-order moments and entropy. In this work, we use the Shannon entropy that measures the amount of information that can be derived from the estimation. Roughly, it decreases when the probability distribution function of the estimator becomes sharper, and *vice versa*.

The Shannon entropy of the estimator $\hat{D}$ is dependent on the value of the private dataset $D$, thus, we write it as $H_D(\hat{D})$, and define the (maximal) entropy of the estimator $\hat{D}$ by

$$H(\hat{D}) = \sup_{D\in\mathbb{R}^{\mathrm{nNT}}} H_D(\hat{D}). \tag{17}$$

We will see later in Section V that if the system is $\varepsilon$-differentially private, then there is a lower bound on $H(\hat{D})$ and the minimum is achieved by mechanisms that add Laplace noise.

## IV. Differentially Private Linear Distributed Control

### A. Aggregated Dynamics

To facilitate further discussion, we derive the aggregated dynamics of the system below. The aggregated state, noisy reported state, noise, and preference are denoted by $x(t)$, $\tilde{x}(t)$, $n(t)$, and

$p(t)$, respectively. It is easy to see that

$$\tilde{x}(t) = x(t) + n(t). \tag{18}$$

In addition, we define the aggregated average state $u(t) = (u'(t), \ldots, u'(t))^{\mathrm{T}}$ by stacking $N$ copies of the average state $u'(t)$.

For simplicity, let

$$\begin{aligned} \mathbf{K} &= I_N \otimes K, \\ \mathbf{C} &= \mathbf{1}_N \otimes \frac{cI_n}{n} \end{aligned} \tag{19}$$

where $I_N$ is the $N \times N$ identity matrix, $\mathbf{1}_N$ is the $N \times N$ matrix with all elements being 1, and $\otimes$ denotes the Kronecker product.

By (10), the aggregated closed loop dynamics is given by

$$x(t+1) = \mathbf{K}x(t) + (I - \mathbf{K})p(t+1) - \mathbf{C}n(t). \tag{20}$$

Iteratively applying the above equation gives

$$\begin{aligned} x(t) = &\ (\mathbf{K} + \mathbf{C})^t x(0) - \sum_{s=0}^{t-1} (\mathbf{K} + \mathbf{C})^{t-s} u(t) \\ &+ \sum_{s=1}^{t} (\mathbf{K} + \mathbf{C})^{t-s} (I - \mathbf{K}) p(s). \end{aligned} \tag{21}$$

Equivalently, we can write (20) as

$$x(t+1) = (\mathbf{K} + \mathbf{C})x(t) - \mathbf{C}\tilde{x}(t) + (I - \mathbf{K})p(t+1). \tag{22}$$

Again, iteratively applying the above equation gives

$$\begin{aligned} x(t) = &\ (\mathbf{K} + \mathbf{C})^t x(0) \\ &+ \sum_{s=0}^{t-1} (\mathbf{K} + \mathbf{C})^{t-s-1} ((I - \mathbf{K})p(s+1) - \mathbf{C}\tilde{x}(t)). \end{aligned} \tag{23}$$

This leads to the following remark.

*Remark 2:* Given the private dataset $D$, the system trajectory $\{x(t)\}_{t<T}$ is uniquely determined by the value of the sequence of reported states $O = \{\tilde{x}(t)\}_{t<T}$. In the rest of this paper, we denote the trajectory $\{x(t)\}_{t<T}$ determined by the private dataset $D$ and the observation $O$ by $\rho(D, O)$.

### B. Sensitivity and Differential Privacy

Recall from Remark 2 that given the private dataset $D$, each observation $O = \{\tilde{x}(t)\}_{t<T}$ uniquely defines to a unique trajectory $\rho(D, O) = \{x(t)\}_{t<T}$ independent of the actual mechanism used. We will propose a differentially private mechanism for linear distributed control systems using the idea of sensitivity.

*Definition 3:* The *sensitivity* of a randomized mechanism $\mathcal{M}$ at time $t \geq 0$ is

$$S(t) = \sup_{D, D' \in \mathcal{D},\ O \in \mathbb{R}^{n N T}} \frac{\|\rho(D, O)(t) - \rho(D', O)(t)\|_1}{\|D - D'\|_1}. \tag{24}$$

If the sensitivity is finite, then, by Lemma 26 in [35], we can derive an $\varepsilon$-differentially private mechanism. The mechanism requires that the noise in (4) is drawn from the Laplace distribution with parameter $S(t)/\varepsilon$.

*Lemma 1:* For $\varepsilon > 0$ and a time horizon $T > 0$, let $M_t \triangleq TS(t)/\varepsilon$. A randomized mechanism defined by

$$n(t) \sim \mathrm{Lap}(M_t, nN) \tag{25}$$

for $t < T$ in (4) is $\varepsilon$-differentially private.

*Proof:* Recall the probability distribution functions of the randomized observations $M(D)$ is given by $f(D, \cdot)$. For a pair of private datasets $D, D'$ and a set of observation $\mathcal{O}$, let $A = \{\rho(D, O) : O \in \mathcal{O}\}$ and $A' = \{\rho(D', O) : O \in \mathcal{O}\}$, then

$$\frac{\mathbb{P}\left[M(D) \in \mathcal{O}\right]}{\mathbb{P}\left[M(D') \in \mathcal{O}\right]} = \frac{\int_{\alpha \in A} f(D, \alpha) d\mu}{\int_{\alpha' \in A'} f(D', \alpha') d\mu'}. \tag{26}$$

There is a bijection $B$ between $A$ and $A'$, such that for $\alpha \in A$ and $\alpha' \in A'$, $B(\alpha) = \alpha'$ if they have the same observation up to time $T$, since $\alpha = \rho(D, O)$ is injective by Remark 2. Using the bijection $B$, the probability distributions on the sets $A$ and $A'$ are related by

$$\begin{aligned} \int_{\alpha' \in A'} f(D', \alpha') d\mu' &= \int_{B(\alpha) \in A'} f(D', B(\alpha)) d\mu \\ &= \int_{\alpha \in A} f(D', B(\alpha)) d\mu. \end{aligned} \tag{27}$$

For a dataset $D$, the trajectory $\alpha = \{x(t)\}_{t<T}$ is uniquely defined by the noise sequence $\{n(t)\}_{t<T}$, which follows $\{\mathrm{Lap}(M_0, nN), \mathrm{Lap}(M_1, nN), \ldots, \mathrm{Lap}(M_{T-1}, nN)\}$. For any observation $O \in \mathcal{O}$ and trajectory $\alpha = \rho(D, O)$, we denote $O_i^{(k)}(t)$ as the $k$th entry of the observation vector $\tilde{x}_i(t)$, and $\alpha_i^{(k)}(t)$ as the $k$th entry of the state vector $x_i(t)$. Then the probability density of trajectory $\alpha$ is

$$f(D, \alpha) = \prod_{\substack{i \in [N],\ k \in [n] \\ t<T}} f_L(O_i^{(k)}(t) - \alpha_i^{(k)}(t), M_t) \tag{28}$$

where $f_L(\cdot, \lambda)$ is the probability density of scalar Laplace distribution $\mathrm{Lap}(\lambda)$. Similarly, for dataset $D'$, the probability distribution function is the same

$$f(D', \alpha) = \prod_{\substack{i \in [N],\ k \in [n] \\ t<T}} f_L(O_i^{(k)}(t) - \alpha_i^{(k)}(t), M_t). \tag{29}$$

Then, we bound the distance between the trajectories $\alpha = \rho(D, O)$ and $B(\alpha)$ with the sensitivity $S(t)$. By the Definition 3, we have

$$\|\rho(D, O)(t) - \rho(D', O)(t)\|_1 \leq S(t)\|D - D'\|_1. \tag{30}$$

By definition of $\ell^1$-norm, we obtain

$$\begin{aligned} \sum_{i=1}^{N} \sum_{k=1}^{n} |\alpha_i^{(k)}(t) - B(\alpha)_i^{(k)}(t)| = &\ \|\rho(D, O)(t) - \rho(D', O) \\ &\times\ (t)\|_1 \leq S(t)\|D - D'\|_1. \end{aligned} \tag{31}$$

