Privacy-Preserving Average Consensus: Fundamental Analysis and a Generic Framework Design

Feng Ye, *Graduate Student Member, IEEE*, Xianghui Cao, *Senior Member, IEEE*, Mo-Yuen Chow, *Fellow, IEEE*, and Lin Cai, *Fellow, IEEE*

***Abstract*— Average consensus is a key component of multi-agent systems coordination, while data privacy becomes a serious concern. Through the information exchange process, the initial state of an agent may be disclosed to its neighbors. The existing privacy-preserving research mainly addressed the situation of single-neighbor eavesdropping and infinite-time consensus, and they cannot deal with the cases of multi-neighbors eavesdropping and collusion inference attack or ensuring finite-time consensus. In this paper, we prove that it is impossible to preserve a node's data privacy if all of its neighbors collusively infer the data. Otherwise, we propose a privacy-preserving framework to support conventional average consensus, push-sum consensus, and finite-time average consensus, which integrates multiplying random variables, finite-time error compensation, and updating rule jump. In this paper, each agent exchanges data with its neighbors by multiplying a random variable to its real-time state at each iteration. To eliminate errors caused by the random multiplier, a finite-time error compensation term and updating rule jump are designed, which ensure the accuracy of consensus. We prove that the proposed framework can converge and preserve privacy facing collusion inference attacks in both finite-time and infinite-time consensus, while traditional adding-noise-based methods cannot solve the finite-time case. We also derive the analytical expressions of the maximum privacy disclosure probability for the initial state of each agent, and present the impact of multiplying random variables. Extensive case studies demonstrate the effectiveness of the proposed framework.**

***Index Terms*— Average consensus, privacy preserving, collusion inference, multiplying random variables, finite-time error compensation, updating rule jump.**

Manuscript received 13 December 2022; revised 15 October 2023; accepted 21 February 2024. Date of publication 26 February 2024; date of current version 19 March 2024. This work was supported in part by the Shenzhen Science and Technology Program under Grant JCYJ20230807114609019 and in part by the National Natural Science Foundation of China under Grant 92067111. *(Corresponding author: Xianghui Cao.)*

Feng Ye is with the School of Automation, Southeast University, Nanjing 210096, China (e-mail: yef@seu.edu.cn).

Xianghui Cao is with the School of Automation, Southeast University, Nanjing 210096, China, and also with the Shenzhen Research Institute, Southeast University, Shenzhen 518057, China (e-mail: xhcao@seu.edu.cn).

Mo-Yuen Chow is with the UM-SJTU Joint Institute, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: moyuen.chow@sjtu.edu.cn).

Lin Cai is with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 3P6, Canada (e-mail: cai@ece.uvic.ca).

Communicated by V. M. Prabhakaran, Associate Editor for Security and Privacy.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2024.3370311.

Digital Object Identifier 10.1109/TIT.2024.3370311

I. Introduction

Consensus in multi-agent systems (MASs) has attracted extensive attention in the past decades for its wide applications in distributed systems [1], [2], [3], [4], such as smart grids [5], [6], Internet of vehicles [7], multi-UAV formation [8], etc. Consensus relies on information exchanges between agents, and states of the agents are updated iteratively and in a distributed manner till the states of all agents converge to the same value. Average consensus is the most studied consensus, in which each agent calculates the weighted average of the states received from its neighbors to update its state and achieves consensus when their states are all equal to the average of the initial states for all agents in the MAS. According to convergence iterations, average consensus can be divided into infinite-time average consensus and finite-time average consensus, where infinite-time average consensus has been thoroughly investigated [1], [9], while research of finite-time average consensus still is in its infancy [10], [11].

On the other hand, privacy preserving becomes a pressing need as private information can be utilized to generate user portraits, analyze user behaviors, and cause security issues [12], [13], [14], [15], [16], [17], [18]. In an average consensus process, the private information to be protected is the initial states of the agents [19]. For instance, in distributed energy management systems of microgrids, the devices apply consensus to distributively make power decisions and during this process, the initial states are the power generation or consumption of the devices, which may be utilized by others to infer sensitive information of a user, e.g., power demands [5]. For a target agent in an averaging process, since it regularly exchanges information with its neighbors, each of its neighbors is potentially able to infer something about the private state of this target agent. Furthermore, if all its neighbors can mutually share their available information and collusively infer the private information of the target agent, the private information can be inferred easier and more accurately. To this end, when an agent does not want to reveal its initial state to any other agent, it needs a suitable privacy-preserving algorithm to preserve its initial state against collusion inference.

There has been active research about privacy-preserving average consensus, where adding-noise-based methods [19], [20], [21], [22], [23] are first proposed and widely used, with which artificial noises are added into the exchanged information to blur the true state during the consensus process. However, what kinds of noise can be utilized is a tricky problem. Differential privacy (DP) is a privacy-preserving algorithm which first applied in database management, then it is introduced into average consensus. In differential-privacy-based approaches, the noise of Laplacian or normal distribution is added into the states of agents. Compared with normally distributed noise, Laplacian distributed noise can achieve probability zero of violating the private information [24]. However, if DP is directly applied in average consensus, the MAS cannot converge. This is because the amplitude of noises does not decrease to zero, and the states of agents cannot reach the same value. Hence, parameter-decay DP is proposed to address this problem, where the magnitudes of the added noises decay to zero with probability 1 (w.p.1) when the average consensus algorithm converges, and the convergence value is expected to be the true average value of initial states [20]. Note that the convergence value is just only expected to be the average value of initial states, i.e., the convergence value is not always the average value of initial states. To guarantee the accuracy of convergence, the noise added into the states of agents should be zero-sum and parameter-decay [21].

However, there lacks a systematic study on privacy preserving average consensus against collusion inference. A fundamental issue remains to answer that, for a collusion inference, whether there exists an algorithm to ensure average consensus convergence while preserving the state privacy. Besides, existing privacy-preserving methods usually focus on a specific average consensus algorithm and hence are not universally applicable. In addition, existing privacy-preserving algorithms mainly consider infinite-time average consensus, while few of them shed light on finite-time average consensus.

In this paper, we address the problems that multiple neighbors collusively infer the initial state of an agent by using the information transmitted between the agent and its colluding neighbors in cases of finite or infinite time average consensus. We first systematically classify and analyze collusion inference, and theoretically prove that the private information cannot be preserved if all neighbors collusively inferring the privacy of the target agent. To ensure both infinite-time and finite-time consensus while preserving data privacy against collusion attack, we propose a generic privacy-preserving framework based on mechanisms including multiplying noise, finite-time error compensation, and updating rule jump. The proposed framework consists of two phases and in the first phase, each agent generates a random variable at each iteration and sends the product of the random variable and an intermediate variable to neighbors. To eliminate the errors caused by the multiplicative noise, a finite-time error compensation term is proposed to finally eliminate the impact of the noise on the consensus convergence. Furthermore, we design the updating rule jump mechanism, which allows the agent jump to phase 2 when each agent performs the original average consensus algorithm. The phase change takes place asynchronously at iterations that can be designed arbitrarily and independently by each agent.

The main contributions of this paper are listed as follows:

1) We systematically investigate collusion inferences in average consensus and theoretically analyze that in the common average consensus scenarios, in which no method can preserve the state privacy of an agent under strong and full collusion attacks when all neighbors of the victim agent collusively infer its private information.
2) We propose a generic privacy-preserving framework, where random variables preserve the private information, the finite-time error compensation term eliminates the error caused by random variables, and the updating rule jump ensures the convergence of average consensus.
3) We prove that the proposed framework converges in both infinite- and finite-time average consensus and preserves the initial state of the agent in the situation that all except one neighbor are collusive, while adding-noise-based methods can only preserve privacy in the case of infinite-time consensus.
4) We analyze the impact of multiplying random variables when normally or Laplacian distributed random variables are utilized, with which the proposed framework performs better with larger variances of random variables.

The rest of this paper is structured as follows: Section II introduces related privacy-preserving methods for average consensus. Section III presents average consensus algorithms in detail and introduces the privacy disclosure problem with average consensus. Section IV proposes our privacy-preserving average consensus framework. Section V analyzes the convergence and privacy-preserving properties and makes comparisons with traditional adding-noise-based methods, and guides parameter design of the multiplicative noises. Section VI presents case studies, followed by concluding remarks in Section VII.

II. Related Work

Privacy-preserving average consensus has been a hot topic, and the approaches have three main categories: adding noise [19], [20], [21], [22], [23], homomorphic encryption [25], [26], [27], and state decomposition [28], [29], [30].

Adding-noise-based methods were first proposed. The work in [20] proposed a differential privacy-based method, where values of noises decay to zero w.p.1 when the average consensus algorithm converges, and the MAS is expected to converge to the average of agents' initial states. Mo and Murray proposed an algorithm in [19], in which a decay factor is utilized and the added noises are zero-sum. This algorithm can guarantee convergence and privacy preserving when only part neighbors of an agent are honest-but-curious. Based on the work in [19], He et al. [21] designed a secret function interaction mechanism to avoid neighbors collecting broadcast information. To evaluate the privacy-preserving performance of adding-noise-based methods, a novel index was defined in [22] to evaluate the privacy-preserving performance, termed (ϵ, δ)-data-privacy, which depicts the maximum privacy disclosure probability (MPDP) of private information, and becomes an efficient evaluation indicator.

Homomorphic encryption is a kind of asymmetric encryption methods, where each agent uses public and private keys to respectively encrypt and decrypt the states of each agent and the associated weights, and the product of data in the form of ciphertext is equal to the sum of that in the form of plaintext. The works in [25] and [26] applied Paillier cryptosystem into average consensus, andachieves privacy-preserving consensus based on homomorphic encryption. The work in [27] further extended the application of this method on push-sum average consensus. However, homomorphic encryption-based algorithms consume much computation and communication resources and may face the problem of running out of memory [31].

State decomposition was first proposed in [28], with which each agent constructs a virtual agent that has only one neighbor, i.e., the corresponding actual agent. In this algorithm, each actual agent updates its state based on the information received from its actual neighbors and its corresponding virtual agent, while each virtual agent updates its state only based on its corresponding actual agent. The works in [29] and [30] extended the method in [28] to push-sum average consensus and asynchronous average consensus, respectively. Further, the works in [32] and [33] proposed node decomposition and edge decomposition methods, respectively, where each agent is decomposed into multiple virtual agents in order to enhance the privacy-preserving performance. However, such methods usually inflate the network topology due to added virtual agents, and hence may decrease the consensus convergence speed.

III. Preliminaries

In this section, we introduce three most commonly known average consensus algorithms and identify the privacy disclosure problem.

A. Network Model

Consider a directed graph $\mathcal{G}$ with N agents, and the set of agents is denoted by $\mathcal{V}$. Let e_{ij} denote the communication link from agent j to agent i. e_{ij} is a $0-1$ variable, where $e_{ij}=1$ means the link exists, and 0 otherwise. Then we define $\mathcal{N}_i^{\text{in}}=\{j\in\mathcal{V}|e_{ij}=1\}$ (resp. $\mathcal{N}_i^{\text{out}}=\{j\in\mathcal{V}|e_{ji}=1\}$) as the in-neighbor (resp. out-neighbor) set of agent i with agent j being an in-neighbor (resp. out-neighbor) of agent i. The set of e_{ij} is represented by $\mathcal{E}\subset\mathcal{V}\times\mathcal{V}$. $\boldsymbol{W}(k)$ denotes the time-varying weighted adjacency matrix of $\mathcal{G}$. In summary, the graph is denoted as $\mathcal{G}=\{\mathcal{V},\mathcal{E},\boldsymbol{W}(k)\}$. Particularly, if $e_{ij}=e_{ji}$ holds for each agent i and j in graph $\mathcal{G}$, we call $\mathcal{G}$ an undirected graph. Then $\mathcal{N}_i^{\text{in}}=\mathcal{N}_i^{\text{out}}=\mathcal{N}_i$ and $d_i^{\text{in}}=d_i^{\text{out}}=d_i$ for each agent.

B. Average Consensus

Consider an undirected or strongly-connected directed graph, where each agent has an initial state $x_i(0)$. The average consensus aims to drive agents' states (or their ratios) converge to the average value $\bar{x}$ of all agents' initial states after infinite (or finite) iterations, e.g, in the infinite cases,

$$\lim_{k\to\infty} x_i(k)=\frac{1}{N}\sum_{i\in\mathcal{V}} x_i(0)=\bar{x}, \tag{1}$$

where k denotes the iteration number. To achieve average consensus, the following three updating rules are commonly used.

Algorithm 1 (Conventional Average Consensus, CAC): For an undirected graph $\mathcal{G}$, the updating rule of the CAC is

$$x_i(k+1)=w_{ii}(k)x_i(k)+\sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k), \tag{2}$$

where $w_{ij}(k)$ is the weighted adjacency for the link e_{ij} of agents i and j. The weights should ensure that $0<w_{ij}(k)\le\frac{1}{d_{\max}+1}$, $\sum_{j\in\mathcal{N}_i} w_{ij}(k)+w_{ii}(k)=1$, $w_{ij}(k)=w_{ji}(k)$, where $d_{\max}=\max_{i\in\mathcal{V}}\{d_i\}$. $\boldsymbol{W}(k)$ is the matrix form of $w_{ij}(k)$, which is a symmetric matrix. It has been proved that CAC converges and (1) holds if $\mathcal{G}$ is undirected and $\boldsymbol{W}(k)$ is doubly-stochastic [1].

Algorithm 2 (Push-Sum Average Consensus, PAC): For a strongly connected and directed graph, each agent designates $x_{i,1}(0)=x_i(0)$ and $x_{i,2}(0)=1$, and randomly generates $w_{pi}(k)$ and $w_{ii}(k)$ satisfying $w_{pi}(k)>0$, $w_{ii}(k)>0$, and $\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)+w_{ii}(k)=1$. At each iteration, each agent receives $w_{ij}(k)$, $x_{j,1}(k)$ and $x_{j,2}(k)$ from its j-th in-neighbor and sends $w_{pi}(k)$, $x_{i,1}(k)$ and $x_{i,2}(k)$ to its p-th out-neighbor. The updating rule for each agent is as follows:

$$x_{i,s}(k+1)=w_{ii}(k)x_{i,s}(k)+\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)x_{j,s}(k), s\in\{1,2\}. \tag{3}$$

The average is achieved in terms of:

$$\lim_{k\to\infty}\frac{x_{i,1}(k)}{x_{i,2}(k)}=\bar{x}. \tag{4}$$

It has been proved that PAC converges and (4) holds if $\mathcal{G}$ is directed connected and $\boldsymbol{W}(k)$ is column-stochastic [34].

