Privacy-preserving Average Consensus: Privacy Analysis and Algorithm Design

Jianping He[1], Lin Cai[2], Chengcheng Zhao[3], Peng Cheng[3], and Xinping Guan[1]

***Abstract*—Privacy-preserving average consensus aims to guarantee the privacy of initial states and asymptotic consensus on the exact average of the initial values. In the existing work, it is achieved by adding variance-decaying and zero-sum random noises to the consensus process. However, there is lack of theoretical analysis to quantify the degree of the data privacy protection. In this paper, we introduce the maximum disclosure probability that other nodes can infer one node's initial state within a given small interval to quantify the data privacy. We utilize a novel privacy definition, named (α, β)-data-privacy, to depict the relationship between the maximum disclosure probability and the estimation accuracy. Then, we prove that the general privacy-preserving average consensus (GPAC) provides (α, β)-data-privacy, and obtain the closed-form expression of the relationship between α and β given the noise distribution. We reveal that the added noise with a uniform distribution is optimal in terms of achieving the highest (α, β)-data-privacy. We also prove that under what condition, the data-privacy will be compromised. Finally, an optimal privacy-preserving average consensus (OPAC) algorithm is proposed to achieve the highest (α, β)-data-privacy. Simulations verify the analytical results.**

I. Introduction

Consensus has attracted extensive attention over the past decades for distributed computing and control. A consensus algorithm refers to the action that nodes in the network reach a global agreement regarding a certain opinion by exchanging information with local neighbors only [1]. Thanks to the robustness and scalability, consensus has been applied in a variety of areas, e.g., coordination and cooperation [2]–[4], distributed estimation and optimization [5], [6], sensor fusion [7], distributed energy management [8], sensing scheduling [9], and time synchronization [10]–[13].

Average consensus is the most commonly adopted consensus algorithm, where the agreement reached by the algorithm equals the average of all nodes' initial states. For traditional average consensus algorithms, each node will broadcast its real state to neighbor nodes during a consensus process. Hence, with the traditional average consensus algorithms, the state information of each node is disclosed to its neighbor nodes. However, in some applications, the initial states of nodes are private information, so nodes do not want to release their real initial states to other nodes [18]. For example, a consensus algorithm can be adopted in social networks for a group of members to compute the common opinion on a subject [19]. In this application, each member may want to keep his/her personal opinion on the subject secret to other members. Also, in the multi-agent rendezvous problem [20], a group of nodes want to eventually rendezvous at a certain location, while the participators may not want to release their initial locations to others. This means that when the privacy is concerned, each node's real state may not be available to others, and thus the traditional consensus algorithm becomes undesirable.

Recently, researchers have investigated the privacy preserving average consensus problem, which aims to guarantee that the privacy of initial state is preserved while the average consensus can still be achieved. It can be addressed using cryptographic techniques, e.g., homomorphic encryption [27]–[30]. When applying cryptographic solutions is unfeasible or unfavorable, this problem can also be solved by using a noise adding mechanism [14]–[18]. The basic idea is to add random noises to the real states during the communication to protect the privacy, and then carefully design the noise adding process such that average consensus is achieved.

However, how to quantify the degree of the data privacy protection in terms of the probability of an estimate within a given range by an eavesdropper is an open issue. To fill this gap, in this paper, we develop a theoretical privacy analysis framework for the average consensus algorithm with a general noise adding process, aiming to bound the disclosure probability that other nodes can infer a node's initial state within a given small interval (a given estimation accuracy range). A privacy definition, named (α, β)-data-privacy, which was first introduced in our work [23], [24], is exploited to depict the maximum disclosure probability. This privacy definition reveals the relationship between privacy and estimation accuracy. Based on the analytical framework, we quantify the degree of the privacy preservation and reveal the quantitative relationship of the estimation accuracy and the privacy under GPAC algorithm. Based on the analysis, it is found that uniform distribution noise is the optimal one in achieving the highest (α, β)-data-privacy. On the other hand, the exact initial state of a node can be perfectly inferred, i.e., privacy is compromised with existing GPAC algorithms, if one node has all the information used in the consensus process. To solve this problem, a novel OPAC algorithm is designed to achieve exact average consensus as well as ensure data-privacy. The main contributions of this paper are summarized as follows.

- We show that the GPAC algorithm provides (α, β)-data-privacy. A closed-form expression of the relationship between the estimation accuracy and the privacy (the

1: Dept. of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Information Processing, Ministry of Education of China, Shanghai, China {jphe, xpguan}@sjtu.edu.cn

2: The Department of Electrical & Computer Engineering at the University of Victoria, BC, Canada cai@ece.uvic.ca

3: The State Key Lab. of Industrial Control Technology, Zhejiang University, Hangzhou, P. R. China. zccsq90@gmail.com; pcheng@iipc.zju.edu.cn

relationship between α and β given the noise distribution) is obtained.
- We prove that for the added random noises, the uniform distribution is optimal in the sense that the GPAC algorithm can achieve the highest privacy when the mean and variance of noises are fixed.
- We prove that with GPAC, if all the information used in the consensus process is available for the estimation, the maximum disclosure probability will converge to one, i.e., the initial state of a node is perfectly inferred. This result also reveals how to infer the exact initial state under this condition.
- We design a novel OPAC algorithm to achieve average consensus while guaranteeing the highest (α, β)-data-privacy. It is also proved that the OPAC algorithm can achieve the exact average consensus, and avoid the privacy to be compromised even if all the information used in the consensus process is available for estimation.

The remainder of this paper is organized as follows. Related works are given in Sec. II. Sec. III introduces the preliminary results and problem formulation. In Sec. IV, we provide theoretical results on the degree of privacy protection. The OPAC algorithm is proposed in Sec. V. Section VI verifies the main results and conclusions are given in Sec. VII.

II. Related Works

Many efforts have been devoted to investigating privacy preserving average consensus problem.

To solve this problem, a widely used approach is adding random noises to traditional average consensus algorithms. For example, Huang et al. [15] designed a differentially private iterative synchronous consensus algorithm by adding independent and exponentially decaying Laplacian noises to the consensus process. Their algorithm can guarantee differential privacy. As the algorithm may converge to a random value, the exact average consensus may not be guaranteed. Nozari et al. [16] pointed out and proved that it is impossible to achieve average consensus and differential privacy simultaneously. Hence, they designed a novel linear Laplacian-based consensus algorithm, which guarantees that an unbiased estimate of the average consensus can be achieved almost surely and with differential privacy. Manitara and Hadjicostis [17] proposed a privacy preserving average consensus algorithm by adding correlated noises to the consensus process. The proposed algorithm guarantees that the initial state of each node cannot be perfectly inferred by other "malicious" nodes. More recently, Mo and Murray in [18] addressed the privacy-preserving average consensus (PPAC) problem by designing a PPAC algorithm, where exponentially decaying and zero-sum normal noises are added to the traditional consensus process, so that the exact average consensus can be achieved in the mean-square sense. Braca et al. in [25] examined the interplay between learning and privacy over multi-agent consensus networks. They provided an analytical characterization of the interplay between learning and privacy for the consensus perturbing and preserving strategy, respectively.

On the other hand, there are several cryptography based privacy-preserving consensus protocols emerged [27]–[30]. For instance, homomorphic encryption was used for private average consensus [27], [28]. Abbe et al. [29] proposed a secret sharing protocol for performing privacy preserving computation of sum, where the used secure multi-party computation technique can be viewed as a special setting of the secret function used in OPCA. [30] exploited a secure multi-party computing strategy to perform private distributed optimization, which extended the sharing protocol proposed in [29] to a distributed network. Different from the above approaches, with the proposed OPCA, each node can apply different secret functions to the message to different neighbor nodes, and a simple secret function, e.g., linear function, can be used to largely decrease the commutation complexity.

III. Preliminaries and Problem Formulation

The network is abstracted as an undirected and connected graph, $G = (V, E)$, where V is the set of nodes and E is the set of the communication links (edges) between nodes. $(i, j) \in E$ if and only if (iff) nodes i and j can communicate with each other. Let N_i be the neighbor set of node i, where $j \in N_i$ iff $(i, j) \in E$, i.e., $N_i = \{j | j \in V, (i, j) \in E, j \neq i\}$.