For scalar Laplace distribution $\mathrm{Lap}(\lambda)$ and any $x, x' \in \mathbb{R}$, we have $\frac{f_L(x,\lambda)}{f_L(x',\lambda)} \leq e^{\frac{|x-x'|}{\lambda}}$. Using this property, we have

$$\begin{aligned}
&\prod_{i\in[N]k\in[n]} \frac{f_L(O_i^{(k)}(t) - \alpha_i^{(k)}(t), M_t)}{f_L(O_i^{(k)}(t) - B(\alpha)_i^{(k)}(t), M_t)} \\
&\leq \prod_{i\in[N],k\in[n]} e^{\frac{|(O_i^{(k)}(t) - \alpha_i^{(k)}(t), M_t) - (O_i^{(k)}(t) - B(\alpha)_i^{(k)}(t)|}{M_t}} \\
&= \exp\left(\sum_{i\in[N],k\in[n]} \frac{|\alpha_i^{(k)}(t) - B(\alpha)_i^{(k)}(t)}{M_t}\right) \\
&\leq \exp\left(\frac{S(t)\|D - D'\|_1}{M_t}\right). \qquad (32)
\end{aligned}$$

Combining (26)–(32), we derive

$$\begin{aligned}
\frac{\mathbb{P}\left[M(D) \in \mathcal{O}\right]}{\mathbb{P}\left[M(D') \in \mathcal{O}\right]} &\leq \prod_{t=0}^{T-1} \exp\left(\frac{S(t)}{M_t}\right) \\
&\leq \exp\left(\sum_{t=0}^{T-1} \frac{S(t)\|D - D'\|_1}{M_t}\right). \qquad (33)
\end{aligned}$$

If the sequence of $M_t$ satisfies $\sum_{t\in[T]} \frac{S(t)}{M_t} \leq \varepsilon$, then we have $\frac{\mathbb{P}[M(D)\in\mathcal{O}]}{\mathbb{P}[M(D')\in\mathcal{O}]} \leq \exp(\varepsilon\|D - D'\|_1)$. Thus the mechanism is $\varepsilon$-differentially private. ■

The following theorem gives a bound on the sensitivity for the system. To prove it, we fix two private datasets $D$ and $D'$, and calculate the bound on the distance between the two corresponding trajectories under the same observation by decomposing it into (1) the change in agent $i$'s state, and (2) the sum of changes in other agents' state.

*Theorem 1:* For the linear distributed control system, for all $t \in \mathbb{N}$ the sensitivity $S(t) \leq \kappa(t)$, where $\kappa$ is defined as

$$\begin{aligned}
\kappa(t) \triangleq\ &\|G^t - K^t\|_1 + \|K^t\|_1 + \|H\|_1 \sum_{s=0}^{t-1}(\|G^s - K^s\|_1 \\
&+ \|K^s\|_1) \qquad (34)
\end{aligned}$$

with $G \triangleq cI + K$ and $H \triangleq I - K$.

*Proof:* Take a pair of private datasets $D$ and $D'$, and a sequence of observations $O = \{\tilde{x}(t)\}_{t<T}$. By (8), the input $\{u(t)\}_{t<T}$ is also fixed. Then, by (21) we get

$$\begin{aligned}
\|\rho(D,O)(t) - \rho(D',O)(t))\|_1 &= \|(\mathbf{K}+\mathbf{C})^t(x(0) - x'(0)) \\
&+ \sum_{s=1}^{t}(\mathbf{K}+\mathbf{C})^{t-s}(I - \mathbf{K})(p(s) - p'(s))\|_1. \qquad (35)
\end{aligned}$$

We will first expand the term $(\mathbf{K}+\mathbf{C})^s$ on the right-hand side of (35). In block matrix form

$$(\mathbf{K}+\mathbf{C})^s = \left(\begin{bmatrix} K & & \\ & \ddots & \\ & & K \end{bmatrix} + \frac{c}{N}\begin{bmatrix} I & \dots & I \\ \vdots & \ddots & \vdots \\ I & \dots & I \end{bmatrix}\right)^s. \qquad (36)$$

The matrix $(\mathbf{K}+\mathbf{C})$ has two types of blocks:

1) $K + \frac{c}{N}I$ as the diagonal blocks and
2) $\frac{c}{N}I$ as the off-diagonal blocks.

As $K$ and $I$ are commutative, applying binomial expansion of the (36) and after some lengthy but elementary linear algebra the product matrix $(\mathbf{K}+\mathbf{C})^s$ becomes

$$(\mathbf{K}+\mathbf{C})^s = \begin{bmatrix} P_s & Q_s & \dots & Q_s \\ Q_s & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & Q_s \\ Q_s & \dots & Q_s & P_s \end{bmatrix} \qquad (37)$$

where

$$Q_s = \frac{1}{N}(G^s - K^s), \text{ and } P_s = Q_s + K^s \qquad (38)$$

where $G \triangleq cI + K$. From (37), we also obtain

$$(\mathbf{K}+\mathbf{C})^s(I - \mathbf{K}) = \begin{bmatrix} P'_s & Q'_s & \dots & Q'_s \\ Q'_s & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & Q'_s \\ Q'_s & \dots & Q'_s & P'_s \end{bmatrix} \qquad (39)$$

where $Q'_s = Q_s H$, $P'_s = Q'_s + K^s H$, and $H = I - K$. With (37) and (39) we bound the right-hand side of (35).

Without loss of generality, we assume that they differ only in the private data of the $i$th agent. That is, for any $s \leq t$,

$$p(s) - p'(s) = \left[0,\ \dots, 0, [p_i(s) - p'_i(s)]^{\mathrm{T}}, 0, \dots, 0\right]^{\mathrm{T}} \qquad (40)$$

has $n$ nonzero entries corresponding to the preferences of some agent $i$, and all other entries are 0. Then, $(\mathbf{K}+\mathbf{C})^s(p(s) - p'(s))$ is a vector with the $i$th block as $P_s(p_i(s) - p'_i(s))$ and other blocks as $Q_s(p_i(s) - p'_i(s))$. Similarly $(\mathbf{K}+\mathbf{C})^s(I - K)(p(s) - p'(s))$ is a vector with the $i$th block as $P'_s(p_i(s) - p'_i(s))$ and other blocks as $Q'_s(p_i(s) - p'_i(s))$. Therefore, the term inside the norm on the right-hand side of (35) is a vector where the $i$th block is

$$P_t(x_i(0) - x'_i(0)) + \sum_{s=1}^{t} P'_{t-s}(p_i(s) - p'_i(s)) \qquad (41)$$

and all the other $N-1$ components are

$$Q_t(x_i(0) - x'_i(0)) + \sum_{s=1}^{t} Q'_{t-s}(p_i(s) - p'_i(s)). \qquad (42)$$

Substituting (41) and (42) into (35), combining with $\|x_i(0) - x'_i(0)\|_1 + \|(p_i(s) - p'_i(s)\|_1 = \|D - D'\|_1$, we have

$$S(t) \leq (N-1)(\|Q_t\|_1 + \sum_{s=0}^{t-1}\|Q'_s\|_1) + \|P_t\|_1 + \sum_{s=1}^{t}\|P'_s\|_1. \qquad (43)$$

