2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Privacy Analysis for Quantized Networked Control Systems

Le Liu, Yu Kawano, Ming Cao

Abstract— **Quantized signals are widely used in engineering applications. Although quantization can potentially degrade system performances, previous research has demonstrated its usage to preserve privacy of the signals that are quantized. In this paper, we investigate the privacy-preserving properties of two types of quantizers: deterministic and stochastic ones. Specifically, for deterministic quantizers, we demonstrate that an eavesdropper cannot uniquely determine the initial state of a system if the system is Schur stable. Additionally, we propose a necessary condition on the system matrix A to ensure the initial state remains private. For stochastic quantizers, we investigate their differential privacy properties and show that appropriate quantization steps can guarantee differential privacy. However, the quantization step can lead to impreciseness of the quantized signal and we therefore also examine the trade-off between differential privacy and system performance. To optimize the quantization step, we formulate a convex optimization problem, which can be solved efficiently.**

I. Introduction

Data sharing is a fundamental feature of the Internet of Things (IoT), which greatly enhances the efficiency of modern industry. However, this can create risks of private information leakage; for example, Google Maps can be used to monitor its user's motion [1]. To address such concerns, various mechanisms have been proposed to preserve users' privacy [2]–[5]. In the realm of systems and control, researchers typically focus on the privacy of the states of a system of interest [6], [7]. In many engineering applications, measurements are quantized before transmission due to communication capacity constraints, and then sent to a remote fusion center for signal processing and decision-making. As communication channels can be vulnerable to unintended third-party inquiry, eavesdroppers may be able to infer system states from the sensor outputs; in this context, quantization mechanisms have been shown to be effective in preserving the privacy of states [8], [9].

In this paper, we investigate the relationship between quantization mechanisms and privacy, specifically focusing on initial state privacy, which is a common concern in the control community [10]–[12]. The authors of [10] propose a dynamic output mask approach to maintain the privacy of the initial state, while in [11], a state decomposition method is used to preserve the initial state privacy of each agent. A coarser quantizer is more likely to preserve the initial state privacy, as it provides a higher level of privacy protection. However, using a coarser quantizer may also have a negative impact on system performances. Therefore, it is crucial to consider the trade-off between privacy and system performance.

The objective of this manuscript is to explore the relationship between initial state privacy and quantization mechanisms. Specifically, we investigate the privacy of the initial state in an autonomous system equipped with deterministic quantizers. Due to quantization, the initial state of the system is subject to linear inequality constraints, and the volume of the resulting set can be used to measure the privacy level. We begin by presenting an example that shows how a larger quantization step may not always result in higher privacy. Subsequently, we prove that the initial state is private when the spectrum of the system matrix is less than 1, and we provide a necessary condition which states the initial state can be private only if the system matrix's spectrum is less than or equal to 1. Moreover, for the case where the spectrum of the system matrix is equal to 1, we provide two examples that demonstrate that the initial state's privacy preservation cannot be determined by the spectrum.

In addition to the privacy properties of deterministic quantizers, we also investigate the differential privacy properties of stochastic quantizers. It is shown that the $(0, r)$ differential privacy for a finite time t can be guaranteed via choosing an appropriate quantization step. Moreover, we show that under mild conditions, the $(0, r)$ differential privacy with infinite time steps can also be achieved if the quantization step is chosen according to system matrices and r.

To illustrate the trade-off between quantization steps and system performance, we start by designing a Luenberger observer to estimate the system state. Then, we design an output tracking controller and analyze the tracking error. By computing the upper bound of the tracking error covariance, we establish a direct correlation between the covariance and the quantization step. To optimize this trade-off, we formulate a convex optimization problem to find the optimal quantization step d that balances the system tracking performance and the privacy of the initial state.

The remainder of this paper is given as follows. In Section II, we formulate the system models and give the definitions of differential privacy. In Section III, we consider a deterministic quantizer and give a sufficient condition to keep the initial state private. A necessary condition is also provided to analyze the initial state privacy. Furthermore, the differential

The work of Liu and Cao was supported in part by the European Research Council (ERC-CoG-771687). The work of Yu Kawano was supported in part by JSPS KAKENHI Grant Number JP22KK0155.

