

Privacy Preservation by Intermittent Transmission in Cooperative LQG Control Systems

Wenhao Lin^{*}, Yuqing Ni[†], Wen Yang^{*}, and Chao Yang^{*}

Abstract—In this paper, we study a cooperative linear quadratic Gaussian (LQG) control system with a single user and a server. In this system, the user runs a process and employs the server to meet the needs of computation. However, the user regards its state trajectories as privacy. Therefore, we propose a privacy scheme, in which the user sends data to the server intermittently. By this scheme, the server's received information of the user is reduced, and consequently the user's privacy is preserved. In this paper, we consider a periodic transmission scheme. We analyze the performance of privacy preservation and LQG control of different transmission periods. Under the given threshold of the control performance loss, a trade-off optimization problem is proposed. Finally, we give the solution to the optimization problem.

Index Terms—privacy preservation, Kalman filter, cooperative networked control systems

I. INTRODUCTION

Networked control systems (NCSs) have been widely deployed in many fields of our lives for a long time [1], such as smart grids, intelligent transportation and intelligent manufacturing. Due to the reliability of information and communication technologies, NCSs can effectively perform a multitude of complex functions. In NCSs, various components of the system are connected through a network, which enables them to cooperate more conveniently. For example, the system could belong to different parties, and the system's operation is achieved through the cooperative efforts by various parties. We call systems characterized by this behavior as *cooperative networked control systems*. Such cooperative behavior should indeed become a prevailing trend in the future. For example, in the domain of computer science, data owners frequently out-source their data to servers to access functions such as storage, management, and computation, thus significantly reducing the cost associated with data maintenance [2]. For example, cloud services and cooperative networked control systems serve as robust enablers for this paradigm, offering robust support and facilitation.

In this paper, we consider a basic cooperative control system called *user-server system*, which is composed of a single user and a server. In this system, the user needs to ask the server for services and thus shares information with it, but

the information may contain what the user think is privacy. Meanwhile, the server is considered to be “honest but curious”, i.e., it will honestly provide the user with services it needs, but also analyzes the user's information and explores its behavior as much as possible. Therefore, it is necessary to study the privacy preservation at the user side in cooperative NCSs, which is the focus of this paper.

A. Related Studies

Several various frameworks are proposed to study privacy preservation based on different understandings. Three important frameworks are *differential privacy* [3], *information-theoretic* [4], and *homomorphic encryption* [5].

Differential privacy, which is originally applied in the privacy preservation of static databases [6], due to its strong privacy guarantees, has attracted attention recently. The Laplace mechanism for differential privacy is proposed in [7]. Yu Kawano et al. [8] analyzed the differential privacy level of the Laplace mechanism in the cloud-based control system. Jerome Le Ny et al. [9] developed approximate MIMO filters to implement differential privacy guarantees. Kasra Yazdani et al. [10] presented a multi-agent LQ control framework which guarantees differential privacy. Kwassi H. Degue et al. [11] studied a cooperative differentially private LQG control problem with measurement aggregation, and proposed a two-stage architecture to solve it. Martin Abadi et al. [12] studied the applications of differential privacy in deep learning and developed new algorithmic techniques for it. Arik Friedman et al. [13] applied differential privacy in data mining and proposed an improved algorithm. Tie Ding et al. [14] proposed an algorithm that guarantees differential privacy to deal with a constrained resource allocation problem. Francois Gauthier et al. [15] proposed a privacy-preserving personalized graph federated learning algorithm by applying differential privacy.

Information-theoretic framework focuses on the nature of information, using quantitative metrics such as conditional entropy, mutual information, and directed information to evaluate privacy level. Peng Hao et al. [16] applied the proposed offline maximum entropy-based quantization rule to the security in Internet of things. Ehsan Nekouei et al. [17] designed a privacy-aware estimator by an entropy constrained approach. Ruoxi Jia et al. [18] used mutual information between the location trace and the reported occupancy measurement as a privacy metric, and designed a scheme that can balance the privacy and control performance. Ehsan Nekouei et al. [19] considered a multi-sensor estimation problem, where the conditional entropy of each sensor is applied as a privacy

^{*}: Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, Dept. of Automation, East China University of Science and Technology, Shanghai, China, 200237. Email: y30220957@mail.ecust.edu.cn, {weny, yangchao}@ecust.edu.cn. [†]: Key Laboratory of Advanced Process Control for Light Industry (Ministry of Education), School of Internet of Things Engineering, Jiangnan University, Wuxi, China. Email: yuqingni@jiangnan.edu.cn. The corresponding author is Chao Yang.

level. Causal conditioned directed information was proposed in [20]. Takashi Tanaka et al. [21] studied an optimization problem of cloud-based LQG systems, in which Kramer's causal conditioned directed information is used as a privacy metric, and an algorithm is proposed to solve the problem.

Homomorphic encryption permits third parties to operate on the encrypted data without requiring prior decryption. Kiminao Kogiso et al. [22] proposed a controller encryption scheme by using the modified homomorphic encryption. Farhad Farokhi et al. in [23] applied labeled homomorphic encryption in LQG control systems. Farhad Farokhi et al. [24] considered the sensors using the Paillier encryption which is a semi-homomorphic encryption in cloud-based systems. Mohammad Faiz et al. [25] used the particle swarm optimization to improve homomorphic encryption for cloud security.

B. The Study of This Paper

In this paper, we consider a basic user-server cooperative networked LQG control system. The user shares its information with the server and asks the server to compute control inputs. From the user's view, certain shared information is private. To guarantee the privacy level, we consider designing a privacy scheme at the user side. The main contributions of this paper could be summarized as follows.

- 1) We design a novel privacy preservation scheme, which is achieved by intermittent transmission, for the user in a user-server cooperative networked control system, which is based on a closed-loop LQG control system.
- 2) For our proposed intermittent transmission scheme, we analyze the estimation performance for infinite-time horizon at the estimator, and propose a novel privacy metric.
- 3) We analyze the privacy level and the LQG control performance, and study the trade-off problems between them.

Notations: $\mathbb{Z}_+$ is the set of non-negative integers and $k \in \mathbb{Z}_+$ is the time index. $\mathbb{N}$ is the set of natural numbers. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is n -dimensional Euclidean space. $\mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$) is the set of n by n positive semi-definite matrices (and positive definite matrices); when $X \in \mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$), it is written as $X \geq 0$ (and $X > 0$). It is defined by $X \geq Y$ if $X - Y \in \mathbb{S}_+^n$. $\mathbf{E}(\cdot)$ or $\mathbf{E}[\cdot]$ is the expectation of a random variable and $\mathbf{E}(\cdot|\cdot)$ or $\mathbf{E}[\cdot|\cdot]$ is the conditional expectation. $\text{tr}(\cdot)$ is the trace of a matrix. $\rho(\cdot)$ is the spectrum radius of a matrix.

II. PROBLEM SETUP

In this section, we introduce the model of the ordinary user-server system for cooperative LQG control, and propose a framework that simultaneously balances the control performance and the user's privacy preservation.

A. Ordinary System Model

The ordinary user-server system for cooperative LQG control is illustrated in Fig. 1. The user has a state process to control and a sensor which measures the process states. The server has sufficient computation capability. The user sends its data to the server for the optimal LQG control input.