A. Average Consensus

Suppose that there are n ($n \geq 3$) nodes in the network (i.e., $|V| = n$), and each node i has an initial scalar state $x_i(0)$, where $x_i(0) \in R$. For an average consensus algorithm, each node will communicate with its neighbor nodes and update its state based on the received information to obtain the average of all initial states' values. Hence, the traditional average consensus algorithm is given as follows,

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

for $\forall i \in V$, which can be written in the matrix form as

$$x(k+1) = Wx(k), \tag{2}$$

where w_{ii} and w_{ij} are weights, and W is the weight matrix. It is well known from [21] that if, 1) $w_{ii} > 0$, and $w_{ij} > 0$ for $(i, j) \in E$ and $w_{ij} = 0$ for otherwise; and 2) $W\mathbf{1} = \mathbf{1}^T W = \mathbf{1}$, i.e., W is a doubly stochastic matrix, then average consensus can be achieved by (1), i.e.,

$$\lim_{k \to \infty} x_i(k) = \frac{\sum_{\ell=1}^{n} x_\ell(0)}{n} = \bar{x}. \tag{3}$$

When the privacy of nodes' initial states are concerned, all nodes are unwilling to release its real state to the neighbor nodes at each iteration. It means that each $x_j(k)$ is unavailable in (1). To preserve the privacy of nodes' initial states, a widely used approach is to add a random noise to the real state when a node needs to communicate with its neighbor nodes at each iteration. We define a new state as

$$x_i^+(k) = x_i(k) + \theta_i(k), i \in V, \tag{4}$$

where $\theta_i(k)$ is the added random noise for privacy preservation at iteration k. With the noise adding process, the update

equation (1) is changed to,

$$x_i(k+1) = w_{ii}x_i^+(k) + \sum_{j\in N_i} w_{ij}x_j^+(k) \quad (5)$$

$$= w_{ii}[x_i(k)+\theta_i(k)] + \sum_{j\in N_i} w_{ij}[x_j(k)+\theta_j(k)], \quad (6)$$

for $\forall i \in V$. Therefore, a privacy-preserving average consensus algorithm is to design the added noises (including the distribution and the correlations among them), such that the goal of (1) is achieved under (5). Note that in (4), the noise $\theta_i(k)$ is a general random noise (where its distribution is not fixed), the algorithm (4)–(6) is thus named as the general privacy-preserving average consensus (GPAC) algorithm in the rest part of this paper.

B. Privacy Definitions

Privacy Attack. Under (4), the broadcast information sequence of node i is $x_i^+(0), x_i^+(1), ..., x_i^+(k)$, which will be received by its neighbor nodes. Hence, each neighbor node j can infer/estimate the initial state $x_i(0)$ with the received information sequence from node i. Note that each of the information output, $x_i^+(k)$, equals the weighted sum of the received information in the previous round plus noises. Based on the information output, neighbor node j will take the probability over the space of all noises $\{\theta_i(k)\}_{k=0}^{\infty}$ (denoted by $\Theta \subseteq \mathcal{R}$) to estimate the values of the added noises, where the probability distribution and the space depend on the observable information. It then can infer $x_i(0)$ by using the difference between each information output and the estimated noises, i.e., $\hat{x}_i(0) = x_i^+(k) - \hat{\eta}_i^k$, where $\hat{\eta}_i^k$ is the estimation of random noise η_i^k ($\eta_i^k = x_i^+(k) - x_i(0)$). This state inference is named privacy attack. The attacker is a node who knows the basic rule of the state updating and noise adding process, and can eavesdrop its neighbor nodes' information output. It is assumed that each attacker cannot collude with other nodes to attack. Under this privacy attack, we have

$$\Pr\{|\hat{x}_i(0) - x_i(0)| \le \alpha\} = \Pr\{|\hat{\eta}_i^k - \eta_i^k| \le \alpha\}, \quad (7)$$

where $\alpha \ge 0$ is a small constant.

Privacy Definition. To quantify the relationship between the estimation accuracy (α) and privacy (β), a privacy definition, named (α,β)-data-privacy, where $0 \le \alpha$ and $0 \le \beta \le 1$, is defined as follows.

Definition 3.1: A GPAC algorithm provides (α,β)-data-privacy, if and only if (iff),

$$\beta = \max_{\hat{\eta}_i^k \in \Theta, k\ge 0, i\in V} \Pr\{|\hat{\eta}_i^k - \eta_i^k| \le \alpha\}, \quad (8)$$

where $\eta_i^k = x_i^+(k) - x_i(0)$ and $\hat{\eta}_i^k$ is the estimation of η_i^k.

In the above definition, the estimation accuracy is denoted by parameter α and the privacy is expressed by parameter β. From (8), it follows that β is the maximum probability that each neighbor node j can successfully estimate the initial state $x_i(0)$ in a given interval $[x_i(0)-\alpha, x_i(0)+\alpha]$ with the information output of node i only. β is thus named as the maximum disclosure probability. Note that when $x_i^+(k)$ is released, the value of random variable η_i^k is fixed. However, for the other nodes, η_i^k is still viewed as a random variable with the probability density function (PDF) $f_{\eta_i^k|\mathcal{I}(k)}(y)$ when it is estimated/inferred by those nodes, where $\mathcal{I}(k)$ is the information that is available to the inference at iteration k. Therefore, given an estimation $\hat{\eta}_i^k$, it is assumed that

$$\Pr\{|\hat{\eta}_i^k - \eta_i^k| \le \alpha | x_i^+(k)\} = \int_{\hat{\eta}_i^k-\alpha}^{\hat{\eta}_i^k+\alpha} f_{\eta_i^k|\mathcal{I}(k)}(y)\mathrm{d}y.$$

Definition 3.2: If there exists an $\tilde{\alpha} > 0$ so that for any given $\alpha \in (0,\tilde{\alpha})$, algorithms A_1 and A_2 provide (α,β_1)-data-privacy and (α,β_2)-data-privacy, respectively, and $\beta_1 < \beta_2$, then A_1 achieves a higher (α,β)-data-privacy than A_2.

C. Problem Formulation

In this paper, we will investigate the privacy of the GPAC algorithm (4)–(6) based on the definition of (α,β)-data-privacy, and then design an optimal privacy-preserving average consensus (OPAC) algorithm in terms of (α,β)-data-privacy protection. In summary, we will consider the following four critical problems: i) how to quantify and analyze the privacy of the GPAC algorithm; ii) how will the distributions and correlations of the added random noises affect the privacy; iii) when and how will a node's exact initial state be inferred by the other nodes; iv) how to achieve the optimal (α,β)-data-privacy and the exact average consensus, and to avoid the privacy of nodes' initial states to be disclosed.

IV. Privacy Analysis of GPAC

Before presenting the main results, we first give the basic assumptions and the information set used for state estimation. Assume that the distribution and the correlation of the random variable $\theta_i(k), k = 0, 1, ...$, and the update rule of the GPAC algorithm are available to all nodes. The full topology information and n are assumed to be unknown to any node, which means that each node cannot know the set of its neighbor nodes and the number of nodes in the whole network. Suppose that each node has no information about the other nodes' states initially. For estimation, if there is no information of a variable, then the variable is viewed with domain R. For simplicity, we assume that $\theta_i(k)$ and $\theta_j(k)$ are independently and identically distributed (i.i.d) $\forall k \ge 0$ and $i \ne j$. Let X be the output of a random variable whose distribution is unknown and with domain R. Without the knowledge of the distribution, one can randomly guess over all possible values of the random variable to estimate the values of X, and then the probability $\Pr\{|\hat{X} - X| \le \alpha\}$ would be very small. Therefore, it is reasonable to assume that

$$\Pr\{|\hat{X} - X| \le \alpha\} \le \epsilon, \quad (9)$$

where ϵ is a small constant and satisfies

$$\epsilon \ll \max_{\omega\in\Theta} \int_{\omega-\alpha}^{\omega+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y.$$

Then, we define two information sets of node i up to iteration k as follows,

$$\mathcal{I}_i^0(k) = \{x_i^+(0), ..., x_i^+(k)\}, \quad (10)$$

and

$$\begin{aligned}\mathcal{I}_i^1(k) =&\{N_i, w_{ii}, w_{ij}, x_i^+(0), x_j^+(0),\\ &..., x_i^+(k), x_j^+(k)|j \in N_i\}.\end{aligned} \tag{11}$$

The information set $\mathcal{I}_i^0(k)$ only includes the states $x_i^+(\ell), \ell = 0, 1, ..., k$, which are used for communication at iteration ℓ. Thus, its neighbor nodes can easily obtain $\mathcal{I}_i^0(k)$ by storing the information received from node i at each iteration. The information set $\mathcal{I}_i^1(k)$ includes all information used in consensus process (6) for node i. Other nodes may obtain these information by an eavesdropping attack.

A. Privacy of the Algorithm

In this subsection, based on the definition of (α, β)-data-privacy, we first analyze the privacy of the GPAC algorithm and reveal the relationship between the privacy and estimation accuracy, when $\mathcal{I}_i^0(k)$ is available only.

Theorem 4.1: If $\mathcal{I}_i^0(k)$ is the only information available to node j to estimate the value of $x_i(0)$ at iteration k, then

$$\begin{aligned}\beta(k) &= \max_{\hat{\eta}_i^k \in \Theta, k \in \mathbf{N}^+} \Pr\{|\hat{\eta}_i^k - \eta_i^k| \le \alpha|_{\mathcal{I}_i^0(k)}\}\\ &= \max_{\hat{\eta}_i^0 \in \Theta} \Pr\{|\hat{\eta}_i^0 - \eta_i^0| \le \alpha|_{\mathcal{I}_i^0(0)}\} \qquad (12)\\ &= \max_{\hat{\theta}_i(0) \in \Theta} \int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y, \qquad (13)\end{aligned}$$

i.e., the relationship between the privacy and the estimation accuracy always satisfies (13), and the maximum disclosure probability does not increase with iteration.