Le Liu and Ming Cao are with the Faculty of Science and Engineering, Univerisity of Groningen, 9747 AG Groningen, The Netherlands {le.liu, m.cao}@rug.nl

Yu Kawano is with the Graduate School of Advance Science and Engineering, Hiroshima Univeristy, Higashi-hiroshima 739-8527, Japan ykawano@hiroshima-u.ac.ip

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

privacy properties of stochastic quantizers are investigated. We give an explicit connection between differential privacy and the quantization step over finite time and infinite time. In Section IV, we analyze the output tracking problem when the system is equipped with the stochastic quantizer. Specifically, we show the trade-off between the privacy and the system performance. Section V provides a numerical example, which shows the validity of the proposed stochastic quantizers. Finally, Section VI concludes the paper.

Notation: We denote the sets of real numbers and non-negative integer as $\mathbb{R}$ and $\mathbb{Z}_+$, respectively. $\mathbb{1}$ represents the vector with 1 in each coordinate. For two vectors a and b with the same size, $a \preceq b$ ($a \prec b$) stands for the element-wise inequality, i.e., $a_i \leq b_i$ ($a_i < b_i$) for all elements. $\Gamma(\cdot)$ is the Gamma function, i.e., $\Gamma(z) \equiv \int_0^\infty t^{-1}e^{-t}dt$. $\lambda_{\max}(X)$ and $\lambda_{\min}(X)$ represent the largest and smallest eigenvalue for a positive semi-definite matrix X. $\rho(X)$ is the spectrum of a matrix X.

II. Background and Problem Formulation

In this section, we introduce the system model and the definitions about differential privacy. For simplicity, we consider a discrete-time, linear, time invariant model, which is commonly discussed in papers considering the privacy issues, e.g., [7], [6] and [13]. Let $x_0 \in \mathbb{R}^{n_1}$ be a variable that the system wants to keep private. The model is given as follows:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k), x(0) = x_0 && \text{(1a)} \\ y(k) &= Cx(k), && \text{(1b)} \\ y_p(k) &= H_p x(k), && \text{(1c)} \end{aligned}$$

and the estimator system is given by:

$$\begin{aligned} \hat{x}(k+1) &= A\hat{x}(k) + Bu(k) \\ &\quad + L\Big(C\hat{x}(k) - v(k)\Big), \quad \hat{x}(0) = \hat{x}_0, && (2) \\ u(k) &= K_x\hat{x}(k) + K_r x_r(k), && (3) \end{aligned}$$

where $x \in \mathbb{R}^{n_1}$, $\hat{x} \in \mathbb{R}^{n_1}$ are states and estimates respectively, $u \in \mathbb{R}^m, x_r \in \mathbb{R}^{n_2}$ are control inputs and reference signals respectively, $y \in \mathbb{R}^p$ is the measured output, and $y_p \in \mathbb{R}^q$ is the tracking output. The matrix dimensions are compatible. Instead of assuming that the systems can communicate with each other perfectly, we consider the sensors can only transmit quantized signals, i.e.,

$$v = \mathcal{Q}_v(y) \tag{4}$$

where $\mathcal{Q}_v$ is the chosen quantizer subject to communication capacity constraints and privacy requirements. For the control input, we assume the fusion center have enough energy to transmit accurate $u(k)$ (One can also consider the case where $u(k)$ is quantized and the results will be similar to those in this paper). In this paper, we will consider the system is eavesdropped by an eavesdropper. The corresponding diagram is shown in Figure 1. In what follows, we assume the eavesdropper has full information about the system model and has the ability to eavesdrop control inputs, i.e., A, B, C, L, K_x, K_r and $u(k)$. Furthermore, the eavesdropper has the ability to eavesdrop the quantized measurements $v(k)$. We would like to protect the initial state x_0 with the quantizers in the sensors. It should be noted that we discuss two different types of privacy notions in this paper, the volume of possible initial states and the differential privacy.