Using (38), we represent $P_s, P'_s$ by $Q_s, Q'_s, K$, and $H$. Therefore,

$$\begin{aligned} S(t) &\le (N-1)(\|Q_t\|_1 + \sum_{s=0}^{t-1}\|Q'_s\|_1) + \|Q_t\|_1 + \|K^t\|_1 \\ &\quad + \sum_{s=1}^{t}\|Q'_s\| + \sum_{s=1}^{t}\|K^s\|_1\|H\|_1 \\ &= N(\|Q_t\|_1 + \sum_{s=0}^{t-1}\|Q'_s\|_1) + \|K^t\|_1 + \|H\|_1\sum_{s=1}^{t}\|K^s\|_1 \end{aligned} \tag{44}$$

Again from (38), substitute $Q_s$ and $Q'_s$ by $H, G$, and $K$, we get

$$\begin{aligned} S(t) &\le \|G^t - K^t\|_1 + \|K^t\|_1 \\ &\quad + \|H\|_1\sum_{s=1}^{t}(\|G^s - K^s\|_1 + \|K^s\|_1). \end{aligned} \tag{45}$$

■

*Remark 3:* The upper bound on the sensitivity at time $t$, $\kappa(t)$ has two components:

1) $\|K^t\|_1 + \|H\|_1\sum_{s=1}^{t}\|K^s\|_1$ over-approximates the change in the $i$th agent's state $x_i$ if its own preference changes at each time up to $t$, and
2) $\|G^t - K^t\|_1 + \|H\|_1\sum_{s=0}^{t-1}\|G^s - K^s\|_1$ over-approximates the sum of the changes in other agents' state given agent $i$'s preference changes up to $t$.

*Remark 4:* $\kappa(t)$ is independent of the number of agents. It only depends on matrix $K$ and the coupling coefficient $c$ and time $t$. $K$ is specified by the individual's control function.

When $K$ is stable, $\|K^t\|_1$ decays to 0. The coupling coefficient $c$ quantifies the influence of the aggregate on each individual agent. The matrix $G = cI + K$ captures the combined dynamics under the influence of the environment and the dynamics of the individual agents. The weaker the physical coupling, the smaller $\|G^t\|_1$. As the individual agent dynamics becomes more stable or the physical coupling between agents becomes weaker, the sensitivity of the system decreases.

*Remark 5:* The convergence of $\kappa(t)$ depends on $K$ and $G$. If $G$ and $K$ are stable, $\kappa(t)$ converges to a constant as $t \to \infty$. Otherwise $\kappa(t)$ grows exponentially with $t$.

*Example 1:* We apply the strategy explained above to a specific system with $K = \frac{1}{5}I_2$. $G = (c + \frac{1}{5})I_2$. By Theorem 1, the sensitivity bound is

$$S(t) \le \kappa(t) = \frac{4 + 20c}{20 - 25c} + \frac{16 - 45c}{20 - 25c}\left(c + \frac{1}{5}\right)^t \tag{46}$$

As stated in Remark 4, the sensitivity bound is independent of $N$. We choose the parameter of the Laplace distribution in the mechanism to be $M_t = \frac{\kappa(t)T}{\varepsilon}$. By Lemma 1, the system guarantees $\varepsilon$-differential privacy up to time $T-1$ for arbitrary $T$. Note that if $G$ is stable, namely $c \in [-6/5, 4/5]$, the sensitivity $S(t)$ is bounded and converges to a constant as $t \to \infty$; otherwise, $\kappa(t)$ diverges.

### C. Cost of Privacy in Linear Distributed Control

In this section, we discuss the cost of privacy for the randomized mechanism. First, from (10), we note that the tracking behavior of the system depends on the matrix $K$.

*Remark 6:* By taking expectation on both sides of (10), we have $\mathbb{E}[x_i(t) - p_i(t)] = K\mathbb{E}[x_i(t-1) - p_i(t)]$. If the closed loop matrix $K$ is Hurwitz and $p_i(t)$ is identical for all $t$, then the state of each agent converges to the preference in expectation.

The growth of cost of privacy over time depends on the stability of the system.

*Theorem 2:* The cost of privacy of the $\varepsilon$-differentially private mechanism $\mathcal{M}$ of Lemma 1 is of the order of $O(\frac{T^3}{N\varepsilon^2})$ if the matrix $K$ is Hurwitz. Otherwise it grows exponentially with $T$.

*Proof:* Given the $\varepsilon$-differentially private mechanism $\mathcal{M}$, the perfectly observable system is obtained by setting the noise values to be 0. We denote by $\bar{x}_i(t)$ the state of agent $i$ for the perfectly observable system at time $t$. From (10), we obtain

$$\begin{aligned} x_i(t) &= K^t x_i(0) + \sum_{s=1}^{t}K^{t-s}(I-K)p_i(s) \\ &\quad - \frac{c}{N}\sum_{s=0}^{t-1}K^{t-s-1}\sum_{j\in[N]}n_j(s). \end{aligned} \tag{47}$$

By fixing $n_i(t) = 0$, we get

$$\bar{x}_i(t) = K^t p_i(0) + \sum_{s=1}^{t}K^{t-s}(I-K)p_i(s).$$

We define a $n \times nN$ matrix $\mathbf{B} \triangleq \frac{c}{N}[I, \ldots, I]$. Again from (47), the state of an individual agent $i$ is

$$x_i(t) = \bar{x}_i(t) - \sum_{s=0}^{t-1}K^{t-s-1}\mathbf{B}n(s).$$

The cost of the mechanism $\mathcal{M}$ can be written as

$$\begin{aligned} \mathrm{cost}_{\varepsilon,D,i} &= \mathbb{E}\left[\sum_{t=1}^{T-1}\|x_i(t) - p_i(t)\|_2^2\right] \\ &= \mathbb{E}\left[\sum_{t=1}^{T-1}\|\bar{x}_i(t) - \sum_{s=0}^{t-1}K^{t-s-1}\mathbf{B}n(s) - p_i(t)\|_2^2\right] \\ &= \sum_{t=1}^{T-1}\mathbb{E}\left[\|\bar{x}_i(t) - p_i(t)\|_2^2 + \|\sum_{s=0}^{t-1}K^{t-s-1}\mathbf{B}n(s)\|_2^2\right. \\ &\qquad \left. - 2(\bar{x}_i(t) - p_i(t))^{\mathrm{T}}\sum_{s=0}^{t-1}K^{t-s-1}\mathbf{B}n(s)\right] \end{aligned}$$

The first term on the right-hand side is the cost of the system with perfect observations, that is, $\overline{\mathrm{cost}}_{D,i}$. The last term on the right-hand side is the expectation of a linear combination of

mean-zero noise terms, and therefore, equals 0. By Definition

$$\Delta(\varepsilon,T) = \sup_{D,i}[\text{cost}_{\varepsilon,D,i} - \overline{\text{cost}}_{D,i}] = \sum_{t=1}^{T-1}\mathbb{E}\left[\|\sum_{s=0}^{t-1}K^{t-s-1}\mathbf{B}n(s)\|_2^2\right] \quad (48)$$

In our mechanism $\mathcal{M}$, for different time steps $s,\tau$, the noise $n(s)$ and $n(\tau)$ are independent. Thus, the right-hand side of (48) reduces to

$$\sum_{t=1}^{T-1}\mathbb{E}\left[\sum_{s=0}^{t-1}n(s)^{\mathrm{T}}\mathbf{B}^{\mathrm{T}}(K^{t-s-1})^{\mathrm{T}}K^{t-s-1}\mathbf{B}n(s)\right].$$

Denote $n^{(k)}(s), k\in[nN]$, be the $k$th element of the vector $n(s)$. It follows that

1) for $k\neq j\in[nN]$, $\mathbb{E}\left[n^{(k)}(s)n^{(j)}(s)\right]=0$, and
2) for any $k\in[nN]$, $\mathbb{E}\left[n^{(k)}(s)n^{(k)}(s)\right]=2M_s^2$.