Proof: We first prove that, under $\mathcal{I}_i^0(0)$, (13) holds. With $\mathcal{I}_i^0(0)$, node j can estimate $x_i(0)$ based on the fact that

$$x_i^+(0) = x_i(0) + \theta_i(0) = x_i(0) + \eta_i^0, \tag{14}$$

and the corresponding estimation $\hat{x}_i(0)$ satisfies

$$\hat{x}_i(0) = x_i^+(0) - \hat{\eta}_i^0 = x_i^+(0) - \hat{\theta}_i(0). \tag{15}$$

Then, for any estimation $\hat{\theta}_i(0)$, we have

$$\begin{aligned}&\Pr\left\{|\hat{\eta}_i^0 - \eta_i^0| \le \alpha|_{\mathcal{I}_i^0(0)}\right\}\\ =&\Pr\left\{\theta_i(0) \in [\hat{\theta}_i(0) - \alpha, \hat{\theta}_i(0) + \alpha]|_{\mathcal{I}_i^0(0)}\right\}\\ =&\int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)|\mathcal{I}_i^0(0)}(y)\mathrm{d}y\\ \le&\max_{\hat{\theta}_i(0)\in\Theta} \int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y, \qquad (16)\end{aligned}$$

which means that (13) holds under information $\mathcal{I}_i^0(0)$ at iteration $k = 0$.

Then, we prove that (13) holds under $\mathcal{I}_i^0(1)$. With $\mathcal{I}_i^0(1)$, node j can estimate $x_i(0)$ by using the fact of both (14) and the following equation for estimation,

$$\begin{aligned}\frac{x_i^+(1)}{w_{ii}} =&\frac{x_i(1) + \theta_i(1)}{w_{ii}}\\ =&x_i^+(0) + \sum_{l\in N_i} \frac{w_{il}}{w_{ii}} x_l^+(0) + \frac{1}{w_{ii}}\theta_i(1)\\ =&x_i(0) + \theta_i(0) + \frac{1}{w_{ii}}\theta_i(1) + \sum_{l\in N_i} \frac{w_{il}}{w_{ii}} x_l^+(0). \qquad (17)\end{aligned}$$

Using (14) only, we have

$$\begin{aligned}&\Pr\left\{|\hat{\eta}_i^0 - \eta_i^0| \le \alpha|_{\mathcal{I}_i^0(1)}\right\} = \int_{\hat{\eta}_i^0-\alpha}^{\hat{\eta}_i^0+\alpha} f_{\theta_i(0)|\mathcal{I}_i^0(1)}(y)\mathrm{d}y\\ &\le \max_{\hat{\theta}_i(0)\in\Theta} \int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y. \qquad (18)\end{aligned}$$

Then, we consider the estimation using (17) only. Let

$$\begin{aligned}\eta_i^1 &= x_i^+(1) - x_i(0)\\ &= \frac{x_i^+(1)}{w_{ii}} - x_i(0) + \left(x_i^+(1) - \frac{x_i^+(1)}{w_{ii}}\right)\\ &= \theta_i(0) + \frac{1}{w_{ii}}\theta_i(1) + \left(x_i^+(1) - \frac{x_i^+(1)}{w_{ii}}\right) + \sum_{l\in N_i} \frac{w_{il}}{w_{ii}} x_l^+(0)\\ &= \eta_i^1(0) + \eta_i^1(1), \qquad (19)\end{aligned}$$

where $\eta_i^1(1) = \sum_{l\in N_i} \frac{w_{il}}{w_{ii}} x_l^+(0)$. For any $\hat{\eta}_i^1$, we have

$$\begin{aligned}&\max_{\hat{\eta}_i^1\in\Theta} \Pr\left\{|\hat{\eta}_i^1 - \eta_i^1| \le \alpha|_{\mathcal{I}_i^0(1)}\right\}\\ \le&\max_{\hat{\eta}_i^1\in\Theta} \Pr\left\{|\eta_i^1 - \hat{\eta}_i^1| \le \alpha|_{\mathcal{I}_i^0(1), w_{ii}, \theta_i(1), \theta_i(0)}\right\}\\ \le&\max_{\hat{\eta}_i^1\in\Theta} \Pr\left\{|\eta_i^1 - \eta_i^1(0) - \hat{\eta}_i^1 + \eta_i^1(0)| \le \alpha|_{\mathcal{I}_i^0(1), w_{ii}, \eta_i^1(0)}\right\}\\ \le&\max_{\hat{\eta}_i^1(1)\in\Theta} \Pr\left\{|\eta_i^1(1) - \hat{\eta}_i^1(1)| \le \alpha|_{\mathcal{I}_i^0(1), w_{ii}}\right\}, \qquad (20)\end{aligned}$$

where $\hat{\eta}_i^1(1) = \hat{\eta}_i^1 - \eta_i^1(0)$ can be viewed as one of the estimation of $\eta_i^1(1)$. Since the topology information is unavailable for estimating/inferrence, there is at least one variable included in $\eta_i^1(1)$ which is unknown to the other nodes. Hence, $\eta_i^1(1)$ is viewed as a random variable in (20) and its distribution is unavailable to the estimation. It follows that

$$\begin{aligned}&\max_{\hat{\eta}_i^1(1)\in\Theta} \Pr\left\{|\eta_i^1(1) - \hat{\eta}_i^1(1)| \le \alpha|_{\mathcal{I}_i^0(1)}\right\}\\ \le&\max_{\omega\in\Theta} \int_{\omega-\alpha}^{\omega+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y, \qquad (21)\end{aligned}$$

where we have used (9). Meanwhile, note that one node can combine (14) and (17) together for estimation. In this case, we have

$$\begin{aligned}&\Pr\{\hat{x}_i(0) \in [x_i(0) - \alpha, x_i(0) + \alpha]|_{\mathcal{I}_i^0(1)}\}\\ \le&\max_{t_1,t_2\in\Theta} \int_{t_1-\alpha}^{t_1+\alpha} \int_{t_2-\alpha}^{t_2+\alpha} f_{\eta_i^0,\eta_i^1}(y,z)dz\mathrm{d}y\\ \le&\max_{t_1,t_2\in\Theta} \int_{t_1-\alpha}^{t_1+\alpha} \int_{t_2-\alpha}^{t_2+\alpha} f_{\eta_i^1|\eta_i^0}(z|y) f_{\eta_i^0}(y)dz\mathrm{d}y\\ \le&\max_{\omega\in\Theta} \int_{\omega-\alpha}^{\omega+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y. \qquad (22)\end{aligned}$$

From (18), (21), and (22), one concludes that (13) holds under information $\mathcal{I}_i^0(1)$ at iteration $k=1$.

Following the similar analysis, we prove that (13) holds under information set $\mathcal{I}_i^0(k)$ at any iteration k. It means that $\beta(k)$ is not an increasing function of the number of iterations, although there is more information of $\mathcal{I}_i^0(k)$ than $\mathcal{I}_i^0(0)$ for $k>0$, i.e., $\mathcal{I}_i^0(0)\subset\mathcal{I}_i^0(k)$.

We thus have completed the proof. ■

From the above proof, it is observed that the privacy does not decrease with iteration when only the information set $\mathcal{I}_i^0$ $(=\{\mathcal{I}_i^0(k)|k=0,1,...,\infty\})$ is available for estimation. The main reason is that based on $\mathcal{I}_i^0$, node j cannot know the neighbor set information of node i, so that after one iteration there is unknown information embedded into $x_i^+(k)$ for $k\geq 1$. Hence, after one iteration, using $x_i^+(k)$ for $k\geq 1$ cannot improve the estimation accuracy. Also, one can see that the value of β does not depend on the estimation approaches. Hence, we state the following theorem.

Theorem 4.2: If $\mathcal{I}_i^0$ is the only information available to the other nodes to estimate the value of $x_i(0)$, the GPAC algorithm achieves (α,β)-data-privacy, where α and β satisfy

$$\beta=\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)}(y)\mathrm{d}y \tag{23}$$

and $\lim_{\alpha\to 0}\beta=0$.

Remark 4.1: It should be noticed that the results in the above two theorems are obtained under the assumption that the topology information is unknown to the nodes. If the assumption is relaxed, the above results could not be true for the GPAC algorithm in some cases. For example, if the topology information is available and $N_i\subseteq N_j$, then $x_i^+(0)$, $\sum_{l\in N_i}\frac{w_{il}}{w_{ii}}x_l^+(0)$, and $\frac{x_i^+(1)}{w_{ii}}$ in (17) are available to node j. It leads to the value of $\theta_i(1)$ being released, which may decrease the uncertainty of $\theta_i(0)$ due to the correlation between them. Then, $f_{\theta_i(0)|\mathcal{I}_i^0(1)}(y)$ in (18) will have a smaller variance than $f_{\theta_i(0)}(y)$, such that β increases w.r.t. k in this case. Therefore, (12) and (13) are no longer guaranteed.