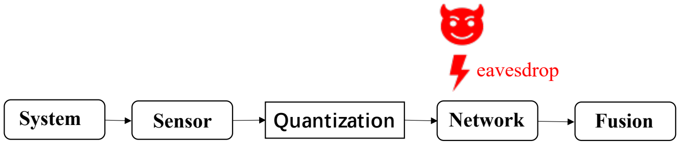

Fig. 1. The Diagram of Quantized Communications and an Eavesdropper

Let us define

$$O_t := \begin{bmatrix} C^\top & (CA)^\top & \cdots & (CA^t)^\top \end{bmatrix}^\top,$$

$$N_t := \begin{bmatrix} 0 & 0 & \cdots & \cdots & 0 \\ CB & 0 & \ddots & & \vdots \\ CAB & CB & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ CA^{t-1}B & CA^{t-2}B & \cdots & CB & 0 \end{bmatrix}.$$

These two matrices are useful to introduce the following definitions of differential privacy.

Definition 2.1: Given $\zeta > 0$, a pair of initial states $(x_0, x_0') \in \mathbb{R}^{n_1} \times \mathbb{R}^{n_1}$ is said to belong to the binary relation ζ-adjacency if $||x_0 - x_0'||_1 \leq \zeta$. The set of all pairs of the initial states that are ζ-adjacent under the 1-norm is denoted by Adj_1^ζ. ◁

Definition 2.2: Let $\left(\mathbb{R}^{(t+1)p}, \mathcal{F}, \mathbb{P}\right)$ be a probability space. The mechanism (1) and (4) is said to be (ε, δ)-differentially private for Adj_1^ζ at a finite time instant $t \in \mathbb{Z}_+$if there exist $\varepsilon > 0$ and $\delta \geq 0$ such that

$$\begin{aligned} &\mathbb{P}\left(\mathcal{Q}_v(O_t x_0 + N_t U_t) \in \mathcal{S}\right) \\ &\quad \leq \mathrm{e}^{\varepsilon}\mathbb{P}\left(\mathcal{Q}_v(O_t x_0' + N_t U_t) \in \mathcal{S}\right) + \delta, \forall \mathcal{S} \in \mathcal{F} \end{aligned}$$

for any $(x_0, x_0') \in \mathrm{Adj}_1^\zeta$. ◁

Roughly speaking, the definitions above show that the probability of getting the same output sequence is larger when the distance between two different initial states, i.e., x_0 and x_0' is smaller. One can find that the privacy increases in the sense that distinguishing the initial state from the output sequence is harder. Therefore, for smaller constants ϵ and δ, the system will be more private.

The above definitions are important in stochastic quantizers. As for deterministic quantizers, we will introduce a new privacy definition in the next section. Moreover, as it can be seen in the next section, the system is more private when a stochastic quantizer is coarser. Accordingly, the tracking control performance for the system is worse. Therefore, there should be a trade-off between the tracking control performance and the privacy. Such a trade-off is discussed in Section IV.

III. Main Results

A. Deterministic Quantizer and Privacy Analysis

In this section, we will discuss some privacy properties in autonomous systems with deterministic quantizers. Suppose the quantizer is given by

$$\mathcal{Q}_v(z+nd)=nd \quad \text{for} \quad z\in\left(-\frac{d}{2},\frac{d}{2}\right], \quad n\in\mathbb{Z}, \quad d>0, \tag{5}$$

where d is the quantization step. The system model is given by the following equations.

$$\begin{cases} x(k+1)=Ax(k), x(0)=x_0, \\ v(t)=\mathcal{Q}_v(Cx(t)). \end{cases} \tag{6}$$

We define

$$v_t=\begin{bmatrix} v(0) \\ v(1) \\ \vdots \\ v(t) \end{bmatrix}.$$

Then, it is trivial to see from the definition that if v_t is observed, the initial state x_0 is in the following set:

$$S_t(v_t):=\left\{x_0\in\mathbb{R}^n : -\frac{d}{2}\mathbb{1}\prec O_t x_0-v_t\preceq\frac{d}{2}\mathbb{1}\right\}, \tag{7}$$

It should be noticed that when the system is not observable, an eavesdropper cannot determine the exact value of x_0 even if the quantization step is arbitrarily small. Therefore, in the following part, we will assume the system is observable.

Consider the state space of x_0 is equipped with Lebesgue measure. Let $\mu(S_t)$ denote the Lebesgue measure of $S_t(v_t)$. Then, it is intuitive to give the following privacy definition with deterministic quantizers.

