2024 American Control Conference (ACC)
July 8-12, 2024. Toronto, Canada

System Design Approach for Control of Differentially Private Dynamical Systems

Raman Goyal, Dhrubajit Chowdhury, and Shantanu Rane

Abstract— **This paper introduces a novel approach to concurrently design dynamic controllers and correlated differential privacy noise in dynamic control systems. An increase in privacy noise increases the system's privacy but adversely affects the system's performance. Our approach optimizes the noise distribution while shaping closed-loop system dynamics such that the privacy noise has the least impact on system performance and the most effect on system privacy. We further add privacy noise to both control input and system output to privatize the system's state for an adversary with access to both communication channels and direct output measurements. The study also suggests tailored privacy bounds for different states, providing a comprehensive framework for jointly optimizing system performance and privacy in the context of differential privacy.**

I. Introduction

In today's increasingly interconnected and data-driven world, it has become important for connected entities to share information with each other to work efficiently. This applies not just to individuals, but also to Cyber-Physical Systems (CPS) in various sectors, including industrial control systems, power grids, financial markets, and commercial and military communication networks. This pervasive data sharing has also brought forth heightened concerns regarding system security, safety and privacy. The risk of exposing sensitive information to adversaries has significantly increased, posing potential harm to both individuals and critical systems. This has led to the development of mechanisms providing different kinds of privacy guarantees. Examples include differential privacy, information-theoretic privacy, and privacy based on secure multiparty computation.

Differential privacy was originally designed to protect the data of individuals in static databases, but its application has expanded to address the privacy challenges posed by dynamic and interconnected data ecosystems, such as CPS and IoT devices [1]. At a basic level, a differentially private mechanism ensures that the results of a query remain approximately unchanged if data belonging to any single user in the database is modified [2]. Informally, differential privacy makes similar data appear *approximately* indistinguishable from one another [3]. The most important feature of differential privacy is its protection from post-processing or its robustness in the presence of side information [4]. However, there is a price associated with making the system differentially private. Differential privacy works by adding noise to the system which leads to a degradation in system performance both in static and dynamic cases [4], [5].

In recent years, researchers have extended the work on differential privacy for static databases to differential privacy for dynamic filters [5], control and dynamical systems [2], differentially private LQ Control [3], multi-agent formation control [6], and Differentially private distributed constrained optimization [7]. In differentially private LQ control [3], the authors consider a multi-agent system described using linear system dynamics and add privacy noise such that every agent's state trajectory is made approximately indistinguishable from all other state trajectories. The paper provides lower and upper bounds on mean square error (MSE) in state estimation for some minimum and maximum privacy noise among agents, where the combined state is estimated using a standard Kalman filter while designing an LQG control for the overall system. The paper further provides guidelines for choosing the privacy level ϵ_i to bound the MSE in the cloud's state estimates and further provides the cost of privacy in terms of the increase of the quadratic cost. Kawan and Cao [8], [9] show that the Gaussian mechanism evaluates the maximum eigenvalue of the input observability Gramian and thus the addition of even small noise is enough to make the less input observable Gaussian mechanism highly differentially private.

In this paper, we consider the joint design of dynamic controller and differentially private noise (correlated noise with different variances across channels) such that the system performance loss is minimized for a given privacy metric or the privacy metric is maximized for a given system performance. The idea is to find the optimal privacy noise distribution and simultaneously design the closed-loop system dynamics such that the larger noise would only be added through the input/output channels whose effect on the system state has been minimized by designing the closed-loop poles. We assume a smart adversary that will develop an optimal estimator to generate individual signals for more accurate state estimation by leveraging the additional information about the system dynamics. We consider two kinds of adversaries, one that has access to the communication channel and another that has direct access to the measurements. We express a privacy metric in the presence of smart adversaries in terms of uncertainty in the estimation of individual states. We further design different privacy/performance bounds in different states as some states might need stricter privacy/performance guarantees than other states.

R. Goyal, D. Chowdhury, and S. Rane are with Palo Alto Research Center - Part of SRI International, Palo Alto, CA, USA. {raman.goyal, dhruba.chowdhury, shantanu.rane}@sri.com,

979-8-3503-8265-5/$31.00 ©2024 AACC

The organization of the paper can be laid out as follows: Section §II provides the necessary background on differential privacy and Section §III gives the relationship between differential privacy and error in state estimate and then formulates the final design problem. Section §IV elaborates the system design approach for a general dynamic controller and correlated differential privacy input and output noises and provides the solution as a convex optimization problem. Section §V gives simulation results for differential privacy of a networked power distribution system with load frequency control under unknown power demand and §VI provides the final concluding remarks along with the future work.

II. Review of Differential Privacy

Let us consider agent's state trajectories of the form $x = (x_1, x_2, \ldots)$, where $x_k \in \mathbb{R}^{n_x}$ and $\|x_k\|_2 < \infty$ for all k, and let us denote the set of all such sequences by $x \in \ell_2^{n_x}$. Let us define our adjacency relation over $\ell_2^{n_x}$.

Definition 1. *(Adjacency for trajectories): Let us choose $\beta > 0$ as the adjacency parameter and $v, w \in \ell_2^{n_x}$ as two trajectories that are adjacent if $\|v - w\|_{\ell_2} \leq \beta$. We write $\mathrm{Adj}_\beta(v, w) = 1$ if v and w are adjacent, and $\mathrm{Adj}_\beta(v, w) = 0$, otherwise.*

This adjacency relation requires that an agent's state trajectory be made approximately indistinguishable within distance β from all other state trajectories. Let us consider that the agent's output signal is of dimension n_y at each point in time and is in the set $\ell_2^{n_y}$.