From the above theorem, it is observed that given any distribution of the additive noises, there always exists $\beta\geq 0$. β depends on $f_{\theta_i(0)}(y)$ and α only since the estimation $\hat{\theta}_i(0)$ can be any value in the domain of $\theta_i(0)$. Thus, β is a function of $f_{\theta_i(0)}(y)$ and α, i.e, $\beta=\beta(f_{\theta_i(0)}(y),\alpha)$. Based on Definition 3.2, a smaller β can provide a higher (α,β)-data-privacy for any given α. We aim to find the optimal distribution of $\theta_i(0)$ to minimize β such that the algorithm achieves the highest (α,β)-data-privacy.

B. Optimal Noise Distribution

In this subsection, we find an optimal distribution for the noise adding process in the sense of achieving the highest (α,β)-data-privacy for the GPAC algorithm. Note that a smaller α means a higher accuracy estimation. It means that when α becomes smaller, the value of β is more important for the privacy preservation. Hence, we define the optimal distribution for privacy concerns as follows.

Definition 4.3: Let $f^*_{\theta_i(0)}(y)$ be the optimal distribution of $\theta_i(0)$, which means that for any given distribution $f^1_{\theta_i(0)}(y)$, there exists an α_1 such that $\beta(f^*_{\theta_i(0)}(y),\alpha)<\beta(f^1_{\theta_i(0)}(y),\alpha)$ holds for $\forall\alpha\in(0,\alpha_1]$.

To obtain the optimal distribution described in Definition 4.3, we define $\arg\min_{f_{\theta_i(0)}(y)}\beta=f^*_{\theta_i(0)}(y)$. Then, we formulate the following minimization problem,

$$\begin{aligned}\min_{f_{\theta_i(0)}(y)}\ & \beta\\ s.t.\ & \mathbf{E}\{\theta_i(0)\}=0,\\ & \mathbf{Var}\{\theta_i(0)\}=\sigma^2.\end{aligned} \tag{24}$$

The solution of (24) is the optimal distribution for the added noises with a given mean and variance in terms of (α,β)-data-privacy for the GPAC algorithm.

Theorem 4.4: If $\mathcal{I}_i^0$ is the only information available to node j to estimate the value of $x_i(0)$, then the optimal solution of problem (24) is that

$$f^*_{\theta_i(0)}(y)=\begin{cases}\dfrac{1}{2\sqrt{3}\sigma}, & \text{if } y\in[-\sqrt{3}\sigma,\sqrt{3}\sigma],\\ 0, & \text{otherwise},\end{cases} \tag{25}$$

i.e., given the finite variance of noises, the uniform distribution is optimal in the sense of (α,β)-data-privacy.

Proof: We prove this theorem by contradiction. Without loss of generality, we assume that $\sigma^2=\frac{1}{3}$. Let $f_1(y)$ and $f_2(y)$ be the PDF of two random variables with mean 0 and variance $\sigma^2=\frac{1}{3}$, and they follow a uniform and non-uniform distribution, respectively. Clearly, we have

$$f_1(y)=\begin{cases}\dfrac{1}{2}, & \text{if } y\in[-1,1],\\ 0, & \text{otherwise}.\end{cases} \tag{26}$$

Suppose that the non-uniform distribution $f_2(y)$ is the optimal distribution. From Definition 4.3, there exists an α_2, such that

$$\max_{t\in R}\int_{t-\alpha}^{t+\alpha} f_1(y)\mathrm{d}y>\max_{t\in R}\int_{t-\alpha}^{t+\alpha} f_2(y)\mathrm{d}y, \tag{27}$$

holds for $\forall\alpha\in(0,\alpha_2]$. Since the above equation holds for arbitrarily small value of α, we infer that

$$\max_{y\in R} f_1(y)>\max_{y\in R} f_2(y).$$

Since $f_1(y)$ is a uniform distribution satisfying (26),

$$f_1(y)-f_2(y)>0,\ y\in[-1,1].$$

It directly follows that

$$\int_{-1}^{1} f_1(y)\mathrm{d}y-\int_{-1}^{1} f_2(y)\mathrm{d}y>0. \tag{28}$$

From the definition of a PDF, we have $\int_{-1}^{1} f_1(y)\mathrm{d}y=1$. Then, we infer from (28) that

$$\int_{-1}^{1} f_2(y)\mathrm{d}y<1. \tag{29}$$

Since both $f_1(y)$ and $f_2(y)$ have mean 0 and variance $\sigma^2=\frac{1}{3}$, we have

$$\int_{-\infty}^{+\infty} f_1(y)y^2\mathrm{d}y-\int_{-\infty}^{\infty} f_2(y)y^2\mathrm{d}y=0, \tag{30}$$

which means that

$$\int_{-1}^{1}\left(f_1(y)-f_2(y)\right)y^2\mathrm{d}y=\left(\int_{-\infty}^{-1}+\int_{1}^{+\infty}\right)f_2(y)y^2\mathrm{d}y. \tag{31}$$

For the left hand side of (31), we have

$$\begin{aligned}\int_{-1}^{1}\left(f_1(y)-f_2(y)\right)y^2\mathrm{d}y&<\int_{-1}^{1}\left(f_1(y)-f_2(y)\right)\mathrm{d}y\\&=1-\int_{-1}^{1}f_2(y)\mathrm{d}y.\end{aligned} \tag{32}$$

For the right hand side of (31), since we have $\int_{-\infty}^{+\infty}f_2(y)\mathrm{d}y=1$ and (29), it holds that

$$\begin{aligned}\left(\int_{-\infty}^{-1}+\int_{1}^{+\infty}\right)f_2(y)y^2\mathrm{d}y&>\left(\int_{-\infty}^{-1}+\int_{1}^{+\infty}\right)f_2(y)\mathrm{d}y\\&=1-\int_{-1}^{1}f_2(y)\mathrm{d}y.\end{aligned} \tag{33}$$

Combining (31), (32), and (33) renders a contradiction that

$$\begin{aligned}1-\int_{-1}^{1}f_2(y)\mathrm{d}y&<\int_{-1}^{1}\left(f_1(y)-f_2(y)\right)y^2\mathrm{d}y\\&<1-\int_{-1}^{1}f_2(y)\mathrm{d}y.\end{aligned} \tag{34}$$

Hence, we cannot find a non-uniform distribution $f_2(y)$ such that the value of β is smaller than that under uniform distribution $f_1(y)$. It means that, given the finite variance, the uniform distribution is the optimal solution of (24). Then, based on the definition of uniform distribution, we obtain (25).

We thus have completed the proof. ∎

For the PPAC algorithm proposed in [18], normal distribution noises are used in the noise adding process. It follows from Theorem 4.2 that the GPAC algorithm provides (α,β)-data-privacy with

$$\beta=\frac{1}{\sigma\sqrt{2\pi}}\int_{-\alpha}^{\alpha}\exp\left(-\frac{y^2}{2\sigma^2}\right)\mathrm{d}y.$$

If we use the uniform distribution noises to substitute the normal distribution noises, it can still provide (α,β)-data-privacy, where $\beta=\frac{\alpha}{\sqrt{3}\sigma}$. Therefore, when

$$\frac{\alpha}{\sqrt{3}\sigma}<\frac{1}{\sigma\sqrt{2\pi}}\int_{-\alpha}^{\alpha}\exp\left(-\frac{y^2}{2\sigma^2}\right)\mathrm{d}y,$$

the privacy of PPAC is enhanced by using uniform distribution for substitution, where the possible values of α are obtained from solving the above equation.

C. Privacy Compromise

In this subsection, we reveal that for the GPAC algorithm, when $\mathcal{I}_i^1(k)$ (including more information than $\mathcal{I}_i^0(k)$, e.g., the topology information and information used in consensus process) is available to other nodes for estimation, the exact initial state of node i can be perfectly inferred, and thus the privacy of the initial state is compromised.

Theorem 4.5: If the information set $\mathcal{I}_i^1(k)$ of node i is available to the other nodes for estimation, then

$$\beta(k)\geq\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha}f_{\theta_i(0)|\theta_i(1),\ldots,\theta_i(k)}(y)\mathrm{d}y,\forall k\geq 0, \tag{35}$$

where $f_{\theta_i(0)|\theta_i(1),\ldots,\theta_i(k)}(y)$ is the conditional PDF of $\theta_i(0)$ given conditions $\theta_i(1),\ldots,\theta_i(k)$. Then, if $\sum_{\ell=0}^{\infty}\theta_i(\ell)=0$, we have $\beta=1$, i.e., $x_i(0)$ is disclosed and the privacy is compromised.

Proof: Based on $\mathcal{I}_i^1(k)$, the information of weights and states used in (5) is available. That is, the state sequence $x_i(1),x_i(2),\ldots,x_i(k)$ of node i is released to other nodes. Then, with (4), one obtains the values of $\theta_i(1),\theta_i(2),\ldots,\theta_i(k)$. Thus, when $k>0$, all the additive noises and the states of node i are available to other nodes, except $x_i(0)$ and $\theta_i(0)$.