Definition 3.1: The system (6) equipped with deterministic quantizers (5) is said to be *private* at time t if $\mu(S_t)>0$. $\triangleleft$

It is worth pointing out that there are infinitely many possible initial states in S_t if $\mu(S_t)>0$. Furthermore, it should be noticed that $\mu(S_t)$ is a decreasing sequence of t. Therefore, the initial state is private for any time index t if the volume of $\lim_{t\to\infty}\mu(S_t)>0$.

Intuitively, one may consider the initial state will be more private with a larger d. However, this intuition is wrong as illustrated by the following example.

Example 3.2: Suppose the system is specified by the following parameters:

$$A=1, C=\begin{bmatrix}1 & 0.6\end{bmatrix}^\top, d=1+\epsilon, x_0=\frac{3}{2}+\delta,$$

where $\delta>0$ is a sufficiently small number and $\epsilon\geq 0$. Obviously, this system is observable. First we consider the case where $\epsilon=0$. One can obtain $v(t)=v(0)=\begin{bmatrix}2 & 1\end{bmatrix}^\top, \forall t$ and

$$S_t(V_t)=\left\{x_0\in\mathbb{R} : \frac{5}{2}\geq x_0>\frac{3}{2}\right\}.$$

It follows that

$$\mu(S_t)=1.$$

Then, we consider the case where $\epsilon=\delta$. In this case, $v(t)=v(0)=\begin{bmatrix}2+\delta & 1+\delta\end{bmatrix}^\top, \forall t$ and

$$S_t(V_t)=\{x_0\in\mathbb{R} : \frac{3(1+\delta)}{2}\geq x_0>\frac{5(1+\delta)}{6}\}.$$

One can also calculate that

$$\mu(S_t)=\frac{2(1+\delta)}{3}.$$

Therefore, the system is even less private with $d=1+\delta$ if $\delta<\frac{1}{2}$. $\triangleleft$

From the example, it can be concluded that a larger d does not always guarantee more privacy. Therefore, it is hard to find the relationship between d and $\mu(S_t)$ for abitrary x_0. However, privacy under Definition 3.1 can be preserved with deterministic quantizers under mild conditions.

The following theorem provides some connections between privacy and the spectral radius of the system matrix A.

Theorem 3.3: Suppose (A,C) is observable. Then, the initial state is private at any time step t if $\rho(A)<1$. Moreover, the initial state is private at any time step t only if $\rho(A)\leq 1$.

Proof: The proof will in the full version of this paper. ■

We have shown that deterministic quantized output can preserve the initial state in the sense that the eavesdropper cannot deduce the initial state after eavesdropping the outputs. In the next section, we will discuss the differential privacy property when the sensors are equipped with stochastic quantizers.

B. Stochastic Quantizer and Privacy Analysis

In this section, we consider the differential privacy property of the system (1a) and (1b) with the stochastic quantizer $\mathcal{Q}_v$ (function on each element of a vector) designed as

$$\begin{aligned}&\mathcal{Q}_v(z+nd)\\ &=\begin{cases} nd, \text{with Prob. } 1-\frac{z}{d} \\ (n+1)d, \text{with Prob. } \frac{z}{d} \end{cases} \text{for } z\in(0,d], n\in\mathbb{Z}, d>0.\end{aligned} \tag{8}$$

It is worth pointing out that the quantization step d is the parameter to be designed. Considering the notion of the differential privacy, we have the following theorem:

Theorem 3.4: For a fixed time step t and a given $r\in(0,1)$,$(0,r)$ differential privacy for Adj_1^ζ can be achieved if the quantizer $\mathcal{Q}_v$ in the form of (8) chooses the quantization step $d\geq\frac{||O_t||_1\zeta}{r}$.

Proof: The proof is reported in Appendix I. ■

The above theorem investigates the differential privacy property for a finite time instant t. As for the infinite time case, we have the following theorem :

Theorem 3.5: Suppose the system matrix A is Schur stable. Let $||O_\infty||_1$ denote $\lim_{t\to\infty}||O_t||_1$. Then, for all $t\geq 0$, $(0,r)$ differential privacy for Adj_1^ζ can be achieved if the quantizer $\mathcal{Q}_v$ in the form of (8) chooses the quantization step $d\geq\frac{||O_\infty||_1\zeta}{r}$.