Thus, the above expression is reduced to

$$\sum_{t=1}^{T-1}\sum_{s=0}^{t-1}2M_s^2\text{Tr}(\mathbf{B}^{\mathrm{T}}(K^{t-s-1})^{\mathrm{T}}K^{t-s-1}\mathbf{B}) \quad (49)$$

where $\text{Tr}(A)$ stands for the trace of matrix $A$. Recall that $\mathbf{B}=\frac{c}{N}[I,\ldots,I]$. It follows that

$$\text{Tr}(\mathbf{B}^{\mathrm{T}}(K^{t-s-1})^{\mathrm{T}}K^{t-s-1}\mathbf{B}) = \frac{c^2}{N}\text{Tr}((K^{t-s-1})^{\mathrm{T}}K^{t-s-1}) = \frac{c^2}{N}\|K^{t-s-1}\|_2^2.$$

Substituting the above equation into (49) yields

$$\Delta(\varepsilon,T)=\frac{2c^2}{N}\sum_{t=1}^{T-1}\sum_{s=0}^{t-1}M_s^2\|K^{t-s-1}\|_2^2.$$

By interchanging the order of summation we get

$$\Delta(\varepsilon,T)=\frac{2c^2}{N}\sum_{s=0}^{T-2}\sum_{t=s+1}^{T-1}M_s^2\|K^{t-s-1}\|_2^2 = \frac{2c^2}{N}\sum_{s=0}^{T-2}M_s^2\sum_{t=0}^{T-s-2}\|K^t\|_2^2. \quad (50)$$

Recall that in Lemma 1, $M_s=\frac{T\kappa(s)}{\varepsilon}$. Combining this with (50), we have

$$\Delta(\varepsilon,T)=\frac{2c^2(T-1)^2}{N\varepsilon^2}\sum_{s=0}^{T-2}\kappa(s)^2\sum_{t=0}^{T-s-2}\|K^t\|_2^2.$$

From the above expression it is clear $\Delta(\varepsilon,T)$ is inversely proportional to $N$ and $\varepsilon^2$. As the matrix $K$ is Hurwitz, $\sum_{t=0}^{T-s-2}\|K^t\|^2$ converges to some constant as $T\longrightarrow\infty$. By Remark 5, if $G$ is stable then $\kappa(s)$ converges to some constant as $s\longrightarrow\infty$, $\sum_{s=0}^{T-2}\kappa(s)^2$ grows linearly with $T$ and we have $\Delta(\varepsilon,T)\sim O(\frac{T^3}{N\varepsilon^2})$. Otherwise if $G$ is unstable, $\Delta(\varepsilon,T)$ grows exponentially with $T$. ■

*Example 2:* Continuing with the system described in Example 1, we now establish the cost of privacy associated with the communication strategy of (50). In this example, $K=0.2\,\mathrm{I}$.

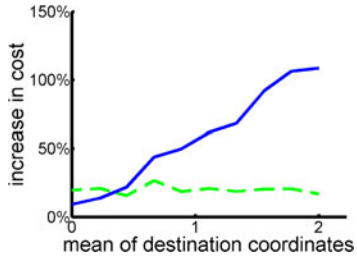



Fig. 2. Increase in cost with biased sampled destinations. The solid and dashed lines capture the relative cost of control with no communication and private communication with respect to the cost of control with broadcast preferences respectively.

We choose the coupling parameter $c$ to be 0.4. Then, the close-loop system is stable. Therefore, the sensitivity is bounded by $\kappa(t)=1.2-0.2\times0.6^t$. The cost of privacy of the system with $N$ agents at time $T$ follows $\frac{0.24(T-1)^3}{N\varepsilon^2}+O(\frac{T^2}{N\varepsilon^2})$.

*Example 3:* We conclude with a simulation-based analysis of Example 1. Consider a linear distributed control system in which each agent is a point on the plane moving toward a randomly chosen destination with dynamics described in Example 2 and control strategies given in Example 2.

The cost of each agent is defined by the distance between its position to its destination. The coupling between agents is the repulsive force in the direction of the center of gravity (CM) of the population. Thus, if the control of an individual fights the force too strongly without the knowledge of the CM then a higher cost is incurred. We numerically simulated the system with different levels of privacy and different distributions of destinations and make the following observations.

Fig. 2 shows the relative costs of control with (dark blue) no communication and (light green) private communication, with respect to cost of control with complete (or broadcast) communication. First of all, if both the initial positions and the destinations are chosen with mean zero, then the CM of the population hovers around the origin and in that case, the contribution of the coupling is small. As a result, there is not much to be gained through communication and we see that the cost of the system with privacy is comparable to the cost of the system with no communication. When the destination comes from some biased (nonzero mean) distributions, we start to see that the cost of control with private communication starts to become smaller compared to those of systems with no communications.

Fig. 3 shows that for the same distribution of initial positions and destinations the cost of privacy changes as predicted by Theorem 2. First of all, higher level of privacy comes with higher cost [Fig. 3(a)]. Second, larger number of agents ($N$) gives lower cost of privacy [Fig. 3(b)]. As $N$ changes from 10 to 100, the CoP decreases from 4 to 0.4. And finally a longer time horizon ($T$) translates to higher costs [Fig. 3(c)]. The simulation results matches the theoretical result that the cost of privacy has the order of $O(\frac{T^3}{N\varepsilon^2})$.

## V. Estimation of Differentially Private Linear Distributed Systems

In this section, we study the problem of estimating the private data of a participants using privacy preserving mechanisms like

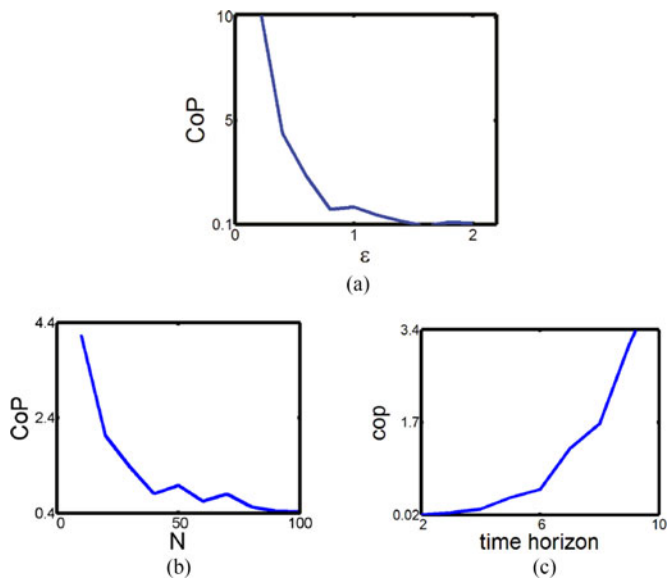



Fig. 3. Cost of privacy for different privacy level, number of agents and time horizon. (a) CoP versus privacy level $\varepsilon$. (b) CoP versus number of agents $N$. (c) CoP versus time horizon $T$.

the ones discussed above. Specifically, given the sequence of observations $O = \{\tilde{x}(t)\}_{t<T}$, how well the estimation on the private data of participants can be. We will show that there is an optimal mechanism of adding possibly correlated noise that minimizes the entropy of unbiased estimators on the private dataset.

Recall from Section III-D that $\hat{D}$ is an unbiased estimator of the private dataset $D$ given observation $O$ up to time $T-1$. Now we show that there is a lower bound on the entropy of such estimators for any $\varepsilon$-differentially private mechanism $\mathcal{M}$.