Then, under information set $\mathcal{I}_i^1(k)$, using (14), we have

$$\begin{aligned}&\Pr\left\{|\hat{\eta}_i^0-\eta_i^0|\leq\alpha|_{\mathcal{I}_i^1(k)}\right\}\\&=\int_{\hat{\eta}_i^0-\alpha}^{\hat{\eta}_i^0+\alpha}f_{\theta_i(0)|\mathcal{I}_i^1(k)}(y)\mathrm{d}y\\&=\int_{\hat{\eta}_i^0-\alpha}^{\hat{\eta}_i^0+\alpha}f_{\theta_i(0)|\theta_i(1),\ldots,\theta_i(k)}(y)\mathrm{d}y.\end{aligned} \tag{36}$$

According the definition of β, it follows that

$$\begin{aligned}\beta(k)&\geq\max_{\hat{\eta}_i^0\in\Theta}\Pr\left\{|\hat{\theta}_i(0)-\eta_i^0|\leq\alpha|_{\mathcal{I}_i^1(k)}\right\}\\&\geq\max_{\hat{\eta}_i^0\in\Theta}\int_{\hat{\eta}_i^0-\alpha}^{\hat{\eta}_i^0+\alpha}f_{\theta_i(0)|\theta_i(1),\ldots,\theta_i(k)}(y)\mathrm{d}y,\end{aligned} \tag{37}$$

which means that (35) holds.

When $\sum_{\ell=0}^{\infty}\theta_i(\ell)=0$, we have

$$\theta_i(0)=-\sum_{\ell=1}^{\infty}\theta_i(\ell). \tag{38}$$

Since $\theta_i(1),\theta_i(2),\ldots,\theta_i(k)$ are available under $\mathcal{I}_i^1(k)$ for any positive integer k, $\theta_i(0)$ is inferred with (38) when $k\to\infty$, i.e., $\theta_i(0)$ is fixed and no longer a random variable given $\theta_i(1),\theta_i(2),\ldots,\theta_i(\infty)$. It follows that

$$\lim_{k\to\infty}\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha}f_{\theta_i(0)|\theta_i(1),\ldots,\theta_i(k)}(y)\mathrm{d}y=1,$$

which implies that $\beta=1$. Actually, when both $x_i^+(0)$ and $\theta_i(0)$ in (14) are disclosed, $x_i(0)$ is disclosed.

We thus have completed the proof. ∎

Consider the existing PPAC algorithms, e.g., [18], [23]. One obtains that the correlation of the added noises satisfies

$$\begin{aligned}\sum_{\ell=0}^{k}\theta_i(\ell)&=\theta_i(0)+\sum_{\ell=1}^{k}\left[\varrho^{\ell}\nu_i(\ell)-\varrho^{\ell-1}\nu_i(\ell-1)\right]\\&=\nu_i(0)-\varrho^0\nu_i(0)+\varrho^1\nu_i(1)-\varrho^1\nu_i(1)+\varrho^2\nu_i(2)\\&\quad-\ldots-\varrho^{k-1}\nu_i(k-1)+\varrho^k\nu_i(k)\\&=\varrho^k\nu_i(k)=\phi_i(k),\end{aligned} \tag{39}$$

where $\nu_i(k)$ is a random variable with fixed mean ($=0$) and variance ($=\sigma^2$). Given $\theta_i(1),...,\theta_i(k)$, we obtain that $\theta_i(0) = \phi_i(k) - \sum_{\ell=1}^{k}\theta_i(\ell)$, where $\sum_{\ell=1}^{k}\theta_i(\ell)$ is known. Then,

$$\begin{aligned}&\Pr\left\{|\hat{\theta}_i(0)-\theta_i(0)|\le\alpha|_{\mathcal{I}_i^1(k)}\right\}\\&=\Pr\left\{|\hat{\phi}_i(k)-\phi_i(k)|\le\alpha\right\}\\&=\int_{\hat{\phi}_i(k)-\alpha}^{\hat{\phi}_i(k)+\alpha} f_{\phi_i(k)}(y)\mathrm{d}y,\end{aligned}\tag{40}$$

and

$$\begin{aligned}&\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\theta}_i(0)-\alpha}^{\hat{\theta}_i(0)+\alpha} f_{\theta_i(0)|\theta_i(1),...,\theta_i(k)}(y)\mathrm{d}y\\&=\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\phi}_i(k)-\alpha}^{\hat{\phi}_i(k)+\alpha} f_{\phi_i(k)}(y)\mathrm{d}y,\end{aligned}$$

which satisfies (35). When $k\to\infty$, we have

$$\lim_{k\to\infty}\max_{\hat{\theta}_i(0)\in\Theta}\int_{\hat{\phi}_i(k)-\alpha}^{\hat{\phi}_i(k)+\alpha} f_{\phi_i(k)}(y)\mathrm{d}y = 1,$$

since the variance of $\hat{\phi}_i$ satisfies $\lim_{k\to\infty}\varrho^{2k}\sigma^2 = 0$, and thus $\beta = 1$. Therefore, it verifies the result given in Theorem 4.5.

D. Further Discussion on Privacy

Differential privacy is a well-known and widely used privacy concept in computer and communication areas [22], and it has been employed in control and network systems recently [26]. A differentially private algorithm ensures that any two similar/close inputs will have approximately the same outputs, so that an adversary cannot infer from the data output with a high probability whether the data is associated with a single user or not. It has been proved by Nozari et al. in [16] that states of nodes in a network cannot simultaneously converge to the average of their initial states and preserve differential privacy of their initial states. However, differential privacy cannot quantify the degree of data privacy protection in terms of the probability of an estimate by an eavesdropper is within a given range. This motivates us to develop the definition of the (α,β)-data-privacy. The proposed (α,β)-data privacy can be used to reveal the relationship between the maximum data disclosure probability (β) and the estimation accuracy range (α).

Consider the general noise addition that adding a random noise to the initial data for data publishing. It is well known that when the additive noise is Laplacian noise, the mechanism ensures α-differential privacy, but if the noise is Gaussian or Uniform distribution, the α-differential privacy cannot be guaranteed. Hence, the uniform noise is not good in the sense of differential privacy. However, in term of (α,β)-data-privacy, it is shown in this paper that both the Gaussian and Uniform noise are (α,β)-data-private, and using the Uniform noise can achieve the highest privacy. The privacy of (α,β)-data-privacy is different from that of differential privacy. It is worth to investigate the relationship between these two kinds of privacy definitions in theory, which beckons further investigation.

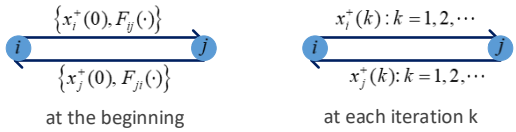


Fig. 1. The information flow between two neighboring nodes in OPAC.

V. OPAC Algorithm

In this section, we design an OPAC algorithm to achieve the highest (α,β)-data-privacy, and at the same time to avoid privacy to be compromised even if the information $\mathcal{I}_i^1(\infty)$ of each node i is available to other nodes.

A. Algorithm Design

From the privacy analysis in the above section, we note that the uniform distribution is optimal for the added noise in terms of achieving the highest (α,β)-data-privacy with $\beta = \frac{\alpha}{\sqrt{3}\sigma}$ (given variance σ). Hence, in each iteration of the OPAC algorithm, we will use uniformly distributed noise. We also note that privacy is compromised when $\mathcal{I}_i^1(\infty)$ is available. It is because that the nodes can use $\mathcal{I}_i^1(\infty)$ to obtain the real values of $\theta_i(1),\theta_i(2),....,\theta_i(\infty)$, and use the correlation $\sum_{k=0}^{\infty}\theta_i(k) = 0$ to infer $\theta_i(0)$, and thus the value of $x_i(0)$ is revealed. To avoid the privacy compromise in this case, we introduce a secret continuous function $F_{ij}(z): R\to R$ for node i with respect to its neighbor node j. Suppose that $F_{ij}(z)$ and $F_{ji}(z)$ are only available to nodes i and j, and $F_{ij}(z)$ may or may not equal to $F_{ji}(z)$. Then, the OPAC algorithm is described as in Algorithm 1.