Proof: The proof is directly from Theorem 3.4. ■

IV. Trade-off Between System Performance and Privacy

In this section, we consider an output tracking control problem and analyze the trade-off between the privacy and the tracking error. The reference model is given by the following equation [14].

$$x_r(k+1) = A_r x_r(k), \tag{9a}$$

$$y_r(k) = H_r x_r(k) \tag{9b}$$

where $x_r \in \mathbb{R}^{n_2}$ is the reference signal and $y_r \in \mathbb{R}^q$. $A_r \in \mathbb{R}^{n_2 \times n_2}, H_r \in \mathbb{R}^{q \times n_2}$ are the corresponding matrices. Let $\xi(k) = y_p(k) - y_r(k)$. The control objective can be written as $\lim_{k\to\infty} \xi(k) = 0$.

To establish the reference model tracking control, we have the following standard assumptions [14].

Assumption 4.1: A_r has no eigenvalues with modulus smaller than 1. ◁

Assumption 4.2: The pair (A, B) is stabilizable. ◁

Assumption 4.3: The pair (C, A) is detectable. ◁

Assumption 4.4: The following two equations:

$$\begin{aligned} XA_r &= AX + BU, \\ 0 &= H_p X - H_r \end{aligned}$$

have a pair of solutions $X \in \mathbb{R}^{n_1 \times n_2}$ and $U \in \mathbb{R}^{m \times n_2}$. ◁

We evaluate the tracking error by the following control performance index:

$$J = \lim_{T\to\infty} \sum_{k=0}^{T} \frac{1}{T} \mathbb{E}[\xi(k)^\top Q \xi(k)], \tag{10}$$

where $Q \in \mathbb{R}^{n \times n}$ is a given matrix. Its upper bound is obtained as follows.

Theorem 4.5: Suppose Assumptions 4.1-.4.4 hold, K_x is designed such that $A + BK_x$ is asymptotically stable, $K_r = U - K_x X$ and L is designed according to Lemma 2.2. Then, the performance index J in (10) is upper bounded, i.e.,

$$J \le \frac{pd^2\gamma^2}{4} \operatorname{trace}(H_p^\top Q H_p \mathcal{X}),$$

where $(A + BK_x)\mathcal{X}(A + BK_x)^\top + BK_x K_x^\top B^\top = \mathcal{X}$.

Proof: The proof is in Appendix II. ■

Let $\beta > 0$ denote the weight parameter between the privacy index r and system tracking performance index J. Using the bounds, one can obtain the following optimization problem if A is Schur stable, which also shows the trade-off between privacy and the system performance.

Optimization problem 1

$$\begin{aligned} \min_{d} \quad & \frac{p^2 d^2 \gamma^2}{4} \operatorname{trace}(H_p^\top Q H_p \mathcal{X}) + \beta \frac{||O_\infty||_1 \zeta}{d} \\ \text{subject to} \quad & d > 0. \end{aligned} \tag{11}$$

One can check that this is a convex optimization problem and hence can be solved efficiently.

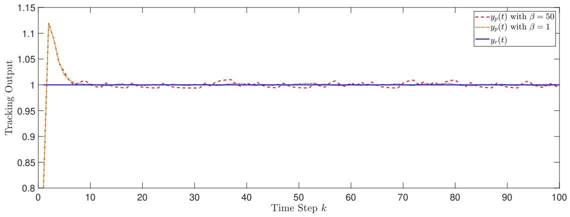

Fig. 2. The Tracking Outputs of the System

V. Simulation

In this section, we give a simulation to show the efficiency of the stochastic quantizers. The system parameters are given as below:

$$A = \begin{bmatrix} 0.2 & 1 \\ 0 & 0.4 \end{bmatrix}, B = \begin{bmatrix} 1 \\ 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \gamma = 1,$$

$$H_p = \begin{bmatrix} 0 & 1 \end{bmatrix}, A_r = 1, H_r = 1, x_r \equiv 1, Q = 1$$

and

$$K_x = \begin{bmatrix} 0 & -0.2 \end{bmatrix}.$$

One can compute that $L = \begin{bmatrix} -0.1503 \\ -0.0087 \end{bmatrix}$ and $K_r = U - K_x X = 0.8$. One can also obtain $||O_\infty||_1 = 3.7500$. If we wish to protect privacy with parameters $\zeta = 0.1, r = 0.1, \beta_1 = 1, \beta_2 = 50$, solving Optimization Problem 1 gives $d_1^* = 1.4620, d_2^* = 5.3602$ respectively. Assume $x_0 = \begin{bmatrix} 0 \\ 0.8 \end{bmatrix}$ and $\hat{x}_0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$. The system tracking outputs are given in Figure 2.