*Theorem 3:* If the private dataset $D$ is $\varepsilon$-differentially private up to time $T-1$ and $I-K$ is invertible, then the entropy of any unbiased estimator $\hat{D}$ of the private dataset is at least

$$Nn(1-\ln(\varepsilon/2)) + N(T-1)H((I-K)w)$$

where $w \sim \text{Lap}(1/\varepsilon, n)$. The minimum is achieved by

$$n(0) = \lambda(0) \tag{51}$$

$$n(t) = (\mathbf{K}+\mathbf{C})^t\lambda(0) + \sum_{s=1}^{t}(\mathbf{K}+\mathbf{C})^{t-s}(I-\mathbf{K})\lambda(s) \tag{52}$$

for $t \geq 1$, where $\lambda(t) \sim \text{Lap}(1/\varepsilon, nN)$ are independent $nN$-dimensional Laplace noise for $t = 0, \ldots, T-1$.

To prove Theorem 3, we first derive the following necessary condition for the unbiased estimators $\hat{D}$ of the private dataset $D$. In the rest of this section, we assume that the probability distribution function $f(D,\theta)$ of the estimator $\hat{D}$ is absolutely continuous in both $D$ and $\theta$.

*Proposition 1:* If the randomized mechanism $\mathcal{M}$ is $\varepsilon$-differentially private, then the probability distribution function $f(D,\theta)$ of the estimator $\hat{D}$ satisfies

$$|\hat{m}\cdot\nabla_D f(D,\theta)| \leq \varepsilon f(D,\theta) \tag{53}$$

almost everywhere, where the gradient $\nabla_D$ is taken with respect to $D$ and $\hat{m}$ is an arbitrary unit vector.

*Proof:* By (16), for a pair of private datasets $D, D' \in \mathbb{R}^{\text{nNT}}$, we have $f(D',\theta) \leq e^{\varepsilon\|D'-D\|_1} f(D,\theta)$. Thus,

$$\frac{f(D',\theta)-f(D,\theta)}{\|D'-D\|_1} \leq \frac{e^{\varepsilon\|D'-D\|_1}-1}{\|D'-D\|_1} f(D,\theta). \tag{54}$$

By letting $D' \to D$, we have

$$\left|\frac{D'-D}{\|D'-D\|_1}\cdot\nabla f(D,\theta)\right| \leq \varepsilon f(D,\theta) \tag{55}$$

almost everywhere, abbreviated as a.e. Since $D'$ can approach $D$ in arbitrary direction, the proposition holds. ■

### A. Estimation From One-Shot Observation

We first look at a simple case with $T=1$, that is,

$$D = (x_1(0), x_2(0), \ldots, x_N(0)) \in \mathbb{R}^{\text{nN}}$$
$$O = (\tilde{x}_1(0), \tilde{x}_2(0), \ldots, \tilde{x}_N(0)) \in \mathbb{R}^{\text{nN}}$$

and

$$\tilde{x}_i(0) = x_i(0) + n_i(0). \tag{56}$$

This one-shot case corresponds to the protection of the initial states of the participating agents that perform a single noisy broadcast. The noise $n_i(0)$ may depend on the value of $x_i(0)$. Obviously, in this case, the entropy-minimizing unbiased estimator $\hat{D}$ of $D$ is given by

$$\hat{D} = O. \tag{57}$$

Recall from Section III-D that, given the private dataset $D$, $f(D,\theta)$ is the probability distribution function of the estimator $\hat{D}$. Now we show that, to minimize the entropy of the estimation $\hat{D}$, the function

$$q(D,\theta) = f(D,\theta-D) \tag{58}$$

should have the following symmetry properties. In the rest of this section, we denote the $i$th coordinate of $D, \theta \in \mathbb{R}^{\text{nN}}$ by $D_i, \theta_i \in \mathbb{R}$, respectively.

*Lemma 2:* The entropy of the estimator $\hat{D}$ is minimized when the function $q(D,\theta)$ defined in (58) is even in each coordinate $\theta_k \in \mathbb{R}$ of $\theta$.

*Proof:* Without loss of generality, assume $k=1$. Let

$$H_1^+(D) = \int_{[0,\infty)\times\mathbb{R}^{n\,N-1}} -q(D,\theta)\ln q(D,\theta)\mathrm{d}\theta \tag{59}$$

$$H_1^-(D) = \int_{(-\infty,0]\times\mathbb{R}^{n\,N-1}} -q(D,\theta)\ln q(D,\theta)\mathrm{d}\theta \tag{60}$$

and define

$$q'(D,\theta) = \begin{cases} q(D,\theta) & \text{if } \theta_1 > 0, H_1^+(D) \leq H_1^-(D) \\ & \text{or } \theta_1 < 0, H_1^+(D) > H_1^-(D) \\ q(D,\zeta) & \text{if } \theta_1 > 0, H_1^+(D) > H_1^-(D) \\ & \text{or } \theta_1 < 0, H_1^+(D) \leq H_1^-(D). \end{cases} \tag{61}$$

where

$$\zeta_i = \begin{cases} -\theta_i, & \text{if } i = 1, \\ \theta_i, & \text{if } i = 2, 3, \ldots, nN. \end{cases} \tag{62}$$

By construction, $q'(D, \theta + D)$ is even in $\theta_1$. Let $f'(D, \theta) = q'(D, \theta + D)$. Since $H_1^+(D), H_1^-(D)$ is continuous in $D$, the function $f'(D, \theta)$ is also absolutely continuous in both $D$ and $\theta$.

It is easy to check that it satisfies the necessary condition (53), and the unbiased estimator $\hat{D}'$ defined by $f'(D, \theta)$ achieves lower entropy since

$$\begin{aligned} H_D(\hat{D}') &= 2\min\{H_1^+(D), H_1^-(D)\} \\ &\leq H_1^+(D) + H_1^-(D) = H_D(\hat{D}) \end{aligned} \tag{63}$$

for any $D \in \mathbb{R}^{\mathrm{nN}}$, where the equality holds iff $H_1^+(D) = H_1^-(D)$. ■

*Lemma 3:* The entropy of the estimator $\hat{D}$ is minimized when the function $q(D, \theta)$ defined in (58) is independent of $D$.

*Proof:* By Lemma 2, without loss of generality, assume $k = 1$ and $q(D, \theta)$ even in $\theta$. For any

$$a = (a_1, 0, \ldots, 0) \in \mathbb{R}^{\mathrm{nN}}, \quad a_1 \in \mathbb{R}$$

let

$$L^+ = \left\{ D \in \mathbb{R}^{\mathrm{nN}} \mid D_1 \geq a_1 \right\}$$

$$L^- = \left\{ D \in \mathbb{R}^{\mathrm{nN}} \mid D_1 < a_1 \right\}.$$

Define

$$H^+ = \sup_{D \in L^+} \int_{\mathbb{R}^{\mathrm{nN}}} -q(D, \theta) \ln q(D, \theta) \mathrm{d}\theta \tag{64}$$

$$H^- = \sup_{D \in L^-} \int_{\mathbb{R}^{\mathrm{nN}}} -q(D, \theta) \ln q(D, \theta) \mathrm{d}\theta. \tag{65}$$

If $H^+ \leq H^-$, then define

$$q'(D, \theta) = \begin{cases} q(D, \theta), & D \in L^+ \\ q(2a - D, \theta), & D \in L^- \end{cases} \tag{66}$$

otherwise, define

$$q'(D, \theta) = \begin{cases} q(2a - D, \theta), & D \in L^+ \\ f(D, \theta), & D \in L^-. \end{cases} \tag{67}$$

It is well-defined and absolutely continuous, since $q(D, \theta)$ is even in $\theta$. By construction, $q'(D, \theta) = q'(2a - D, \theta)$.

Again, $f'(D, \theta) = q'(D, \theta + D)$ satisfies (53), and the unbiased estimator $\hat{D}'$ defined by $f'(D, \theta)$ achieves lower entropy since

$$H(\hat{D}') = \min\{H^+, H^-\} \leq \max\{H^+, H^-\} = H(\hat{D}') \tag{68}$$

where the equality holds iff $H^+ = H^-$.