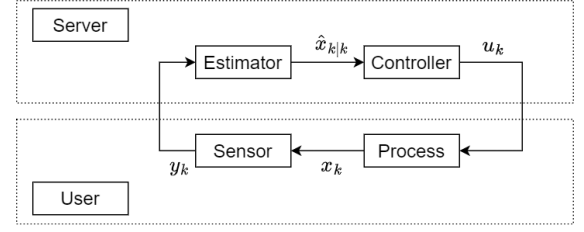


Fig. 1: The ordinary cooperative LQG control system.

The user needs to control the following dynamic process:

$$x_{k+1} = Ax_k + Bu_k + w_k, \quad (1)$$

where $x_k \in \mathbb{R}^n$ is the state of the process at time k , $u_k \in \mathbb{R}^m$ is the control input, and w_k is the Gaussian white noise whose mean is zero and covariance is $Q(Q \geq 0)$. The matrix $A \in \mathbb{R}^{n \times n}$ is the system matrix, and $B \in \mathbb{R}^{n \times m}$ is the input matrix. The initial condition is assumed that x_0 is Gaussian with distribution $\mathcal{N}(\bar{x}_0, \Sigma_0)$. The time horizon of the process is assumed to be infinite. We assume that (A, B) is controllable.

The user cannot directly get the state value and has a sensor to measure the state as follows:

$$y_k = Cx_k + v_k, \quad (2)$$

where $y_k \in \mathbb{R}^q$ is the measurement of x_k , and v_k is the Gaussian white noise whose mean is zero and covariance is $R(R > 0)$. The matrix $C \in \mathbb{R}^{q \times n}$ is the measurement matrix. The noises $\{w_k\}$ and $\{v_k\}$ and the initial state x_0 are mutually independent of each other. The pairs $(A, \sqrt{Q})$ and (C, A) are assumed to be stabilizable and detectable, respectively.

For the user, its demand is the optimal LQG control input. The considered infinite-time quadratic objective function for the LQG control is denoted as $\mathcal{J}$, and is defined as follows:

$$\mathcal{J} \triangleq \lim_{N \rightarrow \infty} \frac{1}{N} \mathbf{E} \left[\sum_{k=0}^{N-1} (x_k' W x_k + u_k' U u_k) \right], \quad (3)$$

where W and U are weight matrices satisfying $W \geq 0$ and $U > 0$, and the expectation is taken with respect to the possible randomness.

In this cooperative system, the user employs the server for the needs of control, and the server computes the optimal control input and returns it to the user. The server serves as the estimator and the controller. Since the user's process state is unavailable, it needs to be estimated by the server at first, and the server computes the optimal control input based on it. The system parameters A, B, W, U for LQG control, C, Q, R for state estimation, and the initial condition x_0 with Gaussian distribution $\mathcal{N}(\bar{x}_0, \Sigma_0)$ are shared by the user with the server, and the user is also supposed to provide y_k at each time k .

When the process begins, the user sends y_k to the server at each time k . Let $Y_k \triangleq \{y_1, y_2, \dots, y_k\}$ denote the set of the received measurements. Then the server computes the *a priori* and *a posteriori* estimates $\hat{x}_{k|k-1}$ and $\hat{x}_{k|k}$ defined as follows:

$$\hat{x}_{k|k-1} \triangleq \mathbf{E}[x_k | Y_{k-1}],$$

$$\hat{x}_{k|k} \triangleq \mathbf{E}[x_k|Y_k].$$

Meanwhile, we define $P_{k|k-1}$ and $P_{k|k}$ as the estimate error covariance matrices associated with $\hat{x}_{k|k-1}$ and $\hat{x}_{k|k}$, respectively:

$$P_{k|k-1} \triangleq \mathbf{E}[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})'|Y_{k-1}],$$

$$P_{k|k} \triangleq \mathbf{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})'|Y_k].$$

The server runs the standard Kalman filter under the given initial condition $\hat{x}_{0|0} = \bar{x}_0$ and $P_{0|0} = \Sigma_0$, and the estimates and the associated error covariances satisfy the following recursion:

$$\hat{x}_{k|k-1} = A\hat{x}_{k-1|k-1} + Bu_{k-1}, \quad (4)$$

$$P_{k|k-1} = AP_{k-1|k-1}A' + Q, \quad (5)$$

$$K_k = P_{k|k-1}C'(CP_{k|k-1}C' + R)^{-1}, \quad (6)$$

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k(y_k - C\hat{x}_{k|k-1}), \quad (7)$$

$$P_{k|k} = (I - K_kC)P_{k|k-1}. \quad (8)$$

Then the server computes the optimal control input and returns it to the user. The computation follows

$$S_T = W, \quad (9)$$

$$S_k = A'S_{k+1}A + W - A'S_{k+1}B(B'S_{k+1}B + U)^{-1}B'S_{k+1}A, \quad (10)$$

$$L_k = -(B'S_{k+1}B + U)^{-1}B'S_{k+1}A, \quad (11)$$

$$u_k^* = L_k\hat{x}_{k|k}, \quad (12)$$

where eqn. (9)-(11) are computed before the process.

For the Kalman filter used in this paper, it has an asymptotic steady error covariance [26], and we denote it as

$$\lim_{k \rightarrow \infty} P_{k|k} = \bar{P}.$$

The error covariance converges at an exponential rate. Hence, for convenience, under the considered infinite-time horizon, we assume that the initial covariance $P_{0|0} = \bar{P}$. Consequently for all $k \geq 1$, we have

$$P_{k|k} = \bar{P},$$

$$K_k = K.$$

Meanwhile, for the LQG controller, the matrix S_k also converges to a steady value and becomes time-invariant, and we have

$$\lim_{N \rightarrow \infty} S_k = S,$$

where

$$S = A'SA + W - A'SB(B'SB + U)^{-1}B'SA.$$

Then we evaluate the performance of the optimal LQG control. The optimal objective function value in infinite-time horizon, denoted as $\mathcal{J}^*$, is given as follows [27]:

$$\mathcal{J}^* = \text{tr}(SQ) + \text{tr}(\Phi\bar{P}), \quad (13)$$

where

$$\Phi = A'SB(B'SB + U)^{-1}B'SA.$$

B. Privacy Preservation Model

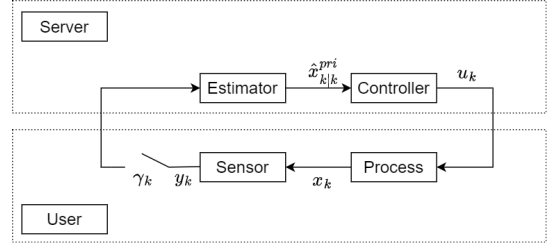


Fig. 2: The privacy scheme is used.

In the ordinary cooperative LQG control system, the user's information of state is also known to the server. However, the user treats the information of state as its privacy, so it decides to employ a privacy scheme to preserve the privacy.