From Figure 2, it can be concluded that the tracking outputs are very close to the reference signal. Moreover, it can be observed that tracking performance is worse with a larger β, which shows the trade-off between the privacy and the system performance.

VI. Conclusions

This paper aims to investigate the privacy properties of networked control systems equipped with quantizers and analyze the trade-off between privacy and system performance. We first analyze the privacy of the system with deterministic quantizers and establish that the system is private when it is Schur stable. We also provide a necessary condition based on the spectrum of the system matrix to study the privacy of the initial state. Additionally, we investigate the differential privacy properties of stochastic quantizers and demonstrate that differential privacy can be guaranteed with a well-designed quantization step. To further study the trade-off between privacy and system performance, we design an output tracking controller and compute the upper bound of the tracking error covariance. As for the design of the quantization step, we propose an optimization problem to balance the trade-off. The optimization problem is convex and can be solved efficiently.

Appendix I
Proof of Theorem 3.4

It should be noticed that since the control inputs can be eavesdropped, U_t is the same for different initial states from the viewpoint of the eavesdropper. Let $y_t = O_t x_0 + N_t U_t$, $y'_t = O_t x'_0 + N_t U_t$, $v_t = \mathcal{Q}_v(y_t)$ and $v'_t = \mathcal{Q}_v(y'_t)$. Then, we have

Lemma 1.1: If $s \leq ||O_t||_1 \zeta$, we have $\sup_{\|y_{t,1}-y'_{t,1}\|_1 \leq s} \left|\mathbb{P}\left(v_{t,1} \in \mathcal{S}_1 \mid y_{t,1}\right) - \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid y'_{t,1}\right)\right| \leq \frac{s}{d}$.

Proof: The proof will be in the full version of this paper. ■

Next, we prove Theorem 3.4.

Proof of Theorem 3.4: It can be firstly observed that

$$||y_t - y'_t||_1 = ||O_t x_0 - O_t x'_0||_1 \leq ||O_t||_1 \zeta \leq d.$$

This means that each coordinate differs at most one quantization level.

Suppose the stochastic quantizer output set from time 0 to time $t-1$ is given by $\mathcal{S}$ and $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_{tp}$. Since $\mathbb{P}\left(v_t \in \mathcal{S}\right)$ is uniquely determined by x_0 and U_t, we have

$$\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) = \prod_{i=1}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right),$$

where $v_{t,i}$ is the ith element of v_t. Based on the mechanism of the stochastic quantizer (8), it can be obtained that

$$\begin{aligned}
&\sup_{\|x_0-x'_0\|_1 \leq \zeta} \left|\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) - \mathbb{P}\left(v'_t \in \mathcal{S} \mid x'_0\right)\right| \\
\leq &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left|\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) - \mathbb{P}\left(v'_t \in \mathcal{S} \mid x'_0\right)\right| \\
= &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left| \prod_{i=1}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \right. \\
&\left. - \prod_{i=1}^{tp} \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right| \\
= &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left| \mathbb{P}\left(v_{t,1} \in \mathcal{S}_1 \mid x_0\right) \prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \right. \\
&\left. - \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \prod_{i=2}^{tp} \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right| \\
= &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left| \left(\mathbb{P}\left(v_{t,1} \in \mathcal{S}_1 \mid x_0\right) - \right. \right. \\
&\left. \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \right) \prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) + \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \\
&\left. \times \left(\prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) - \prod_{i=2}^{tp} \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right) \right|
\end{aligned}$$

By the property of the absolute value, we have

$$\begin{aligned}
&\sup_{\|x_0-x'_0\|_1 \leq \zeta} \left|\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) - \mathbb{P}\left(v'_t \in \mathcal{S} \mid x'_0\right)\right| \\
\leq &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left| \left(\mathbb{P}\left(v_{t,1} \in \mathcal{S}_1 \mid x_0\right) - \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \right) \right. \\
&\left. \times \prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \right| + \left| \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \right. \\
&\left. \times \left(\prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) - \prod_{i=2}^{tp} \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right) \right|,
\end{aligned}$$

Since $\prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \leq 1$ and $\mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \leq 1$, it follows that

$$\begin{aligned}
&\sup_{\|x_t-x'_t\|_1 \leq \zeta} \left|\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) - \mathbb{P}\left(v'_t \in \mathcal{S} \mid x'_0\right)\right| \\
\leq &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \left| \mathbb{P}\left(v_{t,1} \in \mathcal{S}_1 \mid x_0\right) - \mathbb{P}\left(v'_{t,1} \in \mathcal{S}_1 \mid x'_0\right) \right| \\
&+ \left| \prod_{i=2}^{tp} \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) - \prod_{i=2}^{tp} \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right|.
\end{aligned}$$

With a similar process as before, one can obtain

$$\begin{aligned}
&\sup_{\|x_t-x'_t\|_1 \leq \zeta} \left|\mathbb{P}\left(v_t \in \mathcal{S} \mid x_0\right) - \mathbb{P}\left(v'_t \in \mathcal{S} \mid x'_0\right)\right| \\
\leq &\sup_{\|y_t-y'_t\|_1 \leq ||O_t||_1\zeta} \sum_{i=1}^{tp} \left| \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \right. \\
&\left. - \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right| \\
= &\sup_{\sum_{i=1}^{tp} c_i \leq ||O_t||_1\zeta} \sum_{i=1}^{tp} \sup_{|y_{t,i}-y'_{t,i}| \leq c_i} \left| \mathbb{P}\left(v_{t,i} \in \mathcal{S}_i \mid x_0\right) \right. \\
&\left. - \mathbb{P}\left(v'_{t,i} \in \mathcal{S}_i \mid x'_0\right) \right| \\
\leq &r.
\end{aligned}$$

The last inequality follows from Lemma 1.1. ■

Appendix II
Proof of Theorem 4.5

First, we have the following lemma which characterizing the property of $w_v(k) := \mathcal{Q}_v(y(k)) - y(k)$, which is a vector version of Proposition 1 in [15].

Lemma 2.1: For the stochastic quantizer Q_v defined in (8), we have

(i)$\mathbb{E}[w_v(k)] = 0$

(ii)$\mathbb{E}[w_v(k)w_v(k)^\top] \leq \frac{pd^2}{4} I$

(iii)

$$\mathbb{E}[w_v(k_1)w_v(k_2)^\top] = \begin{cases} 0, & k_1 \neq k_2, \\ \mathbb{E}[w_v(k_1)w_v(k_1)^\top], & k_1 = k_2. \end{cases}$$

Proof: The proof will be in the full version of this paper. ■

Let $e(k) = \hat{x}(k) - x(k)$. The system dynamics in the estimator can be written as

$$e(k+1) = (A + LC)e(k) - Lw_v(k). \tag{12}$$

Since $\mathbb{E}[w_v(k)] = 0$, one can immediately see that

$$||\mathbb{E}[e(k+1)]|| \leq ||(A+LC)\mathbb{E}[e(k)]||.$$

This shows that if $A+LC$ is Schur stable, the expectation of the state will converge to the origin. Compared to the deterministic quantizers that may have a periodic behavior [16], the stochastic quantizers have the potential to increase the system performance. Moreover, we can consider the quantization error as a bounded noise here. It is desirable to design estimator gain L here to satisfy the H_∞-norm performance, which is given by the following proposition.

Lemma 2.2: The H_∞-norm from the quantization error $w_v(k)$ to the state $e(k)$ is not greater than $\gamma > 0$ if the following LMI has solutions P and Y.

$$\begin{bmatrix} P & 0 & (PA+YC)^\top & I \\ 0 & \gamma^2 I & Y^\top & 0 \\ PA+YC & Y & P & 0 \\ I & 0 & 0 & I \end{bmatrix} \succ 0.$$

Moreover, the estimator gain L is given by $L := P^{-1}Y$

Proof: This is a simple application of bounded real lemma [17] and hence the proof is omitted here. ■

The next lemma evaluates the performance of the proposed estimator.

Lemma 2.3: Consider the system with quantized error. Suppose $A+LC$ is Schur stable, and the estimator H_∞-norm is not greater than γ. Then, it follows that

$$\lim_{k\to\infty} \mathbb{E}[(e(k)^\top e(k)] \leq \frac{p^2 d^2 \gamma^2}{4}. \tag{13}$$

Proof: The proof will be in the full version of this paper. ■

Now, we are ready to provide the proof of Theorem 4.5.

Proof of Theorem 4.5: Let $\bar{x}(k) = x(k) - Xx_r(k)$. One can check that

$$\bar{x}(k+1) = (A+BK_x)\bar{x}(k) + BK_x e(k)$$

and

$$\xi(k) = H_p\bar{x}(k) + (H_pX - H_r)x_r(k) = H_p\bar{x}(k).$$

Let $\tilde{A} = A + BK_x$. Since $\tilde{A}$ is Schur stable, we can assume $\bar{x}(0) = 0$ without loss of generality. $\xi(T+1)$ can be rewritten as

$$\xi(T+1) = H_p \sum_{k=0}^{T} \tilde{A}^{T-k+1} BK_x e(k). \tag{14}$$

Then, it follows that

$$\begin{aligned} &\mathbb{E}[(\xi(T+1)^\top Q\xi(T+1)] \\ =&\mathbb{E}[\mathrm{trace}(H_p^\top QH_p \sum_{k=0}^{T} \tilde{A}^{T-k+1}BK_x e(k) \\ &\times e(k)^\top K_x^\top B^\top (\tilde{A}^{T-k+1})^\top)] \\ \leq& \frac{pd^2\gamma^2}{4}\,\mathrm{trace}(H_p^\top QH_p \sum_{k=0}^{T} \tilde{A}^{T-k+1}BK_xK_x^\top B^\top (\tilde{A}^{T-k+1})^\top) \end{aligned}$$

Then, taking the limit will give the result, i.e.,

$$\lim_{T\to\infty} \mathbb{E}[(\xi(T+1)^\top Q\xi(T+1)] \leq \frac{pd^2\gamma^2}{4}\,\mathrm{trace}(H_p^\top QH_p\mathcal{X}).$$

This ends the proof. ■

References

[1] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, "Defending against sybil devices in crowdsourced mapping services," in *Proceedings of the 14th annual international conference on mobile systems, applications, and services*, pp. 179–191, 2016.

[2] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *2016 IEEE 55th Conference on Decision and Control*, pp. 4252–4272, 2016.

[3] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[4] K. Chaudhuri and C. Monteleoni, "Privacy-preserving logistic regression," *Advances in neural information processing systems*, vol. 21, 2008.

[5] Y. Wang and T. Başar, "Quantization enabled privacy protection in decentralized stochastic optimization," *IEEE Transactions on Automatic Control*, 2022.

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

[7] Y. Kawano, K. Kashima, and M. Cao, "Modular control under privacy protection: Fundamental trade-offs," *Automatica*, vol. 127, p. 109518, 2021.

[8] C. Murguia, I. Shames, F. Farokhi, and D. Nešić, "On privacy of quantized sensor measurements through additive noise," in *2018 IEEE Conference on Decision and Control*, pp. 2531–2536, IEEE, 2018.

[9] Y. Kawano and M. Cao, "Effects of quantization and dithering in privacy analysis for a networked control system," in *2021 60th IEEE Conference on Decision and Control*, pp. 2758–2763, 2021.

[10] C. Altafini, "A dynamical approach to privacy preserving average consensus," in *2019 IEEE 58th Conference on decision and control*, pp. 4501–4506, IEEE, 2019.

[11] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4711–4716, 2019.

[12] L. Wang, I. R. Manchester, J. Trumpf, and G. Shi, "Differential initial-value privacy and observability of linear dynamical systems," *Automatica*, vol. 148, p. 110722, 2023.

[13] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, 2017.

[14] J. Huang, *Nonlinear output regulation: theory and applications*. SIAM, 2004.

[15] K. Kashima and D. Inoue, "Stationary performance evaluation of control systems with random dither quantization," in *2014 European Control Conference*, pp. 1625–1630, 2014.

[16] F. Ferrante, F. Gouaisbaut, and S. Tarbouriech, "Stabilization of continuous-time linear systems subject to input quantization," *Automatica*, vol. 58, pp. 167–172, 2015.

[17] R. E. Skelton, T. Iwasaki, and D. E. Grigoriadis, *A unified algebraic approach to control design*. CRC Press, 1997.