Definition 2. *(Sensitivity): The p-norm sensitivity of a system $\mathcal{G}$ is the greatest distance between two output trajectories that correspond to adjacent state trajectories:*

$$\Delta_p \mathcal{G} := \sup_{x, \tilde{x} |\, \mathrm{Adj}_\beta(x, \tilde{x}) = 1} \|\mathcal{G}(x) - \mathcal{G}(\tilde{x})\|_p.$$

Definition 3. *(DP for trajectories) [5]: Let $\epsilon > 0$ and $\delta \in (0, 1/2)$. A mechanism $\mathcal{M}(\cdot) \in \ell_2^{n_y}$ is (ϵ, δ)-differentially private if, for all adjacent $x, x' \in \ell_2^{n_x}$, we have:*

$$\mathbb{P}[\mathcal{M}(x) \in S] \leq e^\epsilon \mathbb{P}[\mathcal{M}(x') \in S] + \delta \text{ for all } S \in \Sigma_2^{n_y}.$$

Lemma 1. *(Gaussian mechanism) [5]: Let us use privacy parameters $\epsilon > 0$ and $\delta \in (0, 1/2)$ and adjacency parameter $\beta > 0$. Let $\mathcal{G}$ denote a dynamical system and $\Delta_2 \mathcal{G}$ denote its 2-norm sensitivity. The Gaussian mechanism $\mathcal{M} = \mathcal{G}(x) + v^p$ makes the system (ϵ, δ)-differentially private with respect to Adj_β, if $v^p(k) \sim \mathcal{N}\left(0, \sigma^2 I_{n_y}\right)$, and $\sigma \geq \Delta_2 \mathcal{G}\ \beta\ \kappa(\delta, \epsilon)$, where $\kappa(\delta, \epsilon) = \frac{1}{2\epsilon}\left(K_\delta + \sqrt{K_\delta^2 + 2\epsilon}\right)$, $K_\delta := \mathcal{Q}^{-1}(\delta)$, and $\mathcal{Q}$ representing the Gaussian tail integral.*

III. Problem Formulation

The main objective of the research is to make the state of the agents differentially private by adding privacy noise while achieving the desired system performance. The privacy noise can be added to the outputs measured by the sensors as v_k^p and/or to the control input as w_k^p. Notice that the actual privacy noise should be calculated by accounting for the actuator noise present in the system.

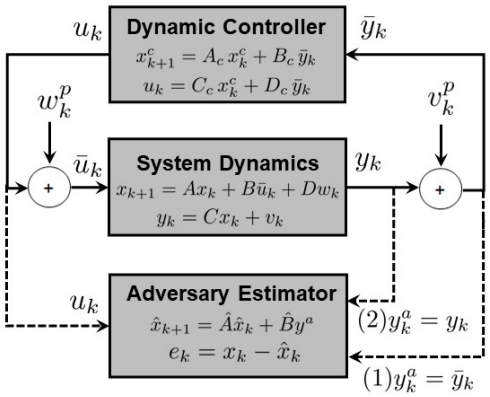

Fig. 1. Design architecture for making agent's state differentially private by adding privacy noise to both system inputs and output.

We consider two cases based on the capability of the adversary (refer fig. 1):

1) The adversary listens to the communication between the agents and the centralized controller ((1) $y_k^a = \bar{y}_k$). We add privacy noise to both the sensor outputs and the control inputs to make the state differentially private.
2) The adversary has his own sensors and has direct access to the output of the system ((2) $y_k^a = y_k$), and thus adding output privacy noise alone would not make the system differentially private. Although there is no benefit in adding privacy noise to the sensor side, we still add it and expect the design to remove the privacy noise on the output side.

Let us consider a discrete-time linear time-invariant (LTI) system, along with the addition of output privacy noise and control input privacy noise described as:

$$x_{k+1} = Ax_k + B(u_k + w_k^p) + Dw_k, \tag{1}$$
$$y_k = Cx_k + v_k, \tag{2}$$
$$\bar{y}_k = Cx_k + v_k + v_k^p, \tag{3}$$
$$z_k = C_z x_k, \tag{4}$$

where $x_k \in \mathbb{R}^{n_x}$ is the state, $u_k \in \mathbb{R}^{n_u}$ is the control, $y_k \in \mathbb{R}^{n_y}$ is the output measured by a sensor network, and $z_k \in \mathbb{R}^{n_z}$ is the variables of interest/performance variable for the system. The initial state vector x_0 and the process noise, w_k, and sensor noise, v_k, are assumed to be independent random variables. In particular, $w_k \sim \mathcal{N}(\mathbf{0}, W)$, and $v_k \sim \mathcal{N}(\mathbf{0}, V)$, $\forall k$, with $W \in \mathbb{R}^{n_w \times n_w}$ and $V \in \mathbb{R}^{n_v \times n_v}$ to be the known and fixed covariance matrix.

The control input privacy noise, w_k^p, and output privacy noise, v_k^p, are modeled as random variables, $w_k^p \sim \mathcal{N}(\mathbf{0}, W^p)$ and $v_k^p \sim \mathcal{N}(\mathbf{0}, V^p)$, $\forall k$, with W^p and V^p being the covariance matrix, representing the strength of the added noise. We further define the inverse of the respective noise covariance matrices as: $\Gamma_w = {W^p}^{-1}$, $\Gamma_v = {V^p}^{-1}$.