Finally, due to the arbitrariness of $a_1$, $q'(D, \theta)$ is independent of $D_1$, thus the lemma holds. ■

*Remark 7:* By Lemma 3, when the entropy of the estimator $\hat{D}$ is minimized, we can write the probability distribution function $f(D, \theta)$ of the estimator $\hat{D}$ on the private dataset $D$ as an even function $f(\theta - D)$.

Now we are at the point of finding out the exact form of $f(\theta - D)$. we will first consider the case of $\theta$ and $D$ being scalars, namely $nN = 1$, and then extend the result to the case of $\theta$ and $D$ being vectors, namely $nN > 1$. For $nN = 1$, minimizing the entropy of $\hat{D}$ is equivalent to solving the following problem.

*Problem 1 (Scalar Case):*

$$\text{Minimize: } H(f) = -\int_{[0,\infty)} f(x) \ln f(x) \mathrm{d}x,$$

$$\begin{aligned} \text{subject to: } & f(x) \text{ is absolutely continuous,} \\ & f(x) \geq 0, \\ & |f'(x)| \leq \varepsilon f(x) \text{ a.e.,} \\ & \int_{[0,\infty)} f(x) \mathrm{d}x = \frac{1}{2}. \end{aligned}$$

We proceed to prove results characterizing the solutions of Problem 1.

*Lemma 4:* Any function $f(x)$ that solves Problem 1 is nonincreasing.

*Proof:* Suppose for the sake of contradiction that $f(x)$ solves Problem 1 and is increasing on some interval in $[0, \infty)$. We will construct another nonincreasing function $h(x)$ such that $H(h) < H(f)$.

Let $g(x) = \sup_{y \geq x} f(y)$. Clearly, $g(x) \geq f(x)$ for $x \geq 0$. Then for some $x^* > 0$, $g(x^*) > f(x^*)$. By continuity of $f$, there exists a "largest" nonempty interval $(a, b)$ containing $x^*$, on which $g(x) > f(x)$. Note that $b$ is finite since $f(x) > 0$ and $\lim_{x \to \infty} f(x) = 0$. In addition, $g(b) = f(b)$. Let

$$d = \frac{1}{f(a)} \int_a^b f(x) \mathrm{d}x. \tag{69}$$

By construction, $d \in [0, b - a)$. There are two cases on the value of $a$. If $a > 0$, then $f(a) = g(a) = f(b) = g(b)$. Define

$$h(x) = \begin{cases} f(x), & x \in [0, a] \\ f(b), & x \in [a, a + d] \\ f(x + b - a - d), & x \in [a + d, \infty]. \end{cases} \tag{70}$$

Otherwise, $a = 0$. Define

$$h(x) = \begin{cases} f(b), & x \in [0, d] \\ f(x + b - d), & x \in [d, \infty] \end{cases} \tag{71}$$

In both cases, $h(x)$ satisfies the constraints in Problem 1 and $H(h) < H(f)$. This is in contradiction with the assumption. ■

*Solution of Problem 1:* Let $F(x) = \int_x^\infty f(y) \mathrm{d}y$ and note that $f(\infty) = \lim_{x \to \infty} f(x) = 0$. By the definition of $\varepsilon$-differential privacy

$$\begin{aligned} \varepsilon F(x) \geq & \int_x^\infty |f'(x)| \mathrm{d}y \geq \left| \int_x^\infty f'(x) \mathrm{d}y \right| \\ = & |f(\infty) - f(x)| = f(x) \end{aligned} \tag{72}$$

where the equalities hold iff $f'(x) = -\varepsilon f(x)$ for $x$ a.e. In particular, $f(0) \leq \varepsilon F(0) = \varepsilon/2$.

By Lemma 4, we have $f'(y) \leq 0$ a.e., thus

$$\begin{aligned} H(f) =& -\int_0^\infty f(x)\ln f(x)\mathrm{d}x \\ =& -\int_0^\infty f(x)\left(\ln f(0)+\int_0^x \frac{f'(y)}{f(y)}\mathrm{d}y\right)\mathrm{d}x \\ =& -\frac{\ln f(0)}{2}-\int_0^\infty \frac{f'(y)}{f(y)}\left(\int_x^\infty f(x)\mathrm{d}x\right)\mathrm{d}y \\ =& -\frac{\ln f(0)}{2}-\int_0^\infty \frac{f'(y)F(y)}{f(y)}\mathrm{d}y \\ \geq& -\frac{\ln f(0)}{2}-\int_0^\infty \frac{f'(y)}{\varepsilon}\mathrm{d}y \\ =& \frac{f(0)}{\varepsilon}-\frac{\ln f(0)}{2} \end{aligned} \tag{73}$$

where the equality holds iff $f'(x) = -\varepsilon f(x)$.

Recalling that $f(0) \in (0, \varepsilon/2]$, on which $\varepsilon f(0) - \frac{1}{2}\ln f(0)$ is decreasing, we have $H(f) \geq (1-\ln(\varepsilon/2))/2$. Again, the equality holds if $f'(x) = -\varepsilon f(x)$ a.e.

In sum, $H(f)$ achieves the minimum $(1-\ln(\varepsilon/2))/2$ at $f'(x) = -\varepsilon f(x)$. Using the conditions that $f(x) \geq 0$ and $\int_{[0,\infty)} f(x)\mathrm{d}x = 1/2$, we derive that the solution to Problem 1 is

$$f(x) = \frac{\varepsilon e^{-x\varepsilon}}{2}. \tag{74}$$

■

Building upon the above scalar case, we now consider the general case $nN > 1$. In this case, minimizing the entropy of the estimator $\hat{D}$ is equivalent to solve the following problem.

*Problem 2 (Vector Case):*

$$\text{Minimize: } H(f) = -\int_{\mathbb{R}_+^{\mathrm{nN}}} f(x)\ln f(x)\mathrm{d}x,$$

subject to: $f(x)$ is absolutely continuous,

$$f(x) \geq 0,$$

$$|\frac{\partial f(x)}{\partial x_i}| \leq \varepsilon f(x), \forall i \in [nN] \text{ a.e.},$$

$$\int_{\mathbb{R}_+^{\mathrm{nN}}} f(x)\mathrm{d}x = \frac{1}{2^{\mathrm{nN}}}.$$

*Solution of Problem 2:* For each fixed $x_2, x_3, \ldots, x_n$, let

$$g_{x_2,x_3,\ldots,x_n}(x_1) = f(x_1, x_2, \ldots, x_n) \tag{75}$$

then we have $g_{x_2,x_3,\ldots,x_n}(x_1) \geq 0$, $|g'_{x_2,x_3,\ldots,x_n}(x_1)| \leq \varepsilon g_{x_2,x_3,\ldots,x_n}(x_1)$ and

$$\begin{aligned} H(f) = -\int_{\mathbb{R}_+^{n-1}}\int_{[0,\infty)} & g_{x_2,x_3,\ldots,x_n}(x_1) \\ & \ln g_{x_2,x_3,\ldots,x_n}(x_1)\mathrm{d}x_1\mathrm{d}x_2\mathrm{d}x_3\ldots\mathrm{d}x_n. \end{aligned} \tag{76}$$

To minimize $H$, we should have

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) =& \ g_{x_2,x_3,\ldots,x_n}(x_1) \\ =& \ e^{-\varepsilon x_1} h(x_2, x_3, \ldots, x_n) \end{aligned} \tag{77}$$

where $h(x_2, x_3, \ldots, x_n)$ is some function of $x_2, x_3, \ldots, x_n$. By repeating the above argument, we derive that the minimum is achieved by

$$f(x_1, x_2, \ldots, x_n) = ke^{-\varepsilon(x_1+x_2+\cdots+x_n)} \tag{78}$$

where $k$ is some constant. Finally, by $\int_{\mathbb{R}_+^{\mathrm{nN}}} f(x)\mathrm{d}x = \frac{1}{2^{\mathrm{nN}}}$, we have $k = (\frac{\varepsilon}{2})^{\mathrm{nN}}$. In this case, the lower bound is $H(f) = \frac{nN}{2}(1-\ln(\varepsilon/2))$. ■

In sum, we have studied a randomized mechanism $\tilde{D} = D + w$ that protects the $\varepsilon$-differential privacy of dataset $D$ from one-shot observation $\tilde{D}$ by adding mean-zero noise $w$. We show that the entropy of any unbiased estimator $\hat{D}$ of the private dataset $D$ has a lower bound, and the minimum is achieved when $w$ is Laplace noise. This shows that Theorem 3 holds for $T = 1$. In addition, we can generalize this result to the following theorem.