Remark 1: In PAC, the communication topology is a directed graph where $w_{ij}(k)=w_{ji}(k)$ is not necessary, i.e., each agent can define its own adjacency weights. The convergence value in PAC is also the average value of the sum of all initial states, which is the same as CAC. Thus, PAC can be viewed as a form of average consensus.

Algorithm 3 (Finite-Time Average Consensus, FAC): For a strongly connected directed graph, where each agent designates $x_{i,1}(0)=x_i(0)$ and $x_{i,2}(0)=1$, and randomly generates w_{pi} and w_{ii} that satisfy $0<w_{pi}\le\frac{1}{d_i^{\text{out}}+1}$ and $\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}+w_{ii}=1$. At each iteration, each agent receives w_{ij}, $x_{j,1}(k)$ and $x_{j,2}(k)$ from its j-th in-neighbor and sends w_{pi}, $x_{i,1}(k)$ and $x_{i,2}(k)$ to its p-th out-neighbor. The updating rule for each agent is as follows:

$$x_{i,s}(k+1)=w_{ii}x_{i,s}(k)+\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}x_{j,s}(k), s\in\{1,2\}. \tag{5}$$

Convergence to the average value is achieved in a finite number of iterations, where each agent checks the convergence conditions as follows. For any $k=2h\ge 0$ where h is a positive integer, let

$$\Delta\boldsymbol{x}_{i,s}(0{:}2h)=(x_{i,s}(1)-x_{i,s}(0),\ldots,x_{i,s}(2h+1)-x_{i,s}(2h))^T, \tag{6}$$

where $s \in \{1,2\}$. Then the associated Hankel matrix of $\Delta \boldsymbol{x}_{i,s}(0\!:2h)^T$ is

$$\boldsymbol{H}(\Delta \boldsymbol{x}_{i,s}(0\!:2h)) = \begin{bmatrix} x_{i,s}(1)-x_{i,s}(0) & \cdots & x_{i,s}(h+1)-x_{i,s}(h) \\ x_{i,s}(2)-x_{i,s}(1) & \cdots & x_{i,s}(h+2)-x_{i,s}(h+1) \\ \vdots & \ddots & \vdots \\ x_{i,s}(h+1)-x_{i,s}(h) & \cdots & x_{i,s}(2h+1)-x_{i,s}(2h) \end{bmatrix}. \tag{7}$$

Each agent computes the rank of $\boldsymbol{H}(\Delta \boldsymbol{x}_{i,s}(0\!:2h))(s \in \{1,2\})$, and records the first defective matrix and iteration $2h_i$ when $\boldsymbol{H}(\Delta x_{i,s}(0\!:2h))$ firstly loses full rank. Let

$$\boldsymbol{\beta}_i = (\beta_i(0), \cdots, \beta_i(h_i-1), 1)^T \tag{8}$$

denote the kernel of the first defective matrix $\boldsymbol{H}(\Delta x_{i,s}(0\!:2h_i))$ of agent i, then each agent can obtain $\bar{x}$ by

$$\frac{\boldsymbol{x}_{i,1}(0\!:h_i)^T \boldsymbol{\beta}_i}{\boldsymbol{x}_{i,2}(0\!:h_i)^T \boldsymbol{\beta}_i} = \bar{x}, \tag{9}$$

where $\boldsymbol{x}_{i,s}(0\!:h_i) = (x_{i,s}(0), \ldots, x_{i,s}(h_i))^T$ [10]. It has been proved that FAC converges except for situations related to Lebesgue measure zero set [10]. FAC can be viewed as a special case of PAC, with which each agent can compute the convergence value in finite iterations and in a distributed manner.

To distinguish these updating rules in normal cases from the privacy-preserving algorithms in presence of inferrers as follows, we call the former the original average consensus algorithms.

C. Privacy Disclosure Under Collusion Inference

In the average consensus, consider the situation that there are a set of honest-but-curious agents (called inferrers in the following) who want to infer the initial states of a target agent i, i.e., $x_i(0)$. We call this case internal collusion inference.

Assumption 1: In this paper, we assume that all inferrers are honest-but-curious, and they do not tamper with other agents' data or the updating rule of the average consensus.

Based on the distribution of inferrers, internal collusion inference can be categorized into four types, as illustrated in Fig. 1.

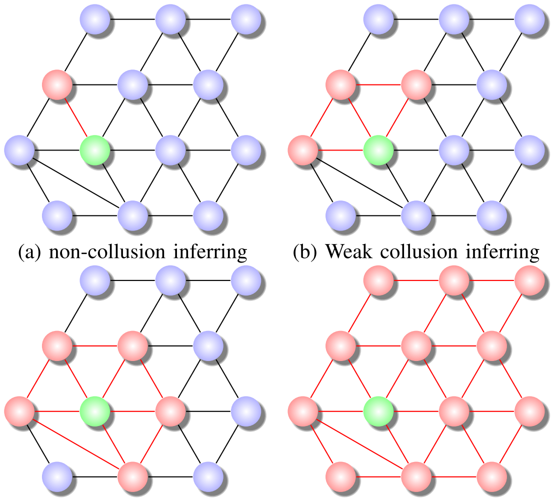
Definition 1 (Non-Collusion Inference): An inferrer infers the initial state of one of its neighbors, without colluding with any other agents.

Definition 2 (Weak Collusion Inference): For a target agent, a portion of its neighbors collaborate to infer the initial state of the agent, while there is at least one neighbor of the target agent who does not collude.

Definition 3 (Strong Collusion Inference): For a target agent, all of its neighbors collusively infer its initial state.

Definition 4 (Full Collusion Inference): For a target agent, all other agents in the network collusively infer its initial state.

Note that Definition 3 only considers one-hop neighbors of the target agent. Definition 4 also specifies the role of its other multi-hop neighbors. Hence, we can view the full collusion inference as a special case of the strong collusion inference.



(a) non-collusion inferring (b) Weak collusion inferring

(c) Strong collusion inferring (d) Full collusion inferring

Fig. 1. Four types of internal inferences, where green nodes denote the target agent, red nodes denote inferrers, and blue nodes denote normal ones.

Then we analyze the information about the target agent i known to the inferrers based on the updating rule in Algorithm 1. In the case of non-collusion inference, let $\mathcal{I}_i^j(k)$ be the information set about the target agent i accessible to the inferrer j at iteration k. Due to the existence of common neighbors of agents i and j, the information originating from the common neighbors can be utilized to infer the initial state of agent i. Hence, $\mathcal{I}_i^j(k)$ can be expressed as

$$\mathcal{I}_i^j(k) = \{w_{ij}(k)\} \cup \{\zeta_l(k) \,|\, l \in (\mathcal{N}_i \cap \mathcal{N}_j) \cup \{i\} \cup \{j\}\}, \tag{10}$$

where $\zeta_l(k)$ is the exchanged information of agent l, which has different meanings in different algorithms. For example, if agents do not apply any privacy-preserving algorithm, then $\zeta_l(k) = x_l(k)$; while if agents apply adding-noise-based methods, then $\zeta_l(k) = x_l(k) + \vartheta_l(k)$, where $\vartheta_l(k)$ denotes the added noise. Similarly, in the case of weak collusion inference, the information set of agent i accessible to the inferrers at iteration k can be defined as

$$\mathcal{I}_i^{\mathcal{A}_i}(k) = \bigcup_{j \in \mathcal{A}_i} \mathcal{I}_i^j(k) = (\cup_{j \in \mathcal{A}_i} \{w_{ij}(k)\}) \bigcup \{\zeta_l(k) \mid l \in (\mathcal{N}_i \cap (\cup_{j \in \mathcal{A}_i} \mathcal{N}_j)) \cup \mathcal{A}_i \cup \{i\}\}, \tag{11}$$

where $\mathcal{A}_i$ denotes the set of the inferrers of agent i. In the case of weak collusion inference, $\mathcal{A}_i \subsetneqq \mathcal{N}_i$. Specifically, $\mathcal{A}_i = j$ in the case of non-conclusion inference where agent j is the inferrer. Further, by letting $\mathcal{A}_i = \mathcal{N}_i$, we obtain the information set about agent i accessible to the inferrers in the case of strong collusion inference (i.e., all the neighbors) at iteration k

$$\mathcal{I}_i^{\mathcal{N}_i}(k) = \bigcup_{j \in \mathcal{N}_i} \mathcal{I}_i^j(k) = \{w_{li}(k), \zeta_l(k) \mid l \in \mathcal{N}_i \cup \{i\}\}. \tag{12}$$

Note that the information set accessible to the inferrers in the case of full collusion inference at iteration k is the same as $\mathcal{I}_i^{\mathcal{N}_i}(k)$, i.e., $\mathcal{I}_i^{\mathcal{V} \backslash \{i\}}(k) = \mathcal{I}_i^{\mathcal{N}_i}(k)$. This is because for any agent who is out of agent i's neighbors (i.e., $\mathcal{V} \backslash (\mathcal{N}_i \cup \{i\})$), its incoming information originated from agent i must be transferred by neighbors of agent i, and the neighbors cannot obtain any extra information of agent i. Also, we define the state set of agent i as $\mathcal{S}_i(k)$ at iteration k, i.e., $\mathcal{S}_i(k) = \{x_i(k)\}$ in the case of CAC, and $\mathcal{S}_i(k) = \{x_{i,2}(k), x_{i,2}(k)\}$ in the cases of PAC and FAC.

In this paper, we assume that for each individual inferrer (resp. weak, strong, and full collusion inferrers), the inferring process for $x_i(0)$ is based on $\mathcal{S}_j(0\colon k)$ (resp. $\mathcal{S}_{\mathcal{A}_i}(0\colon k)$, $\mathcal{S}_{\mathcal{N}_i}(0\colon k)$, $\mathcal{S}_{\mathcal{V}\backslash\{i\}}(0\colon k)$) and $\mathcal{I}_i^j(0\colon k)$ (resp. $\mathcal{I}_i^{\mathcal{A}_i}(0\colon k)$, $\mathcal{I}_i^{\mathcal{N}_i}(0\colon k)$, $\mathcal{I}_i^{\mathcal{V}\backslash\{i\}}(0\colon k)$), where $\mathcal{S}_{\mathcal{A}_i}(0\colon k)$ and $\mathcal{I}_i^{\mathcal{A}_i}(0\colon k)$ denote the state and information sets available to the inferrers $\mathcal{A}_i$ across iterations from 0 to k, respectively. Generally, collusion inferrers can utilize more information to infer $x_i(0)$ than an individual inferrer. If an agent has only one neighbor, the information sets and state sets in the cases of non-, weak, and strong collusion inferences are the same. If an agent has two or more neighbors while all non-inferrer neighbors of the target agent are the neighbors of inferrers, i.e., $\mathcal{N}_i\backslash\mathcal{A}_i \subset \bigcup_{j\in\mathcal{A}_i}\mathcal{N}_j$, the information available to the inferrers is the adjacency weight between the agent and infrerrers and the exchanged information between the agent and all its neighbors, i.e.,

$$\mathcal{I}_i^{\mathcal{A}_i}(0\!:\!k) = \bigcup_{h=0}^{k}\{w_{ji}(h), \zeta_l(h) \mid l \in \mathcal{N}_i \cup \{i\}, j \in \mathcal{A}_i\}. \quad (13)$$

It is obvious that (13) is also the most information available to the inferrers in the case of weak collusion inference. Compared with strong and full collusion inference, the information unavailable to the inferrers in the weak inference case is $\bigcup_{h=0}^{k}\{w_{ij}(h) \mid j \in \mathcal{N}_i\backslash\mathcal{A}_i\}$. Hence, inferrers can obtain more information in the case of strong and full collusion inference than weak collusion inference.

Next, we define privacy preserving in average consensus.

Definition 5: The private information of the target agent's initial state $x_i(0)$ is preserved if the inferrers cannot utilize their received information and state sets to estimate $x_i(0)$ with any guaranteed accuracy.

Definition 6: A privacy-preserving average consensus algorithm should preserve the information of the target agent's initial state $x_i(0)$ while ensuring that the MAS accurately converges to $\bar{x}$.

For quantitatively describing the performance of privacy-preserving algorithms, we introduce the following metric.

Definition 7 ([22]): Let x and $\hat{x}$ denote the true value and its corresponding inference, respectively, then the MPDP δ with a given error bound $\epsilon \geq 0$ is

$$\delta = \sup_{\hat{x}} \mathbb{P}\{|\hat{x} - x| \leq \epsilon | \mathcal{I}\},$$

where $\mathbb{P}\{\cdot\}$ denotes the probability of an event, $\mathcal{I}$ represents the information set utilized to infer x, sup denote the supremum of a set. For a given $\epsilon > 0$, if

$$\hat{x}^* \langle \epsilon \rangle = \operatorname*{argsup}_{\hat{x}} \mathbb{P}\{|\hat{x} - x| \leq \epsilon | \mathcal{I}\},$$

then $\hat{x}^* \langle \epsilon \rangle$ is called the optimal inference of x with ϵ.

In Definition 7, ϵ and δ are parameters that describe the privacy-preserving property of the algorithm, and with a given ϵ, the smaller δ, the better the privacy-preserving performance of the algorithm. Furthermore, $\hat{x}^* \langle \epsilon \rangle$ is a variable related to ϵ, i.e., if ϵ changes, $\hat{x}^* \langle \epsilon \rangle$ may also change.