Algorithm 1 : *OPAC Algorithm*

1: **Input:** $x_i(0)$, N_i, w_{ij}, $F_{ij}(\cdot)$, $\forall j\in N_i$, σ and ϱ for each $i\in V$.
2: **Initialization:** Each node i selects a uniform distribution random variable $\nu_i(0)$ from interval $[-\sqrt{3}\sigma,\sqrt{3}\sigma]$, and arbitrarily selects a constant sequence z_{ij} ($\in R$) for $j\in N_i$.
3: Let $\theta_i(0)=\nu_i(0)$ and $\mathbf{x}_i^+(0)=\mathbf{x}_i(0)+\theta_i(0)$. Then, each node i transmits $\mathbf{x}_i^+(0)$ and z_{ij} to its neighbor node j.
4: Each node i calculates $\tilde{\nu}_i(0)$ by

$$\tilde{\nu}_i(0) = \nu_i(0) - \sum_{j\in N_i}\left[F_{ij}(z_{ij}) - F_{ji}(z_{ji})\right], \forall i\in V. \tag{41}$$

5: **Iteration:** Each node updates its state with (5).
6: Each node generates a uniform distribution random variable $\nu_i(k)$ from interval $[-\sqrt{3}\sigma,\sqrt{3}\sigma]$ for $k\ge 1$.
7: Each node i uses $\theta_i(k)$ in (4) to get $x_i^+(k)$, where

$$\theta_i(k) = \begin{cases}\varrho\nu_i(1) - \tilde{\nu}_i(0), & \text{if } k=1;\\ \varrho^k\nu_i(k) - \varrho^{k-1}\nu_i(k-1), & \text{if } k\ge 2,\end{cases} \tag{42}$$

where $\varrho\in(0,1)$ is a constant for all nodes.
8: Each node i communicates with its neighbors with $x_i^+(k)$.
9: Let $k=k+1$ and go to step 5.
10: **Output:** $x_i(\infty)$ for each $i\in V$.

In OPAC, the information flow between neighboring nodes i and j is shown in Fig. 1. The secrete functions are exchanged at the initial stage, and at each iteration $k=0,1,\cdots$, they only exchange the $x_l^+(k)$ for $l=i,j$. It should be pointed out that using the secret function, the privacy can be preserved even with the classic consensus algorithm without adding

noises. However, the noise adding process is kept in OPAC for enhancing the protection of the initial states, so that OPAC can guarantee the same level of privacy as GPAC even when secret functions are released.

B. Convergence and Privacy Analysis

In this subsection, we analyze the convergence and the privacy of the OPAC algorithm.

Theorem 5.1: Using the OPAC algorithm, we have (3) hold for $\forall i \in V$, i.e., an exact average consensus is achieved.

Proof: From Theorem 4.1 of [23], we know that if the added noises in (4) are bounded and decaying, and the sum of all nodes' added noises equals zero, then average consensus can be achieved. In the following, we prove that the added noises used for the OPAC algorithm satisfy these conditions.

We first prove that the added noises are bounded and exponentially decaying. Clearly, $\theta_i(0) = \nu_i(0) \in [-\sqrt{3}\sigma, \sqrt{3}\sigma]$ is bounded. Since each $F_{ij}(z)$ is a continuous function, its value is bounded for any given z. Then, it follows from (41) that $\tilde{\nu}_i(0)$ is bounded. For $k \geq 1$, since $\nu_i(k)$ is selected from interval $[-\sqrt{3}\sigma, \sqrt{3}\sigma]$ and $\theta_i(k)$ is generated by (42), it is not difficult to infer that each $\theta_i(k)$ is bounded. Meanwhile, it follows from (42) that

$$\begin{aligned}\lim_{k\to\infty} |\theta_i(k)| &\leq \lim_{k\to\infty} |\varrho^k \nu_i(k) - \varrho^{k-1}\nu_i(k-1)| \\ &\leq \lim_{k\to\infty} [\varrho^k\sqrt{3}\sigma + \varrho^{k-1}\sqrt{3}\sigma] = 0,\end{aligned}$$

i.e., the noises decay and converge to zero.

Next, we prove that the sum of all nodes' added noises are equal to zero. Note that

$$\begin{aligned}\sum_{i=1}^{n}\sum_{k=0}^{\infty}\theta_i(k) &= \sum_{i=1}^{n}\theta_i(0) + \sum_{i=1}^{n}\theta_i(1) \\ &\quad + \sum_{i=1}^{n}\sum_{k=2}^{\infty}(\varrho^k\nu_i(k) - \varrho^{k-1}\nu_i(k-1)) \\ &= \sum_{i=1}^{n}\nu_i(0) + \sum_{i=1}^{n}(\varrho\nu_i(1) - \tilde{\nu}_i(0)) \\ &\quad + \sum_{i=1}^{n}(\varrho^\infty\nu_i(\infty) - \varrho^1\nu_i(1)) \\ &= \sum_{i=1}^{n}\nu_i(0) - \sum_{i=1}^{n}\tilde{\nu}_i(0),\end{aligned}$$

where we have used the fact that $\varrho^\infty\nu_i(\infty) = 0$. Substituting (41) into the above equation yields that

$$\begin{aligned}\sum_{i=1}^{n}\sum_{k=0}^{\infty}\theta_i(k) &= \sum_{i=1}^{n}\nu_i(0) \\ &\quad - \sum_{i=1}^{n}\left[\nu_i(0) - \sum_{j\in N_i}(F_{ij}(z_{ij}) - F_{ji}(z_{ji}))\right] \\ &= \sum_{i=1}^{n}\sum_{j\in N_i}\left[F_{ji}(z_{ji}) - F_{ij}(z_{ij})\right].\end{aligned}$$

Since for each pair of $F_{ji}(z_{ji}) - F_{ij}(z_{ij})$ used in node i, there exists a pair of $F_{ij}(z_{ij}) - F_{ji}(z_{ji})$ with negative value used in node j, it follows that

$$\sum_{i=1}^{n}\sum_{j\in N_i}\left[F_{ji}(z_{ji}) - F_{ij}(z_{ij})\right] = 0.$$

Hence, we have $\sum_{i=1}^{n}\sum_{k=0}^{\infty}\theta_i(k) = 0$.

Thus, the proof is completed. ■

The following theorem can be obtained from Theorem 4.2 directly, since the OPAC is one of the GPAC algorithm.

Theorem 5.2: If $\mathcal{I}_i^0$ is the only information available to the other nodes to estimate the value of $x_i(0)$, then the OPAC algorithm achieves (α, β)-data-privacy, where $\beta = \frac{\alpha}{\sqrt{3}\sigma}$ and $\lim_{\alpha\to 0}\beta = 0$.

Then, the following theorem shows that under $\mathcal{I}_i^1$, the privacy compromise can be avoided by the OPAC.

Theorem 5.3: Suppose that the information set $\mathcal{I}_i^1$ of node i is available to the other nodes and each node has at least two neighbors (i.e., $|N_i| \geq 2$ for all $i \in V$). Then, the privacy compromise can be avoided by the OPAC.

Proof: It has been known that when $\mathcal{I}_i^1$ of node i is available to other nodes, its neighbor node j can obtain the real values of $\theta_i(1), \theta_i(2), ..., \theta_i(\infty)$. Then, the value of $\sum_{k=1}^{\infty}\theta_i(k)$ is released. Note that

$$\begin{aligned}&\sum_{k=1}^{\infty}\theta_i(k) = (\varrho^1\nu_i(1) - \tilde{\nu}_i(0)) + \sum_{k=2}^{\infty}\theta_i(k) \\ &= (\varrho^1\nu_i(1) - \tilde{\nu}_i(0)) + (\varrho^\infty\nu_i(\infty) - \varrho^1\nu_i(1)) = \tilde{\nu}_i(0).\end{aligned}$$

It means that the value of $\tilde{\nu}_i(0)$ is released and available to node j. From (41), one sees that $\tilde{\nu}_i(0) \neq \theta_i(0)$[1] and

$$\tilde{\nu}_i(0) = \theta_i(0) - \sum_{j\in N_i}\left[F_{ij}(z_{ij}) - F_{ji}(z_{ji})\right]. \tag{43}$$

Since $|N_i| \geq 2$ and only F_{ij} and F_{ji} are known by node j, there exists $F_{ij_o}(z_{ij_o}) - F_{j_oi}(z_{j_oi})$ for $j_0 \in N_i$ in (43) that is not known by node j. It means that there are no neighbor nodes who can know all the information used for node i's updates. Meanwhile, $F_{ij_o}(z_{ij_o}) - F_{j_oi}(z_{j_oi})$ has domain R, thus one infers that for any $c \in [-\sqrt{3}\sigma, \sqrt{3}\sigma]$,

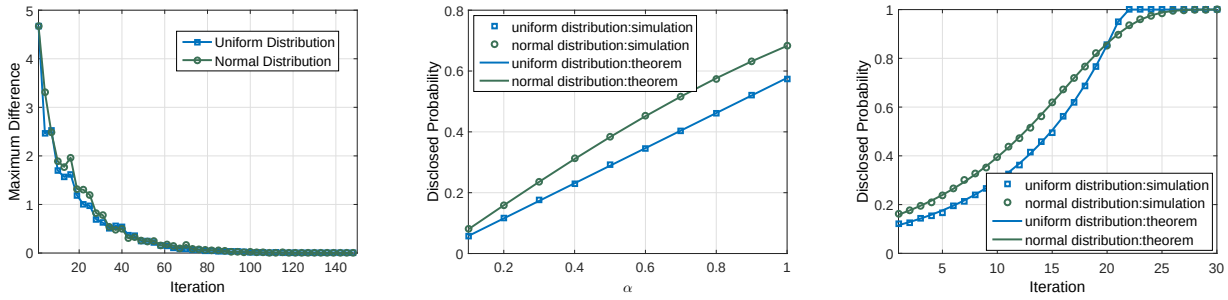
$$\Pr\{\theta_i(0) = c|\tilde{\nu}_i(0)\} = \Pr\{\theta_i(0) = c\}.$$

Hence, even if the value of $\tilde{\nu}_i(0)$ is released, node j cannot increase the estimation accuracy of $\theta_i(0)$ with (43). One thus concludes that based on the OPAC algorithm, the privacy compromise is avoided.