In this paper, we consider applying a scheme of intermittent transmission (Fig. 2). Let γ_k be the user's decision variable to control the transmission of the measurement y_k to the server at time k , i.e., if $\gamma_k = 1$, y_k is sent to the server, and if $\gamma_k = 0$, y_k is not sent. Intuitively, the user transmits measurements intermittently, which reduces the amount of information obtained by the server, thus preserving the privacy.

We consider the scenario that the intervals between measurement transmissions are identical, i.e., the transmission is periodic. We assume at time $k = 1$ the user chooses to transmit the measurement, and denote the transmission period as T . For $l \in \mathbb{Z}_+$, the scheme can be formulated as follows:

$$\gamma_k = \begin{cases} 1, & k = lT + 1, \\ 0, & k \neq lT + 1. \end{cases} \quad (14)$$

An illustration of $T = 3$ is shown as follows:

$$\underbrace{100}_{T=3} 100 100 1 \dots$$

C. Privacy Metric

In the system under the privacy scheme, the server is unable to receive all the measurements from the user. Let $\tilde{Y}_k \triangleq \{\gamma_1 y_1, \gamma_2 y_2, \dots, \gamma_k y_k\}$ denote the set of measurements actually received by the server. The *a priori* and *a posteriori* estimates in this scenario, denoted as $\hat{x}_{k|k-1}^{pri}$ and $\hat{x}_{k|k}^{pri}$, defined as follows:

$$\hat{x}_{k|k-1}^{pri} \triangleq \mathbf{E}[x_k | \tilde{Y}_{k-1}],$$

$$\hat{x}_{k|k}^{pri} \triangleq \mathbf{E}[x_k | \tilde{Y}_k].$$

Meanwhile, the estimate error covariance matrices associated with $\hat{x}_{k|k-1}^{pri}$ and $\hat{x}_{k|k}^{pri}$ are denoted as $P_{k|k-1}^{pri}$ and $P_{k|k}^{pri}$, defined as follows:

$$P_{k|k-1}^{pri} \triangleq \mathbf{E}[(x_k - \hat{x}_{k|k-1}^{pri})(x_k - \hat{x}_{k|k-1}^{pri})'| \tilde{Y}_{k-1}],$$

$$P_{k|k}^{pri} \triangleq \mathbf{E}[(x_k - \hat{x}_{k|k}^{pri})(x_k - \hat{x}_{k|k}^{pri})'| \tilde{Y}_k].$$

When $\gamma_k = 1$, they evolve as

$$\hat{x}_{k|k-1}^{pri} = A\hat{x}_{k-1|k-1}^{pri} + Bu_{k-1}, \quad (15)$$

$$P_{k|k-1}^{pri} = AP_{k-1|k-1}^{pri}A' + Q, \quad (16)$$

$$K_k^{pri} = P_{k|k-1}^{pri} C' (C P_{k|k-1}^{pri} C' + R)^{-1}, \quad (17)$$

$$\hat{x}_{k|k}^{pri} = \hat{x}_{k|k-1}^{pri} + K_k^{pri} (y_k - C \hat{x}_{k|k-1}^{pri}), \quad (18)$$

$$P_{k|k}^{pri} = (I - K_k^{pri} C) P_{k|k-1}^{pri}, \quad (19)$$

and when $\gamma_k = 0$, we have

$$\hat{x}_{k|k}^{pri} = \hat{x}_{k|k-1}^{pri}, \quad (20)$$

$$P_{k|k}^{pri} = P_{k|k-1}^{pri}. \quad (21)$$

Hence, the privacy scheme will cause the increase of the estimate error covariance. Based on it, we propose the privacy metric to measure the quality of privacy preservation. For each time k , we define the privacy metric as the deviation between the estimate error covariance after using the privacy scheme and the one in the ordinary system. Specifically, it is defined as follows:

$$\mathcal{Q}_{privacy}^k \triangleq P_{k|k}^{pri} - P_{k|k}.$$

To study the privacy performance of infinite-time horizon, we define the averaged privacy metric at all time as

$$\mathcal{Q}_{privacy} = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} \mathcal{Q}_{privacy}^k.$$

D. Problems to Study

With respect to the proposed privacy preservation scheme, our attention will be directed towards the following problems.

- 1 We evaluate the privacy preservation effectiveness. Meanwhile, the privacy scheme incurs a decrease in service quality, which results in a relative loss for LQG control performance, denoted by $\mathcal{Q}_{LQG}$. We also analyze this performance degradation.
- 2 We study the trade-off between the privacy preservation and LQG control performances:

$$\begin{aligned} \max \quad & \text{tr}(\mathcal{Q}_{privacy}) \\ \text{s.t.} \quad & \mathcal{Q}_{LQG} \leq \alpha, \end{aligned}$$

where $\alpha > 0$ represents a given loss level of LQG control performance.

III. PERFORMANCE ANALYSIS

In this section, we firstly introduce preliminaries of Kalman filtering and present the explicit forms of privacy and LQG control performances. Secondly, we study and solve the trade-off optimization problem about them.

A. Kalman Filtering Preliminaries

Before stating the main results of the paper, we provide a summary of necessary properties of the Kalman filter.

The function $h(X) : \mathbb{S}_+^n \rightarrow \mathbb{S}_+^n$ is defined as

$$h(X) \triangleq X A X A' + Q, \quad (22)$$

which is also called the Lyapunov function. The function $\tilde{g} : \mathbb{S}_+^n \rightarrow \mathbb{S}_+^n$ is defined as follows:

$$\tilde{g}(X) \triangleq X - X C' (C X C' + R)^{-1} C X. \quad (23)$$

Define $g = \tilde{g} \circ h(X)$. In the ordinary system, we have

$$P_{k|k-1} = h(P_{k-1|k-1}), \quad (24)$$

$$P_{k|k} = g(P_{k-1|k-1}). \quad (25)$$

When $k \rightarrow \infty$, it follows $\bar{P} = g(\bar{P})$, and $\bar{P}$ is the unique solution to $X = g(X)$.

B. Privacy Performance

For the estimate error covariance at the server side, we have the following results.

Theorem 1. *Given the transmission period T , based on the assumption that (C, A^T) is detectable, we have*

$$\lim_{l \rightarrow \infty} P_{lT+1|lT+1}^{pri} = \tilde{P},$$

in which $\tilde{P}$ is the unique solution to the following equation:

$$\tilde{P} = g \circ h^{T-1}(\tilde{P}).$$

Meanwhile two limits exist as follows:

$$\begin{aligned} \liminf_{k \rightarrow \infty} P_{k|k}^{pri} &= \tilde{P}, \\ \limsup_{k \rightarrow \infty} P_{k|k}^{pri} &= h^{T-1}(\tilde{P}). \end{aligned}$$

Proof: In appendix. ■

From Theorem 1, $\tilde{P}$ is the error covariance at the time when the measurement is transmitted, and the server's calculation of $P_{k|k}^{pri}$ follows eqn. (21) until the next transmission. Hence, we can see that the estimate error covariance at the server side is

$$P_{k|k}^{pri} = \begin{cases} \tilde{P}, & \text{if } \gamma_k = 1, \\ h(P_{k-1|k-1}^{pri}), & \text{if } \gamma_k = 0. \end{cases} \quad (26)$$

In the original system, we have $P_{k|k} = \bar{P}$. We can now obtain the metric of privacy performance:

$$\mathcal{Q}_{privacy} = \frac{1}{T} \sum_{i=0}^{T-1} h^i(\tilde{P}) - \bar{P}. \quad (27)$$

C. LQG Control Performance

The server computes the control policy based on the user's state estimate. Adding the privacy scheme, the control input computed by the server is

$$u_k = L_k \hat{x}_{k|k}^{pri}. \quad (28)$$

From the above equation, we can see that a deviation is caused by the privacy scheme for the control input. This deviation is caused by the estimate without transmitting the measurement. At that time, the result corresponds to the *a priori* estimate of the original system, which makes the control law $\{u_k\}$ be non-optimal under the scheme. Hence, the resulting state trajectories $\{x_k\}$ is also non-optimal. Therefore, privacy scheme can enhance the privacy performance while it will lead to the sacrifice in the LQG performance. The optimal LQG performance under the privacy scheme, denoted as $\mathcal{O}^*$, is studied below.

Theorem 2. Under the privacy scheme, it holds that

$$\mathcal{O}^* = \text{tr}(SQ) + \text{tr}\left(\Phi \frac{1}{T} \sum_{i=0}^{T-1} h^i(\tilde{P})\right),$$

where

$$\Phi = A'SB(U + B'SB)^{-1}B'SA.$$

Proof: In appendix. ■

Now we can define the quality loss in LQG performance:

$$\mathcal{Q}_{LQG} \triangleq \mathcal{O}^* - \mathcal{J}^* = \text{tr}(\Phi \mathcal{Q}_{privacy}).$$

D. Optimization Problem

Through previous study, we can see that privacy preservation is gained while requiring the sacrifice in LQG control performance. Hence, an optimization problem is proposed to study the trade-off: to maximize the privacy metric $\mathcal{Q}_{privacy}$ while the loss of LQG performance $\mathcal{Q}_{LQG}$ is under a given level α . The problem is as follows:

Problem 1.

$$\begin{aligned} \max_T \quad & \text{tr}(\mathcal{Q}_{privacy}) \\ \text{s.t.} \quad & \text{tr}(\Phi \mathcal{Q}_{privacy}) \leq \alpha, \\ & \mathcal{Q}_{privacy} = \frac{1}{T} \sum_{i=0}^{T-1} h^i(\tilde{P}) - \bar{P}. \end{aligned}$$

The function involved in this problem is discrete, so we consider using dichotomy (Algorithm 1) to solve it.

Algorithm 1 Optimal T by Using Dichotomy

Input: $\mathcal{Q}_{LQG}(T)$: the objective function; T_l : the left bound of search range;

T_r : the right bound of search range; α : the given threshold;

Output: T^* : optimal T ;

```

1: Initialize  $T^*$ ;
2: repeat
3:   compute the mid index and round down:  $T_m = \text{floor}((T_l + T_r)/2)$ ;
4:   compute the objective value of mid index:  $\mathcal{Q}_m = \mathcal{Q}_{LQG}(T_m)$ ;
5:   if  $\mathcal{Q}_m < \alpha$  then
6:      $T^* = T_m$ ;
7:      $T_l = T_m + 1$ ;
8:   else
9:      $T_r = T_m - 1$ ;
10:  end if
11: until  $T_l > T_r$ 

```

IV. EXAMPLE

We consider a second-order system with infinite-time horizon, whose parameters are as follows:

$$\begin{aligned} A &= \begin{bmatrix} 0.19 & 0.46 \\ 0.31 & 0.8 \end{bmatrix}, \quad B = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \\ C &= \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 1.9 & 0.9 \\ 0.9 & 2.8 \end{bmatrix}, \\ R &= 1, \quad W = \begin{bmatrix} 1.5 & 0.5 \\ 0.5 & 1.5 \end{bmatrix}, \quad U = 1. \end{aligned}$$

Firstly we plot the traces of $\mathcal{Q}_{privacy}$ in different T (Fig. 3).

We find the curve is monotonically increasing, and it means the larger T is, the greater the period between transmitting

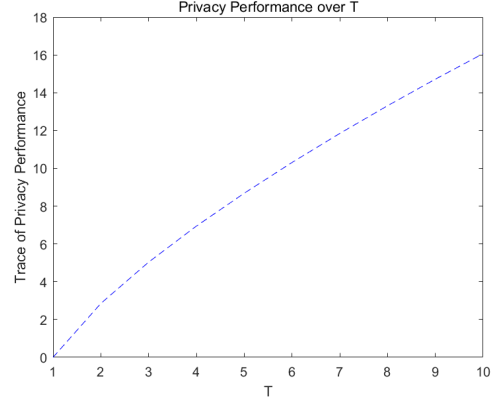


Fig. 3: $\mathcal{Q}_{privacy}$ with T varying from 1 to 10.

the measurement is, and the better the privacy performance is, which conforms to eqn. (27).

Then we study the relationship between LQG performance loss $\mathcal{Q}_{LQG}$ and transmission period T (Fig. 4). From the

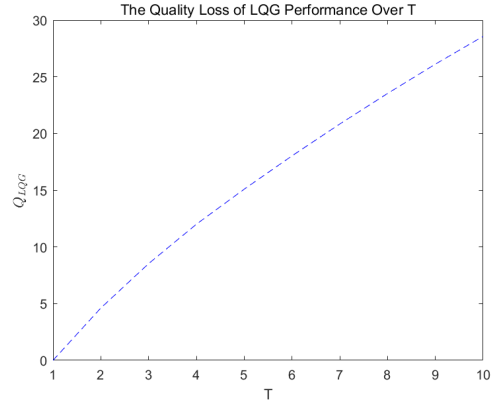


Fig. 4: $\mathcal{Q}_{LQG}$ with T varying from 1 to 10.

Fig. 4, $\mathcal{Q}_{LQG}$ is also monotonically increasing, which means the less information transmitted, the larger the cost of LQG control is. Recalling Theorem 2, we can find $\mathcal{Q}_{LQG}$ is linear to $\mathcal{Q}_{privacy}$. Hence their curves are similar.

Given different thresholds of LQG performance loss α , we can get optimal T . We plot optimal T when α varies from 7 to 27 (Fig. 5). We can find that the curve is stepped, and it means for a continuous range of α the optimal T is the same because it is discrete. As the given LQG performance loss threshold increases, a larger transmission period can be selected.

Finally we plot the estimates in two different schemes when $T = 3$ (Fig. 6), and we find that $\hat{x}_{k|k}^{pri}$ is deviated from $\hat{x}_{k|k}$.

V. CONCLUSION

In this paper, we consider a cooperative LQG control system with a single user and a server. We propose a scheme of intermittently transmission to preserve the user's privacy, and the corresponding privacy metric. Then we analyze the privacy level under the privacy scheme and the loss in LQG control

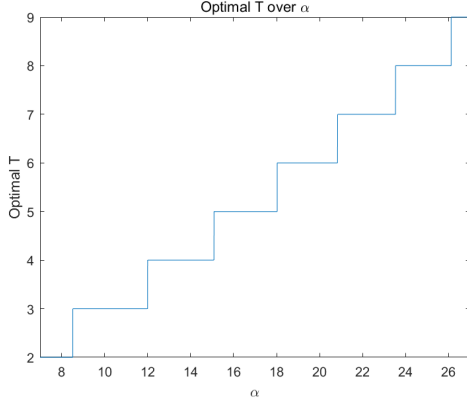


Fig. 5: Optimal T with α varying from 7 to 27.

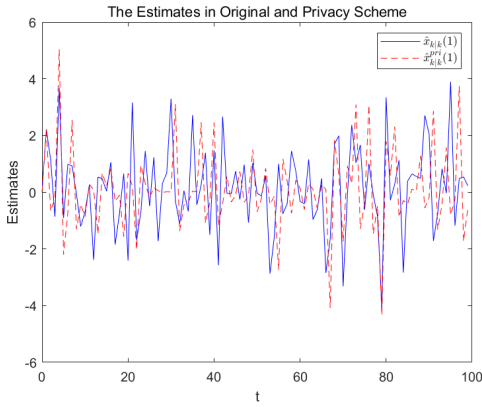


Fig. 6: Estimates in two different schemes.

performance. Finally, we propose an optimization problem and solve it based on the trade-off between the privacy level and the loss in LQG control performance. For the future work, the multi-sensor system and new privacy metric could be considered.

APPENDIX

For notional convenience, in the following sections, we omit the superscript “*pri*” in $\hat{x}_{k|k}^{pri}$, $P_{k|k}^{pri}$, $x_{k|k-1}^{pri}$, and $P_{k|k-1}^{pri}$ under the privacy scheme. Furthermore, we use $\hat{x}_k$ and P_k to replace $\hat{x}_{k|k}$ and $P_{k|k}$, and use $\hat{x}_k^-$ and P_k^- to replace $\hat{x}_{k|k-1}$ and $P_{k|k-1}$.

A. Proof of Theorem 1

To prove the theorem, we follow the procedure in Sec. 4.4 of [26]. We show that P_k has two limits. When $k \rightarrow \infty$, the infimum limit corresponds to the covariance at the time the server receives y_k , i.e., P_{lT+1} ($l \in \mathbb{Z}_+$). Meanwhile the supremum limit corresponds to the covariance at the previous time before the server receives y_k , i.e., P_{lT} ($l \in \mathbb{N}$). Since if P_{lT+1}^- converges, $P_{lT+1} = \tilde{g}(P_{lT+1}^-)$ also converges. Hence, we focus on the sequence of $\{P_{lT+1}^-\}$. For general k , we firstly have

$$\hat{x}_k = \hat{x}_k^- + K_k(y_k - C\hat{x}_k^-)$$

$$= (I - K_k C)\hat{x}_k^- + K_k C x_k + K_k v_k.$$

Then

$$x_k - \hat{x}_k = (I - K_k C)(x_k - \hat{x}_k^-) - K_k v_k.$$

We have

$$P_k = (I - K_k C)P_k^- (I - K_k C)' + K_k R K_k'.$$

Hence, when $k = (l-1)T + 1$, we obtain

$$P_{(l-1)T+1} = (I - K_{(l-1)T+1} C)P_{(l-1)T+1}^- (I - K_{(l-1)T+1} C)' + K_{(l-1)T+1} R K_{(l-1)T+1}'.$$

Since when the estimator does not receive y_k , the calculation of estimate error covariance follows eqn. (21), and we have

$$P_{lT} = h^{T-1}(P_{(l-1)T+1}).$$

Then

$$\begin{aligned} P_{lT+1}^- &= h(P_{lT}) \\ &= A^T(I - K_{(l-1)T+1} C)P_{(l-1)T+1}^- (I - K_{(l-1)T+1} C)'(A')^T \\ &\quad + A^T K_{(l-1)T+1} R K_{(l-1)T+1}'(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i. \end{aligned}$$

We present the following steps to complete the proof.

Step 1

Firstly we prove that P_{lT+1}^- is bounded. Since we assume (C, A) is detectable, there exists a $\tilde{K}$ which can formulate a suboptimal, asymptotically stable filter by

$$\tilde{x}_k^- = A\tilde{x}_{k-1}^- + A\tilde{K}(y_k - C\tilde{x}_k^-) + Bu_{k-1},$$

and its corresponding error covariance is

$$\tilde{P}_k^- = A(I - \tilde{K}C)\tilde{P}_{k-1}^- (I - \tilde{K}C)'A' + A\tilde{K}R\tilde{K}'A' + Q.$$

Hence, we can obtain

$$\begin{aligned} \tilde{P}_{lT+1}^- &= A^T(I - \tilde{K}C)\tilde{P}_{(l-1)T+1}^- (I - \tilde{K}C)'(A')^T \\ &\quad + A^T \tilde{K}R\tilde{K}'(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i. \end{aligned}$$

We assume (C, A^T) is detectable, which makes $\rho(A^T(I - \tilde{K}C)) < 1$, and $A^T(I - \tilde{K}C)$ is stable and a constant matrix. Therefore, the result has a bounded solution. Based on the optimality of Kalman filter, we have $P_{lT+1}^- \leq \tilde{P}_{lT+1}^-$, hence P_{lT+1}^- is also bounded.

Step 2

Next we prove the incrementality of P_{lT+1}^- . We firstly assume $P_1^- = 0$. By simple computation, it can be obtained that $P_{T+1}^- \geq P_1^- = 0$. For general l ,

$$\begin{aligned} P_{lT+1}^- &= A^T(I - K_{(l-1)T+1} C)P_{(l-1)T+1}^- (I - K_{(l-1)T+1} C)'(A')^T \\ &\quad + A^T K_{(l-1)T+1} R K_{(l-1)T+1}'(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i \end{aligned}$$

$$\begin{aligned}
&= \min_K [A^T(I - KC)P_{(l-1)T+1}^-(I - KC)'(A')^T \\
&\quad + A^T K R K'(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i] \\
&\leq A^T(I - K_{lT+1}C)P_{(l-1)T+1}^-(I - K_{lT+1}C)'(A')^T \\
&\quad + A^T K_{lT+1} R K'_{lT+1}(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i \\
&\leq A^T(I - K_{lT+1}C)P_{lT+1}^-(I - K_{lT+1}C)'(A')^T \\
&\quad + A^T K_{lT+1} R K'_{lT+1}(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i \\
&= P_{(l+1)T+1}^-.
\end{aligned}$$

Now we have proved the incrementality and boundedness of P_{lT+1}^- , hence P_{lT+1}^- is asymptotically stable, and so is P_{lT+1} . For P_{lT+1}^- we have

$$P_{lT+1}^- = h^T \circ \tilde{g}(P_{(l-1)T+1}^-).$$

Denote $\bar{\Sigma}$ is the asymptotically stable value of P_{lT+1}^- , and it is the unique solution to the following equation:

$$\bar{\Sigma} = h^T \circ \tilde{g}(\bar{\Sigma}).$$

We denote the infimum value of P_k as $\tilde{P}$, and it is simple to see that $\tilde{P}$ is the asymptotically stable value of P_{lT+1} , hence we have

$$\tilde{P} = \tilde{g}(\bar{\Sigma}) = \tilde{g} \circ h^T \circ \tilde{g}(\bar{\Sigma}) = g \circ h^{T-1}(\tilde{P}).$$

Therefore, we obtain the following results:

$$\lim_{l \rightarrow \infty} P_{lT+1} = \tilde{P},$$

where $\tilde{P}$ is the unique solution to follows:

$$\tilde{P} = g \circ h^{T-1}(\tilde{P}).$$

Meanwhile, two limits of P_k are given as

$$\begin{aligned}
\liminf_{k \rightarrow \infty} P_k &= \tilde{P}, \\
\limsup_{k \rightarrow \infty} P_k &= h^{T-1}(\tilde{P}).
\end{aligned}$$

In summary, we prove Theorem 1 under the zero initial covariance condition.

Step 3

Finally we consider $P_1^- \neq 0$. Define a transition matrix Ψ_l as

$$\begin{aligned}
\Psi_l &= [A^T(I - K_{(l-1)T+1}C)][A^T(I - K_{(l-2)T+1}C)] \\
&\quad [A^T(I - K_{(l-3)T+1}C)] \cdots [A^T(I - K_1C)].
\end{aligned}$$

Then P_{lT+1}^- follows

$$\begin{aligned}
P_{lT+1}^- &= \Psi_l P_1^- \Psi_l' + \text{nonnegative definite terms} \\
&\geq \Psi_l P_1^- \Psi_l'.
\end{aligned}$$

We firstly take $P_1^- = \beta I$ ($\beta > 0$), and it follows that $\beta \Psi_l \Psi_l'$. Since P_{lT+1}^- is proved to be bounded before, Ψ_l is also bounded. Assume that P_{lT+1}^- has a asymptotically stable value

at this scenario. We rewrite P_{lT+1}^- as follows:

$$P_{lT+1}^- = h^T \circ \tilde{g}(P_{(l-1)T+1}^-) = h^{T-1} \circ (h \circ \tilde{g}(P_{(l-1)T+1}^-)).$$

Hence, we have

$$\begin{aligned}
P_{lT+1}^- &= h^{T-1}(A(I - K_{(l-1)T+1}C)P_{(l-1)T+1}^- A' + Q) \\
&= h^{T-1}(A P_{(l-1)T+1}^- (I - K_{(l-1)T+1}C)' A' + Q) \\
&= A^T P_{(l-1)T+1}^- (I - K_{(l-1)T+1}C)'(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i.
\end{aligned}$$

And $\bar{\Sigma}$ can also be computed as follows:

$$\begin{aligned}
\bar{\Sigma} &= h^{T-1}(A(I - KC)\bar{\Sigma}A' + Q) \\
&= A^T(I - KC)\bar{\Sigma}(A')^T + \sum_{i=0}^{T-1} A^i Q(A')^i.
\end{aligned}$$

By subtraction, it is follows that

$$\begin{aligned}
P_{lT+1}^- - \bar{\Sigma} &= A^T(I - KC)(P_{(l-1)T+1}^- - \bar{\Sigma})(I - K_{(l-1)T+1}C)'(A')^T \\
&\quad + A^T K C P_{(l-1)T+1}^- (I - K_{(l-1)T+1}C)'(A')^T \\
&\quad - A^T(I - KC)\bar{\Sigma}C'K'_{(l-1)T+1}(A')^T.
\end{aligned}$$

For the last two terms, we have

$$\begin{aligned}
&A^T K C P_{(l-1)T+1}^- (I - K_{(l-1)T+1}C)'(A')^T \\
&- A^T(I - KC)\bar{\Sigma}C'K'_{(l-1)T+1}(A')^T \\
&= A^T K C P_{(l-1)T+1}^- (A')^T - A^T \tilde{P} C' K'_{(l-1)T+1}(A')^T.
\end{aligned}$$

Substitute $K_k = P_k C' R^{-1}$ to it, and we obtain the result is zero. Hence, we get

$$\begin{aligned}
P_{lT+1}^- - \bar{\Sigma} &= A^T(I - KC)(P_{(l-1)T+1}^- - \bar{\Sigma})(I - K_{(l-1)T+1}C)'(A')^T.
\end{aligned}$$

Suppose $P_T = \beta I$, we have

$$P_{lT+1}^- - \bar{\Sigma} = [A^T(I - KC)]^l (P_1^- - \bar{\Sigma}) \Psi_l'.$$

Due to (C, A^T) is detectable, and Ψ_l is bounded, when $l \rightarrow \infty$, we have $P_{lT+1}^- = \bar{\Sigma}$.

For an arbitrary P_1^- , we take such $\beta > 0$ that $\beta I > P_1^-$, and denote the solution to $X = h^T \circ \tilde{g}(X)$ as $\bar{\Sigma}_{\beta I^-}$. Meanwhile we denote $\bar{\Sigma}_0$ and $\bar{\Sigma}_{\beta I}$ as the solution to the same equation when $P_1^- = 0$ and $P_1^- = \beta I$. We can simply get

$$\bar{\Sigma}_0 < \bar{\Sigma}_{\beta I^-} < \bar{\Sigma}_{\beta I}.$$

From the previous proof, both $\bar{\Sigma}_0$ and $\bar{\Sigma}_{\beta I}$ tend to $\bar{\Sigma}$, hence $\bar{\Sigma}_{\beta I^-}$ converges to $\bar{\Sigma}$ as well, i.e., P_{lT+1}^- converges at this scenario. Therefore, P_{lT+1} also converges. Then we can obtain the same conclusions as in the case of zero initial covariance.

B. Proof of Theorem 2

We consider the case of transmission period $T = 2$, and other cases can also be proved similarly. In this case, according

to eqn. (14), for $l \in \mathbb{Z}_+$, the transmission scheme is formulated as follows:

$$\gamma_k = \begin{cases} 1, & k = 2l + 1, \\ 0, & k \neq 2l + 1. \end{cases}$$

Firstly we consider the scenario of a finite-time horizon N , and assume that $N = 2L + 1$, where L is a positive integer. Then at time $k = N - 1$ the measurement is not sent, and at time $k = N - 2$ it is sent. Define the information set I_k as

$$I_0 = \{\emptyset\}, \\ I_k = \{\gamma_1 y_1, \dots, \gamma_k y_k, u_0, \dots, u_{k-1}\}, \quad k = 1, \dots, N.$$

The finite-time quadratic objective function for the LQG control is denoted as $J_{0:N}$, and is defined as follows:

$$J_{0:N} \triangleq \mathbf{E} \left[\sum_{k=0}^{N-1} (x'_k W x_k + u'_k U u_k) + x'_N W x_N \right].$$

Meanwhile, we define $J_{k:N}$ as

$$J_{k:N} = \min_{u_k} \mathbf{E} [x'_k W x_k + u'_k U u_k + J_{k+1:N} | I_k].$$

At time N , we have $J_{N:N} = \mathbf{E}[x'_N W x_N | I_N]$. Therefore, at time $k = N - 1$,

$$\begin{aligned} J_{N-1:N} &= \min_{u_{N-1}} \mathbf{E} [x'_{N-1} W x_{N-1} + u'_{N-1} U u_{N-1} + J_{N:N} | I_{N-1}] \\ &= \min_{u_{N-1}} \mathbf{E} [x'_{N-1} W x_{N-1} + u'_{N-1} U u_{N-1} + x'_N W x_N | I_{N-1}] \\ &= \min_{u_{N-1}} \mathbf{E} [u'_{N-1} U u_{N-1} + x'_{N-1} A' W B u_{N-1} \\ &\quad + u'_{N-1} B' W A x_{N-1} + u'_{N-1} B' W B u_{N-1} | I_{N-1}] \\ &\quad + \mathbf{E} [x'_{N-1} W x_{N-1} + x'_{N-1} A' W A x_{N-1} | I_{N-1}] + tr(WQ). \end{aligned}$$

Since the measurement is not sent at this time, for the server we have $\hat{x}_{N-1} = \hat{x}_{N-1}^-$, i.e., $\mathbf{E}(x_{N-1} | I_{N-1}) = \hat{x}_{N-1}^- = \hat{x}_{N-1}^-$. Hence, we have

$$\begin{aligned} J_{N-1:N} &= \min_{u_{N-1}} [u'_{N-1} (U + B' W B) u_{N-1} + 2u'_{N-1} B' W A \hat{x}_{N-1}^-] \\ &\quad + \mathbf{E} [x'_{N-1} (W + A' W A) x_{N-1} | I_{N-1}] + tr(WQ). \end{aligned}$$

To find the minimum value, we take the derivative of the term containing u_{N-1} in the above result and let it be zero:

$$2(B' W B + U) u_{N-1}^* + 2B' W A \hat{x}_{N-1}^- = 0,$$

which leads to

$$u_{N-1}^* = -(B' W B + U)^{-1} B' W A \hat{x}_{N-1}^-.$$

Substituting it into the above equation:

$$\begin{aligned} J_{N-1:N} &= \mathbf{E} [x'_{N-1} (W + A' W A) x_{N-1} | I_{N-1}] + tr(WQ) \\ &\quad - (\hat{x}_{N-1}^-)' A' W B (B' W B + U)^{-1} B' W A \hat{x}_{N-1}^-. \end{aligned}$$

Let

$$\begin{aligned} S_N &= W, \\ \Phi_{N-1} &= A' S_N B (B' S_N B + U)^{-1} B' S_N A, \\ S_{N-1} &= A' S_N A + W - \Phi_{N-1}. \end{aligned}$$

Then we have

$$\begin{aligned} J_{N-1:N} &= \mathbf{E} [x'_{N-1} S_{N-1} x_{N-1} | I_{N-1}] + tr(S_N Q) \\ &\quad + \mathbf{E} [x'_{N-1} \Phi_{N-1} x_{N-1} | I_{N-1}] - (\hat{x}_{N-1}^-)' \Phi_{N-1} \hat{x}_{N-1}^- \\ &= \mathbf{E} [x'_{N-1} S_{N-1} x_{N-1} | I_{N-1}] + tr(S_N Q) + tr(\Phi_{N-1} P_{N-1}^-). \end{aligned}$$

At time $k = N - 2$,

$$\begin{aligned} J_{N-2:N} &= \min_{u_{N-2}} \mathbf{E} [x'_{N-2} W x_{N-2} + u'_{N-2} U u_{N-2} + J_{N-1:N} | I_{N-2}] \\ &= \min_{u_{N-2}} \left\{ u'_{N-2} U u_{N-2} + \mathbf{E} [x'_{N-1} S_{N-1} x_{N-1} | I_{N-2}] \right\} \\ &\quad + \mathbf{E} [x'_{N-2} W x_{N-2} | I_{N-2}] + tr(S_N Q) + tr(\Phi_{N-1} P_{N-1}^-) \\ &= \min_{u_{N-2}} \left\{ u'_{N-2} U u_{N-2} + \mathbf{E} [(A x_{N-2} + B u_{N-2} + w_{N-2})' \right. \\ &\quad \left. S_{N-1} (A x_{N-2} + B u_{N-2} + w_{N-2}) | I_{N-2}] \right\} \\ &\quad + \mathbf{E} [x'_{N-2} W x_{N-2} | I_{N-2}] + tr(S_N Q) + tr(\Phi_{N-1} P_{N-1}^-) \\ &= \min_{u_{N-2}} \left\{ u'_{N-2} (U + B' S_{N-1} B) u_{N-2} \right. \\ &\quad \left. + \mathbf{E} [x'_{N-2} A' S_{N-1} B u_{N-2} + u'_{N-2} B' S_{N-1} A x_{N-2} | I_{N-2}] \right\} \\ &\quad + \mathbf{E} [x'_{N-2} A' S_{N-1} A x_{N-2} | I_{N-2}] + tr(S_{N-1} Q) \\ &\quad + \mathbf{E} [x'_{N-2} W x_{N-2} | I_{N-2}] + tr(S_N Q) + tr(\Phi_{N-1} P_{N-1}^-) \\ &= \min_{u_{N-2}} \left\{ u'_{N-2} (U + B' S_{N-1} B) u_{N-2} \right. \\ &\quad \left. + \mathbf{E} [x'_{N-2} A' S_{N-1} B u_{N-2} + u'_{N-2} B' S_{N-1} A x_{N-2} | I_{N-2}] \right\} \\ &\quad + \mathbf{E} [x'_{N-2} (A' S_{N-1} A + W) x_{N-2} | I_{N-2}] \\ &\quad + tr[(S_{N-1} + S_N) Q] + tr(\Phi_{N-1} P_{N-1}^-). \end{aligned}$$

Similarly, we take the derivative of the term containing u_{N-2} in the above result and let it be zero:

$$2(U + B' S_{N-1} B) u_{N-2}^* + 2B' S_{N-1} A \hat{x}_{N-2} = 0,$$

which leads to

$$u_{N-2}^* = -(U + B' S_{N-1} B)^{-1} B' S_{N-1} A \hat{x}_{N-2}.$$

Substituting it into the above equation, we obtain

$$\begin{aligned} J_{N-2:N} &= \mathbf{E} [x'_{N-2} (A' S_{N-1} A + W) x_{N-2} | I_{N-2}] \\ &\quad + tr[(S_{N-1} + S_N) Q] + tr(\Phi_{N-1} P_{N-1}^-) \\ &\quad - x'_{N-2} A' S_{N-1} B (U + B' S_{N-1} B)^{-1} B' S_{N-1} A \hat{x}_{N-2}. \end{aligned}$$

Let

$$\begin{aligned}\Phi_{N-2} &= A'S_{N-1}B(U + B'S_{N-1}B)^{-1}B'S_{N-1}A, \\ S_{N-2} &= A'S_{N-1}A + W - \Phi_{N-2}.\end{aligned}$$

Then

$$\begin{aligned}J_{N-2:N} &= \mathbf{E}\left[x'_{N-2}S_{N-2}x_{N-2}|I_{N-2}\right] + \mathbf{E}\left[x'_{N-2}\Phi_{N-2}x_{N-2}|I_{N-2}\right] \\ &\quad - \hat{x}'_{N-2}\Phi_{N-2}\hat{x}_{N-2} + tr\left[(S_{N-1} + S_N)Q\right] + tr(\Phi_{N-1}P_{N-1}^-) \\ &= \mathbf{E}\left[x'_{N-2}S_{N-2}x_{N-2}|I_{N-2}\right] + tr\left[(S_{N-1} + S_N)Q\right] \\ &\quad + tr(\Phi_{N-1}P_{N-1}^-) + tr(\Phi_{N-2}P_{N-2}).\end{aligned}$$

Similarly, for any time k , we have

$$\begin{aligned}\Phi_k &= A'S_{k+1}B(U + B'S_{k+1}B)^{-1}B'S_{k+1}A, \\ S_N &= W, \\ S_k &= A'S_{k+1}A + W - \Phi_k, \\ L_k &= -(B'S_{k+1}B + U)^{-1}B'S_{k+1}A, \\ u_k^* &= L_k\mathbf{E}[x_k|I_k].\end{aligned}$$

Then the optimal objective function at time k is

$$J_{k:N} = \mathbf{E}(x'_k S_k x_k | I_k) + r_k + t_k,$$

where

$$\begin{aligned}r_N &= 0, \\ r_k &= r_{k+1} + tr(S_{k+1}Q), \\ t_N &= 0, \\ t_k &= \begin{cases} t_{k+1} + tr(\Phi_k P_k^-), & k \neq 2l+1, \\ t_{k+1} + tr(\Phi_k P_k), & k = 2l+1. \end{cases}\end{aligned}$$

Hence, the optimal objective function is

$$\begin{aligned}J_{0:N} &= \mathbf{E}(x'_0 S_0 x_0) + \sum_{k=0}^{N-1} tr(S_{k+1}Q) \\ &\quad + \sum_{k \neq 2l+1, k \in [0, N-1]} tr(\Phi_k P_k^-) + \sum_{k=2l+1, k \in [0, N-1]} tr(\Phi_k P_k).\end{aligned}$$

After straightforward calculation we can see that, for other values of T , the similar conclusions can also be drawn through the similar proof steps. For general T , we have

$$\begin{aligned}J_{0:N} &= \mathbf{E}(x'_0 S_0 x_0) + \sum_{k=0}^{N-1} tr(S_{k+1}Q) \\ &\quad + \sum_{k \neq lT+1, k \in [0, N-1]} tr(\Phi_k P_k^-) + \sum_{k=lT+1, k \in [0, N-1]} tr(\Phi_k P_k).\end{aligned}$$

Under the infinite-time horizon, we have

$$\mathcal{O}^* = \lim_{N \rightarrow \infty} \frac{1}{N} J_{0:N}.$$

According to eqn. (26) and the above equations, we can write $\mathcal{O}^*$ as

$$\mathcal{O}^* = tr(SQ) + tr\left(\Phi \frac{1}{T} \sum_{i=0}^{T-1} h^i(\tilde{P})\right).$$

ACKNOWLEDGMENT

The work by Wen Yang and Chao Yang is supported by the National Natural Science Foundation of China under Grant 62336005.

The work by Yuqing Ni is supported by the National Natural Science Foundation of China under Grant 62303196, the Natural Science Foundation of Jiangsu Province of China under Grant BK20231036, and the Basic Research Funds of Wuxi Taihu Light Project under Grant K20221005.

REFERENCES

- [1] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.
- [2] T. K. Mendhe, P. Kamble, and A. K. Thakre, "Survey on security, storage, and networking of cloud computing," *International Journal on Computer Science and Engineering*, vol. 4, no. 11, p. 1780, 2012.
- [3] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2013.
- [4] E. Nekouei, T. Tanaka, M. Skoglund, and K. H. Johansson, "Information-theoretic approaches to privacy in estimation and control," *Annual Reviews in Control*, vol. 47, pp. 412–422, 2019.
- [5] X. Yi, R. Paulet, E. Bertino, X. Yi, R. Paulet, and E. Bertino, *Homomorphic encryption*, 2014.
- [6] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*, 2006, pp. 1–12.
- [7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography: Third Theory of Cryptography Conference. Proceedings 3*, 2006, pp. 265–284.
- [8] Y. Kawano, K. Kashima, and M. Cao, "A fundamental performance limit of cloud-based control in terms of differential privacy level," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 11 018–11 023, 2020.
- [9] J. Le Ny and M. Mohammady, "Differentially private MIMO filtering for event streams," *IEEE Transactions on Automatic Control*, vol. 63, no. 1, pp. 145–157, 2017.
- [10] 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, 2023.
- [11] K. H. Degue and J. Le Ny, "Cooperative differentially private LQG control with measurement aggregation," *IEEE Control Systems Letters*, vol. 7, pp. 1093–1098, 2023.
- [12] M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep learning with differential privacy," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 308–318.
- [13] A. Friedman and A. Schuster, "Data mining with differential privacy," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2010, pp. 493–502.
- [14] T. Ding, S. Zhu, C. Chen, J. Xu, and X. Guan, "Differentially private distributed resource allocation via deviation tracking," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 222–235, 2021.
- [15] F. Gauthier, V. C. Gogineni, S. Werner, Y.-F. Huang, and A. Kuh, "Personalized graph federated learning with differential privacy," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 9, pp. 736–749, 2023.
- [16] P. Hao and X. Wang, "Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 5, no. 4, pp. 792–806, 2019.
- [17] E. Nekouei, H. Sandberg, M. Skoglund, and K. H. Johansson, "Privacy-aware minimum error probability estimation: An entropy constrained approach," *arXiv preprint arXiv:1808.02271*, 2018.
- [18] R. Jia, R. Dong, S. S. Sastry, and C. J. Spanos, "Privacy-enhanced architecture for occupancy-based hvac control," in *Proceedings of the 8th international conference on cyber-physical systems*, 2017, pp. 177–186.
- [19] E. Nekouei, M. Skoglund, and K. H. Johansson, "Privacy of information sharing schemes in a cloud-based multi-sensor estimation problem," in *2018 annual american control conference (ACC)*, 2018, pp. 998–1002.
- [20] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 4–21, 2003.

- [21] T. Tanaka, M. Skoglund, H. Sandberg, and K. H. Johansson, "Directed information and privacy loss in cloud-based control," in *2017 American Control Conference (ACC)*, 2017, pp. 1666–1672.
- [22] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 6836–6843.
- [23] A. B. Alexandru and G. J. Pappas, "Encrypted LQG using labeled homomorphic encryption," in *Proceedings of the 10th ACM/IEEE international conference on cyber-physical systems*, 2019, pp. 129–140.
- [24] F. Farokhi, I. Shames, and N. Batterham, "Secure and private cloud-based control using semi-homomorphic encryption," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 163–168, 2016.
- [25] M. Faiz, N. Fatima, R. Sandhu, M. Kaur, and V. Narayan, "Improved homomorphic encryption for security in cloud using particle swarm optimization," *Journal of Pharmaceutical Negative Results*, pp. 4761–4771, 2022.
- [26] B. D. Anderson and J. B. Moore, *Optimal filtering*, 2012.
- [27] D. Bertsekas, *Dynamic programming and optimal control: Volume I*, 2012, vol. 4.