We assume that the adversary is smart and has full information about the system dynamics, i.e., A, B, C, D. The adversary will design an optimal estimator to estimate the

system state $\hat{x}_k$ using a general estimator of the form:

$$\hat{x}_{k+1} = \hat{A}\hat{x}_k + Bu_k + \hat{B}y_k^a, \tag{5}$$

$$e_k = x_k - \hat{x}_k, \tag{6}$$

such that the error in the state estimate e_k is minimized.

A. Relationship between differential privacy and error in state estimates due to control input and output privacy noise

In this subsection, we show that the differential privacy of the system state can be represented by the error in the estimation of the state while using the optimal state estimator by the adversary of the form eqs. (5) and (6). In particular, the covariance of the state error estimates $E_k = \mathbb{E}[e_k e_k^T]$ can be used as a metric to quantify differential privacy, and an increase in error covariance results in an increase in (ϵ, δ)-differentially privacy.

Lemma 2. *(Gaussian mechanism for dynamical system; [5]): Let $\mathcal{G}$ denote an LTI dynamical system and $\|\mathcal{G}\|_\infty < \infty$ and let us use privacy parameters $\epsilon, \delta > 0$. Then the Gaussian mechanism $\mathcal{M}u = \mathcal{G}u + w^p$, where w^p is a Gaussian noise with $w^p \sim \mathcal{N}\left(0, \sigma^2 I_{n_y}\right)$, and $\sigma \geq \beta\, \kappa\left(\delta, \epsilon\right) \|\mathcal{G}\|_\infty$, makes the system (ϵ, δ)-differentially private with respect to Adj_β in u , i.e., $\|u - u'\|_2 \leq \beta$ with $\beta > 0$.*

Remark 1. *The above lemma allows us to make the control input differential private by directly adding the noise to the control inputs when the output is queried.*

Yazdani et. al. [3] used the level of privacy to calculate the impact on estimation error and showed the relationship between the privacy noise and the trace of covariance of the state error estimates $\mathrm{tr}(E_k)$ where the state estimates are calculated using a Kalman filter. However, another way to look at the impact of differential privacy from the point of view of an adversary is to hinder his capability to estimate the state trajectories accurately. So if an adversary designs an optimal estimator, the error in estimating state trajectories can be used as a metric of differential privacy. Next, we expand on the results generated in [3] to quantify standard (ϵ, δ)-differential privacy as the error in adversary's state estimates due to both control input and output privacy noise.

Lemma 3. *For the given dynamical systems in (Eq. (1)-(3)) with both control input privacy noise $w_k^p \sim \mathcal{N}(\mathbf{0}, W^p)$ and output privacy noise $v_k^p \sim \mathcal{N}(\mathbf{0}, \sigma^2 I_{n_y} - V)$, with $\sigma = \bar{S}(C)\beta k(\delta, \epsilon)$, and for a given adjacency $\|x - x'\|_2 \leq \beta$ with $\beta > 0$, if the states are (ϵ, δ)-differential private with $\delta \in [10^{-5}, 10^{-1}]$ and*

$$\epsilon \leq \left(\frac{\bar{S}(C)^2 \beta^2 (n_x - \mathrm{tr}\left(\underline{E}\right)\underline{\lambda}(\Psi)^{-1})}{\mathrm{tr}(\underline{E}) C_u^2} \right)^{1/2},$$

$$\Psi = DWD^T + BW^pB^T, \quad V^p = \sigma^2 I_{n_y} - V,$$

where $\bar{S}(\cdot)$ represents the maximum singular value, $\underline{\lambda}(\cdot)$ represents the smallest eigenvalue of the matrix, and C_u is the value of C corresponding to the index for which the diagonal element of $C^T(V + V^p)^{-1}C)$ is maximum, then the state error estimate is lower bounded by $\mathrm{tr}(\underline{E})$ with $\mathbb{E}[e_k e_k^T] > \underline{E}$.

Proof. Here we consider both control input privacy noise and output privacy noise along with the already present process and measurement noise. Thus the equation for *a priori* state error covariance follows:

$$\Sigma = A(\Sigma^{-1} + C^T(V + V^p)^{-1}C)^{-1}A^T + DWD^T + BW^pW^T,$$

and for *a posteriori* state error covariance follows:

$$\overline{\Sigma} = (\Sigma^{-1} + C^T(V + V^p)^{-1}C)^{-1}.$$

After that, it follows directly from (Theorem 2 of [3]) where we consider a single agent with state dimension n_x instead of the multi-agent case. □

The above result is used to show that enforcing differential privacy to the systems' state ensures a lower bound on state estimation error. Please note that the above result provides a necessary condition for differential privacy based on the lower bound on state estimation error. More work is needed to find the bounds for sufficiency.

Remark 2. *Please note that both the performance norm $\mathbb{E}[z_k z_k^T]$ and the estimator error covariance $\mathbb{E}[e_k e_k^T]$ increases with an increase in output and control input privacy noises, and our objective is to find the optimum noise level along with the controller and estimator to minimize the performance norm for a given error covariance.*

Main Design Problem Formulation: Design the strength of privacy noises, $W^p(\Gamma_w)$ and $V^p(\Gamma_v)$, and an optimal state estimator of the form eqs. (5) and (6), and a general linear dynamic controller of the form:

$$x_{k+1}^c = A_c\, x_k^c + B_c\, \bar{y}_k, \tag{7}$$

$$u_k = C_c\, x_k^c + D_c\, \bar{y}_k, \tag{8}$$

such that the state error covariance $\mathbb{E}[e_k e_k^T]$ is maximized while closed-loop system performance is bounded $\mathbb{E}[z_k z_k^T] \leq \bar{\mathbf{Z}}$.