*Theorem 4:* Given a invertible $M \in \mathbb{R}^{n\times n}$ and a randomized mechanism $\tilde{x} = Mx + w$ that protects the $\varepsilon$-differential privacy of the private dataset $x \in \mathbb{R}^n$ by adding mean-zero noise $w \in \mathbb{R}^n$ from one-shot observation $\tilde{x}$, the entropy of any unbiased estimator $\hat{x}$ from observation $\tilde{x}$ satisfies

$$H(\hat{x}) \geq H(M\lambda) \tag{79}$$

and the minimum is achieved by using $\hat{x} = M^{-1}\tilde{x}$ and adding noise $n = M\lambda$ where $\lambda \sim \mathrm{Lap}(1/\varepsilon, n)$. In particular, when $M = I$, we have

$$H(\hat{x}) \geq n(1-\ln(\varepsilon/2)). \tag{80}$$

*Proof:* First we know that the proposition holds for $M = I$. In general, since $M$ is invertible, from

$$M^{-1}\tilde{x} = x + M^{-1}w$$

we know that the minimal entropy of the estimator is achieved by $M^{-1}w \sim \mathrm{Lap}(1/\varepsilon, n)$, namely $w = M\lambda$ where $\lambda \sim \mathrm{Lap}(1/\varepsilon, n)$, and the minimal entropy is $H(M\lambda)$. ■

### B. Generalization to Estimation From Sequential Observation

Turning to the case of protecting a sequence of private data from a sequence of observations, we will divide this task into protecting the private dataset $\varepsilon$-differentially private at each time $t < T$ using the dynamics of the distributed system and then apply Theorem 4 iteratively. This will give us a scheme where the noise added to protect the private dataset propagates and accumulates over time.

*Proof of Theorem 3:* For simplicity, define

$$m(t) = \begin{cases} n(0), & \text{if } t = 0, \\ n(t) - (\mathbf{K}+\mathbf{C})n(t-1), & \text{otherwise.} \end{cases} \tag{81}$$

By (22), (23), and (18), we have

$$\tilde{x}(0) = x(0) + m(0) \tag{82}$$

and for $t \geq 1$,

$$\tilde{x}(t) - \mathbf{K}\tilde{x}(t-1) = (I-\mathbf{K})p(t) + m(t). \tag{83}$$

Therefore, the privacy and estimation of $x(0), p(1), \ldots, p(T-1)$ are independent. Noting that

$$I - \mathbf{K} = I_N \otimes (I - K)$$

is invertible, by Theorem 4, the entropy-minimizing mechanism that protects the $\varepsilon$-differential privacy of $D = (x(0), p(1), \ldots, p(T))$ is given by

$$m(t) = \begin{cases} \lambda(0), & \text{if } t = 0 \\ (I - \mathbf{K})\lambda(t), & \text{else} \end{cases} \tag{84}$$

namely

$$n(0) = \lambda(0) \tag{85}$$

and for $t \geq 1$

$$n(t) = (\mathbf{K} + \mathbf{C})^t \lambda(0) + \sum_{s=1}^{t} (\mathbf{K} + \mathbf{C})^{t-s} (I - \mathbf{K}) \lambda(s) \tag{86}$$

where $\lambda(t) \sim \text{Lap}(1/\varepsilon, nN)$ are independent for $t = 0, \ldots, T-1$. The minimal entropy of any unbiased estimator $\hat{D}$ of the private dataset is

$$\begin{aligned} H(\hat{D}) &= \sum_{t=0}^{T-1} H(m(t)) \\ &= Nn(1 - \ln(\varepsilon/2)) + N(T-1)H((I-K)w) \end{aligned} \tag{87}$$

where $w \sim \text{Lap}(1/\varepsilon, n)$. ■

To summarize, we have shown that using a randomized mechanism of adding Laplace noise minimizes the entropy of estimating the private dataset of the distributed system, while keeping it $\varepsilon$-differentially private. This is done by gradually extending from the private data being scalars to vectors, and from one shot to multiple, using the symmetry property of the probability distribution function $f(D, \theta)$ of the estimator $\hat{D}$ on the private dataset $D$, which we assume to be absolutely continuous. As shown by Theorem 3, the minimal entropy of the estimator depends linearly on the number of agents $N$, the dimension $n$ of the state of each agent and the time horizon $T$. In addition, the minimal entropy increases as the privacy level increases, namely $\varepsilon$ decreases. Finally, it only depends on the dynamics of each agent and independent of the coupling coefficient $c$. This is because by communicating with others, the coupling in the dynamic of the agents has been canceled (with some noise left), thus, the initial state and the preferences of each agent propagate only by the local dynamics $K$.

## VI. Conclusion

In this work, we introduced a notion of $\varepsilon$-differential privacy to the setting of distributed dynamical systems of $N$ agents, studied the impact of $\varepsilon$-differential privacy on the tracking performance, and proposed an entropy-minimizing estimation problem on the private dataset. We augmented the traditional definition of differential privacy with a special metric defined on the space of private datasets. In performance analysis, we studied the mechanisms of adding noise in the communication between the agents and the server to keep the system $\varepsilon$-differentially private and proved that the loss of performance, measured by the cost of privacy, grows as $O(T^3/N\varepsilon^2)$ when the system is stable, and it grows exponentially when the system is unstable. In estimation analysis, we prove that, for such noise-adding mechanisms, when the system is $\varepsilon$-differentially private, the entropy of any unbiased estimator on the private dataset from the noisy communication has a lower bound and the noise-adding mechanism that achieves the lower bound is given.

## References


[1] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. & Commun. Secur.*, 2013, pp. 901–914.

[2] M. Xue, W. Wang, and S. Roy, "Security concepts for the dynamics of autonomous vehicle networks," *Automatica*, vol. 50, no. 3, pp. 852–857, 2014.

[3] E. Shi, T.-H. H. Chan, E. G. Rieffel, R. Chow, and D. Song, "Privacy-preserving aggregation of time-series data," in *Proc. 19th Annu. Netw. Distrib. Syst. Secur. Symp.*, vol. 2, no. 3, 2011, Paper 4.

[4] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, "Defending against sybil devices in crowdsourced mapping services," in *Proc. 14th Annu. Int. Conf. Mobile Syst., Appl. Serv.*, 2016, pp. 179–191.

[5] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 901–914.

[6] C. Y. T. Ma, D. K. Y. Yau, N. K. Yip, and N. S. V. Rao, "Privacy vulnerability of published anonymous mobility traces," *IEEE/ACM Trans. Netw.*, vol. 21, no. 3, pp. 720–733, Jun. 2013.

[7] R. Shokri, G. Theodorakopoulos, J. Y. L. Boudec, and J. P. Hubaux, "Quantifying location privacy," in *Proc. Symp. Secur. Privacy*, May 2011, pp. 247–262.

[8] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[9] F. Koufogiannis, S. Han, and G. J. Pappas, "Computation of privacy-preserving prices in smart grids," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, 2014, pp. 2142–2147.