We thus have completed the proof. ■

If node i has only one neighbor node j, node j can infer the value of $F_{ij}(z_{ij}) - F_{ji}(z_{ji})$. Then, from (43), node j can obtain the value of $\theta_i(0)$ and $x_i(0)$ when $\tilde{\nu}_i(0)$ is known. Therefore, one can further infer that even if the attack node has the information of $\mathcal{I}_i^1$ and knows the secret functions F_{ij} for some but not all $j \in N_i$, the privacy compromise can be avoided by the OPAC.

[1]This is the main difference between the OPAC and PPAC algorithm, and the main reason why OPAC can avoid privacy compromise.



(a) convergence (b) privacy under $\mathcal{I}_i^0$ (c) privacy under $\mathcal{I}_i^1$

Fig. 2. The convergence and privacy comparison under different random noise distribution.

Remark 5.1: From the above two theorems, one sees that using OPAC algorithm, we have $\beta = \frac{\alpha}{\sqrt{3}\sigma}$, which is the optimal privacy that can be achieved from solving problem (24). Furthermore, $\beta = \frac{\alpha}{\sqrt{3}\sigma}$ can be guaranteed by the OPAC algorithm under $\mathcal{I}_i^1(\infty)$. Thus, OPAC algorithm can achieve much higher (α, β)-data-privacy than the existing PPAC. In this paper, we consider that the attacker can be an internal node of the network who knows the basic rule of the state updating and noise adding process, and can hear its neighboring nodes' information output. Hence, it is possible for the attacker to obtain the weights $(w_{ii},\ w_{ij})$ or other information in $\mathcal{I}_i^1$ through eavesdropping (local observation). For example, if node i sets $w_{ij} = \frac{1}{n}$ for each neighbor node, the attacker who can eavesdrop message exchanges of node i can learn w_{ij} directly and infer w_{ii} using $w_{ii} = 1 - \frac{|N_i|}{n}$. Under OPAC, attack node j knows F_{ij} and does not know $F_{ij'}$ for $j' \neq j, j', j \in N_i$, and thus the privacy cannot be compromised (This has been proved in Theorem 5.3).

VI. Performance Evaluation

In this section, we conduct simulations to verify the obtained theoretical results and evaluate the performance of the proposed OPAC algorithm.

A. Simulation Scenario

Consider the network with 50 nodes which are randomly deployed in a 100m $\times$ 100m area, and the maximum communication range of each node is 30m. We consider the normal distribution and uniform distribution of the added noises, respectively, where the mean and variance of them are set as 0 and $\sigma^2 = 1$. We set $\varrho = 0.9$. The initial states of the nodes are randomly selected from $[0, 10]$. The function, $d(t) = \max_{i\in\mathcal{V}} |x_i(t) - \bar{x}|$, is defined as the maximum deviation between the nodes' states and the average value.

B. Verification

Fig. 2(a) compares the convergence speed of the PPAC algorithm using normal and uniform distribution noises, in which the basic design is the same as PPAC proposed in [18]. It is observed that under the two different distributions, the PPAC algorithm has the same convergence speed. This justifies that the convergence speed only depends on the eigenvalues of the weight matrix W and the value of ϱ as proved in [18].

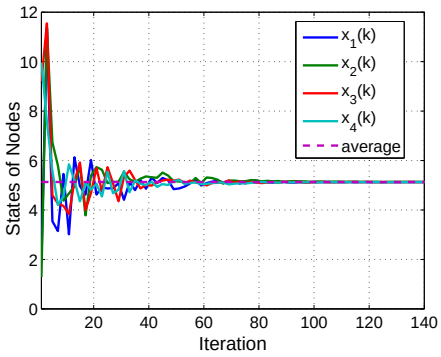
Fig. 2(b) compares the (α, β)-data-privacy under $\mathcal{I}_i^0$ with normal and uniform distribution noises. In simulation, we conduct $10,000$ simulation runs. For each run, one node first generates a noise $\theta_i(0)$ randomly with the given distribution, and the other nodes generate $10,000$ random numbers with the same distribution and use them as the estimation of $\theta_i(0)$ (i.e., $\hat{\theta}_i(0)$). Then, one obtains the probability of $|\hat{\theta}_i(0) - \theta_i(0)| \leq \alpha$ in each run, and we use the maximum probability among these in all simulation runs as the value of β. For the theoretical results, we use (23) to calculate the value of β under two different distributions. Clearly, one can observe from Fig. 2(b) that uniform distribution is much better than normal distribution in the sense of (α, β)-data-privacy. It is also observed that β in simulation matches its value in theory.

Fig. 2(c) compares the (α, β)-data-privacy under $\mathcal{I}_i^1$ using normal and uniform distribution noises. The simulations here are conducted similarly as those in Fig. 2(b), except that when the iteration increases, the variance of the noises will be changed to $\sigma^2 = \varrho^{2k}$ since (40) will be used for estimation at iteration k. We use (23) to calculate the value of β, and the corresponding results are denoted by theoretical results. Both in simulation and theory, we set $\alpha = 0.2$. As shown in Fig. 2(c), the maximum disclosure probability increases with iteration and will converge to 1, i.e., the privacy decays with iteration and will eventually be compromised.

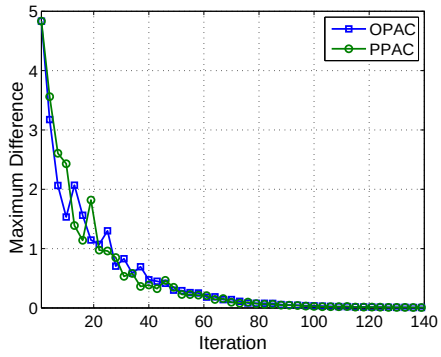
C. Evaluation

In this subsection, we will evaluate the performance of the OPAC algorithm. Using the same setting as the above subsection, the OPAC algorithm can guarantee the similar privacy as the blue line shown in Fig. 2(b) under $\mathcal{I}_i^1$. This is because uniform distribution noise used in OPAC and the secret function makes the subsequent $(k \geq 1)$ information do not increase the disclosure probability. Therefore, the OPAC guarantees a much stronger privacy than the GPAC, since it achieves the same privacy under $\mathcal{I}_i^1$ as the GPAC under $\mathcal{I}_i^0$.

Then, we test the convergence of the OPAC algorithm. Set $F_{ij} = \frac{i+2j}{50}$. As shown in Fig. 3(a), we find that nodes' states will converge to the exact average with the OPAC, which means that an exact average consensus can be achieved by the proposed algorithm. Fig. 3(b) compares the convergence speed of the OPAC and PPAC, it is found that they almost have the same convergence speed. Hence, the added secret function will not affect the convergence speed.



(a) converge to average consensus



(b) same covergence speed

Fig. 3. The performance evaluation of the OPAC algorithm.

VII. Conclusions

In this paper, we investigated the privacy of the GPAC algorithm. We proposed a novel privacy definition, named (α, β)-data-privacy, to depict the relationship between privacy and estimation accuracy, so that the degree of the privacy preservation can be well quantified. We proved that the GPAC algorithm achieves (α, β)-data-privacy, and obtained the closed-form expression of the relationship between α and β. We also proved that the noise with a uniform distribution guarantees the highest privacy when α is small. We revealed that the privacy will be lost when the information used in each consensus iteration is available to the other nodes. To solve this problem and achieve the highest (α, β)-data-privacy, we proposed the OPAC algorithm, followed by the convergence and privacy analysis. Lastly, simulations were conducted to verify the correctness of the theoretical results and demonstrate the effectiveness of the proposed algorithm.

ACKNOWLEDGEMENT

The authors would like to thank the editor and the anonymous reviewers for their helpful and constructive comments, which have helped us improve the manuscript significantly. This work was supported in part by the Natural Science Foundation of China (NSFC) under grant 61773257, 61761136012, 61521063, 61633017 and the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, 95(1): 215–233, 2007.

[2] V. Blondel, J. M. Hendrickx, A. Olshevsky, and J. Tsitsiklis, "Convergence in multiagent coordination, consensus, and flocking," in *Proc. IEEE CDC*, 2005.

[3] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband internet of things: Implementations and applications," in *IEEE Internet Things J.*, 4(6): 2309-2314, 2017.