$$\begin{array}{ll} \max_{\{A_c, B_c, C_c, D_c, \Gamma_w, \Gamma_v, \hat{A}, \hat{B}\}} & \mathrm{tr}(\mathbb{E}[e_k e_k^T]) \\ s.t. & \mathbb{E}[z_k z_k^T] \leq \bar{\mathbf{Z}}. \end{array} \tag{9}$$

Another problem of interest can be to minimize the closed-loop system performance $\mathbb{E}[z_k z_k^T]$ while lower bounding the state error covariance $\mathbb{E}[e_k e_k^T] > \underline{\mathrm{E}}$ for some given $\underline{\mathrm{E}}$, i.e., to have higher differential privacy than some specified limit.

$$\begin{array}{ll} \min_{\{A_c, B_c, C_c, D_c, \Gamma_w, \Gamma_v, \hat{A}, \hat{B}\}} & \mathrm{tr}(\mathbb{E}[z_k z_k^T]) \\ s.t. & \mathbb{E}[e_k e_k^T] \geq \underline{\mathrm{E}}. \end{array} \tag{10}$$

For the two cases that we discussed based on the capabilities of the adversary, the information available to the estimator would change from (1) $y_k^a = \bar{y}_k$ to (2) $y_k^a = y_k$.

Remark 3. *Notice that the estimator design from the point of view of the adversary is general and can be used to simultaneously design the estimator with the privacy noise for the case of open loop system dynamics also.*

IV. Final Design Solution Development

In this section, we develop frameworks for the co-design of input and output privacy noise with a dynamic feedback controller; and the co-design of input and output privacy noise with an optimal estimator. We further provide the final design algorithm for the two cases of adversarial capabilities. In both cases, we formulate the problem such that the controller gets the output signal with added privacy noise v^p and let the optimization solve the optimal privacy noise.

A. Adversary with access to communication channels

For the case where the adversary listens to the noisy output passed through the communication channel $y_k^a = \bar{y}_k = Cx_k + v_k + v_k^p$, the final design problem can be as:

Theorem 1. *For the dynamical system given in eqs.* (1) *and* (3) *with adversary listening through the communication channel, and to maximize differential privacy for a fixed performance bound, the optimal design solution with privacy noises, $W^p(\Gamma_w)$ and $V^p(\Gamma_v)$, an optimal state estimator of the form eqs.* (5) *and* (6)*, and a general linear dynamic controller of the form eqs.* (7) *and* (8)*, can be solved as a convex optimization problem using the following LMIs:*

$$\textit{minimize}_{\{A_c,B_c,C_c,\Gamma_w,\Gamma_v,\hat{A},\hat{B}\}} \ \operatorname{trace}(\Gamma_w+\Gamma_v),$$

$$\begin{bmatrix} X & I & (\star) & A & D & B & O & O \\ (\cdot)^T & Y & Q & (\bullet) & YD & YB & F & F \\ (\cdot)^T & (\cdot)^T & X & I & O & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & Y & O & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & W^{-1} & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_w & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & V^{-1} & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_v \end{bmatrix} > O, \tag{11}$$

$$\begin{bmatrix} \bar{\mathbf{Z}} & C_zX & C_z \\ (\cdot)^T & X & I \\ (\cdot)^T & (\cdot)^T & Y \end{bmatrix} > O, \tag{12}$$

$$\begin{bmatrix} \hat{X} & I & A\hat{X} & A & D & B & O & O \\ (\cdot)^T & \hat{Y} & \hat{Q} & (\hat{\bullet}) & \hat{Y}D & \hat{Y}B & \hat{F} & \hat{F} \\ (\cdot)^T & (\cdot)^T & \hat{X} & I & O & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & \hat{Y} & O & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & W^{-1} & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_w & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & V^{-1} & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_v \end{bmatrix} > O, \tag{13}$$

$$\begin{bmatrix} \bar{\mathbf{E}} & \hat{X}-\hat{U} & I \\ (\cdot)^T & \hat{X} & I \\ (\cdot)^T & (\cdot)^T & \hat{Y} \end{bmatrix} > O, \tag{14}$$

where $(\star) = AX + BL$, $(\bullet) = YA + FC$, and $(\hat{\bullet}) = \hat{Y}A + \hat{F}C$. Finally, the optimal estimator and dynamic controller can be calculated as:

$$\hat{A} = \hat{S}^{-1}(\hat{Q} - \hat{Y}A\hat{X} - \hat{F}C\hat{X})\hat{U}^{-1}, \tag{15}$$

$$\hat{B} = \hat{S}^{-1}\hat{F}, \tag{16}$$

$$\begin{bmatrix} A_c & B_c \\ C_c & D_c \end{bmatrix} = \begin{bmatrix} S^{-1} & -S^{-1}YB \\ O & I \end{bmatrix} \begin{bmatrix} Q - YAX & F \\ L & O \end{bmatrix} \cdot \begin{bmatrix} U^{-1} & O \\ -CXU^{-1} & I \end{bmatrix}. \tag{17}$$