Remark 2: In this paper, we choose MPDP instead of DP as the privacy metric. Comparing with DP, MPDP has advantages as follows. DP is first utilized as the privacy measure in the database managements, in which privacy of quantities of data needs to be protected. DP compare the similarity of two datasets where only one data in the two datasets is different. However, in the average consensus, for each agent, only the privacy of $x_i(0)$ needs to be preserved. From the perspective of the inferrers, they have the capacity to estimate $x_i(0)$ in the limited range based on the information set and state set. While for each agent, only if the estimation of $x_i(0)$ by the inferrers is close to $x_i(0)$, the privacy of the agent is threatened. In [22], MPDP is developed to measure the performance of privacy preserving average consensus algorithms, in which the *close degree* of the estimated one and the actual one is reflected by ϵ in Definition 7. While in DP, there is no metric of the close degree. Hence, we choose MPDP as the privacy metric in this paper.

As for the four aforementioned inferences, we first discuss the possibility of privacy preserving in presence of strong and full collusion inferences. For each agent i, let the averaging process be expressed as an averaging function $f_i(\cdot)$:

$$\bar{x} = f_i(x_i(0)|\mathcal{S}_{\mathcal{N}_i}(0\colon\infty), \mathcal{I}_i^{\mathcal{N}_i}(0\colon\infty)). \quad (14)$$

The following assumption and lemmas are needed.

Assumption 2: Assume that the averaging function $f_i(\cdot)$ is injective.

Lemma 1: For any agent $i \in \mathcal{V}$, the averaging function $f_i(\cdot)$ under CAC, PAC and FAC is injective.

Proof: See Appendix A. ■

Based on the above lemma, we can derive the following theorem:

Theorem 1: For any privacy-preserving algorithm that meets Assumption 2, it cannot preserve the initial state of agent i against strong and full collusion inferences.

Proof: Given the information and state sets $\mathcal{I}_i^{\mathcal{N}_i}(0\colon k)$ and $\mathcal{S}_{\mathcal{N}_i}(0\colon k)$ available to the inferrers, the convergence value $\bar{x}$ is fixed. Then, for any privacy-preserving algorithm meeting Assumption 2 and Definition 6, by the injectiveness of the resulting averaging function, the initial state $x_i(0)$ is unique. Hence, the inferrers can uniquely infer $x_i(0)$ in the case of strong and full collusion inferences. ■

To the best of our knowledge, the state-of-the-art privacy-preserving algorithms only consider the situations that non- or weak collusion inferences occur. In addition, traditional privacy-preserving infinite-time average consensus algorithms usually add some random variable $\vartheta_i(k)$ into $x_i(k)$ to preserve its privacy, e.g., the updating rule based on CAC is as follows:

$$x_i^+(k) = x_i(k) + \vartheta_i(k), \quad (15)$$

$$x_i(k+1) = w_{ii}x_i^+(k) + \sum_{j\in\mathcal{N}_i} w_{ij}x_j^+(k). \quad (16)$$

These classical methods can preserve the initial states of agent i in the case of non- and weak collusion inferences if the corresponding original average consensus algorithms converge at infinite time horizon, which are not suitable for those in finite-time convergence cases.

IV. Privacy-Preserving Framework

Motivated to handle finite-time convergence cases, in this section, we present a novel and generic privacy-preserving average consensus framework. The proposed framework consists of two phases as divided by a phase-switching time $k_i > 0$ for each agent $i \in \mathcal{V}$. In each iteration k within the first phase (i.e., $k \leq k_i$), each agent calculates a fusion result $\xi_{i,s}(k)$ based on all the information ($\xi_{j,s}(k)$) received from its in-neighbors. It also calculates a finite-time error compensation term $z_{i,s}(k)$. The agent updates its state $x_{i,s}(k)$ by summing $\xi_{j,s}(k)$ and $z_{i,s}(k)$ together, as shown in (20). Meanwhile, it blurs $\xi_{i,s}(k)$ by multiplying a random variable $\theta_{i,s}(k)$ and broadcasts the result $\zeta_{i,s}(k)$ to its out-neighbors, as shown in (17). In phase 2 (i.e., $k \geq k_i$), each agent operates the original consensus algorithm. Note that only $s = 1$ is taken into account in the case of CAC. At each iteration, each agent receives $\zeta_{j,s}(k)$ and $w_{ij}(k)$ from its in-neighbors and sends $\zeta_{i,s}(k)$ and $w_{pi}(k)$ to its out-neighbors. Switching from Phase 1 to Phase 2 is the so-called updating rule jump.

As Fig. 2 shows, the updating rule for the proposed framework is summarized as follows:

- Phase 1: $\forall k \leq k_i$, the state for agent i is updated by

$$\zeta_{i,s}(k) = \theta_{i,s}(k)\xi_{i,s}(k), \tag{17}$$

$$\xi_{i,s}(k+1) = w_{ii}(k)\xi_{i,s}(k) + \sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)\zeta_{j,s}(k), \tag{18}$$

$$z_{i,s}(k+1) = z_{i,s}(k) + \sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)\left(\xi_{i,s}(k) - \zeta_{i,s}(k)\right), \tag{19}$$

$$x_{i,s}(k+1) = \xi_{i,s}(k+1) + z_{i,s}(k+1), \tag{20}$$

where $\xi_{i,s}(0) = x_{i,s}(0)$, $z_{i,s}(0) = 0$.

- Phase 2: $\forall k \geq k_i + 1$, the state for agent i is updated by

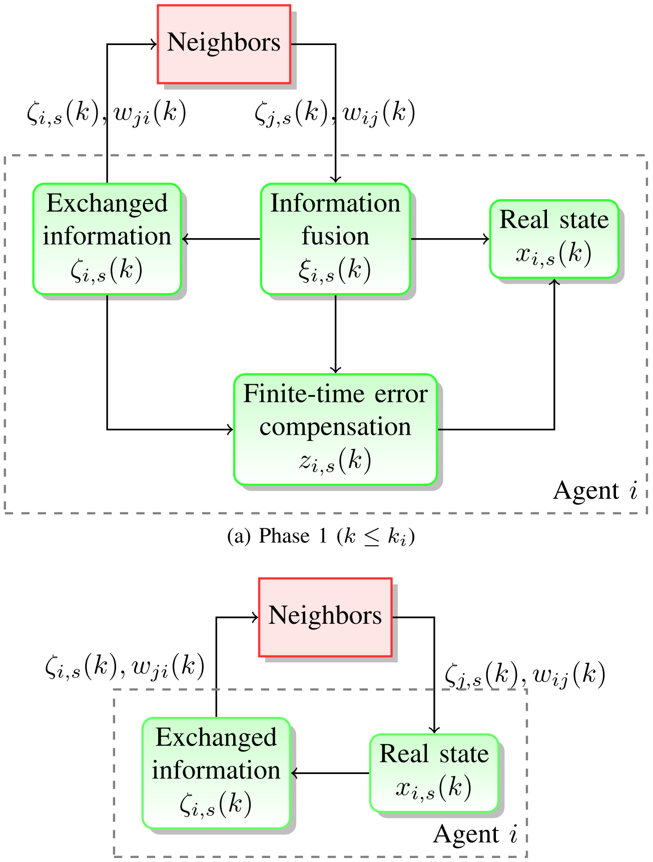
$$\zeta_{i,s}(k) = x_{i,s}(k), \tag{21}$$

$$x_{i,s}(k+1) = w_{ii}(k)x_{i,s}(k) + \sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)\zeta_{j,s}(k), \tag{22}$$

where $w_{ij}(k)$ yields to the constraints in the original updating rules. For example, $w_{ij}(k)$ is time-invariant in FAC, which is also time-invariant at Phase 2.

Remark 3: The proposed framework has two phases. The main purpose of phase 1 is to preserve the privacy of $x_i(0)$, and that of phase 2 is to converge. In phase 1, we design the multiplicative noise as the measure to preserve the data privacy, and develop the finite-time error compensation term to maintain the accuracy of the average value of the real-time states, i.e., $\frac{1}{N}\sum_{i\in\mathcal{V}} x_i(k)$. In phase 2, without of generality, we directly apply the original form of average consensus as it can guarantee the convergence of the framework.

Remark 4: Note that $\theta_{i,s}(k)$ is not specified in the proposed framework, which means a random variable of any probability distribution except for $\theta_{i,s}(k) = 1$ can be utilized in the proposed framework. $\theta_{i,s}(k) = 1$ cannot be applied as $\zeta_{i,s}(k) = \xi_{i,s}(k)$ holds if $\theta_{i,s}(k)$ is constant 1, and the privacy is sure to be disclosed. We will analyze the effects of the types of random variables in Section V-D.


Neighbors
$\zeta_{i,s}(k), w_{ji}(k)$
$\zeta_{j,s}(k), w_{ij}(k)$
Exchanged information $\zeta_{i,s}(k)$
Information fusion $\xi_{i,s}(k)$
Real state $x_{i,s}(k)$
Finite-time error compensation $z_{i,s}(k)$
Agent i

(a) Phase 1 ($k \leq k_i$)

Neighbors
$\zeta_{i,s}(k), w_{ji}(k)$
$\zeta_{j,s}(k), w_{ij}(k)$
Exchanged information $\zeta_{i,s}(k)$
Real state $x_{i,s}(k)$
Agent i

(b) Phase 2 ($k \geq k_i + 1$)

Fig. 2. Updating rules of the proposed framework.

V. Main Results

In this section, we first prove that the proposed framework converges to the true average value. Then we analyze its privacy-preserving performance in the presence of collusion inference. Finally, we discuss the impact of the random variables $\theta_{i,s}(0)$.

A. Convergence

For ease of exposition, let $\underline{k}$ and $\overline{k}$ denote $\min\{k_i, i \in \mathcal{V}\}$, and $\max\{k_i, i \in \mathcal{V}\}$, respectively. The following theorem proves the convergence of the proposed framework.

Theorem 2: If the original average consensus algorithm converges, then the proposed framework converges, and the convergence is irrelevant to the probability distribution of $\theta_{i,s}(k)$.

Proof: The detailed proof is given in Appendix B. Briefly, we first show that, before $k \leq \overline{k}$, the states of the agents maintain that $\sum_{i\in\mathcal{V}} x_{i,s}(k) = \sum_{i\in\mathcal{V}} x_{i,s}(0)$. Therefore, at iteration $\overline{k} + 1$, the states of the agents can be viewed as another set of states that has the same average value. Then, after $k > \overline{k}$, the proposed framework behaves the same as the original consensus algorithm and converges to the same average value. ■

Remark 5: The convergence process of the proposed framework is irrelevant to $\theta_{i,s}(k)$. Hence, the probability distributions of $\theta_{i,s}(k)$ can be designed while the convergence of the proposed framework is not influenced. Even if $\theta_{i,s}(k)=0$ at each iteration, $z_{i,s}(k)=z_{i,s}(k-1)+\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k-1)\xi_{i,s}(k-1)$, and $\sum_{i\in\mathcal{V}} x_{i,s}(k)=\sum_{i\in\mathcal{V}} x_{i,s}(0)$ holds. Hence, $\theta_{i,s}(k)=0$ does not affect the convergence of the proposed framework.

B. Privacy-Preserving Performance

Since we have shown that under Assumption 2, the private information of the agents' initial states cannot be preserved in presence of either strong or full collusion inference, we thus analyze the performance of the proposed framework against non- and weak collusion inference.

It is obvious that if the proposed framework can protect the private information under any weak collusion inference, it can also protect the private information under individual inference. This is because the elements in the information set $\mathcal{I}_i(k)$ obtained in the case of weak collusion inference are more than those in the case of individual inference.

Theorem 3: The private information of any agent i, i.e., $x_i(0)$, can be preserved against non- and weak collusion inference if and only if there is at least one neighbor who does not collude with the inferrers.

Proof: See Appendix C. ■

When all information in $\mathcal{I}_i^{\mathcal{A}_i}(0\colon k)$ and $\mathcal{S}_{\mathcal{A}_i}(0\colon k)$ is utilized to deduce the updating process in (17)-(20), the inferrers still cannot infer $x_i(0)$ due to lack of $\theta_{i,1}(k)(k=0,1,\ldots,k_i)$.

C. Comparison With Adding-Noise-Based Methods

In the literature, the privacy of the agents' initial states can also be preserved by the methods that add noises to the states [22]. Below we show that our framework can achieve the same privacy-preserving performance as those adding-noise methods in cases of CAC and PAC. However, in the case of FAC, our framework still works while the existing adding-noise-based methods such as those in [19] and [21] cannot.

When the inferrers randomly infer $x_i(0)$ by conjecturing $\theta_{i,1}(k)$, there exists a probability that they guess $x_{i,1}(0)$ with a limited error. For quantitatively describing the performance of random inferring and discussing the impact of the multiplicative noise, we adopt MPDP in Definition 7.

1) Comparison in the CAC Case: Under the metric given in Definition 7, the following results can be obtained for privacy-preserving CAC.

Theorem 4: Under the non- (resp. weak) collusion inference in the case of CAC, the proposed framework can achieve the same privacy-preserving performance in terms of MPDP as that of adding-noise-based algorithms.

Proof: See Appendix D. ■

2) Comparison in the PAC Case: Since traditional adding-noise-based methods are mainly for CAC, we hence construct the following privacy-preserving method based on the adding-noise-based method in [19] and [21]. At each iteration, each agent generates a random variable $\vartheta_i(k)$ by

$$\vartheta_i(k)=\begin{cases} v_i(0), & \text{if } k=0\\ \varphi^k v_i(k)-\varphi^{k-1}v_i(k-1), & \text{if } k>0\end{cases}, \tag{23}$$

where $\varphi\in(0,1)$ is a decay factor, $v_i(k)$ is a standard normally distributed noise. Then the agents exchange information and update their states by

$$x_{i,s}^{+}(k)=\begin{cases} x_{i,s}(k)+\vartheta_i(k), & \text{if } s=1\\ x_{i,s}(k), & \text{if } s=2\end{cases}, \tag{24}$$

$$x_{i,s}(k+1)=w_{ii}(k)x_{i,s}^{+}(k)+\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)x_{j,s}^{+}(k), s=1,2. \tag{25}$$

Then we compare the constructed algorithm as in (23)-(25) with our proposed framework, and we can derive the following theorem.

Theorem 5: Under the non- (resp. weak) collusion inference in the case of PAC, the proposed framework can achieve the same privacy-preserving performance in terms of MPDP as that of adding-noise-based algorithms.

The proof is similar to that of Theorem 4 and is omitted herein.

3) Comparison in the FAC Case: It is worth noticing that traditional adding-noise-based methods such as those proposed in [19] and [21] cannot solve the privacy preservation problem under FAC cases. This is because the added noise $\vartheta_i(k)$ in (15) becomes zero-sum over time and decays as k goes infinity, i.e., $\lim_{k\to\infty}\vartheta_i(k)=0$, while $\vartheta_i(k)$ does not vanish in finite time and it is hard to ensure zero-sum over time. Therefore, we have the following remark.

Remark 6: In the case of FAC, the privacy-preserving methods proposed in [19] and [21] cannot ensure the accuracy of convergence of FAC.

Remark 7: To our best knowledge, there is no privacy-preserving FAC algorithm in the literature. The existing works rarely use adding-noise-based methods to protect the private information of FAC, because directly adding noise cannot make FAC converge properly.

However, due to our proposed finite-time error compensation term and updating rule jump mechanism, the privacy preservation problem under FAC is addressed, which is the main difference and innovation compared with adding-noise-based methods.

D. Impact of the Multiplicative Noise

In the proof of Section V-B, we have found that the inferrers cannot infer $x_i(0)$ under non- or weak collusion inference for the sake of the existence of $\frac{1}{\theta_{i,1}(0)}$. However, if the probability density functions (PDFs) of $\frac{1}{\theta_{i,1}(0)}$ are known to the inferrers, they can infer the probability distribution of $x_i(0)$ to make δ as large as possible. Here we assume that the PDFs of $\frac{1}{\theta_{i,1}(k)}$ are different at different iterations. Then we can formulate the problem as follows:

$$\min_{\left\{f_{\frac{1}{\theta_{i,1}(0)}}(t)\right\}}\left\{\sup_{\hat{x}_i(0)}\mathbb{P}\left\{|\hat{x}_i(0)-x_i(0)|\le\epsilon|\mathcal{I}_i^j(0)\right\}\right\}. \tag{26}$$

Under a given ϵ, the objective of designing $\frac{1}{\theta_{i,1}(0)}$ is to make the MDPD δ as small as possible. Since Theorem 2 reveals that the convergence process of the proposed framework is irrelevant to $\theta_{i,s}(k)$, the probability distributions of $\theta_{i,1}(k)$ can be actively designed. Since normal and Laplacian distributions are widely used in privacy preserving, we investigate the impact of $\frac{1}{\theta_{i,1}(0)}$ on the privacy-preserving performance when $\frac{1}{\theta_{i,1}(0)}$ obeys normal or Laplacian distribution, i.e., $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$ or $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$, where $\sigma_{i,1}(0)$ and $\lambda_{i,1}(0)$ are the variances parameters. Then the parameter design problem becomes to design $\sigma_{i,1}(0)$ and $\lambda_{i,1}(0)$. The following theorem depicts the impact of $\sigma_{i,1}(0)$ and $\lambda_{i,1}(0)$.

Theorem 6: If $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$, then the proposed framework based on any of the CAC, PAC and FAC algorithms achieves a smaller MPDP with a larger $\sigma_{i,1}(0)$, and the achieved MPDP is

$$\delta\left\langle\epsilon\right\rangle = \operatorname{erf}\left(\frac{\epsilon}{\sqrt{2}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}\right), \tag{27}$$

where $\operatorname{erf}(\cdot)$ denotes the error function. Similarly, if $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$, the proposed framework can achieve a lower MPDP with a larger $\lambda_{i,1}(0)$, and the achieved MPDP is

$$\delta\left\langle\epsilon\right\rangle = 1 - \exp\left(-\frac{\epsilon}{|\zeta_{i,1}(0)|\lambda_{i,1}(0)}\right). \tag{28}$$

Proof: From the viewpoint of the inferrers, $\zeta_{i,1}(0)$ is a known parameter. Since $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$, they can infer the PDF of $x_i(0)$ via (42):

$$f_{x_i(0)}(t) = \frac{1}{\sqrt{2\pi}|\zeta_{i,1}(0)|\sigma_{i,1}(0)} \exp\left(-\frac{t^2}{2(\zeta_{i,1}^2(0)\sigma_{i,1}^2(0))}\right).$$

Agent i can achieve less MPDP via designing $f_{\frac{1}{\theta_{i,1}(0)}}(t)$ and minimizing $\max f_{\frac{1}{\theta_{i,1}(0)}}(t)$. Computing the first order of $f_{\frac{1}{\theta_{i,1}(0)}}(t)$, termed as $f_{\frac{1}{\theta_{i,1}(0)}}(t)'$, and letting $f_{\frac{1}{\theta_{i,1}(0)}}(t)' = 0$, we have

$$\sup f_{x_i(0)}(t) = f_{x_i(0)}(0) = \frac{1}{\sqrt{2\pi}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}.$$

Hence, $\sup f_{x_i(0)}(t)$ is monotonically decreasing in $\sigma_{i,1}(0)$. Similarly, the MPDP for $x_i(0)$ under the proposed framework can be formulated as follows:

$$\begin{aligned}
\delta\left\langle\epsilon\right\rangle &= \sup_{\hat{x}_i(0)} \mathbb{P}\{|\hat{x}_i(0) - x_i(0)| \leq \epsilon|\mathcal{I}\} \\
&= \sup_{\hat{\theta}_{i,1}(0)} \mathbb{P}\left\{|\frac{1}{\hat{\theta}_{i,1}(0)} - \frac{1}{\theta_{i,1}(0)}| \leq \frac{\epsilon}{|\zeta_{i,1}(0)|} \mid \mathcal{I}_i^j(0)\right\} \\
&= \sup_{\frac{1}{\hat{\theta}_{i,1}(0)}} \int_{\frac{1}{\hat{\theta}_{i,1}(0)} - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}_{i,1}(0)} + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt \\
&= \int_{-\frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt \\
&= \int_{-\frac{\epsilon}{|\zeta_{i,1}(0)|\sigma_{i,1}(0)}}^{\frac{\epsilon}{|\zeta_{i,1}(0)|\sigma_{i,1}(0)}} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}\, dt \\
&= \operatorname{erf}\left(\frac{\epsilon}{\sqrt{2}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}\right).
\end{aligned} \tag{29}$$

The proof process when $\frac{1}{\theta_{i,1}(0)}$ obeys Laplacian distribution is similar to that of normal distribution and is omitted herein. ■

Remark 8: In the above, we only discussed the PDF of $\theta_{i,1}(0)$, while those of $\theta_{i,1}(1)$, $\theta_{i,1}(2)$, ..., and $\theta_{i,1}(k_i)$ are neglected. This is because $w_{ii}(k)$ $(0 \leq k \leq k_i)$ is unknown under non- and weak collusion inferences, which means agent i can set the PDFs of $\theta_{i,1}(1)$, $\theta_{i,1}(2)$, ..., and $\theta_{i,1}(k_i)$ arbitrarily, and does not worry about the change of the probability of indirect inferring.

If $\theta_{i,1}(0)$ obeys normal or Laplace distribution, the initial state of agent i is sure to be disclosed if $x_{i,1}(0) = 0$. Because 0 is out of the domain of $\theta_{i,1}(0)$ if $\theta_{i,1}(0)$ is generated according to the conditions in Theorem 6, the inferrers can easily infer that $\xi_{i,1}(0) = 0$ via $\zeta_{i,1}(0) = 0$. When such a special case occurs, the agent can add noise instead of multiplying noise to preserve the private information at iteration 0. Here we can summarize the method as follows:

$$\zeta_{i,1}(0) = \begin{cases} \xi_{i,1}(0) + \theta_{i,1}(0), & \text{if } \xi_{i,1}(0) = 0 \\ \theta_{i,1}(0)\xi_{i,1}(0), & \text{otherwise} \end{cases}, \tag{30}$$

where $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$ or $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$. Then we analyze the privacy-preserving performance of the method (30), and we derive the following corollary:

Corollary 1: If $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$, then the proposed framework with the method (30) based on any of the CAC, PAC and FAC algorithms achieves a smaller MPDP with a larger $\sigma_{i,1}(0)$, and the achieved MPDP is

$$\begin{aligned}
\delta\left\langle\epsilon\right\rangle = \max\Bigg\{&1 - \operatorname{erf}\left(\frac{1}{\sqrt{2}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}\right), \\
&\operatorname{erf}\left(\frac{\epsilon}{\sqrt{2}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}\right)\Bigg\}.
\end{aligned} \tag{31}$$

Similarly, if $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$, the proposed framework can achieve a lower MPDP with a larger $\lambda_{i,1}(0)$, and the achieved MPDP is

$$\begin{aligned}
\delta\left\langle\epsilon\right\rangle = \max\Bigg\{&\exp\left(-\frac{1}{|\zeta_{i,1}(0)|\lambda_{i,1}(0)}\right), \\
&1 - \exp\left(-\frac{\epsilon}{|\zeta_{i,1}(0)|\lambda_{i,1}(0)}\right)\Bigg\}.
\end{aligned} \tag{32}$$

Proof: From the perspective of the inferrers, they should consider if $\xi_{i,1}(0) = 0$. Here we assume that $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$, and analyze the two cases: $\xi_{i,1}(0) = 0$, and $\xi_{i,1}(0) \neq 0$.

Case I: $\xi_{i,1}(0) = 0$.

In this case, $\zeta_{i,1}(0) = \theta_{i,1}(0)$ holds, and the inferrers evaluate the probability of $\xi_{i,1}(0) = 0$ according to the probability of $\frac{1}{|\theta_{i,1}(0)|}| \geq \frac{1}{|\zeta_{i,1}(0)|}$:

$$\begin{aligned}
&\mathbb{P}\{\xi_{i,1}(0) = 0\} \\
=&\mathbb{P}\left\{\frac{1}{|\theta_{i,1}(0)|}| \geq \frac{1}{|\zeta_{i,1}(0)|}\right\}
\end{aligned}$$

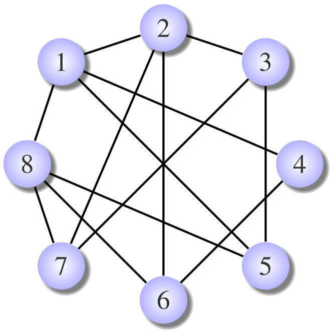


Fig. 3. Topology of the undirected graph for simulating CAC.

$$
\begin{aligned}
&=\int_{\frac{1}{|\zeta_{i,1}(0)|}}^{+\infty} f_{\frac{1}{\theta_{i,1}(0)}}(t)\,dt + \int_{-\infty}^{-\frac{1}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\,dt \\
&=2\int_{\frac{1}{|\zeta_{i,1}(0)|}}^{+\infty} f_{\frac{1}{\theta_{i,1}(0)}}(t)\,dt \\
&=2\int_{\frac{1}{|\zeta_{i,1}(0)|\sigma_{i,1}(0)}}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}}\,dt \\
&=1-\operatorname{erf}\left(\frac{1}{\sqrt{2}|\zeta_{i,1}(0)|\sigma_{i,1}(0)}\right). \qquad (33)
\end{aligned}
$$

Note that (33) is not relevant to ϵ as the inferrers as the inferrers directly estimate $\hat{x}_{i,1}(0) = 0$.

Case II: $\xi_{i,1}(0) \neq 0$.

The MPDP of case II is (27). The proof is the same as that of Theorem 6 and is omitted herein.

By summarizing the above two cases, we deduce that the MPDP of the method (30) is the greater value of (27) and (33), i.e., (31).

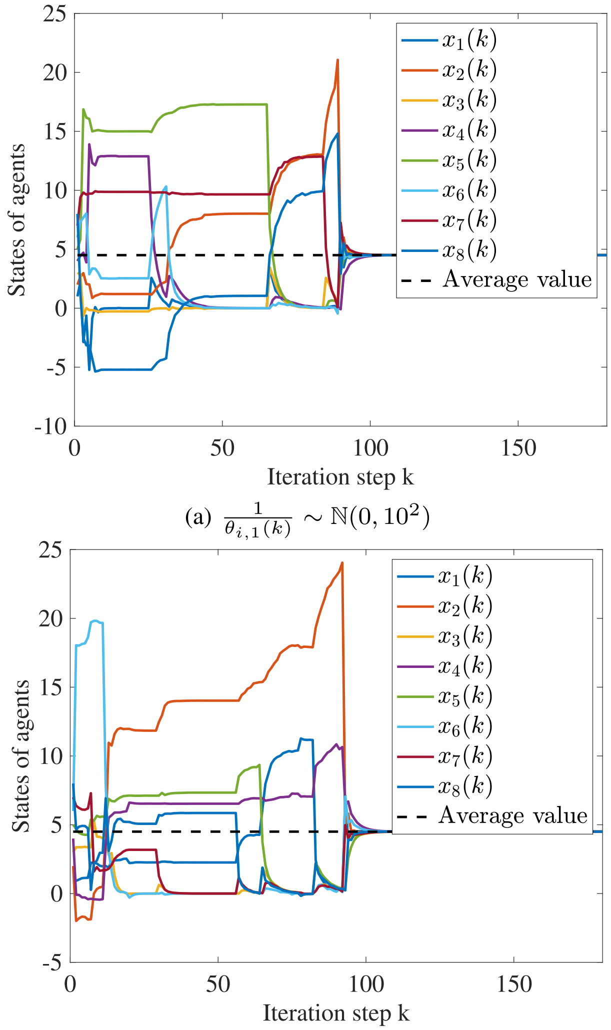
The proof process when $\frac{1}{\theta_{i,1}(0)}$ obeys Laplacian distribution is similar to that of normal distribution and is omitted herein. ∎

VI. Case Studies

In this section, we demonstrate the effectiveness of the proposed framework for CAC, PAC, and FAC via simulations.

For the case of CAC, consider an undirected graph with 8 agents, which is depicted in Fig. 3. The initial state vector for the agents is $(1, 2, \ldots, 8)^T$. Each of the weight, w_{ij} is set as $\frac{1}{5}$ due to $d_{\max} = 4$. As a case study, we assume that the random variable noise $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{N}(0, 10^2)$ or $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{L}(0, 10)$ and for each agent, the phase-switching time k_i is an integer independently and randomly chosen within $[1, 100]$. The evolution of the agents' states under the proposed framework based on CAC is shown in Fig. 4. It can be observed that all agents converge to the correct average value of their initial states validating Theorem 2. Meanwhile, the state of each agent oscillates intensely before the iteration $k = 100$, because the multiplicative noises are added in phase 1 in the purpose of preserving the states' privacy.

For the cases of PAC and FAC, consider a directed graph with 8 agents as depicted in Fig. 5. The multiplicative noise is chosen as $\frac{1}{\theta_{i,s}(k)} \sim \mathbb{N}(0, 10^2)$, and each k_i is set the same as above. The iteration process of the proposed framework with Algorithm 2 and 3 are shown in Fig. 6 and Fig. 7, respectively. Similar as above, with the proposed framework based on PAC and FAC, the state of each agent varies intensively in phase 1 due to the effect of the multiplicative noise for the purpose of privacy preserving. However, the state $x(k)$ of each agent converges to an independent value, and the ratio of $x_{i,1}(k)$ and $x_{i,2}(k)$ converges to the right average value of their initial states. In particular, as Fig. 7 shows, under the proposed



(a) $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{N}(0, 10^2)$

(b) $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{L}(0, 10)$

Fig. 4. Performance of the proposed framework based on CAC.

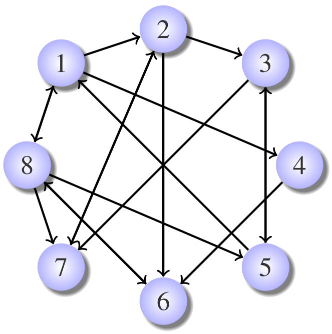
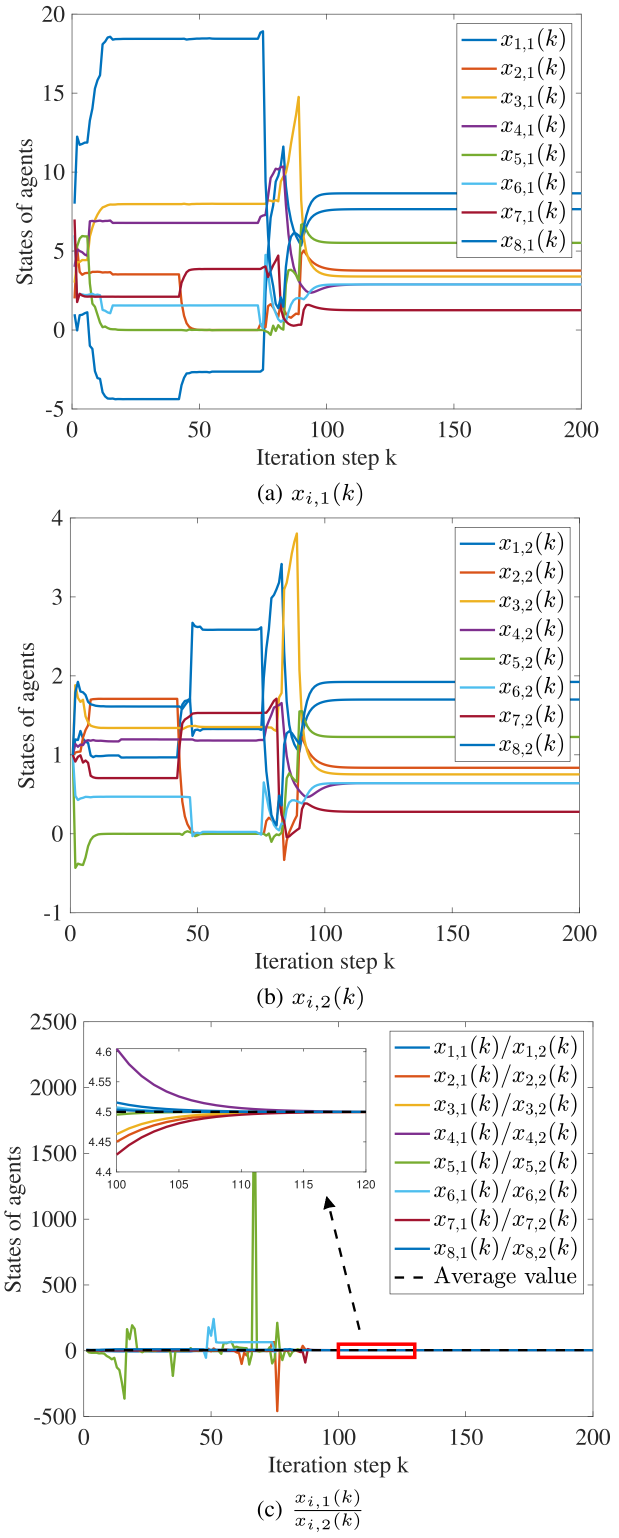


Fig. 5. Topology of the directed graph for simulating PAC and FAC.

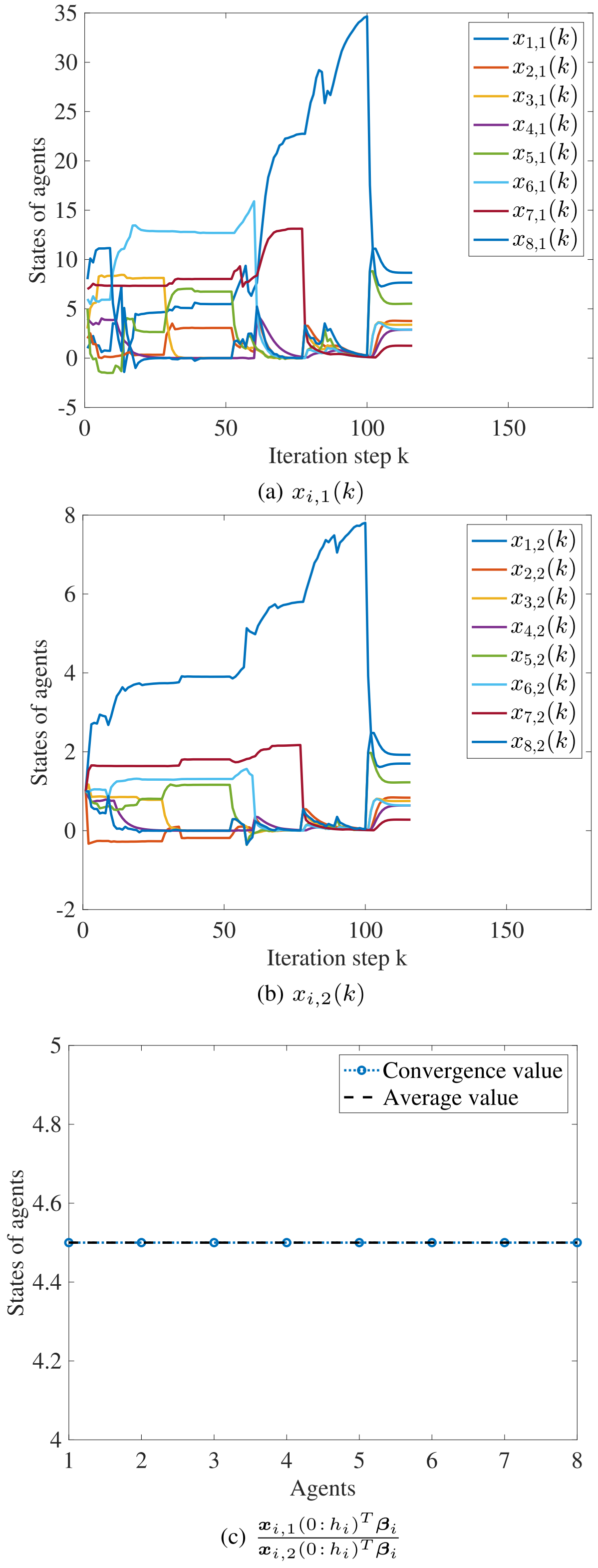


(a) $x_{i,1}(k)$

(b) $x_{i,2}(k)$

(c) $\frac{x_{i,1}(k)}{x_{i,2}(k)}$

Fig. 6. Performance of the proposed framework based on PAC.



(a) $x_{i,1}(k)$

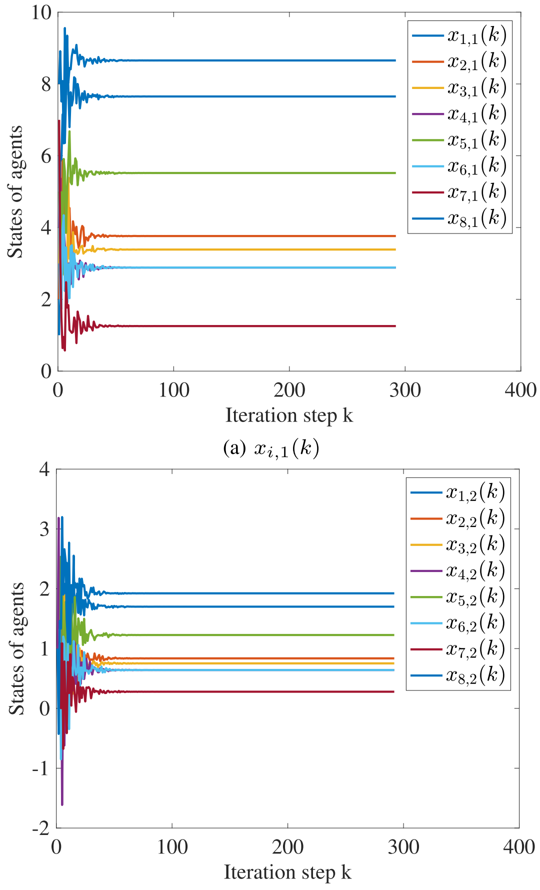
(b) $x_{i,2}(k)$

(c) $\frac{\boldsymbol{x}_{i,1}(0:h_i)^T\boldsymbol{\beta}_i}{\boldsymbol{x}_{i,2}(0:h_i)^T\boldsymbol{\beta}_i}$

Fig. 7. Performance of the proposed framework based on FAC.

framework for FAC, the evolution of the agents' states steps at 100, which means the convergence of the states at a finite time is maintained even with the multiplicative noise injected.

To further demonstrate the performance of the proposed framework in case of FAC, we conduct simulations and compare it with that of the adding-noise-based method described in (23), where $\varphi = 0.9$. Fig. 8 shows the iteration process under the method in (23), which converges at step 115. Compared with the convergence process in Fig. 7, it is obvious that the MAS converges faster under our proposed framework. Furthermore, the mean absolute error of the convergence val-



(a) $x_{i,1}(k)$

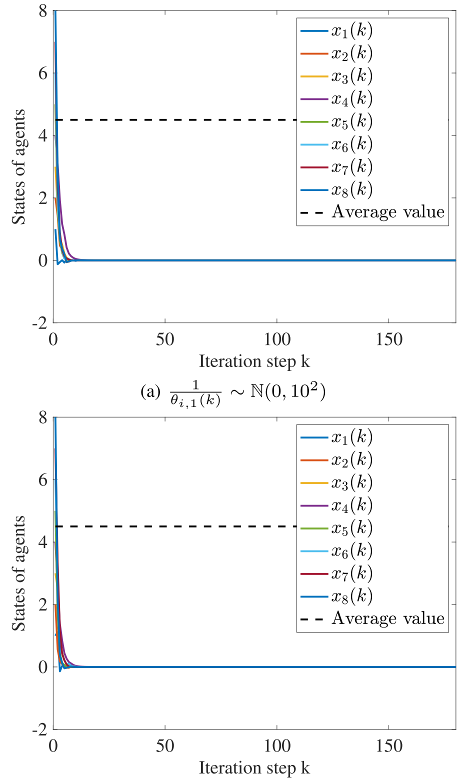
(b) $x_{i,2}(k)$

Fig. 8. Performance of the adding-noise-based method in (23) for FAC.

ues under the method in (23) is 8.175×10^{-6}, which is larger than that of the proposed framework, which is 6.055×10^{-12}. These demonstrate that our proposed framework converges faster and more accurately than the method in (23).

To illustrate the performance of the error compensation term, we simulate the proposed framework without (19) based on CAC. The parameters setting is the same as that of Fig. 4. As Fig. 9 shows, the states of all agents converge to 0, while the average value is 4.5. Hence, the proposed error compensation term is critical to the accurate convergence of average consensus.

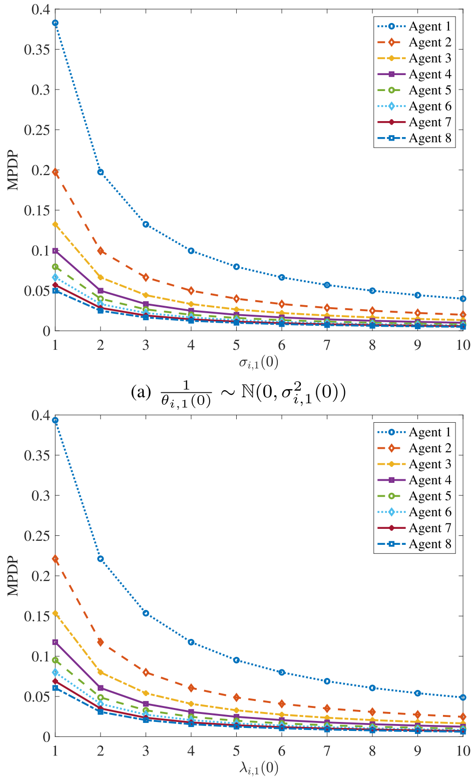
Then we evaluate the proposed framework in terms of the achieved MPDP under different $\sigma_{i,1}(0)$ and $\lambda_{i,1}(0)$, with $\theta_{i,1}(0)$ randomly generated such that $\frac{1}{\theta_{i,s}(k)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$ or $\frac{1}{\theta_{i,s}(k)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$. Since $\zeta_{i,1}(0)$ is known to the inferrers, we set $\zeta_{i,1}(0) = x_{i,1}(0)$. From the results shown in Fig. 10, we observe that, as either $\sigma_{i,1}(0)$ or $\lambda_{i,1}(0)$ increases, the achieved MPDP decreases. This indicates that the agents can choose larger $\sigma_{i,1}(0)$'s or $\lambda_{i,1}(0)$'s for better privacy-preserving performance as showed in Theorem 6. Moreover, the agents are likely to achieve a smaller MPDP with larger initial values. For example, since $x_8(0) > x_4(0)$, the MPDP of agent 8 is smaller than that of agent 4 as shown in Fig. 10a. Because according to Theorem 6, with the given ϵ and $\sigma_{i,1}(0)$ (or $\lambda_{i,1}(0)$), the proposed framework achieves a smaller MPDP with a larger $\zeta_{i,1}(0)$.



(a) $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{N}(0, 10^2)$

(b) $\frac{1}{\theta_{i,1}(k)} \sim \mathbb{L}(0, 10)$

Fig. 9. Performance of the proposed framework without error compensation term based on CAC.



(a) $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{N}(0, \sigma_{i,1}^2(0))$

(b) $\frac{1}{\theta_{i,1}(0)} \sim \mathbb{L}(0, \lambda_{i,1}(0))$

Fig. 10. The MPDP under different $\sigma_{i,1}(0)$ and $\lambda_{i,1}(0)$.

VII. Conclusion

This paper has systematically investigated the privacy disclosure problem caused by collusion inference in average consensus. We have proposed a generic privacy-preserving framework for CAC, PAC, and FAC, with three novel mechanisms including multiplying noise, finite-time error compensation, and updating rules jump. We have proved that the proposed framework ensures consensus convergence to the right value while preserving the privacy the initial states of the agents in the presence of non- and weak collusion inference. Moreover, we have proved that the proposed framework can achieve the same MPDP as adding-noise-based methods in the cases of CAC and PAC. We also have shown that the proposed framework ensures finite-time convergence with privacy preserving, which cannot be achieved by the existing traditional adding-noise-based method. Simulation results demonstrate the effectiveness of the proposed framework.

Appendix A
Proof of Lemma1

Proof: We consider CAC first. According to (2), the averaging process of agent i for iterations $k \geq 1$ can be expressed as:

$$x_i(k+1) = \prod_{h=0}^{k} w_{ii}(h)x_i(0) + \sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k) + \sum_{h=0}^{k-1}\prod_{l=h+1}^{k} w_{ii}(l)\sum_{j\in\mathcal{N}_i} w_{ij}(h)x_j(h). \tag{34}$$

Taking limits on both sides of (34), we have

$$\lim_{k\to\infty} x_i(k+1) = \lim_{k\to\infty}\sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k) + \lim_{k\to\infty}\prod_{h=0}^{k} w_{ii}(h)x_i(0) + \lim_{k\to\infty}\sum_{h=0}^{k-1}\prod_{l=h+1}^{k} w_{ii}(l)\sum_{j\in\mathcal{N}_i} w_{ij}(h)x_j(h). \tag{35}$$

Combining (14) and (35), we can obtain that

$$\begin{aligned} &f_i(x_i(0)|\mathcal{S}_{\mathcal{N}_i}(0), \mathcal{I}_i^{\mathcal{N}_i}(0\colon k)) \\ &= \lim_{k\to\infty}\sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k) + \lim_{k\to\infty}\prod_{h=0}^{k} w_{ii}(h)x_i(0) \\ &\quad + \lim_{k\to\infty}\sum_{h=0}^{k-1}\prod_{l=h+1}^{k} w_{ii}(l)\sum_{j\in\mathcal{N}_i} w_{ij}(h)x_j(h). \end{aligned} \tag{36}$$

For each agent i, suppose that the state of the agent i evolves from two potential initial values, i.e., $x_i^a(0)$ and $x_i^b(0)$, where $x_i^a(0), x_i^b(0) \in \mathcal{R}$, and $\mathcal{R}$ denotes the set of real numbers. Then

$$\begin{aligned} \bar{x} &= f_i(x_i^a(0)|\mathcal{S}_{\mathcal{N}_i}(0), \mathcal{I}_i^{\mathcal{N}_i}(0\colon k)) \\ &= f_i(x_i^b(0)|\mathcal{S}_{\mathcal{N}_i}(0), \mathcal{I}_i^{\mathcal{N}_i}(0\colon k)). \end{aligned}$$

According to (36), it holds that

$$\begin{aligned} &\lim_{k\to\infty}\sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k) + \lim_{k\to\infty}\prod_{h=0}^{k} w_{ii}(h)x_i^a(0) \\ &\quad + \lim_{k\to\infty}\sum_{h=0}^{k-1}\prod_{l=h+1}^{k} w_{ii}(l)\sum_{j\in\mathcal{N}_i} w_{ij}(h)x_j(h) \\ &= \lim_{k\to\infty}\sum_{j\in\mathcal{N}_i} w_{ij}(k)x_j(k) + \lim_{k\to\infty}\prod_{h=0}^{k} w_{ii}(h)x_i^b(0) \\ &\quad + \lim_{k\to\infty}\sum_{h=0}^{k-1}\prod_{l=h+1}^{k} w_{ii}(l)\sum_{j\in\mathcal{N}_i} w_{ij}(h)x_j(h). \end{aligned} \tag{37}$$

Comparing the two sides of the above equation, we have $x_i^a(0) = x_i^b(0)$. Hence, $f_i(\cdot)$ is an injective function in the case of CAC.

In a similar argument, we can prove the injection property of $f_i(\cdot)$ in the cases of PAC and FAC. Thus, Lemma 1 is proved. ■

Appendix B
Proof of Theorem 2

Proof: For ease of description, let $\boldsymbol{\xi}_s(k)$, $\boldsymbol{y}_s(k)$, $\boldsymbol{z}_s(k)$, and $\boldsymbol{x}_s(k)$ denote the vector forms of $\{\xi_{i,s}(k)\}$, $\{\zeta_{i,s}(k)\}$, $\{z_{i,s}(k)\}$, and $\{x_{i,s}(k)\}$, respectively. Since $\underline{k} \leq \overline{k}$, we divide the proof process into three cases, i.e., $k \leq \underline{k}$, $\underline{k}+1 \leq k \leq \overline{k}$ (if $\underline{k} < \overline{k}$), and $k \geq \overline{k}+1$.

When $k \leq \underline{k}$, (18) can be rewritten into the following form:

$$\xi_{i,s}(k+1) = w_{ii}\xi_i(k) + \sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}\theta_j(k)\xi_j(k),$$

and if we calculate the sum of all $\{x_i(k) : i \in \mathcal{V}\}$ in the graph $\mathcal{G}$ at each iteration k, we have

$$\begin{aligned} \mathbf{1}^T\boldsymbol{x}_s(k+1) =& \mathbf{1}^T\boldsymbol{\xi}_s(k+1) + \mathbf{1}^T\boldsymbol{z}_s(k+1) \\ =& \sum_{i\in\mathcal{V}} w_{ii}(k)\xi_{i,s}(k) \\ &+ \sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)\theta_{j,s}(k)\xi_{j,s}(k) + \mathbf{1}^T\boldsymbol{z}_s(k) \\ &+ \sum_{i\in\mathcal{V}}\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)(1-\theta_{i,s}(k))\xi_{i,s}(k), \end{aligned} \tag{38}$$

where $\mathbf{1}$ denotes the column vector of dimension $N \times 1$ with all elements equal to 1. Since all the information sent out by all the agents in $\mathcal{V}$ is the same as that received by them, we have

$$\begin{aligned} &\sum_{i\in\mathcal{V}}\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k)\theta_{j,s}(k)\xi_{j,s}(k) \\ &= \sum_{i\in\mathcal{V}}\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)\theta_{i,s}(k)\xi_{i,s}(k). \end{aligned} \tag{39}$$

From (38)-(39), it can be derived that

$$\begin{aligned} \mathbf{1}^T\boldsymbol{x}_s(k+1) =& \sum_{i\in\mathcal{V}} w_{ii}(k)\xi_{i,s}(k) + \mathbf{1}^T\boldsymbol{z}_s(k) \\ &+ \sum_{i\in\mathcal{V}}\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)(1-\theta_{i,s}(k))\xi_{i,s}(k) \\ &+ \sum_{i\in\mathcal{V}}\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(k)\theta_{i,s}(k)\xi_{i,s}(k). \end{aligned} \tag{40}$$

By merging similar items of (40), we have

$$\mathbf{1}^T\boldsymbol{x}_s(k+1)=\mathbf{1}^T\boldsymbol{\xi}_s(k)+\mathbf{1}^T\boldsymbol{z}_s(k)=\mathbf{1}^T\boldsymbol{x}_s(k).$$

Hence, $\mathbf{1}^T\boldsymbol{x}_s(k+1)=\mathbf{1}^T\boldsymbol{x}_s(k)$ holds at any iteration $k\le\underline{k}$, and this equality is irrelevant to $\theta_{i,s}(k)$.

If $\underline{k}<k<\bar{k}$, a part of the agents are in Phase 1, while others are in Phase 2. We define $\mathcal{V}_1(k)$ and $\mathcal{V}_2(k)$ be the sets of agents that are currently in Phase 1 and Phase 2. The summation of all $x_i(k)$ across the graph $\mathcal{G}$ at each iteration k is

$$\begin{aligned}&\mathbf{1}^T\boldsymbol{x}_s(k+1)\\&=\sum_{i\in\mathcal{V}_1(k+1)}\xi_{i,s}(k+1)+\sum_{i\in\mathcal{V}_1(k+1)}z_{i,s}(k+1)\\&\quad+\sum_{i\in\mathcal{V}_2(k+1)}x_{i,s}(k+1)\\&=\sum_{i\in\mathcal{V}_1(k)}w_{ii}(k)\xi_{i,s}(k)+\sum_{i\in\mathcal{V}_1(k)}\sum_{p\in\mathcal{N}_i^{\text{out}}}w_{pi}(k)\theta_{i,s}(k)\xi_{i,s}(k)\\&\quad+\sum_{i\in\mathcal{V}_1(k)}\sum_{p\in\mathcal{N}_i^{\text{out}}}\sum_{h=0}^{k}w_{pi}(k)(1-\theta_{i,s}(h))\xi_{i,s}(h)\\&\quad+\sum_{i\in\mathcal{V}_2(k)}\left(w_{ii}(k)x_{i,s}(k)+\sum_{p\in\mathcal{N}_i^{\text{out}}}w_{ji}(k)x_{i,s}(k)\right).\end{aligned}\tag{41}$$

After merging similar items of (41), we have

$$\begin{aligned}\mathbf{1}^T\boldsymbol{x}_s(k+1)=&\sum_{i\in\mathcal{V}_1(k)}(\xi_{i,s}(k)+z_{i,s}(k))+\sum_{i\in\mathcal{V}_2(k)}x_{i,s}(k)\\=&\mathbf{1}^T\boldsymbol{x}_s(k).\end{aligned}$$

Hence, $\mathbf{1}^T\boldsymbol{x}(k+1)=\mathbf{1}^T\boldsymbol{x}(k)$ holds when $\underline{k}+1\le k\le\bar{k}$, and this equality is also irrelevant to $\theta_{i,s}(k)$.

From the above proof process, we can easily deduce that $\mathbf{1}^T\boldsymbol{x}(\bar{k}+1+1)=\mathbf{1}^T\boldsymbol{x}(0)$. Then the updating process for iterations $k\ge\bar{k}+1$ can be viewed as another average consensus process in which all agents operate the original average consensus algorithms with the initial states as $\boldsymbol{x}(\bar{k}+1)$. Since we have assumed the original algorithms converge, the proposed framework also converges. Moreover, based on the above proof process, we can see that the convergence is irrelevant to $\theta_{i,s}(k)$. Thus, we have completed the proof. ■

Appendix C
Proof of Theorem 3

Proof: Inspired by [28], we adopt the data disturbance method to prove that the proposed framework can preserve the private information. Specifically, if we change the initial state $x_i(0)$ to an arbitrary value $x_i'(0)\neq x_i(0)$, the privacy of the initial state can be preserved if the information set obtained by the inferrers is the same; otherwise, the privacy information cannot be preserved. Without loss of generality, for non- and weak conclusion inference, let $\mathcal{A}_i^{\text{in}}$ and $\mathcal{A}_i^{\text{out}}$ denote in- and out-neighboring inferrers of agent i in the inferrers set $\mathcal{A}_i$, respectively.

When $k=0$, from the perspective of the collusive inferrers, all elements in $\mathcal{I}_i^{\mathcal{A}_i}(0)$ are

$$\mathcal{I}_i^{\mathcal{A}_i}(0)=\{x_{i,2}(0),w_{pi}(0),\zeta_{i,s}(0)|p\in\mathcal{A}_i^{\text{out}}\}.$$

Since $w_{pi}(0)$ is irrelevant to $x_i(0)$ and $x_{i,2}(0)=1$, the only clue for the inferrers is $\zeta_{i,1}(0)$. Obviously, $x_i(0)$ can be inferred via $x_i(0)=\frac{\zeta_{i,s}(0)}{\theta_{i,1}(0)}$. In this case, the estimate of $\frac{1}{\theta_{i,1}(0)}$ decides the estimate of $x_1(0)$ as $\zeta_{i,1}(0)$ is known to the inferrers. It is obvious that there are numerous $x_i(0)$ and $\theta_{i,1}(0)$ that satisfy

$$\zeta_{i,1}(0)=\theta_{i,1}(0)x_i(0),\tag{42}$$

then the inferrers cannot infer $x_i(0)$ via $\zeta_i(0)$.

When $0<k\le k_i$, the information set available to the inferrers is

$$\begin{aligned}\mathcal{I}_i^{\mathcal{A}_i}(0\colon k)=&\{x_{i,2}(0),w_{pi}(h),\zeta_{i,s}(h)|p\in\mathcal{A}_i^{\text{out}},0\le h\le k\}\\&\bigcup\{w_{ij}(h),\zeta_{j,s}(h)|j\in\mathcal{A}_i^{\text{in}},0\le h\le k-1\}.\end{aligned}$$

With this, we can express $\zeta_{i,s}(k)$ in the form of (43), as shown at the bottom of the next page, which is deduced by combining (17) and (18). Note that (43) is a combination of the unknown variables $\theta_{i,1}(k)$ and $\xi_{i,1}(0)$. For any $x_{i,1}'(0)\neq x_{i,1}(0)$, there always exists $\theta_{i,1}'(k)$ such that the resulting $\zeta_{i,1}(k)$ by (43) is the same. Thus, the inferrers cannot infer $\xi_{i,1}(0)$, and the privacy of $x_i(0)$ in protected.

When $k=k_i+1$, the information set available to $\mathcal{A}_i$ is

$$\begin{aligned}\mathcal{I}_i^{\mathcal{A}_i}(0\colon k_i{+}1)=&\{w_{pi}(h),\zeta_{i,s}(h)|p\in\mathcal{A}_i^{\text{out}},0\le h\le k_i+1\}\\&\bigcup\{x_{i,2}(0),w_{ij}(h),\zeta_{j,s}(h)|j\in\mathcal{A}_i^{\text{in}},0\le h\le k_i\}.\end{aligned}$$

Assume one of the non-collusive neighbors is agent m, and for any $x_i(0)'\neq x_i(0)$, there exists $x_m(0)'\neq x_m(0)$ such that $x_i(0)+x_m(0)=x_i'(0)+x_m'(0)$. Based on the iterative steps in (18)-(20), we can express $\xi_{i,s}(k_i+1)$, $z_{i,s}(k_i+1)$, and $x_{i,s}(k_i+1)$ in the following forms:

$$\begin{aligned}\xi_{i,s}(k_i+1)=&\sum_{j\in\mathcal{N}_i^{\text{in}}}w_{ij}(k_i)\zeta_{j,s}(k_i)+\prod_{h=0}^{k_i}w_{ii}(h)\xi_{i,s}(0)\\&+\sum_{j\in\mathcal{N}_i^{\text{in}}}\sum_{h=0}^{k_i-1}w_{ij}(h)\zeta_{j,s}(h)\prod_{l=h+1}^{k_i}w_{ii}(l),\end{aligned}$$

$$\begin{aligned}&z_{i,s}(k_i+1)\\&=\sum_{p\in\mathcal{N}_i}\left(w_{pi}(0)\xi_{i,s}(0)+\sum_{h=1}^{k_i}w_{pi}(h)\prod_{l=0}^{h-1}w_{ii}(l)\xi_{i,s}(0)\right)\\&\quad-\sum_{p\in\mathcal{N}_i^{\text{out}}}\sum_{h=0}^{k_i}w_{pi}(h)\zeta_{i,s}(h)\\&\quad+\sum_{p\in\mathcal{N}_i^{\text{in}}}\sum_{h=0}^{k_i-1}w_{pi}(h{+}1)\sum_{j\in\mathcal{N}_i^{\text{in}}}w_{ij}(h)\zeta_{j,s}(h)\\&\quad+\sum_{p\in\mathcal{N}_i^{\text{out}}}\sum_{h=1}^{k_i-1}w_{pi}(h{+}1)\sum_{j\in\mathcal{N}_i^{\text{in}}}\sum_{l=0}^{h-1}w_{ij}(l)\zeta_{j,s}(l)\prod_{s=l+1}^{h}w_{ii}(s),\end{aligned}$$

$$\begin{aligned}&x_{i,s}(k_i+1)\\&=\xi_{i,s}(k_i+1)+z_{i,s}(k_i+1)\\&=\prod_{h=0}^{k_i}w_{ii}(h)\xi_{i,s}(0)-\sum_{p\in\mathcal{N}_i^{\text{out}}}\sum_{h=0}^{k_i}w_{pi}(h)\zeta_{i,s}(h)\end{aligned}$$

$$
\begin{aligned}
&+\sum_{h=0}^{k_i-1}\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(h)\zeta_{j,s}(h)\prod_{l=h+1}^{k_i} w_{ii}(l)\\
&+\sum_{h=1}^{k_i}(1-w_{ii}(h))\prod_{l=0}^{h-1} w_{ii}(l)\xi_{i,s}(0)\\
&+\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(0)\xi_{i,s}(0)+\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(k_i)\zeta_{j,s}(k_i)\\
&+\sum_{h=0}^{k_i-1}(1-w_{ii}(h+1))\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(h)\zeta_{j,s}(h)\\
&+\sum_{h=1}^{k_i-1}\sum_{l=0}^{h-1}\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(l)\zeta_{j,s}(l)\prod_{m=l+1}^{h} w_{ii}(m)\\
&-\sum_{h=1}^{k_i-1} w_{ii}(h+1)\sum_{l=0}^{h-1}\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(l)\zeta_{j,s}(l)\prod_{m=l+1}^{h} w_{ii}(m)\\
=&\xi_{i,s}(0)+\sum_{h=0}^{k_i}\left(\sum_{j\in\mathcal{N}_i^{\text{in}}} w_{ij}(h)\zeta_{j,s}(h)-\sum_{p\in\mathcal{N}_i^{\text{out}}} w_{pi}(h)\zeta_{i,s}(h)\right).
\end{aligned}
\tag{44}
$$

Then, in order to analyze the trusted neighbor m's influence on privacy preserving, we divide the situation into the following two cases: agent m is an in-neighbor or out-neighbor of agent i.

Case I: Agent m is an in-neighbor of agent i. First, let $\xi'_{i,s}(0)$ and $w'_{im}(k)$ denote the assumed fusion information and the weighted adjacency of the agents i and m when $x_i(0)$ is replaced by $x'_i(0)$, respectively. If there exist $\xi'_{i,s}(0)$ and $w'_{im}(k)$ such that let $\mathcal{I}_i^{\mathcal{A}_i}(k)$ unchanged, the inferrers cannot obtain $x_i(0)$.Then, we replace $\xi_{i,s}(0)$ and $w_{im}(k)$ with $\xi'_{i,s}(0)$ (where $\xi'_{i,1}(0)\neq\xi_{i,1}(0)$, $\xi'_{i,2}(0)=\xi_{i,2}(0)=1$) and $w'_{im}(k)$, respectively, and rewrite (44) into the following form:

$$
\begin{aligned}
x_{i,s}(k_i+1)=&\sum_{h=0}^{k_i} w'_{im}(h)\zeta_{m,s}(h)-\sum_{h=0}^{k_i}\sum_{p\in\mathcal{A}_i^{\text{out}}} w_{pi}(h)\zeta_{i,s}(h)\\
&+\xi'_{i,s}(0)+\sum_{h=0}^{k_i}\sum_{j\in\mathcal{A}_i^{\text{in}}} w_{ij}(h)\zeta_{j,s}(h).
\end{aligned}
\tag{45}
$$

For the case of $s=2$, due to $k_i>0$, the number of unknowns ($w'_{im}(h)$) exceeds the number of equations. Hence, the inferrers cannot obtain $w'_{im}(h)$ by solving (45). Since $\xi'_{i,1}(0)$ and $w'_{im}(h)$ $(0\leq h\leq k_i)$ are unknown to the inferrers, for any $\xi'_{i,1}(0)\neq\xi_{i,1}(0)$, there exists $w'_{im}(h)$ $(0\leq h\leq k_i)$ such that (45) holds.

Case II: Agent m is an out-neighbor of agent i. Similarly, we replace $\xi_{i,1}(0)$, $w_{mi}(k)$, and $w_{ii}(k)$ with $\xi'_{i,1}(0)$ ($\xi'_{i,1}(0)\neq\xi_i(0)$), $w'_{mi}(k)$, and $w'_{ii}(k)$, respectively, where $w'_{mi}(k)$ denotes the weighted adjacency of the agents i and m when $x_i(0)$ is replaced by $x'_i(0)$, and rewrite (44) in case of s=1 into the following form:

$$
\begin{aligned}
x_{i,1}(k_i+1)=\xi'_{i,1}(0)&+\sum_{h=0}^{k_i}\sum_{j\in\mathcal{A}_i^{\text{in}}} w_{ij}(h)\zeta_{j,1}(h)\\
&-\sum_{h=0}^{k_i}\sum_{p\in\mathcal{A}_i^{\text{out}}} w_{pi}(h)\zeta_{i,1}(h)-\sum_{h=0}^{k_i} w'_{mi}(h)\zeta_{i,1}(h).
\end{aligned}
\tag{46}
$$

For the case of $s=2$, similarly, the inferrers cannot obtain $w'_{im}(h)$ by solving (45). Since $\xi'_{i,1}(0)$ and $w'_{mi}(h)$ $(0\leq h\leq k_i)$ are unknown to the inferrers, for any $\xi'_{i,1}(0)\neq\xi_{i,1}(0)$, there exists $w'_{mi}(h)$ $(0\leq h\leq k_i)$ such that (46) holds.

Combining Case I and II, we can determine whether agent m is an in- or out-neighbor of agent i. For any $x'_i(0)\neq x_i(0)$, there always exists $w'_{mi}(h)$ or $w'_{im}(h)$ such that the resulting $x_{i,1}(k_i+1)$ by (44) based on $x'_{i,1}(k_i+1)$ is the same as that based on $x_{i,1}(k_i+1)$. Thus, the inferrers cannot infer $\xi_{i,1}(0)$, and the privacy of $x_i(0)$ in protected.

When $k>k_i+1$, the proof process follows the same logic as that for iteration k_i+1 as above and is omitted herein.

In summary, the proposed framework can preserve the privacy of $x_i(0)$. ■

Appendix D
Proof of Theorem 4

Proof: Since for any $i\in\mathcal{V}$ and $s\in\{1,2\}$, the random variables $\{\theta_{i,s}(k)\colon k=0,1,2,\ldots\}$ are independent at different iterations, according to [22], the MPDP is achieved if the inferrers infer the initial state at iteration 0. Therefore, in the following, we analyze the MPDP under adding-noise-based methods and our proposed framework at iteration 0.

As regards adding-noise-based methods, the initial state of agent i, i.e., $x_i(0)$ in (15) can be viewed as a variable, and $\mathbb{E}(x_i(0))=x_i^+(0)-\mathbb{E}(\vartheta_{i,1}(0))=x_i^+(0)$ and $\mathbb{D}(x_{i,1}(0))=\mathbb{D}(\vartheta_{i,1}(0))$, where $\mathbb{E}(\cdot)$ and $\mathbb{D}(\cdot)$ denote the expectation and variance of a random variable, respectively. For the inferrers, the obstacle of inferring $x_i(0)$ is $\vartheta_{i,1}(0)$, and the reasonable method to infer $x_i(0)$ is estimating $\vartheta_{i,1}(0)$ by the PDF of $\vartheta_{i,1}(0)$. In accordance with Definition 7, the way to achieve the optimal inference of $\vartheta_{i,1}(0)$ is maximizing $\int_{\hat{\vartheta}_{i,1}(0)-\epsilon}^{\hat{\vartheta}_{i,1}(0)+\epsilon} f_{\vartheta_{i,1}(0)}(t)\,dt$, where $f_{\vartheta_{i,1}(0)}(t)$ denotes the PDF of $\vartheta_{i,1}(0)$. Without loss of generality, the domain of $f_{\vartheta_{i,1}(0)}(t)$ is assumed to be $\mathcal{R}$. The MPDP for $x_i(0)$ and the optimal inference $\hat{\vartheta}^*_{i,1}(0)\,\langle\epsilon\rangle$ with the given error range $[-\epsilon,\epsilon]$ under the adding-noise-based methods can be formulated as follows:

$$
\begin{aligned}
&\max_{\hat{x}_i(0)}\{\mathbb{P}\{|\hat{x}_i(0)-x_i(0)|\leq\epsilon|\mathcal{I}\}\}\\
&=\max_{\hat{\vartheta}_{i,1}(0)}\left\{\mathbb{P}\left\{\left|(x_i^+(0)-\hat{\vartheta}_{i,1}(0))-(x_i^+(0)-\vartheta_{i,1}(0))\right|\leq\epsilon\middle|\mathcal{I}\right\}\right\}
\end{aligned}
$$

$$
\zeta_{i,s}(k)=\theta_{i,s}(k)\prod_{h=0}^{k-1} w_{ii}(h)\xi_{i,s}(0)+\theta_{i,s}(k)\begin{cases}\sum_{j\in\mathcal{N}_i^{\text{in}}}\sum_{h=0}^{k-1} w_{ij}(h)\zeta_{j,s}(h), & k=1\\ \sum_{j\in\mathcal{N}_i^{\text{in}}}\left(\sum_{h=0}^{k-2} w_{ij}(h)\zeta_{j,s}(h)\prod_{l=h+1}^{k-1} w_{ii}(l)+w_{ij}(k-1)\zeta_{j,s}(k-1)\right), & k\geq 2\end{cases}
\tag{43}
$$

$$
\begin{aligned}
&= \max_{\hat{\vartheta}_{i,1}(0)} \left\{ \mathbb{P}\left\{ \left| \hat{\vartheta}_{i,1}(0) - \vartheta_{i,1}(0) \right| \le \epsilon \middle| \mathcal{I} \right\} \right\} \\
&= \max_{\hat{\vartheta}_{i,1}(0)} \int_{\hat{\vartheta}_{i,1}(0)-\epsilon}^{\hat{\vartheta}_{i,1}(0)+\epsilon} f_{\vartheta_{i,1}(0)}(t)\, dt, \qquad (47)
\end{aligned}
$$

and

$$
\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle = \arg\max_{\hat{\vartheta}_{i,1}(0)} \int_{\hat{\vartheta}_{i,1}(0)-\epsilon}^{\hat{\vartheta}_{i,1}(0)+\epsilon} f_{\vartheta_{i,1}(0)}(t)\, dt. \qquad (48)
$$

Similarly, in our proposed framework, $\mathbb{E}(x_i(0)) = \zeta_{i,1}(0)\mathbb{E}(\frac{1}{\theta_{i,1}(0)})$ and $\mathbb{D}(x_i(0)) = \zeta_{i,1}(0)^2\mathbb{D}(\frac{1}{\theta_{i,1}(0)})$ if $\zeta_{i,1}(0) \neq 0$. Here we assume $\zeta_{i,1}(0) \neq 0$. Let $f_{\frac{1}{\theta_{i,1}(0)}}(t)$ denote the PDF of $\frac{1}{\theta_{i,1}(0)}$, and assume that

$$
f_{\frac{1}{\theta_{i,1}(0)}}(t) = \begin{cases} f_{\vartheta_{i,1}(0)}(t - \frac{1}{|\xi_{i,1}(0)|}), & \text{if } t \ge \frac{1}{|\xi_{i,1}(0)|} \\ f_{\vartheta_{i,1}(0)}(t + \frac{1}{|\xi_{i,1}(0)|}), & \text{if } t \le -\frac{1}{|\xi_{i,1}(0)|} \end{cases}. \qquad (49)
$$

Note that $f_{\frac{1}{\theta_{i,1}(0)}}(t)$ is a piece-wise function, and the domain is $\left(-\infty, -\frac{1}{|\xi_{i,1}(0)|}\right] \cup \left[\frac{1}{|\xi_{i,1}(0)|}, \infty\right)$. Hence, we can obtain that $|\zeta_{i,1}(0)| \ge 1$. Also, the MPDP for $x_i(0)$ and the optimal inference $\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle$ with the given error range $\left[-\frac{\epsilon}{|\zeta_{i,1}(0)|}, \frac{\epsilon}{|\zeta_{i,1}(0)|}\right]$ under the proposed framework can be formulated as follows:

$$
\begin{aligned}
&\max_{\hat{x}_i(0)} \{\mathbb{P}\{|\hat{x}_i(0) - x_i(0)| \le \epsilon | \mathcal{I}\}\} \\
&= \max_{\hat{\theta}_{i,1}(0)} \left\{ \mathbb{P}\left\{ \left| \frac{\zeta_{i,1}(0)}{\hat{\theta}_{i,1}(0)} - \frac{\zeta_{i,1}(0)}{\theta_{i,1}(0)} \right| \le \epsilon \middle| \mathcal{I} \right\} \right\} \\
&= \max_{\hat{\theta}_{i,1}(0)} \left\{ \mathbb{P}\left\{ \left| \frac{1}{\hat{\theta}_{i,1}(0)} - \frac{1}{\theta_{i,1}(0)} \right| \le \frac{\epsilon}{|\zeta_{i,1}(0)|} \middle| \mathcal{I} \right\} \right\} \\
&= \max_{\hat{\theta}_{i,1}(0)} \int_{\frac{1}{\hat{\theta}_{i,1}(0)} - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}_{i,1}(0)} + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt, \qquad (50)
\end{aligned}
$$

and

$$
\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle = \arg\max_{\frac{1}{\hat{\theta}_{i,1}(0)}} \int_{\frac{1}{\hat{\theta}_{i,1}(0)} - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}_{i,1}(0)} + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt. \qquad (51)
$$

It is worth noticing that $\left[\hat{\vartheta}^*_{i,1}(0) - \epsilon, \hat{\vartheta}_{i,1}(0) + \epsilon\right]$ and $\left[\frac{1}{\hat{\theta}_{i,1}(0)} - \frac{\epsilon}{|\zeta_{i,1}(0)|}, \frac{1}{\hat{\theta}^*_{i,1}(0)} + \frac{\epsilon}{|\zeta^*_{i,1}(0)|}\right]$ should be in the ranges of the domains of $f_{\vartheta_{i,1}(0)}(t)$ and $f_{\frac{1}{\theta_{i,1}(0)}}(t)$, respectively.

Then we can obtain the expressions of the MPDP under adding-noise-based methods and our proposed framework, denoted by δ_0 and δ_1, respectively as follows:

$$
\begin{aligned}
\delta_0 &= \int_{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle-\epsilon}^{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle+\epsilon} f_{\theta_{i,1}(0)}(t)\, dt, \\
\delta_1 &= \int_{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt.
\end{aligned}
$$

According to Definition 7, for any $\alpha, \gamma \in \mathcal{R}$ that satisfy $\gamma \le \epsilon$, we have

$$
\int_{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle-\epsilon}^{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle+\epsilon} f_{\theta_{i,1}(0)}(t)\, dt \ge \int_{\alpha-\gamma}^{\alpha+\gamma} f_{\theta_{i,1}(0)}(t)\, dt. \qquad (52)
$$

To analyze the relationship between δ_0 and δ_1, we divide the situation into two scenarios. For ease of analysis, we firstly assume that $\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle$ is the unique optimal inference of (51).

Scenario I: $\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle > 0$. Considering (49), we have

$$
\begin{aligned}
\delta_1 &= \int_{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\frac{1}{\theta_{i,1}(0)}}(t)\, dt \\
&= \int_{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{1}{|\xi_{i,1}(0)|} - \frac{\epsilon}{|\zeta_{i,1}(0)|}}^{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{1}{|\xi_{i,1}(0)|} + \frac{\epsilon}{|\zeta_{i,1}(0)|}} f_{\theta_{i,1}(0)}(t)\, dt.
\end{aligned}
$$

Then referring (52), we can derive that

$$
\begin{aligned}
\delta_1 &\le \int_{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{1}{|\xi_{i,1}(0)|} - \epsilon}^{\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle - \frac{1}{|\xi_{i,1}(0)|} + \epsilon} f_{\theta_{i,1}(0)}(t)\, dt \\
&\le \int_{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle-\epsilon}^{\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle+\epsilon} f_{\theta_{i,1}(0)}(t)\, dt = \delta_0.
\end{aligned}
$$

Scenario II: $\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle < 0$. $\delta_1 \le \delta_0$ holds, and the proof follows the same logic as that in Scenario I.

Combining Scenario I and II, we can obtain that $\delta_1 \le \delta_0$ if the PDFs of $\frac{1}{\theta_{i,1}(k)}$ and $\vartheta_{i,1}(k)$ are ruled by (49). If there exist multiple optimal inferences for $\frac{1}{\hat{\theta}^*_{i,1}(0)}\left\langle \frac{\epsilon}{|\zeta_{i,1}(0)|} \right\rangle$ and $\hat{\vartheta}^*_{i,1}(0)\langle\epsilon\rangle$, $\delta_1 \le \delta_0$ also holds, and the proof process follows the same logic as above. Thus, Theorem 4 is proved. ■

REFERENCES

[1] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[2] J. W. Yi, L. Chai, and J. Zhang, "Average consensus by graph filtering: New approach, explicit convergence rate, and optimal design," *IEEE Trans. Autom. Control*, vol. 65, no. 1, pp. 191–206, Jan. 2020.

[3] G. S. Seyboth, D. V. Dimarogonas, and K. H. Johansson, "Event-based broadcasting for multi-agent average consensus," *Automatica*, vol. 49, no. 1, pp. 245–252, Jan. 2013.

[4] Q. Lin, Y. Zhou, G.-P. Jiang, S. Ge, and S. Ye, "Prescribed-time containment control based on distributed observer for multi-agent systems," *Neurocomputing*, vol. 431, pp. 69–77, Mar. 2021.

[5] F. Ye, Z. Cheng, X. Cao, and M.-Y. Chow, "A random-weight privacy-preserving algorithm with error compensation for microgrid distributed energy management," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4352–4362, 2021.

[6] Z. Cheng and M.-Y. Chow, "Resilient collaborative distributed energy management system framework for cyber-physical DC microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 4637–4649, Nov. 2020.

[7] C. Zhao, L. Cai, and P. Cheng, "Stability analysis of vehicle platooning with limited communication range and random packet losses," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 262–277, Jan. 2021.

[8] K. Guo, X. Li, and L. Xie, "Ultra-wideband and odometry-based cooperative relative localization with application to multi-UAV formation control," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2590–2603, Jun. 2020.

[9] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[10] T. Charalambous, Y. Yuan, T. Yang, W. Pan, C. N. Hadjicostis, and M. Johansson, "Distributed finite-time average consensus in digraphs in the presence of time delays," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 4, pp. 370–381, Dec. 2015.

[11] A. I. Rikos and C. N. Hadjicostis, "Event-triggered quantized average consensus via ratios of accumulated values," *IEEE Trans. Autom. Control*, vol. 66, no. 3, pp. 1293–1300, Mar. 2021.

[12] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[13] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[14] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 34–42, Mar. 2017.

[15] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Jan. 2017.

[16] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[17] M. Yang and J. Zhai, "Observer-based switching-like event-triggered control of nonlinear networked systems against DoS attacks," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 3, pp. 1375–1384, Sep. 2022.

[18] R. Liu and J. Pan, "CRS: A privacy-preserving two-layered distributed machine learning framework for IoV," *IEEE Internet Things J.*, vol. 11, no. 1, pp. 1080–1095, Jul. 2024.

[19] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 753–765, Feb. 2017.

[20] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.

[21] J. He, L. Cai, C. Zhao, P. Cheng, and X. Guan, "Privacy-preserving average consensus: Privacy analysis and algorithm design," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 5, no. 1, pp. 127–138, Mar. 2019.

[22] J. He, L. Cai, and X. Guan, "Preserving data-privacy with added noises: Optimal estimation and privacy analysis," *IEEE Trans. Inf. Theory*, vol. 64, no. 8, pp. 5677–5690, Aug. 2018.

[23] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, Nov. 2019.

[24] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Trans. Signal Process.*, vol. 68, pp. 4069–4082, 2020.

[25] Q. Liu, X. Ren, and Y. Mo, "Secure and privacy preserving average consensus," in *Proc. 11th Asian Control Conf. (ASCC)*. New York, NY, USA: ACM, Dec. 2017, pp. 274–279.

[26] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

[27] C. N. Hadjicostis and A. D. Domínguez-García, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3887–3894, Sep. 2020.

[28] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, Nov. 2019.

[29] X. Chen, L. Huang, K. Ding, S. Dey, and L. Shi, "Privacy-preserving push-sum average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 68, no. 12, pp. 7974–7981, Dec. 2023.

[30] M. Calis, R. Heusdens, and R. C. Hendriks, "A privacy-preserving asynchronous averaging algorithm based on state decomposition," in *Proc. 28th Eur. Signal Process. Conf. (EUSIPCO)*, Jan. 2021, pp. 2115–2119.

[31] C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semihomomorphic encryption," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3950–3957, Sep. 2020.

[32] Y. Wang, J. Lu, W. X. Zheng, and K. Shi, "Privacy-preserving consensus for multi-agent systems via node decomposition strategy," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 8, pp. 3474–3484, Aug. 2021.

[33] J. Zhang, J. Lu, and X. Chen, "Privacy-preserving average consensus via edge decomposition," *IEEE Control Syst. Lett.*, vol. 6, pp. 2503–2508, 2022.

[34] P. Rezaienia, B. Gharesifard, T. Linder, and B. Touri, "Push-sum on random graphs: Almost sure convergence and convergence rate," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1295–1302, Mar. 2020.

Feng Ye (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering and automation from the College of Information Science and Engineering, Northeastern University, Shenyang, China, in 2019. He is currently pursuing the Ph.D. degree with the School of Automation, Southeast University, Nanjing, China. His current research interests include distributed coordination and optimization, smart grids, privacy-preserving, and cyber security.

Xianghui Cao (Senior Member, IEEE) received the B.S. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2006 and 2011, respectively. From 2012 to 2015, he was a Senior Research Associate with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA. He is currently a Professor with the School of Automation, Southeast University, Nanjing, China. His current research interests include cyber-physical systems, wireless networked control, and network security. He was a recipient of the Best Paper Runner-Up Award from ACM MobiHoc in 2014, the First Prize of Natural Science Award of the Ministry of Education of China in 2017, and the Second Prize of Science and Technology Award of Jiangsu Province in 2021. He serves as an Associate Editor for *ACTA Automatica Sinica* and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

Mo-Yuen Chow (Fellow, IEEE) received the B.S. degree in electrical and computer engineering from the University of Wisconsin–Madison in 1982 and the M.Eng. and Ph.D. degrees in electrical and computer engineering from Cornell University in 1983 and 1987, respectively. He joined as a Professor with the UM-Shanghai Jiao Tong University Joint Institute in 2022. He was a Professor with the Department of Electrical and Computer Engineering, North Carolina State University. He has established the Advanced Diagnosis, Automation, and Control Laboratory. His current research interests include distributed control and management, smart microgrids, batteries, and mechatronics systems. He has received the IEEE Region3 Joseph M. Biedenbach Outstanding Engineering Educator Award, the IEEE ENCS Outstanding Engineering Educator Award, the IEEE ENCS Service Award, the IEEE Industrial Electronics Society Anthony J. Hornfeck Service Award, and the IEEE Industrial Electronics Society Dr.-Ing. Eugene Mittelmann Achievement Award. He is the Co-Editor-in-Chief of IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS from 2014 to 2018 and the Editor-in-Chief of IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS from 2010 to 2012. He is a Distinguished Lecturer of the IEEE Industrial Electronics Society.

Lin Cai (Fellow, IEEE) has been with the Department of Electrical and Computer Engineering, University of Victoria, since 2005, where she is currently a Professor. Her research interests include communications and networking, with a focus on network protocol and architecture design supporting ubiquitous intelligence.

She is an NSERC E. W. R. Steacie Memorial Fellow, a Canadian Academy of Engineering (CAE) Fellow, and an Engineering Institute of Canada (EIC) Fellow. In 2020, she was elected as a member of the Royal Society of Canada's College of New Scholars, Artists and Scientists, and the 2020 "Star in Computer Networking and Communications" by N2Women. She received the NSERC Discovery Accelerator Supplement (DAS) Grants in 2010 and 2015. She co-founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She has been elected to serve the IEEE Vehicular Technology Society (VTS) Board of Governors from 2019 to 2024 and served as its VP of Mobile Radio from 2023 to 2024. She served as a Board Member of the IEEE Women in Engineering from 2022 to 2024 and the IEEE Communications Society (ComSoc) from 2024 to 2026. She has held various editorial roles, including an Associate Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and membership in the Steering Committee of the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON BIG DATA, and IEEE TRANSACTIONS ON CLOUD COMPUTING. She has also been an Associate Editor of IEEE/ACM TRANSACTIONS ON NETWORKING, IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE TRANSACTIONS ON COMMUNICATIONS. She is a Distinguished Lecturer of the IEEE VTS Society and the IEEE Communications Society and a Registered Professional Engineer in British Columbia, Canada.