Automatica 122 (2020) 109283

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems☆

Xiao-Kang Liu [a], Ji-Feng Zhang [b,c,*], Jimin Wang [b,c]

[a] School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan, 430074, China
[b] Key Laboratory of Systems and Control, Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
[c] School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100149, China

ARTICLE INFO

Article history:
Received 18 October 2019
Received in revised form 7 May 2020
Accepted 6 August 2020
Available online xxxx

Keywords:
Multi-agent systems
Networked control systems
Differential privacy

ABSTRACT

This paper investigates the differential private algorithm for the average output consensus control of continuous-time heterogeneous systems. A distributed hybrid controller is designed where agents exchange information at discrete time instants. The proposed controller protects the individual privacy by imposing random noises upon the interactive information. Based on the stochastic approximation method, we employ a series of time-varying control gains to relax the existing mechanisms which require the privacy noises to be exponentially decaying with time. Using non-decaying privacy noises, the delivered information can keep random with an invariant variance, and the real information cannot be directly exposed to the eavesdropper along with time. We further develop a method to design the control gain such that the heterogeneous systems can achieve asymptotically unbiased output average consensus with the desired accuracy and meet the predefined differential privacy index. Finally, a numerical example is provided to demonstrate the effectiveness of the theoretical results.

1. Introduction

Distributed cooperative control of multi-agent systems (MAS) is of great significance as it is widely used in many real applications, such as energy management (Zhang & Chow, 2012), data fusion and falsification (Kailkhura, Brahma, & Varshney, 2017), distributed Kalman filter (Li, Wei, Han, & Liu, 2016), etc. Among others, average consensus control of MAS is a fundamental problem, where it supposes that agents can converge to the average of their initial states via a communication network. So far, a number of works have been developed on the average consensus control of MAS (Olfati-Saber & Murray, 2004; Pasqualetti, Borra, & Bullo, 2014; Zhao, Liu, Li, & Duan, 2017; Zhu & Martínez, 2010), including continuous-time MAS and discrete-time MAS. However, with the increasing need of security and reliability, privacy-preservation of individual dataset is required in many application sceneries (Li, Ma, & Fu, 2015; Ren, Xu, Yang, & Yang, 2019). For example, in a social network (Amelkin, Bullo, & Singh, 2017), people interact with their neighbors and evaluate their opinions by comparison with the opinions of others, but exchanging opinions probably reveals individual privacy. Another example is the cooperative guidance system (Kang, Wang, Li, Shan, & Petersen, 2018), where information interactions may expose the locations of missiles, as well as, the launch stations. It naturally arises a problem that how to achieve average consensus while protecting the information of each agent from being detected by a third malicious party.

To address the problem, one solution is encrypting the interactive information, with approaches like homomorphic encryption (Ruan, Gao, & Wang, 2019). However, cryptographic techniques are often computationally expensive, especially when the calculation resource of each agent is limited. An alternative solution is imposing randomness upon the information (Fung, Wang, Chen, & Yu, 2010). Recently, differential privacy techniques have been widely considered on the publishing data in many technology companies, such as Google and Apple. Based on the original definition given by Dwork (2006), ϵ-differential privacy has been extended to multi-agent scenario, including protecting the initial states of agents in consensus problem (Huang, Mitra, & Dullerud, 2012) and protecting the global state trajectories in Kalman filter (Le Ny & Mohammady, 2018; Le Ny & Pappas, 2014). From a systems and control perspective, Cortés, et al. (2016)

☆ The work was supported by the National Key R&D Program of China under Grant 2018YFA0703800, and by the National Natural Science Foundation of China under Grant 61877057. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Vijay Gupta under the direction of Editor Christos G. Cassandras.

* Corresponding author at: Key Laboratory of Systems and Control, Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China.
E-mail addresses: xkliuhust@hotmail.com (X.-K. Liu), jif@iss.ac.cn (J.-F. Zhang), jimin.wang@amss.ac.cn (J. Wang).

https://doi.org/10.1016/j.automatica.2020.109283
0005-1098/

gave a tutorial and comprehensive framework of differential privacy analysis on dynamical systems. By adding *uncorrelated noises* on information, Nozari, Tallapragada, and Cortés (2017) designed a differentially private consensus algorithm for single-order discrete-time multi-agent systems, where agents achieved unbiased convergence to the average almost surely. Wang, Huang, Mitra, and Dullerud (2017) designed an ϵ-differentially private consensus algorithm for linear discrete-time coupled dynamic systems. Fiore and Russo (2019) combined differential privacy and resilient consensus algorithm in a multi-agent system over a directed communication topology. Gao, Deng, and Ren (2019) proposed an event-triggered scheme to reduce the control updates while also keeping the algorithm to be ϵ-differentially private. By adding *correlated noises* on interaction information, accurate consensus can be achieved (He, Cai, Cheng, Pan & Shi, 2019; He, Cai, Zhao, Cheng & Guan, 2019; Mo & Murray, 2017) while protecting the initial states from neighboring agents. However, if the eavesdropper can obtain all the information received and delivered by node i, then the initial state of this agent can be estimated by an iterative observer under the correlated noises mechanism. Overall, the above literature has two common grounds: (1) all the algorithms are designed for discrete-time multi-agent systems; (2) in order to guarantee the convergence and satisfy the differential privacy index, the privacy noise is required to decay exponentially with time. Many practical plants reveal continuous-time dynamics and it is often the case that they are inherently heterogeneous with different dimensions and dynamics. (Chen & Chen, 2017; Lewis, Cui, Ma, Song, & Zhao, 2016; Su & Huang, 2012; Wang, Liu, Xiao, & Shen, 2018). In addition, decaying noises potentially expose the trajectory of state. These factors motivate us to investigate the privacy-preserving algorithm of continuous-time heterogeneous MAS and relax limitation of using exponentially decaying privacy noises.

In this paper, we design a distributed hybrid dynamic feedback controller based on the hierarchical control framework, where the upper layer aims to achieve consensus of reference states and the lower layer drives the agent to track its reference. Specifically, each agent imposes a Laplace noise on local reference state and then transmits it to neighbors at discrete-time instants. The added noises are i.i.d. with a bounded variance. If the control gain β_k satisfies the stochastic approximation condition, namely, $\sum_{k=0}^{\infty}\beta_k = \infty$, $\sum_{k=0}^{\infty}\beta_k^2 < \infty$ and other gain matrices are in certain forms, then the heterogeneous multi-agent systems (HMAS) can achieve asymptotically unbiased mean square output average consensus. In summary, the contributions of this paper are threefold:

(1) Compared with existing literature that focuses on discrete-time systems, we develop a differentially private consensus algorithm for continuous-time HMAS. By introducing a discrete-time interaction scheme, we design a distributed hybrid dynamic feedback controller, which receives discrete-time information from neighbors and enables the privacy analysis for continuous-time HMAS by the existing tools and techniques on discrete-time systems;
(2) The privacy noises in existing literature are required to decay exponentially with time. Based on the stochastic approximation method, we employ a time-varying control gain to relax this limitation. Moreover, the adding non-decaying noises also avoid directly exposing the information of reference state;
(3) Compared to the existing works on consensus of MAS with communication noises (Li & Zhang, 2010), we present a guideline on how to design the time-varying control gain such that HMAS can achieve asymptotically unbiased output average consensus with the desired accuracy and the predefined differential privacy index.

This paper is organized as follows. Preliminaries and the problem statement are given in Section 2. Distributed differentially private algorithm with convergence and privacy analysis is presented in Section 3. The numerical examples are given in Section 4 and the conclusions are drawn in Section 5.

Notation. Denote $\mathbb{R}$, $\mathbb{R}_{>0}$ as the set of the real number and positive real number, respectively. Denote $\mathbb{R}^{n\times m}$ as the set of $n\times m$ real matrix. I_n represents $n\times n$ identity matrix and $\mathbf{1}_n$ is an n-dimension column vector with all elements being 1. The notation $\otimes$ stands for Kronecker product. The notation $\mathrm{col}(x_1,\ldots,x_N)$ stands for a column vector by stacking them together. The notation $\mathrm{diag}(b_1,\ldots,b_N)$ denotes the diagonal matrix with diagonal elements being $b_1,\ldots,b_N$. The notation $\|\cdot\|$ is the 2-norm for a vector or a matrix. For a matrix A, denote $\mathcal{H}(A)=A^TA$, and the notation $\rho(A)$ is the spectral radius of A. For a random variable $X\in\mathbb{R}$, $\mathbb{E}[X]$ and $\mathrm{Var}(X)$ denotes the expectation and variance of X. For a random vector $Y\in\mathbb{R}^n$, the notation $cov(Y)$ denotes the covariance matrix of Y. $\mathrm{Lap}(\mu,b)$ denotes the Laplace distribution. $\Gamma(x)=\int_0^{+\infty}t^{x-1}e^{-t}dt$ is the gamma function and $\Gamma(x,z)=\int_z^{+\infty}t^{x-1}e^{-t}dt$ is the upper incomplete gamma function.

2. Preliminaries

2.1. Graph theory

Denote $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$ as a directed graph with a set of nodes $\mathcal{V}=\{1,2,\ldots,N\}$, a set of edges $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ and a weighted adjacency matrix $\mathcal{A}=\left(a_{ij}\right)_{N\times N}$. Node i represents the ith system and an edge e_{ji} in graph is denoted by the ordered pair nodes $\{j,i\}$. $\{j,i\}\in\mathcal{E}$ if and only if node i can obtain the information from node j. A path in graph $\mathcal{G}$ is an ordered sequence $v_1,v_2,\ldots,v_k$ of nodes such that any ordered pair of vertices appearing consecutively in the sequence is an edge of the graph, i.e., (v_i,v_{i+1}), for any $i=1,2,\ldots,k-1$. For the adjacency matrix $\mathcal{A}$, $a_{ij}>0$ if $\{j,i\}\in\mathcal{E}$, and $a_{ij}=0$ otherwise. We assume there is no self-loop in the graph $\mathcal{G}$, i.e., $a_{ii}=0$. Define $N_i=\{j|a_{ij}>0\}$ as the set of agent i's neighbors. The Laplacian matrix $\mathcal{L}=(l_{ij})_{N\times N}$ of graph $\mathcal{G}$ is defined as $l_{ij}=-a_{ij}$ if $i\neq j$, otherwise $l_{ij}=\sum_{k=1,k\neq i}^{N}a_{ik}$. Denote $\Delta_i^{in}=\sum_j a_{ij}$ and $\Delta_i^{out}=\sum_j a_{ji}$ as in-degree and out-degree of node i in the directed graph $\mathcal{G}$. A digraph is balanced if $\Delta_i^{in}=\Delta_i^{out}:=\Delta_i$ for $\forall i\in\mathcal{V}$. For a balanced digraph, we define the greatest degree and the smallest degree as $\Delta_{\max}=\max\{\Delta_i,i\in\mathcal{V}\}$ and $\Delta_{\min}=\min\{\Delta_i,i\in\mathcal{V}\}$.

2.2. Problem statement

Consider a set of N continuous-time heterogeneous linear systems coupled by a communication graph $\mathcal{G}$. The dynamics of the ith system is described by

$$\begin{cases}\dot{x}_i(t)=A_ix_i(t)+B_iu_i(t),\\ y_i(t)=C_ix_i(t),\end{cases}\tag{1}$$

where $A_i\in\mathbb{R}^{n_i\times n_i}$, $B_i\in\mathbb{R}^{n_i\times r_i}$, $C_i\in\mathbb{R}^{p\times n_i}$ are matrices in appropriate dimensions, $x_i\in\mathbb{R}^{n_i}$ is the system state, $y_i\in\mathbb{R}^p$ and $u_i\in\mathbb{R}^{r_i}$ are measurement output and control input of the ith system.

Definition 2.1. Heterogeneous systems (1) are said to achieve the average output consensus if for any $i\in\mathcal{V}$, it holds that $\lim_{k\to\infty}y_i(k)=\frac{1}{N}\sum_{i\in\mathcal{V}}y_i(0)$.

For the above coupled dynamical systems, we need following assumptions.

Assumption 2.1. (A_i,B_i) is stabilizable.

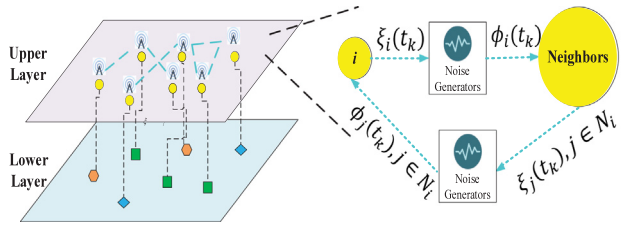


Fig. 1. Hierarchical control framework for HMAS.

Assumption 2.2. For any $i \in \mathcal{V}$, there exists a solution (Π_i, U_i) of the following matrix equation

$$\begin{cases} \mathbf{0} = A_i\Pi_i + B_iU_i, \\ C_i\Pi_i = I_{p\times p}. \end{cases} \tag{2}$$

Assumption 2.3. The digraph $\mathcal{G}$ is balanced and strongly connected.

Remark 2.1. Under Assumption 2.1, there exists a matrix K_i such that $A_i + B_iK_i$ is Hurwitz. The matrix equation (2) in Assumption 2.1 is a typical linear output regulation equation (Su & Huang, 2012). Note that there exists a solution for the matrix equation (2) if and only if

$$rank\begin{bmatrix} A_i & B_i \\ C_i & 0 \end{bmatrix} = n_i + p.$$

Assumption 2.3 describes the connectivity of a digraph and is standard in the average consensus (Olfati-Saber & Murray, 2004). Under Assumption 2.3, we have $1_N^T\mathcal{L} = 0$ and all the eigenvalues of $\bar{\mathcal{L}} \triangleq \frac{\mathcal{L}+\mathcal{L}^T}{2}$ are nonnegative.

To achieve average output consensus of heterogeneous systems (1), generally, we can design a dynamic feedback controller

$$\begin{cases} \dot{\xi}_i(t) = \beta\sum\limits_{j\in N_i}\left(\xi_j(t) - \xi_i(t)\right), \\ u_i(t) = K_{1i}x_i(t) + K_{2i}\xi_i(t), \end{cases} \tag{3}$$

where $\xi_i(t) \in \mathbb{R}^p$ is the reference state with the initial value $\xi_i(0) = y_i(0)$, $K_{1i} \in \mathbb{R}^{r_i\times n_i}$, $K_{2i} \in \mathbb{R}^{r_i\times p}$ are gain matrices, and β is the control parameter.

Remark 2.2. The above controller (3) directly results from Su and Huang (2012) and facilitates average output consensus of HMAS. However, the controller transmits a continuous-time signal, say $\xi_i(t)$. For each agent, delivering $\{\xi_i(t)|t \in \mathbb{R}_{\geq 0}\}$ is very likely to expose its privacy, including the reference trajectory $\xi_i(t)$ and the initial position $y_i(0)$.

Considering that the existing privacy analysis tools are feasible for discrete-time sequences, we introduce a discrete-time interaction scheme and noise generators to deal with continuous-time dynamical systems, as shown in Fig. 1. HMAS only interacts the information at discrete-time instants, denoted as $\mathcal{T}_s = \{t_0, t_1, t_2, \ldots, t_k, \ldots\}$ with $t_0 = 0$ and $t_{k+1} - t_k = h_k \geq h_{\min}$, where $h_{\min} > 0$ is the lower bound of time interval between two adjacent information interactions. In the hierarchical framework, each agent is allowed to transmit data via the communication network only at discrete time instants $\mathcal{T}_s$. With the penetration of noise generators, the original coupled system turns to be a stochastic coupled system. Below we introduce the definition of asymptotically unbiased mean square output average consensus and ϵ-DP for the distributed controller of continuous-time HMAS.

Definition 2.2. For $s \in [0, 1]$ and $r \in \mathbb{R}_{\geq 0}$, heterogeneous systems (1) are said to achieve asymptotically unbiased mean square output average consensus with (s, r)-accuracy, if for any given $y(0) \in \mathbb{R}^{Np}$, there is a random vector $y^\star$, such that $\mathbb{E}[y^\star] = \frac{1}{N}\sum_{i=1}^N y_i(0)$, $\|cov(y^\star)\|$ is bounded, $\lim_{t\to\infty}\mathbb{E}[\|y_i(t) - y^\star\|^2] = 0$ for $i \in \mathcal{V}$, and $\mathbb{P}\{\|y^\star - \frac{(1_N^T\otimes I_p)y(0)}{N}\| < r\} \geq 1 - s$.

We suppose that the eavesdropper has access to all the interaction information through the communication network. Denote $\mathcal{M}(\cdot)$ as a stochastic map from a private dataset D to an observation O. In this paper, we focus on protecting the privacy information of initial states against an external eavesdropper. Thus, the private dataset is $D = \{y_i(0), i \in \mathcal{V}\}$, and the observation set is $O = \{\phi_i(t_k), i \in \mathcal{V}, k = 0, 1, \ldots, T-1\}$. Then, ϵ-differential privacy for the private dataset is introduced.

Definition 2.3 (*Cortés, et al., 2016*)**.** Given a time horizon $T > 0$ and a parameter $\epsilon > 0$, a randomized mechanism $\mathcal{M} : D \to O$ is said to be ϵ-differentially private up to time $T - 1$, if for any subset $\mathcal{O} \subseteq \mathbb{R}^{pNT}$ and any two datasets D and D', it holds that

$$\mathbb{P}[\mathcal{M}(D) \in \mathcal{O}] \leq e^{\epsilon\|D-D'\|_1}\mathbb{P}[\mathcal{M}(D') \in \mathcal{O}]. \tag{4}$$

We call a mechanism $\mathcal{M}$ is ϵ-differentially private over the infinite time horizon if (4) holds for $T \to \infty$. Overall, given a pre-desired privacy index $\epsilon^\star$ and a pair of accuracy indexes $(s^\star, r^\star)$, the objective of this paper is to design a distributed protocol $u_i(t)$ and noise generators over the discrete-time sequence $\mathcal{T}_s$ such that HMAS can achieve asymptotically unbiased mean square output average consensus with $(s^\star, r^\star)$-accuracy and keep $\epsilon^\star$-differentially private over the infinite time horizon.

3. Differentially private consensus

3.1. Hybrid controller design

The distributed hybrid controller $u_i(t)$ is designed as

$$\begin{cases} u_i(t) = K_{1i}x_i(t) + K_{2i}\xi_i(t), \\ \dot{\xi}_i(t) = 0, \quad \text{for } t \in (t_k, t_{k+1}) \\ \xi_i(t_k) = \xi_i(t_k^-) + \beta_{k-1}\sum\limits_{j\in N_i}\left(\phi_j(t_k^-) - \xi_i(t_k^-)\right), k \in \mathbb{N}_{>0} \end{cases} \tag{5}$$

with the noise generator as

$$\begin{cases} \phi_i(t_k^-) = \xi_i(t_k^-) + \eta_i(t_k^-), \\ \eta_{i,l}(t_k^-) \sim \text{Lap}(0, b), \ l \in \{1, 2, \ldots, p\}, k \in \mathbb{N}_{>0} \end{cases} \tag{6}$$

where β_k is a positive time-varying control gain; $K_{2i} = U_i - K_{1i}\Pi_i$ with U_i and Π_i satisfying (2); $\xi_i(t)$ is the reference state with $\xi_i(0) = y_i(0)$, and note that $\xi_i(t)$ is right continuous at time t_k, thus $\lim_{t\to t_k^+}\xi_i(t) = \xi_i(t_k)$; $\eta_i(t_k^-) \in \mathbb{R}^p, i \in \mathcal{V}$ is a random vector with each entry to be i.i.d. Laplace distribution, of which the covariance matrix is $2b^2I_p$. For $\forall i, j \in \mathcal{V}$, $i \neq j$, $\eta_i(t_k^-)$ and $\eta_j(t_k^-)$ are mutually independent. Define the σ-algebra $\bar{\mathcal{F}}_k^\eta = \sigma\{\eta(t_1^-), \eta(t_2^-), \ldots, \eta(t_k^-)\}$ where $\eta(t) = \text{col}(\eta_1(t), \eta_2(t), \ldots, \eta_N(t))$, and we have that $\{\eta(t_k^-), \bar{\mathcal{F}}_k^\eta, k \in \mathbb{N}_{>0}\}$ is a martingale difference sequences and $\sigma_\eta^2 \triangleq \sup_{k\in\mathbb{N}_{>0}}\mathbb{E}\left[\|\eta(t_k^-)\|^2\right] < \infty$.

Remark 3.1. The privacy noise used in this paper always keeps random with the covariance matrix $2b^2I_p$, which is not required to decay to zero as in the existing literature. This results in the information of reference state not being directly inferred with time. Another point worth noting is that we use a time-varying control gain β_k, which makes the controller more flexible than that with a constant.

Denote $A = \mathrm{diag}(A_1, \ldots, A_N)$, $B = \mathrm{diag}(B_1, \ldots, B_N)$, $K_1 = \mathrm{diag}(K_{11}, \ldots, K_{1N})$, $\Pi = \mathrm{diag}(\Pi_1, \ldots, \Pi_N)$, $U = \mathrm{diag}(U_1, \ldots, U_N)$, and define $\tilde{\xi}_i(t) = \xi_i(t) - \frac{1}{N}\sum \xi_i(t)$, $x_{ci}(t) = x_i(t) - \Pi_i \xi_i(t)$, $\tilde{\xi} = \mathrm{col}(\tilde{\xi}_1, \ldots, \tilde{\xi}_N)$, and $x_c = \mathrm{col}(x_{c1}, \ldots, x_{cN})$. Then, substituting (5) and (6) to the dynamics (1) yields:

For $t \in (t_k, t_{k+1})$, $k \in \mathbb{N}_{\geq 0}$, we have $\dot{\tilde{\xi}}(t) = 0$. Under Assumption 2.2 and $K_{2i} = U_i - K_{1i}\Pi_i$, it holds that

$$\begin{aligned}\dot{x}_c(t) &= \dot{x}(t) - \Pi\dot{\xi}(t) = Ax(t) + Bu(t) + \mathbf{0}\\ &= (A + BK_1)x(t) + B(U - K_1\Pi)\xi(t)\\ &= (A + BK_1)x_c(t) + [(A + BK_1)\Pi + B(U - K_1\Pi)]\xi(t)\\ &= (A + BK_1)x_c(t). \end{aligned} \tag{7}$$

For $t = t_k$, $k \in \mathbb{N}_{>0}$, we have

$$\xi(t_k) = \left[(I_N - \beta_{k-1}\mathcal{L}) \otimes I_p\right]\xi(t_k^-) + \beta_{k-1}(\mathcal{A} \otimes I_p)\eta(t_k^-).$$

Then, defining $J = I_N - \mathbf{1}\mathbf{1}^T/N$ yields

$$\begin{aligned}\tilde{\xi}(t_k) &= \left(J \otimes I_p\right)\xi(t_k)\\ &= \left[J - \beta_{k-1}\mathcal{L}) \otimes I_p\right]\tilde{\xi}(t_k^-) + \beta_{k-1}(J\mathcal{A} \otimes I_p)\eta(t_k^-), \end{aligned} \tag{8}$$

and

$$\begin{aligned}x_c(t_k) =& x(t_k) - \Pi\xi(t_k)\\ =& x(t_k^-) - \Pi\left\{\left[(I_N - \beta_{k-1}\mathcal{L}) \otimes I_p\right]\xi(t_k^-) + \beta_{k-1}(\mathcal{A} \otimes I_p)\eta(t_k^-)\right\}\\ =& x_c(t_k^-) + \Pi\beta_{k-1}(\mathcal{L} \otimes I_p)\tilde{\xi}(t_k^-) - \beta_{k-1}\Pi(\mathcal{A} \otimes I_p)\eta(t_k^-). \end{aligned} \tag{9}$$

Note that the last equation of (9) holds because $(\mathcal{L} \otimes I_p)(J \otimes I_p) = (\mathcal{L} \otimes I_p)$ and $\tilde{\xi}(t_k^-) = (J \otimes I_p)\xi(t_k^-)$. Therefore, the closed-loop system with respect to $\tilde{\xi}(t)$ and $x_c(t)$ can be represented in a compact form as

$$\begin{cases} \dot{\tilde{\xi}}(t) = 0, \quad \text{for } t \in (t_k, t_{k+1})\\ \tilde{\xi}(t_k) = \left[(I_N - \beta_{k-1}\mathcal{L} - \mathbf{1}\mathbf{1}^T/N) \otimes I_p\right]\tilde{\xi}(t_k^-)\\ \qquad\qquad + \left[(\beta_{k-1}J\mathcal{A}) \otimes I_p\right]\eta(t_k^-), \ k \in \mathbb{N}_{>0}\\ \dot{x}_c(t) = (A + BK_1)x_c(t), \quad \text{for } t \in (t_k, t_{k+1})\\ x_c(t_k) = x_c(t_k^-) + \beta_{k-1}\Pi(\mathcal{L} \otimes I_p)\tilde{\xi}(t_k^-)\\ \qquad\qquad - \beta_{k-1}\Pi(\mathcal{A} \otimes I_p)\eta(t_k^-), \ k \in \mathbb{N}_{>0}. \end{cases} \tag{10}$$

Denoting $\hat{A} = A + BK_1$, it follows from (10) that $\tilde{\xi}(t_{k+1}^-) = \tilde{\xi}(t_k)$, $x_c(t_{k+1}^-) = e^{\hat{A}h_k}x_c(t_k)$, and

$$\begin{cases} \tilde{\xi}(t_{k+1}) = \left[(I_N - \beta_k\mathcal{L} - \mathbf{1}\mathbf{1}^T/N) \otimes I_p\right]\tilde{\xi}(t_k)\\ \qquad\qquad + \left[(\beta_k J\mathcal{A}) \otimes I_p\right]\eta(t_{k+1}^-)\\ x_c(t_{k+1}) = e^{\hat{A}h_k}x_c(t_k) + \beta_k\Pi(\mathcal{L} \otimes I_p)\tilde{\xi}(t_k)\\ \qquad\qquad - \beta_k\Pi(\mathcal{A} \otimes I_p)\eta(t_{k+1}^-), \ k \in \mathbb{N}_{\geq 0}. \end{cases} \tag{11}$$

Note that if setting β_k to be constant as in existing literature, the above closed-loop system cannot achieve asymptotically unbiased convergence. This is because the influence of privacy noises (6) will not vanish to zero. To this end, we apply the stochastic approximation method to design a time-varying control gain and then give convergence and privacy analysis.

3.2. Convergence analysis

In this subsection, we first prove the output of each heterogeneous system converges to the average of inner controller states in mean square. Then, we further prove that HMAS can achieve asymptotically unbiased mean square output average consensus.

Lemma 3.1 (*Polyak, 1987*). *Let* $\{u(k), k = 0, 1, \ldots\}$, $\{\alpha(k), k = 0, 1, \ldots\}$ *and* $\{q(k), k = 0, 1, \ldots\}$ *be real sequences, satisfying* $0 < q(k) \leq 1$, $\alpha(k) \geq 0$, $k = 0, 1, \ldots$, $\sum_{k=0}^{\infty} q(k) = \infty$, $\alpha(k)/q(k) \to 0$, $k \to \infty$, *and*

$$u(k+1) = (1 - q(k))u(k) + \alpha(k).$$

Then $\limsup_{k\to\infty} u(k) \leq 0$. *In particular, if* $u(k) \geq 0$, $k = 0, 1, \ldots$, *then* $u(k) \to 0$, $k \to \infty$.

Theorem 3.1. *Apply the distributed hybrid controller (5) and noise generator (6) to heterogeneous multi-agent systems (1). If Assumptions 2.1–2.3 hold and* $A_i + B_iK_{1i}$ *is Hurwitz,* $\sum_{k=0}^{\infty}\beta_k = \infty$, $\sum_{k=0}^{\infty}\beta_k^2 < \infty$, *then*

$$\lim_{t\to\infty}\mathbb{E}\left\|y(t) - \frac{1}{N}(\mathbf{1}_N\mathbf{1}_N^T \otimes I_p)\xi(t)\right\|^2 = 0. \tag{12}$$

Proof. Defining $V_1(k) = \tilde{\xi}^T(t_k)\tilde{\xi}(t_k)$ and $V_2(k) = x_c^T(t_k)x_c(t_k)$, it takes from (11) that

$$\begin{aligned} V_1(k+1) &= \tilde{\xi}^T(t_{k+1})\tilde{\xi}(t_{k+1})\\ &= \tilde{\xi}^T(t_k)\left[(I_N - \beta_k(\mathcal{L}^T + \mathcal{L}) + \beta_k^2\mathcal{L}^T\mathcal{L}) \otimes I_p\right]\tilde{\xi}(t_k)\\ &\quad + 2\tilde{\xi}^T(t_k)\left[(I_N - \beta_k\mathcal{L} - \mathbf{1}\mathbf{1}^T/N) \otimes I_p\right]^T\left[(\beta_k J\mathcal{A}) \otimes I_p\right]\eta(t_{k+1}^-)\\ &\quad + \beta_k^2\eta^T(t_{k+1}^-)\left[(\mathcal{A}^T J^T J\mathcal{A}) \otimes I_p\right]\eta(t_{k+1}^-), \end{aligned} \tag{13}$$

and

$$\begin{aligned} V_2(k+1) &= x_c^T(t_{k+1})x_c(t_{k+1})\\ &= x_c^T(t_k)\mathcal{H}(e^{\hat{A}h_k})x_c(t_k) + \beta_k^2\tilde{\xi}^T(t_k)\mathcal{H}\left(\Pi(\mathcal{L} \otimes I_p)\right)\tilde{\xi}(t_k)\\ &\quad + \beta_k^2\eta^T(t_{k+1}^-)\mathcal{H}\left(\Pi(\mathcal{A} \otimes I_p)\right)\eta(t_{k+1}^-)\\ &\quad - 2\beta_k x_c^T(t_k)\left[e^{\hat{A}^T h_k}\Pi(\mathcal{A} \otimes I_p)\right]\eta(t_{k+1}^-)\\ &\quad + 2\beta_k x_c^T(t_k)\left[e^{\hat{A}^T h_k}\Pi(\mathcal{L} \otimes I_p)\right]\tilde{\xi}(t_k)\\ &\quad - 2\beta_k^2\tilde{\xi}^T(t_k)\left[(\mathcal{L}^T \otimes I_p)\Pi^T\Pi(\mathcal{A} \otimes I_p)\right]\eta(t_{k+1}^-). \end{aligned} \tag{14}$$

Define σ-algebra $\mathcal{F}_k^\eta = \sigma\{\xi(t_0), \eta(t_1^-), \eta(t_2^-), \ldots, \eta(t_k^-)\}$, and we have $\xi(t_k) \in \mathcal{F}_k^\eta$ from (10). By $\tilde{\xi}(t_k) = (J \otimes I_p)\xi(t_k)$, it holds that $\tilde{\xi}(t_k) \in \mathcal{F}_k^\eta$. Thus, $\tilde{\xi}(t_k)$ and $\eta(t_{k+1}^-)$ are independent. Taking conditional expectation with respect to $\mathcal{F}_k^\eta$ at both sides of the above equations yields that

$$\begin{aligned}\mathbb{E}\left[V_1(k+1)|\mathcal{F}_k^\eta\right] \leq& \left(1 - 2\beta_k\lambda_2(\bar{\mathcal{L}}) + \beta_k^2\|\mathcal{L}\|^2\right)\tilde{\xi}^T(t_k)\tilde{\xi}(t_k)\\ &+\beta_k^2\|J\mathcal{A}\|^2\mathbb{E}\left[\eta^T(t_{k+1}^-)\eta(t_{k+1}^-)|\mathcal{F}_k^\eta\right]. \end{aligned} \tag{15}$$

Similarly, $x_c(t_k) \in \mathcal{F}_k^\eta$, and there exists $\upsilon > 0$ such that

$$\begin{aligned}\mathbb{E}\left[V_2(k+1)|\mathcal{F}_k^\eta\right] \leq& (1+\upsilon)\|e^{\hat{A}h_k}\|^2x_c^T(t_k)x_c(t_k)\\ &+\left(1 + \frac{1}{\upsilon}\right)\beta_k^2\|\Pi(\mathcal{L} \otimes I_p)\|^2\tilde{\xi}^T(t_k)\xi(t_k)\\ &+\beta_k^2\|\mathcal{A}\|^2\|\Pi\|^2\mathbb{E}\left[\|\eta(t_{k+1}^-)\|^2|\mathcal{F}_k^\eta\right]. \end{aligned} \tag{16}$$

Define a Lyapunov candidate $V = V_1 + V_2$, then

$$\begin{aligned}&\mathbb{E}\left[\mathbb{E}\left[V(k+1)|\mathcal{F}_k^\eta\right]\right]\\ &\leq\left(1 - 2\beta_k\lambda_2(\bar{\mathcal{L}}) + \beta_k^2\left(\|\mathcal{L}\|^2 + \left(1 + \frac{1}{\upsilon}\right)\|\Pi(\mathcal{L} \otimes I_p)\|^2\right)\right)\mathbb{E}\left[V_1(k)\right]\\ &\quad+(1+\upsilon)\|e^{\hat{A}h_k}\|^2\mathbb{E}\left[V_2(k)\right] + \beta_k^2(\|J\mathcal{A}\|^2 + \|\mathcal{A}\|^2\|\Pi\|^2)\sigma_\eta^2. \end{aligned}$$

Note that by the law of total expectation, we have $\mathbb{E}\left[\mathbb{E}\left[V(k+1)|\mathcal{F}_k^\eta\right]\right] = \mathbb{E}\left[V(k+1)\right]$, and

$$\mathbb{E}\left[\mathbb{E}\left[\|\eta(t_{k+1}^-)\|^2|\mathcal{F}_k^\eta\right]\right] = \mathbb{E}\left[\|\eta(t_{k+1}^-)\|^2\right] \leq \sigma_\eta^2 < \infty.$$

Since $\sum_{k=0}^{\infty}\beta_k^2 < \infty$, we have $\lim_{k\to\infty}\beta_k = 0$. As $\hat{A} = A + BK_1$ is Hurwitz, there exists υ such that $\|e^{\hat{A}h_k}\|^2 \leq \|e^{\hat{A}h_{\min}}\|^2 \leq$

$\frac{1-2\beta_k\lambda_2(\bar{\mathcal{L}})+\beta_k^2(\|\mathcal{L}\|^2+(1+\frac{1}{\upsilon})\|\Pi(\mathcal{L}\otimes I_p)\|^2)}{1+\upsilon}$, where $h_{\min}$ is the lower bound of intervals between two adjacent interactions. Hence,

$$\begin{aligned}\mathbb{E}\left[V(k+1)\right] \leq & \left(1-2\beta_k\lambda_2(\bar{\mathcal{L}})+\beta_k^2 S\right)\mathbb{E}\left[V(k)\right]\\ &+\beta_k^2(\|J\mathcal{A}\|^2+\|\mathcal{A}\|^2\|\Pi\|^2)\sigma_\eta^2. \end{aligned} \tag{17}$$

where $S=\|\mathcal{L}\|^2+\left(1+\frac{1}{\upsilon}\right)\|\Pi(\mathcal{L}\otimes I_p)\|^2$. Then, there exists M such that $\beta_k \leq \min\left\{\frac{\lambda_2(\bar{\mathcal{L}})}{\|\mathcal{L}\|^2+(1+\upsilon)\|\Pi(\mathcal{L}\otimes I_p)\|^2}, \frac{1}{\lambda_2(\bar{\mathcal{L}})}\right\}$ for all $k>M$, which holds for

$$0\leq 1-2\beta_k\lambda_2(\bar{\mathcal{L}})+\beta_k^2\left(\|\mathcal{L}\|^2+\left(1+\frac{1}{\upsilon}\right)\|\Pi(\mathcal{L}\otimes I_p)\|^2\right)<1.$$

It also follows that $\sum_{k=0}^{\infty}2\beta_k\lambda_2(\bar{\mathcal{L}})-\beta_k^2(\|\mathcal{L}\|^2+(1+\frac{1}{\upsilon})\|\Pi(\mathcal{L}\otimes I_p)\|^2)\geq\sum_{k=0}^{\infty}\beta_k\lambda_2(\bar{\mathcal{L}})=\infty$ and

$$\lim_{k\to\infty}\frac{\beta_k^2(\|J\mathcal{A}\|^2+\|\mathcal{A}\|^2\|\Pi\|^2)\sigma_\eta^2}{2\beta_k\lambda_2(\bar{\mathcal{L}})-\beta_k^2(\|\mathcal{L}\|^2+(1+\frac{1}{\upsilon})\|\Pi(\mathcal{L}\otimes I_p)\|^2)}=0.$$

Therefore, by Lemma 3.1, we have $\lim_{k\to\infty}\mathbb{E}[V(k)]=0$, which implies that $\lim_{k\to\infty}\mathbb{E}[V_1(k)]=0$ and $\lim_{k\to\infty}\mathbb{E}[V_2(k)]=0$. Then, $\lim_{t\to\infty}\mathbb{E}[\tilde{\xi}^T(t)\tilde{\xi}(t)]=0$, $\lim_{t\to\infty}\mathbb{E}[x_c^T(t)x_c(t)]=0$. Since $C\Pi=I_{Np}$, we have

$$\begin{aligned}&\lim_{t\to\infty}\mathbb{E}\left\|y(t)-\frac{1}{N}(\mathbf{1}_N\mathbf{1}_N^T\otimes I_p)\xi(t)\right\|^2\\ &\leq\lim_{t\to\infty}\mathbb{E}\left[\mathcal{H}\left(Cx(t)-C\Pi\xi(t)+(J\otimes I_p)\xi(t)\right)\right]\\ &\leq\lim_{t\to\infty}\mathbb{E}[2(Cx_c^T(t))Cx_c(t)]+\lim_{t\to\infty}\mathbb{E}[2\tilde{\xi}^T(t)\tilde{\xi}(t)]=0.\end{aligned}$$

This completes the proof. □

Remark 3.2. Theorem 3.1 shows that the output state of each heterogeneous systems converges to the average of reference states in mean square. Note that $A_i+B_iK_{1i}$ is Hurwitz, and it is easy to design K_{1i} by the pole-placement method or solving a Riccati equation $A_i^TP_i+P_iA_i-P_iB_iB_i^TP_i+Q_i=0$ with Q_i as a positive definite matrix, and then we can design $K_{1i}=-B_i^TP_i$. In addition, we can set $\beta_k=\frac{a_1}{(k+a_2)^\alpha}$ with $a_1,a_2>0$ and $\alpha\in(0.5,1]$, such that $\sum_{k=0}^{\infty}\beta_k=\infty$ and $\sum_{k=0}^{\infty}\beta_k^2<\infty$.

Remark 3.3. Theorem 3.1 also holds for the decaying noises, as in Nozari et al. (2017), in form of

$$\begin{cases}\phi_i(t_k^-)=\xi_i(t_k^-)+\eta_i(t_k^-)\\ \eta_{i,l}(t_k^-)\sim\mathrm{Lap}(0,c_iq_i^k),\ l\in\{1,2,\ldots,p\},\ k\in\mathbb{N}_{>0}\end{cases} \tag{18}$$

where $\eta_i(t_k^-)$ and $\eta_j(t_k^-)$ are mutually independent with $c_i>0$, $0<q_i<1$. This is because, under the decaying noises (18), it still holds that $\{\eta(t_k^-),\bar{\mathcal{F}}_k^\eta,k\in\mathbb{N}_{>0}\}$ is a martingale difference sequence and $\sigma_\eta^2\triangleq\sup_{k\in\mathbb{N}_{>0}}\mathbb{E}\left[\|\eta(t_k^-)\|^2\right]$ is bounded, which implies that (17) holds. Therefore, in aid of the stochastic approximation method, we relax the selection of privacy noises in existing literature. However, it rises another problem that how to design β_k to satisfy the requirements on accuracy and $\epsilon^\star$-differential privacy. This issue will be addressed in the following.

Theorem 3.2. *Apply the distributed hybrid controller (5) and noise generator (6) to heterogeneous multi-agent systems (1). If Assumptions 2.1–2.3 hold and $A_i+B_iK_{1i}$ is Hurwitz, $\sum_{k=0}^{\infty}\beta_k=\infty$, $\sum_{k=0}^{\infty}\beta_k^2<\infty$, then $\lim_{t\to\infty}\mathbb{E}\|y_i(t)-y^\star\|^2=0$, where $y^\star$ is a random vector, satisfying $\mathbb{E}[y^\star]=\frac{1}{N}(\mathbf{1}_N^T\otimes I_p)y(t_0)$ and $cov[y^\star]=2b^2\sum_{j=0}^{\infty}\beta_j^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}I_p$.*

Proof. Because the graph is balanced and strongly connected, we have $\mathbf{1}_N^T\mathcal{L}=0$. According to the updating of $\xi(t_k)$ in (5), we can obtain that

$$\begin{aligned}(\mathbf{1}_N^T\otimes I_p)\xi(t_k)&=(\mathbf{1}_N^T(I_N-\beta_{k-1}\mathcal{L})\otimes I_p)\xi(t_k^-)\\ &\quad+\beta_{k-1}(\mathbf{1}_N^T\mathcal{A}\otimes I_p)\eta(t_k^-)\\ &=(\mathbf{1}_N^T\otimes I_p)\xi(t_k^-)+\beta_{k-1}(\mathbf{1}_N^T\mathcal{A}\otimes I_p)\eta(t_k^-)\\ &=(\mathbf{1}_N^T\otimes I_p)\xi(t_{k-1})+\beta_{k-1}(\mathbf{1}_N^T\mathcal{A}\otimes I_p)\eta(t_k^-).\end{aligned}$$

By taking iterations, we have

$$(\mathbf{1}_N^T\otimes I_p)\xi(t_k)=\sum_{i\in\mathcal{V}}\xi_i(t_0)+\sum_{j=1}^{k}\beta_{j-1}(\mathbf{1}_N^T\mathcal{A}\otimes I_p)\eta(t_j^-),$$

which immediately follows that

$$\lim_{t\to\infty}(\mathbf{1}_N^T\otimes I_p)\xi(t)=\sum_{i\in\mathcal{V}}\xi_i(t_0)+\sum_{j=1}^{\infty}\sum_{i\in\mathcal{V}}\beta_{j-1}\Delta_i\eta_i(t_j^-).$$

By Theorem 3.1, we have

$$\begin{aligned}\lim_{t\to\infty}\mathbb{E}\left\|y_i(t)-y^\star\right\|^2\leq&\lim_{t\to\infty}\mathbb{E}\left\|y_i(t)-\frac{1}{N}(\mathbf{1}_N^T\otimes I_p)\xi(t)\right\|^2\\ &+\lim_{t\to\infty}\mathbb{E}\left\|\frac{1}{N}(\mathbf{1}_N^T\otimes I_p)\xi(t)-y^\star\right\|^2=0,\end{aligned}$$

with $y^\star=\frac{1}{N}\sum_{i\in\mathcal{V}}\xi_i(t_0)+\frac{1}{N}\sum_{j=1}^{\infty}\sum_{i\in\mathcal{V}}\beta_{j-1}\Delta_i\eta_i(t_j^-)$. By the fact that $\eta_i(t_k^-)$, $i\in\mathcal{V}$, $k\in\mathbb{N}_{>0}$ are i.i.d.,

$$\begin{aligned}\mathbb{E}\left[y^\star\right]&=\mathbb{E}\left[\frac{1}{N}\sum_{i\in\mathcal{V}}\xi_i(t_0)+\frac{1}{N}\sum_{j=0}^{\infty}\sum_{i\in\mathcal{V}}\beta_j\Delta_i\eta_i(t_j^-)\right]\\ &=\frac{1}{N}\sum_{i\in\mathcal{V}}\xi_i(t_0)=\frac{1}{N}\sum_{i\in\mathcal{V}}y_i(t_0),\end{aligned} \tag{19}$$

and

$$cov\left(y^\star\right)=\sum_{j=0}^{\infty}\sum_{i\in\mathcal{V}}\frac{\beta_j^2\Delta_i^2}{N^2}2b^2I_p. \tag{20}$$

Because $\sum_{j=0}^{\infty}\beta_j^2<\infty$, $\|cov\left(y^\star\right)\|$ is bounded. □

The following theorem provides a way to design control parameter to ensure the $(s^\star,r^\star)$-accuracy.

Theorem 3.3. *Suppose Assumptions 2.1–2.3 hold. Apply the distributed hybrid controller (5) with the noise generator (6). Given a pair of parameters $(s^\star,r^\star)$, if set $\beta_k=\frac{a_1}{(k+a_2)^\alpha}$, $\alpha\in(0.5,1]$, $a_1>0$, $a_2>0$, and $A_i+B_iK_{1i}$ is Hurwitz such that*

$$\frac{a_1^2a_2^{-2\alpha+1}}{2\alpha-1}+\frac{a_1^2}{a_2^{2\alpha}}\leq\frac{s^\star(r^\star)^2}{2pb^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}}, \tag{21}$$

then $\mathbb{P}\{\|y^\star-\mathbb{E}[y^\star]\|<r^\star\}\geq 1-s^\star$.

Proof. By the multidimensional Chebyshev's inequality, we have

$$\mathbb{P}\left\{(y^\star-\mathbb{E}[y^\star])^T(cov(y^\star))^{-1}(y^\star-\mathbb{E}[y^\star])<\epsilon\right\}\geq 1-\frac{p}{\epsilon}.$$

Taking (20) into the above inequality yields

$$\mathbb{P}\left\{\|y^\star-\mathbb{E}[y^\star]\|<\sqrt{\epsilon\kappa}\right\}\geq 1-\frac{p}{\epsilon} \tag{22}$$

where $\kappa=2b^2\sum_{k=0}^{\infty}\beta_k^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}$. Let $r=\sqrt{\epsilon\kappa}$, then $\epsilon=\frac{r^2}{\kappa}$ and thus

$$\mathbb{P}\left\{\|y^\star-\mathbb{E}[y^\star]\|<r\right\}\geq 1-\frac{p\kappa}{r^2}. \tag{23}$$

Therefore, heterogeneous systems achieve asymptotically unbiased mean square output average consensus with (s,r)-accuracy, where $s=\frac{2pb^2}{r^2}\sum_{j=0}^{\infty}\beta_j^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}$.

Clearly, as long as

$$\sum_{k=0}^{\infty}\beta_k^2 \le \frac{s^\star (r^\star)^2}{2pb^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}},$$

it ensures the $(s^\star, r^\star)$-accuracy. By the fact that the function $f(x)=\frac{a_1}{(x+a_2)^\alpha}$, with $\alpha\in(0.5,1]$, $a_1>0$, $a_2>0$, is a strictly decreasing function for $x>0$. Then, for $k\in\mathbb{N}_{>0}$, we have $\left(\frac{a_1}{(k+a_2)^\alpha}\right)^2 \le \int_{k-1}^{k}\left(\frac{a_1}{(x+a_2)^\alpha}\right)^2 \mathrm{d}x$ and thus

$$\begin{aligned}\sum_{k=0}^{\infty}\beta_k^2 &= \frac{a_1^2}{a_2^{2\alpha}}+\sum_{k=1}^{\infty}\left(\frac{a_1}{(k+a_2)^\alpha}\right)^2\\ &\le \frac{a_1^2}{a_2^{2\alpha}}+\int_0^{\infty}\left(\frac{a_1}{(x+a_2)^\alpha}\right)^2\mathrm{d}x\\ &\le \left(\frac{a_1^2(x+a_2)^{-2\alpha+1}}{-2\alpha+1}\right)\Big|_0^{\infty}+\frac{a_1^2}{a_2^{2\alpha}}\\ &\le 0-\frac{a_1^2a_2^{-2\alpha+1}}{-2\alpha+1}+\frac{a_1^2}{a_2^{2\alpha}} \le \frac{s^\star(r^\star)^2}{2pb^2\sum_{i\in\mathcal{V}}\frac{\Delta_i^2}{N^2}}.\end{aligned} \tag{24}$$

This completes the proof. □

Under the non-decaying noises, the proposed controller can ensure the predefined accuracy by selecting a proper control gains $\beta_k, k\in\mathbb{N}_{\ge 0}$. Besides, we can enhance the accuracy by minifying the term $\sum_{k=0}^{\infty}\beta_k^2$.

3.3. Privacy analysis

In this subsection, we will show our algorithms are ϵ-differentially private on the dataset $D=\{y_i(0), i\in\mathcal{V}\}$. For focusing on privacy analysis, we introduce an assumption on control parameters such that heterogeneous multi-agent systems can achieve asymptotically unbiased mean square output average consensus.

Assumption 3.1. Assume $\sum_{k=0}^{\infty}\beta_k=\infty$, $\sum_{k=0}^{\infty}\beta_k^2<\infty$, $\beta_k<\frac{1}{\Delta_{\max}}$ and $A_i+B_iK_{i1}, i\in\mathcal{V}$ is Hurwitz.

Remark 3.4. In Assumption 3.1, besides the basic convergence condition derived in Theorem 3.2, we need $\beta_k<\frac{1}{\Delta_{\max}}$ to ensure that the trajectories of inner controller states converge from the beginning.

Before giving the privacy analysis, let us introduce the definition of sensitivity. For a private dataset D and an observation $O=\{\phi_i(t_k^-), i\in\mathcal{V}\}_{k=1}^T$, there exist a determinate sequence of noises $\{\eta_i(t_k^-), i\in\mathcal{V}\}_{k=1}^T$ and a determinate trajectory $\rho(D,O)=\{\xi_i^{D,O}(t_k^-), i\in\mathcal{V}\}_{k=1}^T$. Based on the sensitivity defined by Cortés, et al. (2016), the sensitivity of the interaction information at discrete-time instants in this paper is defined as follows.

Definition 3.1. The sensitivity of a randomized mechanism $\mathcal{M}$ at time $t_k\ge 0$ is

$$S(t_k)=\sup_{D,D'\in\mathcal{D},O\in\mathcal{O}}\frac{\|\rho(D,O)(t_k^-)-\rho(D',O)(t_k^-)\|_1}{\|D-D'\|_1}. \tag{25}$$

Sensitivity is a measure of the difference of two observed trajectories induced by changing the private dataset.

Theorem 3.4. *Suppose Assumptions 2.1–2.3 and 3.1 hold. Applying the distributed controller (5) and noise generator (6) yields*

$$S(t_k)=\begin{cases}1, & k=1\\ \prod_{l=0}^{k-2}(1-\beta_l\Delta_{\min}), & k\ge 2\end{cases} \tag{26}$$

where $\Delta_{\min}$ is the minimum degree of the graph.

Proof. Assume a pair of private datasets $D=\{y_i(t_0), i\in\mathcal{V}\}$ and $D'=\{y_i'(t_0), i\in\mathcal{V}\}$, and a set of observation $\mathcal{O}$. Denote $\mathcal{P}=\{\rho(D,O): O\in\mathcal{O}\}$ and $\mathcal{P}'=\{\rho(D',O): O\in\mathcal{O}\}$ as the set of possible trajectories under the controller (5) w.r.t. D and D' in the observation set $\mathcal{O}$. The trajectories subject to the probability density functions $f(D,\rho(D,O))$ and $f(D',\rho(D',O))$, respectively. Based on the controller (5), because the observations $O=\{\phi_j(t_k^-), j\in\mathcal{V}\}$ for D and D' are the same, it has

$$\xi_i^{D,O}(t_{k+1}^-)=\xi_i^{D,O}(t_k)=(1-\beta_{k-1}\Delta_i)\xi_i^{D,O}(t_k^-)+\beta_{k-1}\sum_{j\in N_i}\phi_j(t_k^-),$$

and it is similar for D' such that

$$\xi_i^{D',O}(t_{k+1}^-)=\xi_i^{D',O}(t_k)=(1-\beta_{k-1}\Delta_i)\xi_i^{D',O}(t_k^-)+\beta_{k-1}\sum_{j\in N_i}\phi_j(t_k^-).$$

Therefore,

$$\begin{aligned}&\xi_i^{D',O}(t_{k+1}^-)-\xi_i^{D,O}(t_{k+1}^-)\\ &=\xi_i^{D',O}(t_k)-\xi_i^{D,O}(t_k)\\ &=(1-\beta_{k-1}\Delta_i)\left(\xi_i^{D',O}(t_k^-)-\xi_i^{D,O}(t_k^-)\right)\\ &=\prod_{l=0}^{k-1}(1-\beta_l\Delta_i)\left(\xi_i^{D',O}(t_0)-\xi_i^{D,O}(t_0)\right).\end{aligned} \tag{27}$$

Defining $\mathcal{J}=\{1,2,\dots,p\}$, it follows that for $k=1$,

$$\begin{aligned}&\|\rho(D,O)(t_1^-)-\rho(D',O)(t_1^-)\|_1\\ &=\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left|\xi_{i,j}^{D',O}(t_0)-\xi_{i,j}^{D,O}(t_0)\right|\\ &=\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left|y_{i,j}'(t_0)-y_{i,j}(t_0)\right|\\ &=\|D-D'\|_1\le S(t_1)\|D-D'\|_1,\end{aligned} \tag{28}$$

and for $k\ge 2$, it has

$$\begin{aligned}&\|\rho(D,O)(t_k^-)-\rho(D',O)(t_k^-)\|_1\\ &=\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left|\xi_{i,j}^{D',O}(t_k^-)-\xi_{i,j}^{D,O}(t_k^-)\right|\\ &=\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left(\prod_{l=0}^{k-2}(1-\beta_l\Delta_i)\right)\left|\xi_{i,j}^{D',O}(t_0)-\xi_{i,j}^{D,O}(t_0)\right|\\ &\le\left(\prod_{l=0}^{k-2}(1-\beta_l\Delta_{\min})\right)\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left|\xi_{i,j}^{D',O}(t_0)-\xi_{i,j}^{D,O}(t_0)\right|\\ &\le\left(\prod_{l=0}^{k-2}(1-\beta_l\Delta_{\min})\right)\|D-D'\|_1\\ &\le S(t_k)\|D-D'\|_1.\end{aligned} \tag{29}$$

Thus, $S(t_1)=1$ and $S(t_k)=\prod_{l=0}^{k-2}(1-\beta_l\Delta_{\min})$ for $k\ge 2$. This completes the proof. □

Then, it is ready to calculate the differential privacy index ϵ of the proposed algorithm.

Theorem 3.5. *Suppose Assumptions 2.1–2.3 and 3.1 hold. The distributed controller (5) with the noise generator (6) is ϵ-differentially private for heterogeneous systems (1) over time horizon T with*

$$\epsilon=\frac{\sum_{k=1}^{T}S(t_k)}{b}. \tag{30}$$

Proof. Recall that $\mathcal{P} = \{\rho(D, O) : O \in \mathcal{O}\}$ and $\mathcal{P}' = \{\rho(D', O) : O \in \mathcal{O}\}$ are the set of possible trajectories under the controller (5) w.r.t. D and D' in the observation set $\mathcal{O}$, and the trajectories subject to the probability density functions $f(D, \rho(D, O))$ and $f(D', \rho(D', O))$, respectively. Then, it can be obtained that

$$\frac{\mathbb{P}[\mathcal{M}(D) \in \mathcal{O}]}{\mathbb{P}[\mathcal{M}(D') \in \mathcal{O}]} = \frac{\int_{\rho(D,O)\in\mathcal{P}} f\,(D, \rho(D, O))\,\mathrm{d}\tau}{\int_{\rho(D',O)\in\mathcal{P}'} f\,(D', \rho(D', O))\,\mathrm{d}\tau'}.$$

Denoting $\mathcal{T} = \{1, 2, \ldots, T\}$ and $\mathcal{W} = \mathcal{V} \times \mathcal{J} \times \mathcal{T}$, the probability density functions $f(D, \rho(D, O))$ over time horizon T are

$$\begin{aligned} f(D, \rho(D, O)) &= \prod_{i\in\mathcal{V},\ k\in\mathcal{T}} f(D, \rho(D, O)_i(t_k^-)) \\ &= \prod_{(i,j,k)\in\mathcal{W}} \frac{1}{2b} \exp\left(-\frac{\left|\rho(D, O)_{i,j}(t_k^-) - \phi_{i,j}(t_k^-)\right|}{b}\right). \end{aligned} \tag{31}$$

As they have the same observation over time horizon T, there exists a bijection $g(\cdot) : \mathcal{P} \to \mathcal{P}'$, such that for any pair of $\rho(D, O) \in \mathcal{P}$ and $\rho(D', O) \in \mathcal{P}'$, it has $g(\rho(D, O)) = \rho(D', O)$. By the rationale of $\phi_i(t_k^-) = \xi_i(t_k^-) + \eta(t_k^-)$, $\eta_i(t_k^-) \sim \mathrm{Lap}(0, bI_p)$ and the observations $O = \{\phi_i(t_1^-), \phi_i(t_2^-), \ldots, \phi_i(t_T^-)\}$, then combining (31) yields

$$\begin{aligned} \frac{\mathbb{P}[\mathcal{M}(D) \in \mathcal{O}]}{\mathbb{P}[\mathcal{M}(D') \in \mathcal{O}]} &= \frac{\int_{\rho(D,O)\in\mathcal{P}} f\,(D, \rho(D, O))\,\mathrm{d}\tau}{\int_{g(\rho(D,O))\in\mathcal{P}'} f\,(D', g(\rho(D, O)))\,\mathrm{d}\tau} \\ &= \frac{\int_{\rho(D,O)\in\mathcal{P}} f\,(D, \rho(D, O))\,\mathrm{d}\tau}{\int_{\rho(D,O)\in\mathcal{P}} f\,(D', g(\rho(D, O)))\,\mathrm{d}\tau} \\ &= \prod_{(i,j,k)\in\mathcal{W}} \exp\left(-\frac{\left|\rho(D, O)_{i,j}(t_k^-) - \phi_{i,j}(t_k^-)\right|}{b}\right. \\ &\qquad \left. + \frac{\left|\rho(D', O)_{i,j}(t_k^-) - \phi_{i,j}(t_k^-)\right|}{b}\right) \\ &\le \prod_{(i,j,k)\in\mathcal{W}} \exp\left(\frac{\left|\xi_{i,j}^{D',O}(t_k^-) - \xi_{i,j}^{D,O}(t_k^-)\right|}{b}\right). \end{aligned} \tag{32}$$

Combining (29) and (32), it has

$$\begin{aligned} &\frac{\mathbb{P}[\mathcal{M}(D) \in \mathcal{O}]}{\mathbb{P}[\mathcal{M}(D') \in \mathcal{O}]} \\ &= \exp\left(\frac{\sum_{k\in\mathcal{T}}\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{J}}\left|\xi_{i,j}^{D',O}(t_k^-) - \xi_{i,j}^{D,O}(t_k^-)\right|}{b}\right) \\ &\le \exp\left(\frac{\left(1 + \sum_{k\in\mathcal{T}/\{1\}}\prod_{l=0}^{k-2}(1 - \beta_l|N_i|_{\min})\right)\|D - D'\|_1}{b}\right) \\ &\le \exp\left(\frac{\sum_{k=1}^{T} S(t_k)\|D - D'\|_1}{b}\right). \end{aligned} \tag{33}$$

Hence, we can obtain that $\epsilon = \frac{\sum_{k=1}^{T} S(t_k)}{b}$. □

Remark 3.5. Theorem 3.5 reveals that the differential privacy coefficient ϵ can be described by the sum of sensitivity. According to (26), greater $\{\beta_k\}$ gives a smaller $S(t_k)$, which further leads to a smaller ϵ and a better protection. Similarly, if we select privacy noises with a greater parameter b, then ϵ becomes smaller and thus the preservation is stronger.

In the following, we focus on how to design the time-varying gain to satisfy the predefined $\epsilon^\star$-differential privacy over the infinite time horizon.

Theorem 3.6. *Suppose the same assumptions in Theorem 3.5 hold. Apply the distributed hybrid controller (5) with the noise generator (6). Given a parameter $\epsilon^\star$ and set $\beta_k = \frac{a_1}{\Delta_{\min}(k+a_2)^\alpha}$, $\alpha \in (0.5, 1)$, $a_1 > 0$, $a_2 > 0$, then the controller ensures $\epsilon^\star$-differentially private over the infinite time horizon if*

$$\frac{1}{b} + \frac{a_1^{\frac{-1}{\gamma}}\,\gamma^{\frac{1-\gamma}{\gamma}}}{b} \exp\left(\frac{a_1 a_2^\gamma}{\gamma}\right) \Gamma\left(\frac{1}{\gamma}, \frac{a_1 a_2^\gamma}{\gamma}\right) \le \epsilon^\star \tag{34}$$

where $\gamma = 1 - \alpha$ and $\Gamma(\cdot, \cdot)$ is the upper incomplete gamma function.

Proof. Based on the results in Theorems 3.4 and 3.5, under the controller (5), taking $\beta_k = \frac{a_1}{\Delta_{\min}(k+a_2)^\alpha}$ into Eq. (26) yields

$$S(t_k) = \begin{cases} 1, & k = 1 \\ \prod_{l=0}^{k-2}(1 - \frac{a_1}{(l+a_2)^\alpha}), & k \ge 2. \end{cases}$$

Taking logarithm on both sides, we have

$$\ln(S(t_k)) = \begin{cases} 0, & k = 1 \\ \sum_{l=0}^{k-2}\ln(1 - \frac{a_1}{(l+a_2)^\alpha}), & k \ge 2. \end{cases}$$

Let us focus on the case when $k \ge 2$. By Assumption 3.1, $\beta_k\Delta_{\max} < 1$ implies that $\frac{a_1}{(k+a_2)^\alpha} = \beta_k\Delta_{\min} < 1$. Then, due to the fact that $\ln(1 + x) \le x$ holds for any $x > -1$, we have

$$\begin{aligned} \ln(S(t_k)) &\le -\sum_{l=0}^{k-2} \frac{a_1}{(l + a_2)^\alpha} \\ &\le -\int_{a_2}^{a_2+1} \frac{a_1}{x^\alpha}\mathrm{d}x \cdots - \int_{k+a_2-2}^{k+a_2-1} \frac{a_1}{x^\alpha}\mathrm{d}x \\ &\le -\int_{a_2}^{k+a_2-1} \frac{a_1}{x^\alpha}\mathrm{d}x = -\frac{a_1 x^{1-\alpha}}{1-\alpha}\Big|_{a_2}^{k+a_2-1}. \end{aligned}$$

Therefore, denoting $\gamma = 1 - \alpha$, for $k \ge 2$, it has

$$\begin{aligned} S(t_k) &\le \exp\left(-\frac{a_1}{1-\alpha}\left((k + a_2 - 1)^{1-\alpha} - {a_2}^{1-\alpha}\right)\right) \\ &\le \exp\left(\frac{a_1 a_2^\gamma}{\gamma}\right) \exp\left(-\frac{a_1}{\gamma}(k + a_2 - 1)^\gamma\right). \end{aligned} \tag{35}$$

We note that (35) shows an upper bound of $S(t_k)$. It is ready to calculate the sum of $S(t_k)$.

$$\begin{aligned} &\lim_{T\to\infty}\sum_{k=1}^{T} S(t_k) = S(t_1) + \lim_{T\to\infty}\sum_{k=2}^{T} S(t_k) \\ &\le 1 + \exp\left(\frac{a_1 a_2^\gamma}{\gamma}\right) \lim_{T\to\infty}\sum_{k=2}^{T} \exp\left(-\frac{a_1}{\gamma}(k + a_2 - 1)^\gamma\right). \end{aligned} \tag{36}$$

Note that $\gamma \in (0, 0.5)$, hence, for $x > 0$, the function $f(x) = \exp\left(-\frac{a_1}{\gamma}x^\gamma\right)$ decreases as x increases. Denote $\tau = \frac{a_1}{\gamma}x^\gamma$, then it has $\mathrm{d}\tau = a_1 x^{\gamma-1}\mathrm{d}x$, which follows $\mathrm{d}x = (\frac{\gamma}{a_1}\tau)^{\frac{1-\gamma}{\gamma}} a_1^{-1}\mathrm{d}\tau = a_1^{-\frac{1}{\gamma}}(\gamma\tau)^{\frac{1-\gamma}{\gamma}}\mathrm{d}\tau$ and

$$\begin{aligned} &\lim_{T\to\infty}\sum_{k=2}^{T} \exp\left(-\frac{a_1}{\gamma}(k + a_2 - 1)^\gamma\right) \\ &\le \lim_{T\to\infty}\sum_{k=2}^{T} \int_{k+a_2-2}^{k+a_2-1} \exp\left(-\frac{a_1}{\gamma}x^\gamma\right)\mathrm{d}x \\ &\le \lim_{T\to\infty} \int_{a_2}^{T+a_2-1} \exp\left(-\frac{a_1}{\gamma}x^\gamma\right)\mathrm{d}x \end{aligned}$$

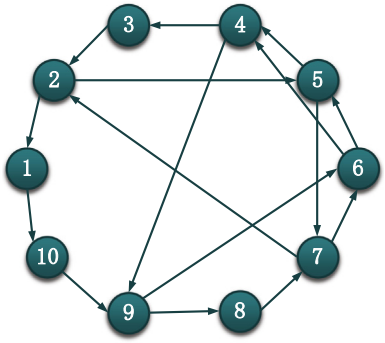


Fig. 2. The topology of communication graph.

$$\leq \lim_{T\to\infty} a_1^{-\frac{1}{\gamma}} \int_{\frac{a_1}{\gamma}a_2^{\gamma}}^{\frac{a_1}{\gamma}(T+a_2-1)^{\gamma}} \exp(-\tau)(\gamma\tau)^{\frac{1-\gamma}{\gamma}} \mathrm{d}\tau$$

$$\leq \lim_{T\to\infty} a_1^{-\frac{1}{\gamma}} \gamma^{\frac{1-\gamma}{\gamma}} \int_{\frac{a_1}{\gamma}a_2^{\gamma}}^{\frac{a_1}{\gamma}(T+a_2-1)^{\gamma}} \exp(-\tau)\tau^{\frac{1}{\gamma}-1} \mathrm{d}\tau$$

$$\leq a_1^{-\frac{1}{\gamma}} \gamma^{\frac{1-\gamma}{\gamma}} \Gamma\left(\frac{1}{\gamma}, \frac{a_1 a_2^{\gamma}}{\gamma}\right), \tag{37}$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function. Hence, combining (36) and (37), it has

$$\epsilon = \lim_{T\to\infty} \frac{\sum_{k=1}^{T} S(t_k)}{b}$$

$$\leq \frac{1}{b} + \frac{a_1^{\frac{-1}{\gamma}} \gamma^{\frac{1-\gamma}{\gamma}}}{b} \exp\left(\frac{a_1 a_2^{\gamma}}{\gamma}\right) \Gamma\left(\frac{1}{\gamma}, \frac{a_1 a_2^{\gamma}}{\gamma}\right) \leq \epsilon^{\star}.$$

This completes the proof. □

Remark 3.6. Theorem 3.6 gives an upper bound of differential privacy coefficient ϵ when β_k is designed in a certain form. When the minimum degree of the graph is unknown. Based on Theorem 3.6, if setting $\beta_k = \frac{a_1}{(k+a_2)^{\alpha}}$ under Assumption 3.1, then

$$\epsilon \leq \frac{1}{b} + \frac{a_1^{\frac{-1}{\gamma}} \Delta_{\min}^{\frac{1}{\gamma}} \gamma^{\frac{1-\gamma}{\gamma}}}{b} \exp\left(\frac{a_1 a_2^{\gamma}}{\Delta_{\min}\gamma}\right) \Gamma\left(\frac{1}{\gamma}, \frac{a_1 a_2^{\gamma}}{\Delta_{\min}\gamma}\right).$$

By (26), (30) and the above inequality, increasing a_1 has the same effect as decreasing $\Delta_{\min}$ on both differential privacy coefficient ϵ and the obtained boundary. Moreover, as we know, ϵ increases as β_k decreases, namely, α increases (or a_1 decreases, or a_2 increases). Similarly, the obtained boundary also increases as α increases (or a_1 decreases, or a_2 increases).

Remark 3.7. Given the predefined indices $(r^{\star}, s^{\star})$-accuracy and $\epsilon^{\star}$-differential privacy. Based on Theorems 3.3 and 3.6, we can design the noise parameter b and the control gain $\beta_k = \frac{a_1}{(k+a_2)^{\alpha}}$ with $a_1, a_2 > 0$ and $\alpha \in (0.5, 1)$, such that (21) holds and

$$\frac{1}{b} + \frac{a_1^{\frac{-1}{\gamma}} \Delta_{\min}^{\frac{1}{\gamma}} \gamma^{\frac{1-\gamma}{\gamma}}}{b} \exp\left(\frac{a_1 a_2^{\gamma}}{\Delta_{\min}\gamma}\right) \Gamma\left(\frac{1}{\gamma}, \frac{a_1 a_2^{\gamma}}{\Delta_{\min}\gamma}\right) \leq \epsilon^{\star}.$$

In Theorem 3.3, we find that $\alpha \in (0.5, 1]$ can guarantee the convergence of algorithm. However, in Theorem 3.6, we require $\alpha \in (0.5, 1)$ to ensure the algorithm to be ϵ-differentially private over the infinite time horizon. This is because if $\alpha = 1$ we have $\lim_{T\to\infty} \sum_{k=1}^{T} S(t_k) = \infty$ and thus $\epsilon = \sum_{k=1}^{\infty} \frac{S(t_k)}{b} \to \infty$.

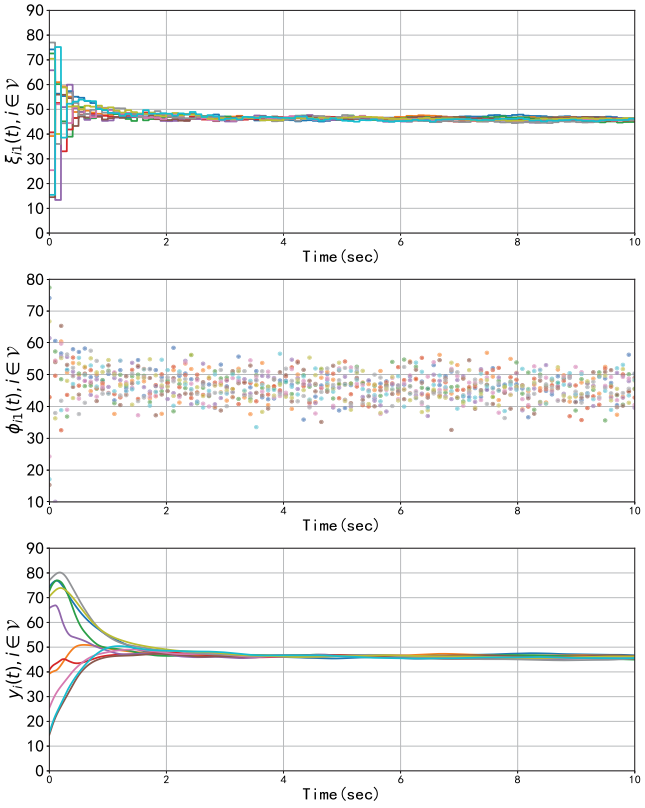


Fig. 3. The trajectories of reference states, delivered states, and output states under the proposed controller (5) with a time-varying control gain and non-decaying noises (6).

4. Simulation

In this section, we consider ten heterogeneous continuous-time multi-agent systems coupled by the communication graph in Fig. 2. In this example, we aim to achieve consensus with $(s^{\star}, r^{\star})$-accuracy and $\epsilon^{\star}$-differential privacy, where $s^{\star} = 0.35$, $r^{\star} = 4$, and $\epsilon^{\star} = 1$.

The dynamics of each agent is

$$\begin{cases} \dot{x}_i(t) = \begin{pmatrix} 0 & 1 \\ a_i & e_i \end{pmatrix} x_i(t) + \begin{pmatrix} 0 \\ b_i \end{pmatrix} u_i(t), \\ y_i = \begin{pmatrix} 1 & 0 \end{pmatrix} x_i, \qquad i \in \mathcal{V}_1 = \{1, \ldots, 5\}, \end{cases} \tag{38}$$

$$\begin{cases} \dot{x}_i(t) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a_i & e_i & f_i \end{pmatrix} x_i(t) + \begin{pmatrix} 0 \\ 0 \\ b_i \end{pmatrix} u_i(t), \\ y_i = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} x_i, \qquad i \in \mathcal{V}_2 = \{6, \ldots, 10\}, \end{cases} \tag{39}$$

where for $i \in \mathcal{V}_1$, $a_i = -0.3 + 0.4 * i$, $b_i = -0.2 + 0.4 * i$, $e_i = -1.6 + 0.6 * i$ and for $i \in \mathcal{V}_2$, $a_i = 1.3 - 0.3 * (i-5)$, $b_i = 2.2 - 0.2 * (i-5)$, $e_i = 3.4 - 0.4 * (i-5)$, $f_i = -0.1 - 0.3 * (i-5)$. The initial states are selected randomly on the interval $[0, 90]$, where the average of the initial outputs is calculated as $y_{\text{ave}} = 47.67$.

We employ the proposed controller (5) and make a comparison between using non-decaying noises (6) with $b = 4$ and using decaying noises (18) as in Nozari et al. (2017) with $c_i = 4q_i = 0.95$. Based on (2), for each agent, the solution (Π_i, U_i) can be presented as: for $i \in \mathcal{V}_1$, $\Pi_i = [1, 0]^T$ and $U_i = -\frac{a_i}{b_i}$; for $i \in \mathcal{V}_2$, $\Pi_i = [1, 0, 0]^T$ and $U_i = -\frac{a_i}{b_i}$. Then, using pole-placement method, we set $K_{11} = [-128, -45.5]$, $K_{12} = [-43.3, -16.2]$, $K_{13} = [-26.4, -10.3]$, $K_{14} = [-19.1, -7.7]$, $K_{15} = [-15.1, -6.4]$,

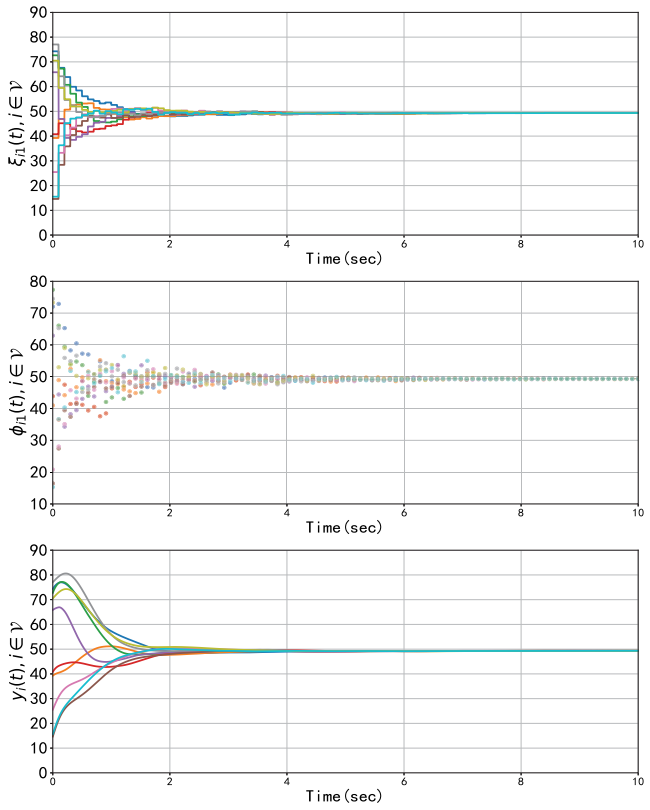


Fig. 4. The trajectories of reference states, delivered states, and output states under the proposed controller (5) with a constant control gain and decaying noises (18) (Nozari et al., 2017).

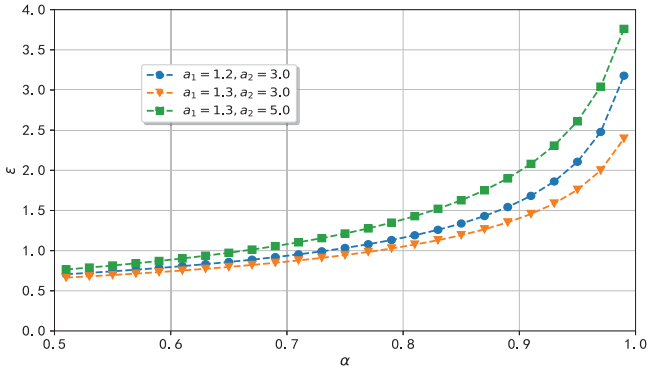


Fig. 5. The boundary of differential privacy coefficient ϵ with respect to the parameter set (α, a_1, a_2) under the privacy noise (6) with $b = 4$.

$K_{16} = [-66.8, -40.5, -7.75]$, $K_{17} = [-74.1, -44.8, -8.8]$, $K_{18} = [-83.1, -50.1, -10]$, $K_{19} = [-94.9, -57, -11.7]$, and $K_{1(10)} = [-110, -66.2, -13.9]$, such that all the poles of $A_i + B_i K_{1i}$ are less than -5. Based on the theoretical results, the impulsive intervals are set as $h_k = 0.1$s. For the case of non-decaying noises, the control gain is set as $\beta_k = 1/(k+3)^{0.75}$. For the case of decaying noises, as in Nozari et al. (2017), we set the control gain a constant, say $\beta_k = \beta = 0.2$. The results are shown in Figs. 3 and 4, respectively, where trajectories of $\xi(t)$, $\phi(t)$, and $y(t)$ are displayed. It is observed that the delivered information $\phi_i(t)$ keeps random under non-decaying noises. Fig. 5 reveals the relation between the privacy index ϵ and the control parameter set (a_1, a_2, α) in form of $\beta_k = \frac{a_1}{(k+a_2)^\alpha}$. It is observed that ϵ increases as a_2 or α increases, and ϵ decreases as a_1 increases.

5. Conclusion

In this paper, we have developed a differentially private consensus algorithm for the average output consensus problem of continuous-time heterogeneous systems. The proposed algorithm has achieved asymptotically unbiased mean square output average consensus and at the same time protected the initial privacy of each agent. We have relaxed the selection of privacy noises in the existing mechanisms by using the stochastic approximation method, such that the privacy noises are no longer required to decay exponentially with time. Furthermore, we have developed a method to design the time-varying control gain to guarantee the desired accuracy and differential privacy. There are still many interesting topics deserving further investigation, including differentially private consensus under time-varying digraphs and how to asynchronously activate privacy noises to meet the differential privacy requirement.

References

Amelkin, V., Bullo, F., & Singh, A. K. (2017). Polar opinion dynamics in social networks. *IEEE Transactions on Automatic Control*, *62*(11), 5650–5665.

Chen, X., & Chen, Z. (2017). Robust sampled-data output synchronization of nonlinear heterogeneous multi-agents. *IEEE Transactions on Automatic Control*, *62*(3), 1458–1464.

Cortés, J., Dullerud, G. E., Han, S., Ny, J. L., Mitra, S., & Pappas, G. J. (2016). Differential privacy in control and network systems. In *2016 IEEE 55th conference on decision and control* (pp. 4252–4272).

Dwork, C. (2006). Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, languages and programming* (pp. 1–12). Berlin, Heidelberg: The Organization, Springer Berlin Heidelberg.

Fiore, D., & Russo, G. (2019). Resilient consensus for multi-agent systems subject to differential privacy requirements. *Automatica*, *106*, 18–26.

Fung, B. C. M., Wang, K., Chen, R., & Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys*, *42*(4), 1–53.

Gao, L., Deng, S., & Ren, W. (2019). Differentially private consensus with an event-triggered mechanism. *IEEE Transactions on Control of Network Systems*, *6*(1), 60–71.

He, J., Cai, L., Cheng, P., Pan, J., & Shi, L. (2019). Consensus-based data-privacy preserving data aggregation. *IEEE Transactions on Automatic Control*, *6*(12), 5222–5229.

He, J., Cai, L., Zhao, C., Cheng, P., & Guan, X. (2019). Privacy-preserving average consensus: Privacy analysis and algorithm design. *IEEE Transactions on Signal and Information Processing over Networks*, *5*(1), 127–138.

Huang, Z., Mitra, S., & Dullerud, G. (2012). Differentially private iterative synchronous consensus. In *Proceedings of the 2012 ACM workshop on privacy in the electronic society* (pp. 81–90).

Kailkhura, B., Brahma, S., & Varshney, P. K. (2017). Data falsification attacks on consensus-based detection systems. *IEEE Transactions on Signal and Information Processing over Networks*, *3*(1), 145–158.

Kang, S., Wang, J., Li, G., Shan, J., & Petersen, I. R. (2018). Optimal cooperative guidance law for salvo attack: An mpc-based consensus perspective. *IEEE Transactions on Aerospace and Electronic Systems*, *54*(5), 2397–2410.

Le Ny, J., & Mohammady, M. (2018). Differentially private MIMO filtering for event streams. *IEEE Transactions on Automatic Control*, *63*(1), 145–157.

Le Ny, J., & Pappas, G. J. (2014). Differentially private filtering. *IEEE Transactions on Automatic Control*, *59*(2), 341–354.

Lewis, F. L., Cui, B., Ma, T., Song, Y., & Zhao, C. (2016). Heterogeneous multi-agent systems: Reduced-order synchronization and geometry. *IEEE Transactions on Automatic Control*, *61*(5), 1391–1396.

Li, H., Ma, J., & Fu, S. (2015). A privacy-preserving data collection model for digital community. *Science China. Information Sciences*, *58*(3), Article 032101.

Li, W., Wei, G., Han, F., & Liu, Y. (2016). Weighted average consensus-based unscented kalman filtering. *IEEE Transactions on Cybernetics*, *46*(2), 558–567.

Li, T., & Zhang, J.-F. (2010). Consensus conditions of multi-agent systems with time-varying topologies and stochastic communication noises. *IEEE Transactions on Automatic Control*, *55*(9), 2043–2057.

Mo, Y., & Murray, R. M. (2017). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, *62*(2), 753–765.

Nozari, E., Tallapragada, P., & Cortés, J. (2017). Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design. *Automatica*, *81*, 221–231.

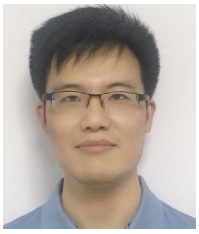
Olfati-Saber, R., & Murray, R. M. (2004). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, *49*(9), 1520–1533.

Pasqualetti, F., Borra, D., & Bullo, F. (2014). Consensus networks over finite fields. *Automatica*, *50*(2), 349–358.
Polyak, B. T. (1987). *Introduction to optimization*. Optimization Software.
Ren, X., Xu, J., Yang, X., & Yang, S. (2019). Bayesian network based high-dimensional crowdsourced data publication with local differential privacy. *SCIENTIA SINICA Informationis*, *49*(12), 1586–1605.
Ruan, M., Gao, H., & Wang, Y. (2019). Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, *64*(10), 4035–4049.
Su, Y., & Huang, J. (2012). Cooperative output regulation of linear multi-agent systems. *IEEE Transactions on Automatic Control*, *57*(4), 1062–1066.
Wang, Y., Huang, Z., Mitra, S., & Dullerud, G. E. (2017). Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance trade-offs. *IEEE Transactions on Control of Network Systems*, *4*(1), 118–130.
Wang, Y.-W., Liu, X.-K., Xiao, J.-W., & Shen, Y. (2018). Output formation-containment of interacted heterogeneous linear systems b distributed hybrid active control. *Automatica*, *93*, 26–32.
Zhang, Z., & Chow, M. Y. (2012). Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid. *IEEE Transactions on Power Systems*, *27*(4), 1761–1768.
Zhao, Y., Liu, Y., Li, Z., & Duan, Z. (2017). Distributed average tracking for multiple signals generated by linear dynamical systems: An edge-based framework. *Automatica*, *75*, 158–166.
Zhu, M., & Martínez, S. (2010). Discrete-time dynamic average consensus. *Automatica*, *46*(2), 322–329.

Xiao-Kang Liu received the B.S. degree in automatic control and the Ph.D. degree in control science and engineering from Huazhong University of Science and Technology, Wuhan, China, in 2014 and 2019, respectively. From Jun. to Sep. 2019, he was a visiting scholar in the Institute of Systems Science (ISS), Chinese Academy of Sciences (CAS), China. Currently, he is working as a research fellow at the School of Electrical & Electronic Engineering, Nanyang Technological University (NTU), Singapore. His research interests include hybrid control, distributed control and optimization.

Ji-Feng Zhang received the B.S. degree in mathematics from Shandong University, China, in 1985, and the Ph.D. degree from the Institute of Systems Science (ISS), Chinese Academy of Sciences (CAS), China, in 1991. Since 1985, he has been with the ISS, CAS, and now is the Director of ISS. His current research interests include system modeling, adaptive control, stochastic systems, and multi-agent systems.

He is a Fellow of IEEE, Fellow of IFAC, member of the European Academy of Sciences and Arts, and Academician of the International Academy for Systems and Cybernetic Sciences. He received twice the Second Prize of the State Natural Science Award of China in 2010 and 2015, respectively. He is a Vice-President of the Chinese Association of Automation, Vice-President of the Chinese Mathematical Society, Associate Editor-in-Chief of *Science China Information Sciences*, and Senior Editor of *IEEE Control Systems Letters*. He was a Vice-Chair of the IFAC Technical Board, member of the Board of Governors, IEEE Control Systems Society; Convenor of Systems Science Discipline, Academic Degree Committee of the State Council of China; Vice-President of the Systems Engineering Society of China; and Editor-in-Chief, Deputy Editor-in-Chief or Associate Editor of more than 10 journals, including *Journal of Systems Science and Mathematical Sciences*, *IEEE Transactions on Automatic Control* and *SIAM Journal on Control and Optimization* etc. He was General Co-Chair or IPC Chair of many control conferences.



Jimin Wang received the B.S. degree in mathematics from Shandong Normal University, China, in 2012 and the Ph.D. degree in operational research and control theory from School of Mathematics, Shandong University, China, in 2018. From May 2017 to May 2018, he was a joint Ph.D. student with the School of Electrical Engineering and Computing, The University of Newcastle, Callaghan, NSW, Australia. He is currently doing Postdoctoral research in the Institute of Systems Science (ISS), Chinese Academy of Sciences (CAS), China. His current research interests include privacy and security in control systems, stochastic systems and networked control systems. He is a recipient of Shandong University's excellent doctoral dissertation in 2019.