Proof. Refer to our arxived version for the detailed proof [10]. Using the dynamic controller (eqs. (7) and (8)) with $D_c = O$ for the bounded control input covariance, the closed-loop system dynamics can be written using the augmented state vector $\mathbf{x}^T := \begin{bmatrix} x^T & x^{cT} \end{bmatrix}$ with augmented process noise $\mathbf{w}^T := \begin{bmatrix} w^T & w^{p^T} & v^T & v^{p^T} \end{bmatrix}$ as: $\mathbf{x}_{k+1} = \mathbf{A}\,\mathbf{x}_k + \mathbf{B}\,\mathbf{w}_k$, $z_k = \mathbf{C}\,\mathbf{x}_k$, where $\mathbf{A} = \begin{bmatrix} A & BC_c \\ B_cC & A_c \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} D & B & O & O \\ O & O & B_c & B_c \end{bmatrix}$, $\mathbf{C} = \begin{bmatrix} C_z & O \end{bmatrix}$ and $\mathbf{w}_k \sim \mathcal{N}(\mathbf{0}, \mathbf{W})$,

$$\mathbf{W}^{-1} = \begin{bmatrix} W^{-1} & O & O & O \\ O & \Gamma_w & O & O \\ O & O & V^{-1} & O \\ O & O & O & \Gamma_v \end{bmatrix}. \tag{18}$$

The above closed loop system is stable and a steady-state state covariance matrix ($\mathbf{X} > 0$) exists, if: $\mathbf{AXA}^T + \mathbf{BWB}^T < \mathbf{X}$. Moreover, the performance covariance can be bounded as: $\mathbf{CXC}^T < \bar{\mathbf{Z}}$. We perform standard congruence transformation and change of variables [11], [12] to convert these matrix inequalities to a set of LMIs eqs. (11) and (12). Once the X, Y are obtained by solving eqs. (11) and (12), matrices S and U need to be constructed using: $YX + SU = I$, and a handy choice for which is $S = Y$, then $U = Y^{-1} - X$. Notice that when the controller has the same order as the plant, S and U are square and non-singular matrices, in which case the controller gain matrices can be calculated using eq. (17).

Although the original problem was to maximize the $\mathbb{E}[e_k e_k^T]$ to increase the differential privacy, but an increase in error covariance can also result from suboptimal estimator gains. However, as we consider a smart adversary, who would always design an optimal estimator, we update the design problem to maximize the privacy noises while bounding the error covariance.

Let us design the estimator to bound the error covariance for different states with the estimator dynamics given as: $\hat{x}_{k+1} = \hat{A}\hat{x}_k + Bu_k + \hat{B}y_k^a$. The combined dynamics with estimator can be written using the augmented state vector $\hat{\mathbf{x}}^T := \begin{bmatrix} x^T & \hat{x}^T \end{bmatrix}$ as: $\hat{\mathbf{x}}_{k+1} = \hat{\mathbf{A}}\,\hat{\mathbf{x}}_\mathbf{k} + \hat{\mathbf{B}}\,\mathbf{w}_k$, where $\hat{\mathbf{A}} = \begin{bmatrix} A & O \\ \hat{B}C & \hat{A} \end{bmatrix}$, $\hat{\mathbf{B}} = \begin{bmatrix} D & B & O & O \\ O & O & \hat{B} & \hat{B} \end{bmatrix}$, and the error in estimation can be written as: $\mathbf{e}_k = \hat{\mathbf{C}}\hat{\mathbf{x}}_k$, $\hat{\mathbf{C}} = \begin{bmatrix} I & -I \end{bmatrix}$.

For the existence of the steady-state state covariance matrix ($\hat{\mathbf{X}} > 0$) and stability of the system, we write: $\hat{\mathbf{A}}\hat{\mathbf{X}}\hat{\mathbf{A}}^T + \hat{\mathbf{B}}\mathbf{W}\hat{\mathbf{B}}^T < \hat{\mathbf{X}}$, and for bounding the error covariance, we write: $\bar{\mathbf{E}} > \hat{\mathbf{C}}\hat{\mathbf{X}}\hat{\mathbf{C}}^T$. Now, we follow a similar procedure, by partitioning the state covariance matrix and performing the congruence transformation to obtain the LMIs given in eqs. (13) and (14). Once the $\hat{X}, \hat{Y}, \hat{U}, \hat{F}, \hat{Q}$

are obtained, matrix $\hat{S}$ can be constructed using: $\hat{S} = (I - \hat{Y}\hat{X})\hat{U}^{-1}$, and the estimator matrices can be constructed using eqs. (15) and (16). □

B. Adversary with direct access to measurements

For the case where the adversary uses his own sensors to measure the system output $y_k^a = y_k = Cx_k + v_k$, the output privacy noise will not help in privatizing the system and the final design problem will change as follows.

Theorem 2. *For the dynamical system given in eqs.* (1) *and* (3) *with an adversary using his own sensors to measure the system output, and to maximize differential privacy for a fixed performance bound, the optimal design solution with privacy noises, $W^p(\Gamma_w)$ and $V^p(\Gamma_v)$, an optimal state estimator (eqs.* (5) *and* (6)*), and a general linear dynamic controller (eqs.* (7) *and* (8)*), can be solved as a convex optimization problem using the following LMIs:*

$$\textit{minimize}_{\{A_c,B_c,C_c,\Gamma_w,\Gamma_v,\hat{A},\hat{B}\}} \ \operatorname{trace}(\Gamma_w),$$

$$\mathbb{E}[z_k z_k^T] < \bar{\mathbf{Z}} \rightarrow \textit{(eqs.}\ (11)\ \textit{and}\ (12)\ \textit{(LMIs),}$$

$$\begin{bmatrix} \hat{X} & I & A\hat{X} & A & D & B & O \\ (\cdot)^T & \hat{Y} & \hat{Q} & \hat{Y}A + \hat{F}C & \hat{Y}D & \hat{Y}B & \hat{F} \\ (\cdot)^T & (\cdot)^T & \hat{X} & I & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & \hat{Y} & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & W^{-1} & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_w & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & V^{-1} \end{bmatrix} > O, \tag{19}$$

$$\begin{bmatrix} \bar{\mathbf{E}} & \hat{X} - \hat{U} & I \\ (\cdot)^T & \hat{X} & I \\ (\cdot)^T & (\cdot)^T & \hat{Y} \end{bmatrix} > O, \tag{20}$$

and finally, the optimal estimator and dynamic controller can be calculated as eqs. (15) *and* (16) *and eq.* (17)*.*