[10] A. S. Masoum, S. Deilami, P. Moses, M. Masoum, and A. Abu-Siada, "Smart load management of plug-in electric vehicles in distribution and residential networks with charging stations for peak shaving and loss minimisation considering voltage regulation," *IET Gener., Transmiss. Distrib.*, vol. 5, no. 8, pp. 877–888, 2011.

[11] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*. New York, NY, USA: Springer, 2006, pp. 1–12.

[12] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*. New York, NY, USA: Springer, 2008, pp. 1–19.

[13] C. Dwork, M. Naor, G. Rothblum, and T. Pitassi, "Differential privacy under continual observation," in *Proc. 42nd ACM Symp. Theory Comput.*, 2010, pp. 715–724.

[14] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proc. 42nd ACM Symp. Theory Comput.*, pp. 705–714, 2010.

[15] Apple Inc, "What's new in iOS 10.0," 2016. [Online]. Available: https://developer.apple.com/library/prerelease/content/releasenotes/general/whatsnewinios/articles/ios10.html

[16] C. Dwork, F. Mcsherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. 3rd Conf. Theory Cryptography*, 2006, pp. 265–284.

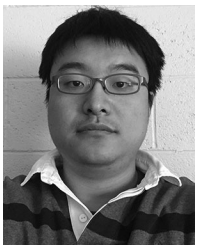
[17] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proc. ACM Workshop Privacy Electron. Soc.*, 2012, pp. 81–90.

[18] J. Le Ny, "On differentially private filtering for event streams," in *Proc. IEEE 52nd Annu. Conf. Decis. Control*, 2013, pp. 3481–3486.

[19] K. Chatzikokolakis, M. E. Andrés, N. E. Bordenabe, and C. Palamidessi, "Broadening the scope of differential privacy using metrics," in *Privacy Enhancing Technologies*. New York, NY, USA: Springer, 2013, pp. 82–102.

[20] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proc. 42nd ACM Symp. Theory Comput.*, 2010, pp. 705–714.

[21] J. Reed and B. C. Pierce, "Distance makes the types grow stronger: a calculus for differential privacy," in *Proc. 15th ACM SIGPLAN Int. Conf. Funct. Program.*, 2010, pp. 157–168.
[22] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. Annu. IEEE Symp. Found. Comput. Sci.*, Oct. 2007, pp. 94 –103.
[23] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, "Optimizing linear counting queries under differential privacy," in *Proc. 29th ACM SIGMOD-SIGACT-SIGART Symp. Princ. Database Syst.*, 2010, pp. 123–134.
[24] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Adv. Cryptol.—EUROCRYPT 2006 (Series Lecture Notes in Computer Science)*, S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 486–503.
[25] J. Le Ny and G. J. Pappas, "Differentially private Kalman filtering," in *Proc. 50th Annu. Allerton Conf. Commun., Control Comput.*, 2012, pp. 1618–1625.
[26] Y. Mo and R. Murray, "Privacy preserving average consensus," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, Dec. 2014, pp. 2154–2159.
[27] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via objective perturbation," in *Proc. Amer. Control Conf.*, Jul. 2016, pp. 2061–2066.
[28] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus with optimal noise selection," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.
[29] M. Hale and M. Egerstedt, "Cloud-based optimization: A quasi-decentralized approach to multi-agent coordination," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, Dec. 2014, pp. 6635–6640.
[30] M. Hale and M. Egerstedt, "Differentially private cloud-based multi-agent optimization with constraints," in *Proc. Amer. Control Conf.*, Jul. 2015, pp. 1235–1240.
[31] S. Han, U. Topcu, and G. Pappas, "Differentially private convex optimization with piecewise affine objectives," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, Dec. 2014, pp. 2160–2166.
[32] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," in *Proc. Int. Conf. Distrib. Comput. Netw.*, 2015, Paper 4.
[33] J. Le Ny and G. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.
[34] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The staircase mechanism in differential privacy," *IEEE J. Sel. Topics. Signal Process.*, vol. 9, no. 7, pp. 1176–1184, Oct. 2015.
[35] Z. Huang, Y. Wang, S. Mitra, and G. E. Dullerud, "On the cost of differential privacy in distributed control systems," in *Proc. 3rd Int. Conf. High Confidence Netw. Syst.*, 2014, pp. 105–114.
[36] Y. Wang, Z. Huang, S. Mitra, and G. Dullerud, "Entropy-minimizing mechanism for differential privacy of discrete-time linear feedback systems," in *Proc. IEEE 53rd Annu. Conf. Decis. Control*, Dec. 2014, pp. 2130–2135.
[37] D. Ghosh and C. Knapp, "Estimation of traffic variables using a linear model of traffic flow," *Transport. Res.*, vol. 12, no. 6, pp. 395–402, 1978.



**Yu Wang** received the B.S. degree from Tsinghua University, Beijing, China, in 2012 and the M.S. degrees in mechanical engineering and mathematics, in 2014 and 2016, respectively, from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, where he is currently working toward the Ph.D. degree in mechanical science and engineering.

**Zhenqi Huang** received the B.Sc. degree in mechanical engineering from Tsinghua University, Beijing, China, in 2010, and the M.Sc. degree and the Ph.D. degree in electrical and computer engineering from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, in 2013 and 2016, respectively.

**Sayan Mitra** (M'01–SM'13) received the undergraduate degree in electrical engineering from Jadavpur University, Kolkata, India, the M.Sc. degree in computer science from Indian Institute of Science, Bangalore, India, and the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2007.

After one year of postdoctoral work at the Center for Mathematics of Information, California Institute of Technology, Pasadena, CA, USA, he joined the University of Illinois at Urbana-Champaign, Urbana, IL, USA, where he is currently an Associate Professor in the Electrical and Computer Engineering Department. He is also an Affiliate Associate Professor of computer science and the Coordinated Science Laboratory. His research interests include formal methods, hybrid systems, distributed systems, and verification of cyberphysical systems and their applications in automotive and aerospace systems.

Prof. Mitra's work has been recognized by the National Science Foundation's CAREER Award, the Air Force Office of Scientific Research Young Investigator Program Award, the IEEE-HKN C. Holmes MacDonald Outstanding Teaching Award, and several best paper awards. He has served as the Program Co-Chair of the 20th International Conference on Hybrid Systems: Computation and Control.

**Geir E. Dullerud** (F'08) received the B.A.Sc. degree in engineering science and the M.A.Sc. degree in electrical engineering both from the University of Toronto, Toronto, ON, Canada, in 1988 and 1990, respectively, and the Ph.D. degree in engineering from the University of Cambridge, Cambridge, U.K., in 1994.

Since 1998, he has been a Faculty Member with the Mechanical Science and Engineering Department, University of Illinois, Urbana-Champaign (UIUC), Urbana, IL, USA, where he is currently a Professor. He is the Director of the Decision and Control Laboratory of the Coordinated Science Laboratory. He has held visiting positions in electrical engineering at KTH, Stockholm, Sweden, in 2013, and in aeronautics and astronautics , Stanford University, Stanford, CA, USA, during 2005.2006. From 1996 to 1998, he was an Assistant Professor of applied mathematics at the University of Waterloo, Waterloo, ON, Canada. He was a Research Fellow and Lecturer in the Control and Dynamical Systems Department, California Institute of Technology, Pasadena, CA, USA, in 1994 and 1995. He has published two books: *A Course in Robust Control Theory* (Springer, 2000) and *Control of Uncertain Sampled-Data Systems* (Birkhauser, 1996). His current research interests include games and networked control, robotic vehicles, hybrid dynamical systems, and cyberphysical systems security.

Dr. Dullerud is currently Associate Editor of the *SIAM Journal on Control and Optimization*, and served in a similar role for *Automatica*. He received the National Science Foundation CAREER Award in 1999, and the Xerox Faculty Research Award at UIUC in 2005. He became an ASME Fellow in 2011. He was an Associate Editor of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL.