2020 American Control Conference
Denver, CO, USA, July 1-3, 2020

Differentially Private Interval Observer Design with Bounded Input Perturbation

Kwassi H. Degue and Jerome Le Ny

Abstract— **Real-time data processing for emerging systems such as intelligent transportation systems requires estimating variables based on privacy-sensitive data gathered from individuals, e.g., their location traces. In this paper, we present a privacy-preserving interval observer architecture for a multi-agent system, where a bounded privacy-preserving noise is added to each participant's data and is subsequently taken into account by the observer. The estimates published by the observer guarantee differential privacy for the agents' data, which means that their statistical distribution is not too sensitive to certain variations in any single agent's signal. A numerical simulation illustrates the behavior of the proposed architecture.**

I. Introduction

The deployment of large scale monitoring and control systems around us has significantly increased over the last decade, as illustrated by intelligent transportation systems, electronic biosurveillance systems and the "Internet of Things". These complex systems require participants to continuously share data, which can compromise the individuals' privacy. For example, one can increase the accuracy of crowd-sourced congestion-aware mapping and routing applications such as Waze and Google Maps by using data provided by smartphones and connected vehicles [1]. However, it is possible to deduce individual users' positions by using Waze [2], and one can deanonymize Google Maps's location data [3]. Therefore, it becomes essential to design rigorous privacy-preserving mechanisms when information must be shared with these systems.

To quantify the notion of privacy, several information theoretic definitions have been suggested, which can be applied to the processing of real-time data streams [4]. This paper uses the notion of *differential privacy*, which has been proposed in the cryptography and database literature [5]. When publishing information about a data set, a differentially private mechanism aims to avoid producing outputs that are too sensitive to a single individual's data. Accordingly, differential privacy guarantees to an individual that whether or not she provides her data does not significantly change a third party's ability to infer new knowledge about her.

Over the last decade, the notion of differential privacy has been extended to dynamical systems and has been applied to filtering [6], [7]. However, these papers assume that the statistical properties of the disturbances in the signal models are available. Furthermore, a differentially private mechanism has been proposed by using *output perturbation* for positive linear systems without disturbance in [8], and for nonlinear systems in [9], both assuming that point-wise estimation (via a Luenberger-type observer design) is possible. Nevertheless, for economical or physical reasons, state disturbances for certain systems are often modeled as bounded uncertain signals. The use of interval estimators [10], [11] instead of point-wise observers can address state estimation problems for such systems. This motivates the design of differentially private observers that handle the presence of disturbances or uncertain parameters whose values are only known to belong to given intervals or polytopes.

The main contribution of this article lies in designing privacy-preserving interval estimators for multi-agents systems in which the signals of individual participants are modeled using uncertain linear time-invariant systems with bounded disturbances. We consider uncertain initial conditions as well as uncertain time-varying inputs and outputs. Extending the differentially private mechanism with bounded noise of [12] for the publication of a single scalar value to the publication of vectors and signals, we obtain an input perturbation mechanism where privacy-preserving noise is added to each individual's data before sending it to an interval observer. Moreover, our estimator handles multi-agent systems in which the dynamics of the agents are coupled, in contrast to [6], [7] that have considered only independent dynamics.

We present the problem statement, describe briefly the concept of differential privacy as well as a privacy-preserving mechanism with input perturbation in Section II. Then, we design a differentially private interval estimator in Section III by using the input perturbation mechanism

This work was supported in part by NSERC under Grant RGPIN-5287-2018 and RGPAS-2018-522686, by the Pierre Arbour Foundation doctoral scholarship and by a doctoral scholarship of the FRQNT.

K. H. Degue and J. Le Ny are with the department of Electrical Engineering, Polytechnique Montreal and GERAD, QC H3T-1J4, Montreal, Canada. kwassi-holali.degue,jerome.le-ny@polymtl.ca

described in Section II. Section IV illustrates the performance of the input perturbation mechanism by presenting numerical simulations that involve dynamic data originating from private firms in a market.

Notation. Throughout this paper, we denote the real numbers by $\mathbb{R}$, the integers by $\mathbb{Z}$, $\mathbb{R}_+ = \{\tau \in \mathbb{R} : \tau \geq 0\}$ and $\mathbb{Z}_+ = \mathbb{Z} \cap \mathbb{R}_+$. We denote the 1-norm of a vector $x \in \mathbb{R}^n$ by $|x|_1 := \sum_{i=1}^n |x_i|$, and the sup-norm by $|x|_\infty := \max_{i\in\{1,\dots,n\}} |x_i|$. For a vector-valued signal $u : \mathbb{Z}_+ \to \mathbb{R}^n$, we denote its ℓ_1-norm by $\|u\|_1 := \sum_{t=0}^\infty |u_t|_1$ (note the usage of the 1-norm here) and its ℓ_∞-norm by $\|u\|_\infty := \sup_{t\geq 0} |u(t)|_\infty$. We denote by $\mathcal{L}_\infty^n$ the set of signals u with the property $||u||_\infty < \infty$. The $n \times n$ identity matrix is denoted by I_n. For two vectors $x_1, x_2 \in \mathbb{R}^n$ or matrices $A_1, A_2 \in \mathbb{R}^{n\times n}$, the relations $x_1 \leq x_2$ and $A_1 \leq A_2$ are understood element-wise. A matrix $A \in \mathbb{R}^{n\times n}$ is called Schur stable if all its eigenvalues have absolute value strictly less than one. We call it nonnegative if all its elements are nonnegative, i.e., if $A \geq 0$. Given a matrix $A \in \mathbb{R}^{m\times n}$, define $A^+ = \max\{0, A\}$, $A^- = A^+ - A$. We fix a generic probability triple $(\Omega, \mathcal{F}, \mathbb{P})$, with $\mathcal{F}$ a σ-algebra on Ω and $\mathbb{P}$ a probability measure defined on $\mathcal{F}$.

II. Background

A. System Model

Let $\left\{y_t^{(i)}, 0 \leq t \leq T\right\}$, $1 \leq i \leq n$ be a set of n measured and privacy-sensitive scalar signals, i.e., $y_t^{(i)} \in \mathbb{R}$, originating from n distinct agents. The case $T = \infty$ is also of interest. A mathematical model for this data is publicly known and consists of a set of linear systems with n individual (vector-valued) states that are coupled and correspond to the n measured signals

$$\begin{aligned} x_{t+1}^{(i)} &= A^{(i)}x_t^{(i)} + \sum_{j\neq i} A^{(i,j)}x_t^{(j)} + w_t^{(i)}, 0 \leq t \leq T-1, \\ y_t^{(i)} &= C^{(i)}x_t^{(i)} + v_t^{(i)}, \ \ 0 \leq t \leq T, \end{aligned} \tag{1}$$

for $i = 1, ..., n$, where $x_t^{(i)} \in \mathbb{R}^{p_i}$ represents the state vector of the agent i, $w^{(i)} : \mathbb{Z}_+ \to \mathbb{R}^{p_i}$ stands for an *unknown* input in $\mathcal{L}_\infty^{p_i}$, $v^{(i)} : \mathbb{Z}_+ \to \mathbb{R}$ is an *unknown* measurement noise in $\mathcal{L}_\infty$, and $A^{(i)}, A^{(i,j)} \in \mathbb{R}^{p_i\times p_j}, C^{(i)} \in \mathbb{R}^{1\times p_i}$ are known constant matrices. The matrices $A^{(i,j)}$ represent coupling matrices that capture the influence of the other agents on the agent i. One can express the dynamics of the global system formed by the n agents as follows

$$\begin{aligned} x_{t+1} &= Ax_t + w_t, \ \ t = 0, 1, ..., T-1, \\ y_t &= Cx_t + v_t, \ \ t = 0, 1, ..., T, \end{aligned} \tag{2}$$

with

$$\begin{aligned} x_t &= \begin{bmatrix} x_t^{(1)\mathrm{T}} & \dots & x_t^{(n)\mathrm{T}} \end{bmatrix}^\mathrm{T}, \ y_t = \begin{bmatrix} y_t^{(1)} & \dots & y_t^{(n)} \end{bmatrix}^\mathrm{T}, \\ w_t &= \begin{bmatrix} w_t^{(1)\mathrm{T}} & \dots & w_t^{(n)\mathrm{T}} \end{bmatrix}^\mathrm{T}, \ v_t = \begin{bmatrix} v_t^{(1)} & \dots & v_t^{(n)} \end{bmatrix}^\mathrm{T}, \\ C &= \mathrm{diag}(C^{(1)}, \dots, C^{(n)}), \\ A &= \begin{bmatrix} A^{(1)} & A^{(1,2)} & \dots & A^{(1,n)} \\ A^{(2,1)} & A^{(2)} & \dots & A^{(2,n)} \\ \vdots & \vdots & \ddots & \vdots \\ A^{(n,1)} & A^{(n,2)} & \dots & A^{(n)} \end{bmatrix}, \end{aligned}$$

where diag() denotes a block-diagonal matrix. Denote $p = \sum_{i=1}^n p_i$. Throughout this paper, we assume that the initial condition x_0 is *unknown* but satisfy the bounds $\underline{x}_0 \leq x_0 \leq \overline{x}_0$, where $\underline{x}_0, \overline{x}_0 \in \mathbb{R}^p$ are given. A data aggregator aims at releasing an estimate $\hat{z}_t$ of a linear combination $z_t = \Phi x_t = \sum_{i=1}^n \Phi_i x_{i,t}$ of the individual states, where the matrices $\Phi_i \geq 0$ are given, by using the data y. To reach this goal, we make the following assumption, stating that the noise signals are bounded.

Assumption 1. *Two functions $\underline{w}, \overline{w} : \mathbb{Z}_+ \to \mathcal{L}_\infty^p$ and two functions $\underline{v}, \overline{v} : \mathbb{Z}_+ \to \mathcal{L}_\infty^n$ are given such that*

$$\underline{w}_t \leq w_t \leq \overline{w}_t \text{ and } \underline{v}_t \leq v_t \leq \overline{v}_t, \ \forall t \geq 0.$$

B. Interval Observer Design and Problem Statement

The following assumption, which is common in the interval observer literature, is needed. It can be relaxed by performing a coordinate transformation [10].

Assumption 2. *There exists a matrix $L \in \mathbb{R}^{m\times n}$ such that the matrix $A - LC$ is Schur stable and nonnegative.*

The equations of an interval observer take the form

$$\begin{aligned} \underline{x}_{t+1} &= (A-LC)\underline{x}_t + Ly_t + \underline{w}_t - L^+\overline{v}_t + L^-\underline{v}_t, \\ \overline{x}_{t+1} &= (A-LC)\overline{x}_t + Ly_t + \overline{w}_t - L^+\underline{v}_t + L^-\overline{v}_t, \end{aligned} \tag{3}$$

where $\underline{x}_t \in \mathbb{R}^m$ and $\overline{x}_t \in \mathbb{R}^m$ stand for the lower and the upper interval estimates of the system state x_t.

Theorem 1. [10] *Let Assumptions 1 and 2 be satisfied. Then, we get for (2)*

$$\underline{x}_t \leq x_t \leq \overline{x}_t, \forall t \geq 0. \tag{4}$$

The data $\underline{x}_0, \overline{x}_0, \underline{w}, \overline{w}, \underline{v}, \overline{v}, A, C, \Phi_i$ is assumed to be public information. By using the publicly released estimates $\Phi\underline{x}_t$ and $\Phi\overline{x}_t$, it might be possible to deduce new information about the data $\{y_t\}_{t\geq 0}$ for example by using *linkage attacks*, where someone can combine the newly published information with other available data to make new inferences about specific individuals [13]. Hence, we aim to ensure that the publicly released estimates $\underline{z}_t$ and

$\overline{z}_t$, which are lower and upper bounds on z_t, also guarantee differential privacy for each agent's data, as defined next.

C. Differential Privacy

A differentially private version of the interval observer (3) must provide estimates that are not too sensitive to some variations in the participating agents' signals y. Let $\mathcal{D}$ denote the space of measured signals $t \mapsto y_t$. Let us define a symmetric binary relation on $\mathcal{D}$, denoted Adj, which identifies the type of variations in y that we aim to make hard to detect. We consider here the following adjacency relation

$$\text{Adj}(y, \tilde{y}) \text{ iff } \|y - \tilde{y}\|_1 \leq \rho, \tag{5}$$

with $\rho \in \mathbb{R}_+$ given. Such an interpretation of adjacent datasets implies that a single participant contributes additively to possibly each $y_t^{(i)}$ in a way that its overall impact on the dataset y is bounded in ℓ_1-norm by ρ. In the special case $T = 0$, we have a single vector $y_0 \in \mathbb{R}^n$, in which case $\mathcal{D} = \mathbb{R}^n$ and the norm in the adjacency relation (5) reduces to the 1-norm $|\cdot|_1$.

Differentially private mechanisms generate randomized outputs that have close distributions for adjacent inputs [5].

Definition 1. *Consider $\mathcal{D}$ a space equipped with a symmetric binary relation denoted Adj, and $(\mathcal{T}, \mathcal{M})$ a measurable space. Let $\epsilon, \delta \geq 0$. A randomized mechanism with inputs in $\mathcal{D}$ and outputs in $\mathcal{T}$ is (ϵ, δ)-differentially private for Adj if for all $d, d' \in \mathcal{D}$ such that Adj(d, d'), we have*

$$\mathbb{P}(M(d) \in S) \leq e^{\epsilon}\mathbb{P}(M(d') \in S) + \delta, \forall S \in \mathcal{M}. \tag{6}$$

If $\delta = 0$, the mechanism is called ϵ-differentially private.

Here we aim to publish estimates $\underline{z}$ and $\overline{z}$ of $z = \Phi x$ that are accurate and respect Definition 1 for given values of ϵ and δ. Smaller values of ϵ and δ give stronger privacy guarantees. We consider an input perturbation architecture [6], where each individual participant perturbs their signal $y^{(i)}$ by adding privacy-preserving white noise in order to render these signals differentially private, before sending them to the data aggregator implementing an observer. In this case, because the signals received by the aggregator are already differentially private, so are the results of the observer's computations, since differential privacy guarantees are preserved by post-processing [6, Theorem 1].

III. Design of the Differentially Private Interval Observer

Normally, to produce a differentially private vector or signal by using additive white noise, the distribution of each noise sample is taken to be Laplace or Gaussian [5], hence has unbounded support. However, to design an interval observer we need to know lower and upper bounds for the noise signals. Therefore, a scheme adding bounded noise is required here. A bounded Laplace mechanism is proposed in [14] but requires to know a priori lower and upper bounds on the signals $y^{(i)}$. Here we do not assume knowledge of such bounds. Instead we build on a noise distribution considered in [12] for the scalar case in which one publishes a single real number in a differentially private way. Here we consider the vector- and signal-valued cases.

Let the privacy parameters be $\epsilon > 0$ and $0 < \delta < \frac{1}{2}$. Define for any integer m the probability density function of a truncated Laplace distribution as follows

$$p(x) = \begin{cases} \phi\, e^{\frac{-|x|}{\lambda}} & \text{if } x \in [-a_m\ a_m], \\ 0 & \text{otherwise,} \end{cases} \tag{7}$$

with

$$\lambda = \frac{\rho}{\epsilon},\ a_m = \frac{\rho}{\epsilon} \ln\left(1 + e^{\epsilon}\frac{m\left(1 - e^{-\epsilon/m}\right)}{2\delta}\right), \tag{8}$$
$$\phi_m = \frac{1}{2\lambda\left(1 - e^{-\frac{a_m}{\lambda}}\right)}.$$

For $m = 1$, we recover the distribution of [12]. Moreover, since $m\left(1 - e^{-\epsilon/m}\right) \leq \epsilon$, and also

$$\lim_{m\to\infty} m\left(1 - e^{-\epsilon/m}\right) = \epsilon,$$

we define

$$a_\infty = \frac{\rho}{\epsilon} \ln\left(1 + \frac{\epsilon\, e^{\epsilon}}{2\delta}\right) \tag{9}$$

and the corresponding distribution with support $[-a_\infty, a_\infty]$ through (7).

Theorem 2. *Let $\epsilon > 0$, $\frac{1}{2} > \delta > 0$. Publishing the sequence of n-dimensional vectors $\hat{y}_t = y_t + \zeta_t$, $0 \leq t \leq T$, where the coordinates of the noise vectors ζ_t are iid with probability distribution* (7) *for $m = n(T + 1)$, and the successive samples of ζ are also iid, is (ϵ, δ)-differentially private for the adjacency relation* (5)*. If $T = \infty$, we take $m = \infty$ and the support for the distribution of each noise component is defined by* (9)*.*

Proof. We prove the result for a single time period ($T = 0$), i.e., for the problem of publishing an n-dimensional vector $\hat{y} = y + \zeta$ so that $\hat{y} \in \mathbb{R}^n$ is differentially private. Hence, we suppress the time index in the rest of the proof. The extension to the publication of signals with $T > 0$ or even $T = \infty$ (i.e., "infinitely long vectors") follows from this result and [6, Lemma 2].

For each measurable set S in $\mathbb{R}^n$,

$$\mathbb{P}(\zeta \in S) = \int_{\mathbb{R}^n} \mathbf{1}_S(x) \prod_{i=1}^{n} p(x_i)\, dx_1 \dots dx_n,$$

where p is the pdf of any component of ζ, of the form (7), and $\mathbf{1}_{\{\cdot\}}$ represents the indicator function. The differential privacy property (6) is equivalent to

$$\sup_{S\in\mathcal{B}(\mathbb{R}^n)} \{\mathbb{P}(y+\zeta\in S) - e^{\epsilon}\mathbb{P}(\tilde{y}+\zeta\in S)\} \le \delta, \quad (10)$$

for any adjacent vectors y and $\tilde{y}$, i.e., such that $|y-\tilde{y}|_1 \le \rho$, where $\mathcal{B}(\mathbb{R}^n)$ represents the Borel σ-algebra. Now, for any set S and vector v, define the notation for the shifted set

$$S - v = \{x | x + v \in S\}.$$

We can rewrite the left-hand side of (10) as $\mathbb{P}(\zeta \in S - y) - e^{\epsilon}\mathbb{P}(\zeta \in S - \tilde{y})$, and then, renaming $S_1 := S - \tilde{y}$, $\mathbb{P}(\zeta \in S_1 - d) - e^{\epsilon}\mathbb{P}(\zeta \in S_1)$, with $d = y - \tilde{y}$. Since (10) must hold for all Borel sets S, the sets S_1 also consist of all Borel sets, and (10) can be rewritten equivalently (we renamed S_1 to S to simplify the notation)

$$\sup_{S\in\mathcal{B}(\mathbb{R}^n)} \{\mathbb{P}(\zeta \in S - d) - e^{\epsilon}\mathbb{P}(\zeta \in S)\} \le \delta, \quad (11)$$

for any vector d such that $|d|_1 \le \rho$. This places a condition on the distribution of ζ.

Let C_a be the hypercube $[-a, a]^n$ (here a denotes the support of the distribution (7), which is determined below, so we omit the subscript m from the notation for now). Since the support of the distribution of ζ is contained in C_a, the expression to be upper bounded by δ in (11) for all S and admissible d can be written

$$\begin{aligned}&\mathbb{P}(\zeta \in S - d) - e^{\epsilon}\mathbb{P}(\zeta \in S)\\ &= \mathbb{P}(\zeta \in (S - d) \cap C_a) - e^{\epsilon}\mathbb{P}(\zeta \in S \cap C_a).\end{aligned}$$

We now exploit the form of the Laplace distribution to work with a more convenient upper bound. We have

$$\begin{aligned}&\mathbb{P}(\zeta \in (S - d) \cap C_a)\\ &= \phi^n \int_{\mathbb{R}^n} e^{-\frac{|x|_1}{\lambda}} \mathbf{1}_{S-d}(x)\, \mathbf{1}_{C_a}(x) dx\\ &= \phi^n \int_{\mathbb{R}^n} e^{-\frac{|x|_1}{\lambda}} \mathbf{1}_{S}(x+d)\, \mathbf{1}_{C_a+d}(x+d) dx\\ &= \phi^n \int_{\mathbb{R}^n} e^{-\frac{|z-d|_1}{\lambda}} \mathbf{1}_{S}(z)\, \mathbf{1}_{C_a+d}(z) dz,\end{aligned}$$

using the fact that $\mathbf{1}_A(x) = \mathbf{1}_{A+d}(x+d)$ and the change of variable $z = x + d$. Since $|z-d|_1 \ge |z|_1 - |d|_1$, if $|d|_1 \le \rho$, we get

$$\mathbb{P}(\zeta \in (S - d) \cap C_a) \le e^{\frac{\rho}{\lambda}} \phi^n \int_{\mathbb{R}^n} e^{-\frac{|x|_1}{\lambda}} \mathbf{1}_{S\cap(C_a+d)}(x) dx.$$

If moreover we take $\frac{\rho}{\lambda} \le \epsilon$, we get the upper bound

$$\begin{aligned}&\mathbb{P}(\zeta \in S - d) - e^{\epsilon}\mathbb{P}(\zeta \in S)\\ &\le e^{\epsilon}\phi^n \int_{\mathbb{R}^n} e^{-\frac{|x|_1}{\lambda}} \left\{\mathbf{1}_{S\cap(C_a+d)}(x) - \mathbf{1}_{S\cap C_a}(x)\right\} dx.\end{aligned}$$

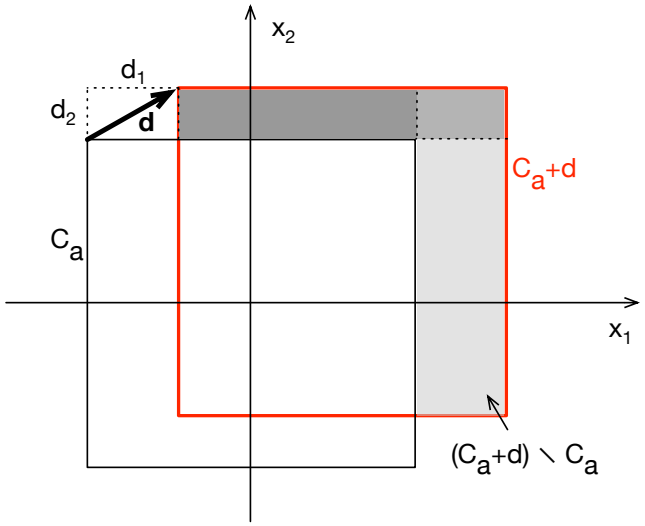

Fig. 1. Geometry for the (ϵ, δ)-differential privacy argument. The set $(C_a + d) \setminus C_a$ has been subdivided into n (here $n = 2$) rectangles, which intersect in the "top-right corner" of $C_a + d$.

From here on, we fix $\lambda = \rho/\epsilon$. Since the only points x that contribute something positive to the integral are those that are simultaneously in S, in $C_a + d$ and not in C_a, the integral is maximized for $S = (C_a + d) \setminus C_a$, and we get

$$\mathbb{P}(\zeta \in S - d) - e^{\epsilon}\mathbb{P}(\zeta \in S) \le e^{\epsilon} F(d), \quad (12)$$

with

$$F(d) := \phi^n \int_{\mathbb{R}^n} e^{-\frac{|x|_1}{\lambda}} \mathbf{1}_{(C_a+d)\setminus C_a}(x)\, dx.$$

We now maximize the upper bound (12) over admissible d (i.e., such that $|d|_1 \le \rho$) and obtain a condition under which this upper bound is less than δ.

By symmetry (see Figure 1), it is sufficient to consider the case $d = [d_1, \ldots, d_n]$ with $d_i \ge 0$ for all i and $\sum_i d_i \le \rho$. Next, note from Figure 1 that $(C_a + d) \setminus C_a \subset \cup_{i=1}^n R_i$, where R_i is the hyperrectangle

$$\begin{aligned}R_i = \{x \in \mathbb{R}^n \,|\, &a \le x_i \le a + d_i, \text{and}\\ &-a + d_j \le x_j \le a + d_j, \forall j \ne i\}.\end{aligned}$$

Therefore, we get the bound

$$F(d) \le \sum_{i=1}^{n} \phi^n \int_{R_i} e^{-|x|_1/\lambda} dx.$$

Now

$$\phi^n \int_{R_i} e^{-|x|_1/\lambda} dx = \phi \int_a^{a+d_i} e^{-x_i/\lambda} dx_i \prod_{j\ne i} T_j,$$

where

$$T_j = \phi \int_{-a+d_j}^{a+d_j} e^{-|x_j|/\lambda} dx_j \leq \phi \int_{-a}^{a} e^{-|x_j|/\lambda} dx_j = 1,$$

because of the shape of the function $e^{-|x_j|/\lambda}$. Hence, we have

$$\begin{aligned} F(d) &\leq \sum_{i=1}^{n} \phi \int_{a}^{a+d_i} e^{-x_i/\lambda} dx_i \\ &= \phi\, \lambda\, e^{-a/\lambda} \sum_{i=1}^{n} \left(1 - e^{-d_i/\lambda}\right). \end{aligned}$$

Consider then the maximization problem

$$\begin{aligned} &\max_{d \in \mathbb{R}^n} \sum_{i=1}^{n} \left(1 - e^{-d_i/\lambda}\right) \\ &\text{s.t. } d_i \geq 0, 1 \leq i \leq n, \text{ and } \sum_{i=1}^{n} d_i \leq \rho. \end{aligned}$$

Since the objective is strictly concave in d and the constraints define a polytope, this problem has a unique maximizer. A straightfoward analysis, e.g., using the KKT conditions, shows that this maximizer is given by $d_i = \rho/n$ for all $1 \leq i \leq n$. Hence, we finally get

$$F(d) \leq \phi\, \lambda\, e^{-a/\lambda}\, n \left(1 - e^{-\frac{\rho}{n\lambda}}\right).$$

We now choose a to ensure that the upper bound on $e^{\epsilon} F(d)$ is always less than δ. We get the condition

$$\begin{aligned} e^{\epsilon} \frac{e^{-\frac{a}{\lambda}} n \left(1 - e^{-\rho/n\lambda}\right)}{1 - e^{-\frac{a}{\lambda}}} &\leq 2\delta \\ \text{hence, } e^{a/\lambda} &\geq 1 + e^{\epsilon} \frac{n \left(1 - e^{-\rho/n\lambda}\right)}{2\delta} \\ a &\geq \frac{\rho}{\epsilon} \ln \left(1 + e^{\epsilon} \frac{n \left(1 - e^{-\epsilon/n}\right)}{2\delta}\right) \end{aligned}$$

where we used $\lambda = \frac{\rho}{\epsilon}$ on the last line. This gives the distribution (7) with $m = n$, as stated in the Theorem for the case $T = 0$. □

The privacy-preserving noise introduced in Theorem 2 is bounded and we get

$$\underline{\zeta}^{(i)} \leq \zeta_t^{(i)} \leq \overline{\zeta}^{(i)}, \quad \forall t \geq 0, \tag{13}$$

with $\overline{\zeta}^{(i)} = -\underline{\zeta}^{(i)} = a_m$ for $i = 1, ..., n$, $m = n(T+1)$. In the sequel, denote $\overline{\zeta} = -\underline{\zeta} = \begin{bmatrix} a_m & \dots & a_m \end{bmatrix}^{\mathrm{T}}$ and $\zeta_t = \begin{bmatrix} \zeta_t^{(1)} & \dots & \zeta_t^{(n)} \end{bmatrix}^{\mathrm{T}}$. When the data aggregator receives the differentially private signal $\hat{y}$, it can design an interval observer and publish lower and upper estimates $\underline{\hat{x}}$ and $\hat{\overline{x}}$ for the state x. Releasing $\Phi\underline{\hat{x}}$ and $\Phi\hat{\overline{x}}$ preserves (ϵ, δ)-differentially privacy for the data y by the resilience to post-processing property. The equations of the interval estimator can be written as follows

$$\begin{aligned} \underline{\hat{x}}_{t+1} &= (A - LC)\underline{\hat{x}}_t + L\hat{y}_t + \underline{w}_t - L^{+}(\overline{v}_t + \overline{\zeta}) \\ &\quad + L^{-}(\underline{v}_t + \underline{\zeta}), \quad \underline{\hat{x}}_0 = \underline{x}_0, \\ \hat{\overline{x}}_{t+1} &= (A - LC)\hat{\overline{x}}_t + L\hat{y}_t + \overline{w}_t - L^{+}(\underline{v}_t + \underline{\zeta}) \\ &\quad + L^{-}(\overline{v}_t + \overline{\zeta}), \quad \hat{\overline{x}}_0 = \overline{x}_0. \end{aligned} \tag{14}$$

Theorem 3. *Let Assumptions 1 and 2 be satisfied. Then, we get for* (2)

$$\underline{\hat{x}}_t \leq x_t \leq \hat{\overline{x}}_t, \ \ \forall t \geq 0. \tag{15}$$

Furthermore, we get $\underline{\hat{e}}, \hat{\overline{e}} \in \mathcal{L}_{\infty}^{p}$ *for the error signals* $\underline{\hat{e}}_t := x_t - \underline{\hat{x}}_t$, $\hat{\overline{e}}_t := \hat{\overline{x}}_t - x_t$.

Note that the differentially private signals $\underline{\hat{x}}, \hat{\overline{x}}$, while random, still maintain the order relation (15) of an interval observer for each trajectory.

Proof. The proof follows interval estimation's standard argumentation [15], [16]. □

IV. Simulations

Consider a scenario involving a dynamic market with n firms that supply the same product [17]. The production dynamics of each firm is modeled as a linear system, which is affected by its neighbor firms. Neighbors of the firm i represent firms in different regions that cooperate or have coordination relationships with i. The firm i, for $1 \leq i \leq n$, is modeled as follows

$$x_{t+1}^{(i)} = (1 - \alpha) x_t^{(i)} + w_t^{(i)} + \frac{\alpha}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} x_t^{(j)},$$

where $x_t^{(i)}$ represents the production output of the firm i, $\mathcal{N}_i$ stands for its neighbors and $|\mathcal{N}_i|$ denotes the number of its neighbors. As in [17], let $\alpha = 0.15$, $\mathcal{N}_i = \{i+1\}$ for $i = 1, \dots, n-1$ and $\mathcal{N}_n = \{1\}$. Consider $n = 5$. Therefore, we get the global matrix A for (2)

$$A = \begin{bmatrix} 1-\alpha & \alpha & 0 & 0 & 0 \\ 0 & 1-\alpha & \alpha & 0 & 0 \\ 0 & 0 & 1-\alpha & \alpha & 0 \\ 0 & 0 & 0 & 1-\alpha & \alpha \\ \alpha & 0 & 0 & 0 & 1-\alpha \end{bmatrix}.$$

The data $y^{(i)}$ of each firm i consists of a noisy measurement of its production output: $y_t^{(i)} = x_t^{(i)} + v_t^{(i)}$. The process noise $w_t^{(i)}$ and the measurement noise $v_t^{(i)}$ of each firm i are iid uniform random variables in the interval $[0, W]$ and $[0, V]$ respectively. Therefore, we have $\underline{w}_t^{(i)} = 0$, $\underline{v}_t^{(i)} = 0$, $\overline{w}_t^{(i)} = W$ and $\overline{v}_t^{(i)} = V$. The initial conditions of the state

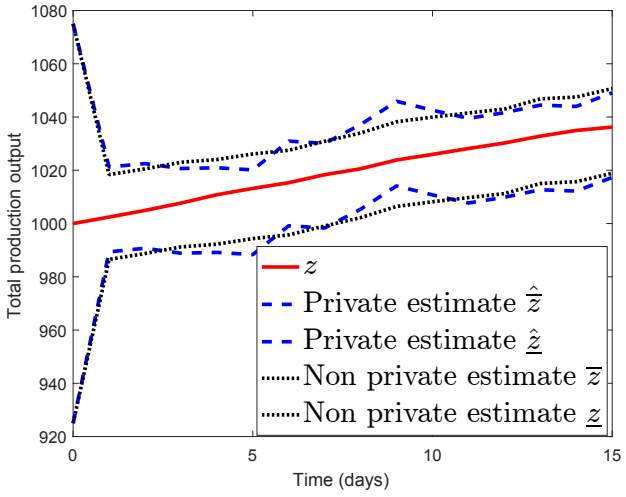

Fig. 2. Evolution of $z = \sum_{i=1}^{5} \Phi_i x_i$, the differentially private observer bounds $\sum_{i=1}^{5} \Phi_i \hat{\underline{x}}_i$ and $\sum_{i=1}^{5} \Phi_i \hat{\overline{x}}_i$ and the non private standard observer bounds.

of each firm i are $x_0^{(i)} = 200$, and for the design of the observer we assume known the bounds on initial conditions $\underline{x}_0^{(i)} = 200-\sigma$, $\overline{x}_0^{(i)} = 200+\sigma$, $\sigma = 15$, $W = 1$ and $V = 1$. We take $T = \infty$.

A data aggregator aims at releasing the total production output from the data of the n firms, so the matrix $\Phi = \begin{bmatrix} 1 & \dots & 1 \end{bmatrix}$. However, it needs to provide privacy guarantees for the firms, since the production data $y^{(i)}$ is highly sensitive. Consider the adjacency relation (5) with $\rho = 1$. We set the privacy parameters to $\epsilon = \ln(3)$ and $\delta = 0.1$. We select the interval observer gain as follows

$$L = 10^{-4} \times \begin{bmatrix} 8498 & 1498 & -1 & -1 & -1 \\ -1 & 8498 & 1498 & -1 & -1 \\ -1 & -1 & 8498 & 1498 & -1 \\ -1 & -1 & -1 & 8498 & 1498 \\ 1498 & -1 & -1 & -1 & 8498 \end{bmatrix},$$

to satisfy Assumption 2. To provide differential privacy guarantees for each firm's data, we compute differentially private interval estimates by applying Theorem 3. Figure 2 shows the difference between the differentially private observed bounds $\hat{\underline{z}}, \hat{\overline{z}}$ and bounds provided by standard non private interval observers obtained from Theorem 1.

V. Conclusion

We have considered the problem of interval estimation under a differential privacy constraint in this article. We have designed an input perturbation architecture for differentially private interval estimation. The performance of our private interval estimator is illustrated through numerical simulations. Future research could consider the design a differentially private interval observer by using output perturbation.

References

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

[2] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," in *Proceedings of the ACM SIGSAC conference on Computer & communications security*, Berlin, Germany, Nov. 2013, pp. 901–914.

[3] 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 Transactions on Networking*, vol. 21, no. 3, pp. 720–733, Jun. 2013.

[4] L. Sankar, W. Trappe, K. Ramachandran, H. V. Poor, and M. Debbah, "The role of signal processing in meeting privacy challenges: An overview," *IEEE Signal Processing Magazine, Special Issue on Cyber-Security and Privacy*, vol. issue 5, pp. 95–106, 2013.

[5] C. Dwork, "Differential privacy," in *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, ser. Lecture Notes in Computer Science, vol. 4052. Springer-Verlag, 2006.

[6] J. Le Ny and G. Pappas, "Differential private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, February 2014.

[7] K. H. Degue and J. Le Ny, "On differentially private Kalman filtering," in *Proceedings of the 5th IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Montreal, Canada, Nov. 2017.

[8] A. McGlinchey and O. Mason, "Differential privacy and the l_1 sensitivity of positive linear observers," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3111–3116, Jul. 2017, 20th IFAC World Congress.

[9] J. Le Ny, "Differentially private nonlinear observer design using contraction analysis," *International Journal of Robust and Nonlinear Control*, pp. 1–19, Nov. 2018.

[10] F. Mazenc, T. N. Dinh, and S. I. Niculescu, "Robust interval observers and stabilization design for discrete-time systems with input and output," *Automatica*, vol. 49, pp. 3490–3497, Sep. 2013.

[11] K. H. Degue and J. Le Ny, "Estimation and outbreak detection with interval observers for uncertain discrete-time SEIR epidemic models," *International Journal of Control*, Jul. 2019.

[12] Q. Geng, W. Ding, R. Guo, and S. Kumar, "Privacy and utility tradeoff in approximate differential privacy," *ArXiv e-prints*, Feb. 2019.

[13] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, pp. 571–588, 2002.

[14] N. Holohan, S. Antonatos, S. Braghin, and P. M. Aonghusa, "The Bounded Laplace Mechanism in Differential Privacy," *ArXiv e-prints*, Aug. 2018.

[15] F. Mazenc and O. Bernard, "Interval observers for linear time-invariant systems with disturbances," *Automatica*, vol. 47, no. 1, pp. 140–147, 2011.

[16] D. Efimov, T. Raïssi, and A. Zolghadri, "Control of nonlinear and LPV systems: interval observer-based framework," *IEEE Transactions on Automatic Control*, vol. 58, no. 3, pp. 773–782, Mar. 2013.

[17] Q. Zhang and J. Zhang, "Adaptive tracking games for coupled stochastic linear multi-agent systems: Stability, optimality and robustness," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2862–2877, Nov. 2013.