Proof. The design solution for the dynamic controller is the same as the previous solution. The proof follows similarly to the previous design solution with $y_k^a = \bar{y}_k$ replaced with $y_k^a = y_k$ and thus the derivation for the equation for the estimator follows naturally from eqs. (13) and (14) to the above-mentioned results. □

C. Estimator for unstable systems

The discrete estimator design approach presented earlier is not valid for unstable systems it requires the system matrix $\hat{\mathbf{A}}$ to be stable for a valid positive definite solution for $\hat{\mathbf{X}} > O$. Thus, we now present the results for unstable system dynamics which restricts the estimator design to:

$$\hat{x}_{k+1} = \hat{A}\hat{x}_k + Bu_k + \hat{B}y_k^a, \text{ where } \hat{A} = A - \hat{B}C,$$

and thus $\hat{B}$ is the only design variable for the estimator. Notice that the control input will cancel out in the estimator as the adversary also has direct access to it. Combining the above estimator and the underlying dynamics given in eqs. (1) and (2), the error dynamics can be written as:

$$e_{k+1} = (A - \hat{B}C)e_k + Dw_k + Bw_k^p - \hat{B}v_k - \hat{B}v_k^p.$$

Now for the unstable dynamical system, the system design problem can be solved using the following results. Notice that the approach can also be used to only design an estimator and input/output privacy noises for the case of an open-loop unstable dynamical process.

Corollary 1. *For the unstable dynamical system given in eqs.* (1) *and* (3) *with an adversary using his own sensors to measure the output, and to maximize differential privacy for a fixed performance bound, the optimal design solution with privacy noises, $W^p(\Gamma_w)$ and $V^p(\Gamma_v)$, an optimal state estimator of the form eqs.* (5) *and* (6)*, and a general linear dynamic controller of the form eqs.* (7) *and* (8)*, can be solved as a convex optimization problem using the following LMIs:*

$$\textit{minimize}_{\{A_c,B_c,C_c,\Gamma_w,\Gamma_v,\hat{B}\}} \ \operatorname{trace}(\Gamma_w + \Gamma_v),$$

$$\mathbb{E}[z_k z_k^T] < \bar{\mathbf{Z}} \rightarrow \textit{(eqs.}\ (11)\ \textit{and}\ (12)\ \textit{(LMIs),}$$

$$\begin{bmatrix} \bar{\mathbf{E}} & I \\ I & \hat{Y} \end{bmatrix} > O, \tag{21}$$

$$\begin{bmatrix} \hat{Y} & \hat{Y}A - \hat{Z}C & \hat{Y}D & \hat{Y}B & \hat{Z} & \hat{Z} \\ (\cdot)^T & \hat{Y} & O & O & O & O \\ (\cdot)^T & (\cdot)^T & W^{-1} & O & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_w & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & V^{-1} & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_v \end{bmatrix} > O, \tag{22}$$

and finally, the dynamic controller can be calculated as eq. (17) *and optimal estimator as: $\hat{B} = \hat{Y}^{-1}\hat{Z}$.*

Proof. The error dynamics is stable and a steady-state error covariance matrix ($E > 0$) is bounded, if:

$$E < \bar{\mathbf{E}}, (A - \hat{B}C)E(A - \hat{B}C)^T + DWD^T + BW^pB^T + \hat{B}V\hat{B}^T + \hat{B}V^p\hat{B}^T < E.$$

We first apply Schur's complement and then define $\hat{Y} = E^{-1}$ and multiply both sides by matrix $[\text{blkdiag}(\hat{Y}, I, I, I)]$ to apply congruence transformation and finally define $\hat{Z} = \hat{Y}\hat{B}$ to obtain the LMIs in $\hat{Y}, \hat{Z}, \Gamma_w$ and Γ_v as eqs. (21) and (22). □

Corollary 2. *Similar to Corollary 1, but with an adversary using his own sensors to measure the system output, the optimal design problem can be solved as a convex optimization problem using the following LMIs:*

$$\textit{minimize}_{\{A_c,B_c,C_c,\Gamma_w,\Gamma_v,\hat{B}\}} \ \operatorname{trace}(\Gamma_w),$$

$$\mathbb{E}[z_k z_k^T] < \bar{\mathbf{Z}} \rightarrow \textit{(eqs.}\ (11)\ \textit{and}\ (12)\ \textit{(LMIs),}$$

$$\begin{bmatrix} \bar{\mathbf{E}} & I \\ I & \hat{Y} \end{bmatrix} > O, \tag{23}$$

$$\begin{bmatrix} \hat{Y} & \hat{Y}A - \hat{Z}C & \hat{Y}D & \hat{Y}B & \hat{Z} \\ (\cdot)^T & \hat{Y} & O & O & O \\ (\cdot)^T & (\cdot)^T & W^{-1} & O & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & \Gamma_w & O \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & (\cdot)^T & V^{-1} \end{bmatrix} > O. \tag{24}$$

and finally, the dynamic controller can be calculated as eq. (17) *and optimal estimator as: $\hat{B} = \hat{Y}^{-1}\hat{Z}$.*

V. Simulation Results

The Load Frequency Control (LFC) system maintains a balanced power distribution across different regions by continuously aligning energy demand with generation. LFC involves the transmission of data from remote areas to a central control center, and back to the power production facilities. This communication process in power grids has well-known privacy concerns and thus becomes the motivation for our example [3], [13]. We illustrate the performance of the proposed architecture on a connected four-area network which is obtained from a network-reduced IEEE New England 39-bus system [14]. We consider a lossless, connected, and network-reduced power system with each generator modeled by the following equation [14]:

$$\begin{aligned}\dot{\theta}_i(t) &= \omega_i(t),\\ M_i\dot{\omega}_i(t) &= -D_i\omega_i(t) - \sum_{j=1}^{n} B_{ij}V_iV_j\sin(\theta_i(t)-\theta_j(t))\\ &\quad + P_{t_i}(t) + w_{p_i}(t),\\ \tau_{t_i}\dot{P}_{t_i}(t) &= -P_{t_i}(t) - R_i^{-1}\omega_i(t) + u_i(t),\end{aligned}$$

where $\theta_i(t)$ is the generator rotor angles w.r.t a synchronously rotating reference axis, $\omega_i(t)$ is the frequency deviation w.r.t a synchronous frequency which is 120π for a 60 Hz system, M_i represents the inertia, D_i represents the damping matrix, w_{p_i} represents the unknown power demand modeled as disturbance, R_i represents the frequency-droop, and $P_{t_i}(t)$ and τ_{t_i} are the turbine power and time constants, respectively [14]. We linearize the generator model and define the state with four-area network system as:

$$\dot{x}(t) = A_cx(t) + B_cu(t) + Dw_p(t),$$

$$x = [\theta_1\ \omega_1\ P_{t_1}\ \theta_2\ \omega_2\ P_{t_2}\ \theta_3\ \omega_3\ P_{t_3}\ \theta_4\ \omega_4\ P_{t_4}]^T,$$

$$u(t) = [u_1(t)\ u_2(t)\ u_3(t)\ u_4(t)]^T,$$

with the parameters for the networked system given in table I. Finally, we discretize the system dynamics with $A = e^{A_c\Delta t}$ and $B = \int_0^{\Delta t} e^{A_c\tau}B_cd\tau$, where Δt is the sampling period.

TABLE I
Network Parameters

Parameters	Area 1	Area 2	Area 3	Area 4
M_i	0.1667	0.2222	0.16	0.1304
D_i	0.0083	0.0088	0.0080	0.0088
R_i	2.4	2.7	2.5	2
τ_t	0.3	0.33	0.35	0.375

The communication graph structure is the same as the physical connection graph (fig. 2), with all the per unit line voltages chosen to be $V_i = V_j = 1$ and line coefficients of the power flow are taken as $B_{12} = B_{21} = B_{13} = B_{31} = B_{23} = B_{32} = B_{14} = B_{41} = 0.545$ p.u. and $B_{24} = B_{42} = B_{34} = B_{43} = 0$ [14]. We assume the measurement model to

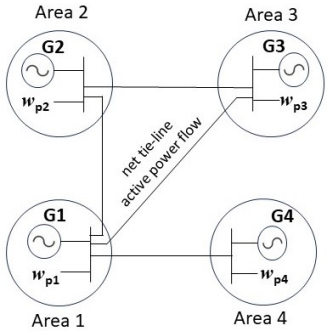

Fig. 2. Interconnected four-area power distribution system

be graph Laplacian:

$$\begin{aligned}y_1 &= (\theta_1-\theta_2)+(\theta_1-\theta_3)+(\theta_1-\theta_4),\\ y_2 &= (\theta_2-\theta_3)+(\theta_2-\theta_1),\\ y_3 &= (\theta_3-\theta_1)+(\theta_3-\theta_2),\\ y_4 &= (\theta_4-\theta_1)+(\theta_4-\theta_{ref}).\end{aligned}$$

The above measurement model implies that each individual area measures the sum of the phase difference between itself and physically connected areas through net tie-line active power flow measurement. We assume that we can measure the absolute phase angle of area 4 by comparing it with known reference $\theta_{ref} = 0$. We bound the deviation in turbine power by choosing the performance variable state as: $z_t = [P_{t_1}\ P_{t_2}\ P_{t_3}\ P_{t_4}]$ and want to obtain the same level of privacy in frequency deviation for each area in the system ω_i.

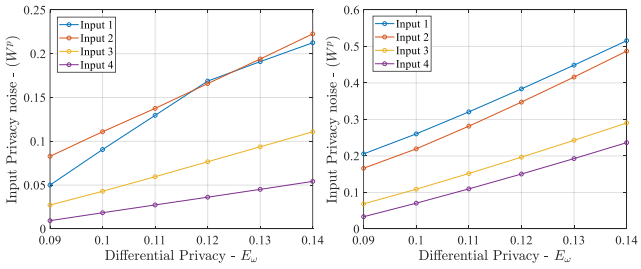

Fig. 3. Optimal input private noise for given values of differential privacy for (L) an adversary with access to communication channels ($y_k^a = \bar{y}_k$), and (R) an adversary with direct access to measurements ($y_k^a = y_k$).

The design problem is to find the optimal privacy noise in control input and output channels and simultaneously design the controller to bound the covariance of the deviation in the turbine power $Z_{P_{t_i}}$ while preserving the privacy of the frequency deviation for each area E_{ω_i}. Figure 3 shows the optimal input privacy noises for each of the control inputs to obtain the same level of privacy for each of E_{ω_i}. Notice that the intensity of the noise required is different in each channel based on the open loop and finally the closed-loop dynamics of each area. Also, the intensity of the noise increases with the level of privacy but there is a change in respective ratios of the noise intensity between different channels showing a non-scaled parameterization of the privacy noise and thus the need for the co-design of the noises and the controller.

Also, notice that the amount of privacy noise required for the second case with ($y_k^a = y_k$) is more than the first case ($y_k^a = \bar{y}_k$) as there is no contribution from the output privacy noise towards the privacy of the system.

Figure 4 shows similar plots for the optimal output privacy noise for two cases that are based on adversarial capabilities. Notice that the amount of privacy signal required to obtain the desired performance bound increases with an increase in desired differential privacy. Moreover, the amount of privacy noise added in the output channel is much higher than the input channels as the output channel directly affects the state estimates and indirectly affects the system performance after passing through the controller dynamics, but the input channel directly affects the system performance and indirectly affects state estimates after passing through the system dynamics. Notice that the amount of noise added in the second case with ($y_k^a = y_k$) is zero as it does not help increase the differential privacy but adversely affects the system performance.

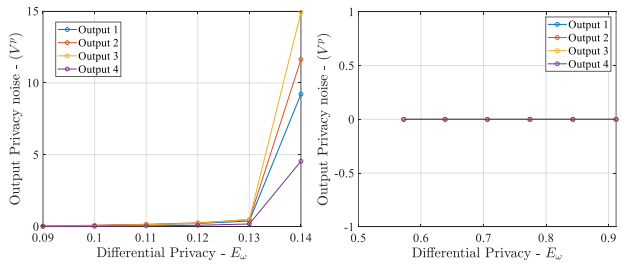

Fig. 4. Optimal output private noise for given values of differential privacy for (L) an adversary with access to communication channels ($y_k^a = \bar{y}_k$), and (R) an adversary with direct access to measurements ($y_k^a = y_k$).

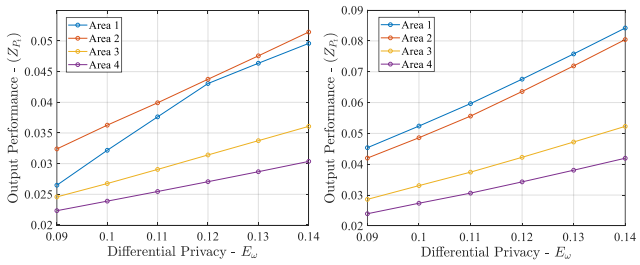

Fig. 5. Optimal system performance norm for given values of differential privacy for (L) an adversary with access to communication channels ($y_k^a = \bar{y}_k$), and (R) an adversary with direct access to measurements ($y_k^a = y_k$).

Finally, fig. 5 shows the plots for the system performance in terms of variance of deviation in turbine power for different areas. Notice that higher differential privacy results in a higher variance in deviation, i.e., an adverse effect on system performance. Notice that we minimized the performance loss for the given privacy level and thus different areas result in different performance levels. Also, the variance in deviation is higher for the second case with a stronger adversary with direct access to the measurement as only input privacy noise is effective in providing privacy which has a worse effect on system performance.

VI. Conclusion

The paper showed that the joint design of differential privacy noise distribution and a general dynamic controller can be posed as a convex optimization problem using the Linear Matrix Inequalities framework. The framework adds privacy noise to both control input and system output to privatize the system's state. The co-design problem also designs an optimal estimator from the perspective of the adversary with access to both communication channels and direct output measurements. The simulation results show the interplay between the controller gains and the privacy noise to obtain the desired level of privacy while minimizing the system performance as a measure of the variance of deviation from reference. The results show the effectiveness of input and output privacy noise based on the capabilities of the adversary and show the need for the co-design of the privacy noises with the controller.

References

[1] C. Dwork, "Differential privacy: A survey of results," in *International conference on theory and applications of models of computation*. Springer, 2008, pp. 1–19.

[2] S. Han and G. J. Pappas, "Privacy in control and dynamical systems," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 309–332, 2018.

[3] K. Yazdani, A. Jones, K. Leahy, and M. Hale, "Differentially private lq control," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 1061–1068, 2022.

[4] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[5] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2013.

[6] C. Hawkins and M. Hale, "Differentially private formation control: Privacy and network co-design," *arXiv preprint arXiv:2205.13406*, 2022.

[7] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2016.

[8] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3863–3878, 2020.

[9] Y. Kawano and M. Cao, "Differential privacy and qualitative privacy analysis for nonlinear dynamical systems," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 52–57, 2018.

[10] R. Goyal, D. Chowdhury, and S. Rane, "System design approach for control of differentially private dynamical systems," *arXiv preprint cs.SY, arXiv:2403.08065*, 2024.

[11] C. Scherer, P. Gahinet, and M. Chilali, "Multiobjective output-feedback control via lmi optimization," *IEEE Transactions on Automatic Control*, vol. 42, no. 7, pp. 896–911, 1997.

[12] R. Goyal, M. Majji, and R. E. Skelton, "Integrating structure, information architecture and control design: Application to tensegrity systems," *Mechanical Systems and Signal Processing*, vol. 161, p. 107913, 2021.

[13] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[14] H. Bevrani, *Robust power system frequency control*. Springer, 2014, vol. 4.