[4] W. Ren, B. Randal, and A. Ella, "Information consensus in multivehicle cooperative control: Collective group behavior through local interaction," *IEEE Control Syst. Mag.*, 27(2): 71–82, 2007.

[5] F. Pasqualetti, R. Carli, A. Bicchi, and F. Bullo, "Distributed estimation and detection under local information," in *Proc. IFAC*, 2010.

[6] G. Mateos, I. Schizas and G. Giannakis, "Distributed recursive least-squares for consensus-based in-network adaptive estimation," *IEEE Trans. Signal Process.*, 57(11): 4583–4588, 2009.

[7] L. Xiao, S. Boyd, and S. Lall, "A scheme for robust distributed sensor fusion based on average consensus," in *Proc. ISIPSN*, 2005.

[8] C. Zhao, J. He, P. Cheng and J. Chen, "Consensus-based energy management in smart grid with transmission losses and directed communication," *IEEE Trans. Smart Grid*, 8(5): 2049–2061, 2017.

[9] J. He, L. Duan, F. Hou, P. Cheng, and J. Chen, "Multi-period scheduling for wireless sensor networks: A distributed consensus approach," *IEEE Trans. Signal Process.*, 63(7): 1651-1663, 2015.

[10] L. Schenato and F. Fiorentin, "Average timesynch: A consensus-based protocol for clock synchronization in wireless sensor networks," *Automatica*, 47(9): 1878–1886, 2011.

[11] J. He, M. Zhou, P. Cheng, L. Shi, and J. Chen. Consensus under bounded noise in discrete network systems: An algorithm with fast convergence and high accuracy. *IEEE Trans. Cybernetics*, 46(12), 2874-2884, 2016.

[12] R. Carli, and S. Zampieri, "Network clock synchronization based on the second order linear consensus algorithm," *IEEE Trans. Automat. Contr.*, 59(2): 409–422, 2014.

[13] J. He, P. Cheng, L. Shi, and J. Chen, "Time synchronization in WSNs: A maximum value based consensus approach," *IEEE Trans. Automat. Contr.*, 59(3): 660–674, 2014.

[14] J. Le Ny and G. Pappas, "Differentially private filtering," *IEEE Trans. Automat. Contr.*, 59(2): 341–354, 2014.

[15] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus." in *Proc. ACM Workshop on Privacy in the Electronic Society*, 2012.

[16] E. Nozari, P. Tallapragada, and J. Cortes, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design." *Automatica*, 81: 221-231, 2017.

[17] N. Manitara and C. Hadjicostis, "Privacy-preserving asymptotic average consensus." in *Proc. IEEE ECC*, 2013.

[18] Y. Mo, and R. Murray, "Privacy preserving average consensus," *IEEE Trans. Automat Contr.*, 62(2): 753–765, 2017.

[19] M. DeGroot, "Reaching a consensus," *J. Amer. Statist. Assoc.*, 69(345), 118–121, 1974.

[20] J. Lin, A. S. Morse, and B. D. Anderson, "The multi-agent rendezvous problem," in *Proc. IEEE CDC*, 2003.

[21] A. Olshevsky and J. Tsitsiklis, "Convergence speed in distributed consensus and averaging," *SIAM Review*, 53(4): 747–772, 2011.

[22] C. Dwork. "Differential privacy," in *Encyclopedia of Cryptography and Security*, Springer US, pp. 338-340, 2011.

[23] J. He, L. Cai, P. Cheng, J. Pan and L. Shi. "Consensus-based privacy-preserving data aggregation," *https://arxiv.org/abs/1609.06381*, 2018.

[24] J. He, L. Cai and X. Guan. "Preserving data-privacy with added noises: optimal estimation and privacy analysis," *IEEE Trans. Inf. Theory*, DOI:10.1109/TIT.2018.2842221, 2018.

[25] P. Braca, R. Lazzeretti, S. Marano, and V. Matta. "Learning with privacy in consensus + obfuscation," *IEEE Signal Process. Lett.*, 23(9): 1174-1178, 2016.

[26] J. Cortes, G. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. Pappas. "Differential privacy in control and network systems," in *Proc. IEEE CDC*, 2016.

[27] Z. Erkin, J. Troncoso-Pastoriza, R. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview." *IEEE Signal Proc. Mag.*, 30(2): 75-86, 2013.

[28] M. Ruan, G. Huan and Y. Wang, "Secure and privacy-preserving consensus." *arXiv preprint arXiv:1707.04491*, 2017.

[29] E. Abbe, E. K. Amir, and W. L. Andrew, "Privacy-preserving methods for sharing financial risk exposures." *Am. Econ. Rev.* 102(3): 65–70, 2012.

[30] S. Gade and H. V. Nitin, "Private learning on networks: Part II." *arXiv preprint arXiv:1703.09185*, 2017.

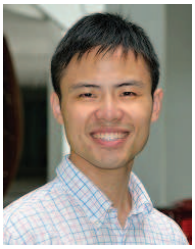
Jianping He (M'15) is currently an associate professor in the Department of Automation at Shanghai Jiao Tong University, Shanghai, China. He received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013, and had been a research fellow in the Department of Electrical and Computer Engineering at the University of Victoria, Canada, from Dec. 2013 to Mar. 2017.

His research interests mainly include the smart sensing and control, security and privacy theory and its applications, distributed learning and big data. He serves as an associate editor for the KSII Transactions on Internet and Information Systems. He also serves/served as the Guest Editor for IEEE Transactions on Automatic Control, International Journal of Robust and Nonlinear Control and Neurocomputing. He was the winner of Outstanding Thesis Award, Chinese Association of Automation, 2015. He received the best paper award of IEEE WCSP'17 and the finalist best student paper award of IEEE ICCA'17. He is the recipient of China National Recruitment Program of 1000 Talented Young Scholars.

Lin Cai (S'00-M'06-SM'10)received her M.A.Sc. and PhD degrees in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical & Computer Engineering at the University of Victoria, Canada, and she is currently a Professor.

Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic over wireless, mobile, ad hoc, and sensor networks. She has served as a TPC symposium co-chair for IEEE Globecom'10 and Globecom'13. She has served as a member of the Steering Committee of the IEEE Transactions on Big Data, an Associate Editor of the IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, EURASIP Journal on Wireless Communications and Networking, International Journal of Sensor Networks, and Journal of Communications and Networks (JCN), and as the Distinguished Lecturer of the IEEE VTS Society. She was a recipient of the NSERC Discovery Accelerator Supplement Grants in 2010 and 2015, respectively, and the Best Paper Awards of IEEE ICC 2008 and IEEE WCNC 2011. She has founded and chaired IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She is a registered professional engineer of British Columbia, Canada.

Chengcheng Zhao received her B.E. degree in Measurement & Control Technology and Instrument from Hunan University, Changsha, China, in 2013. She is currently working toward her Ph.D. degree in College of Control Science and Engineering, Zhejiang University, Hangzhou, China. She is a member of Networked Sensing and Control group (NESC). Her research interests include consensus and distributed optimization, distributed energy management and synchronization in smart grids, security and privacy in networked systems. She received IEEE PESGM 2017 best conference papers award, and one of her paper was shortlisted in IEEE ICCA 2017 best student paper award finalist. She is a peer reviewer for Automatica, IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Industrial Electronics and etc. She was the Technical Program Committee Member for IEEE Global Communications Conference (GLOBECOM) 2017, 2018, and IEEE International Conference on Communications (ICC) 2018.



Peng Cheng (M'10) received the B.E. degree in Automation, and the Ph.D. degree in Control Science and Engineering in 2004 and 2009 respectively, from Zhejiang University, Hangzhou, China. Currently he is Professor with College of Control Science and Engineering, Zhejiang University. He serves as Associate Editor of IEEE Transactions on Control of Network Systems, Wireless Networks, and International Journal of Communication Systems. He also serves/served as the Guest Editor for IEEE Transactions on Automatic Control, IEEE Transactions on Signal and Information Processing over Networks, and IEEE Transactions on Control of Network Systems. He served as the TPC co-chair of IEEE IOV 2016, local arrangement co-chair for ACM MobiHoc 2015, and the publicity co-chair for IEEE MASS 2013. His research interests include networked sensing and control, cyber-physical systems, control system security.

Xinping Guan (SM'04-F'18) is currently a Chair Professor of Shanghai Jiao Tong University, China, where he is the Deputy Director of University Research Management Office, and the Director of the Key Laboratory of Systems Control and Information Processing, Ministry of Education of China. Before that, he was the Professor and Dean of Electrical Engineering, Yanshan University, China.

Dr. Guan's current research interests include industrial cyber-physical systems, wireless networking and applications in smart city and smart factory, and underwater sensor networks. He has authored and/or coauthored 4 research monographs, more than 270 papers in IEEE Transactions and other peer-reviewed journals, and numerous conference papers. As a Principal Investigator, he has finished/been working on many national key projects. He is the leader of the prestigious Innovative Research Team of the National Natural Science Foundation of China (NSFC). Dr. Guan is an Executive Committee Member of Chinese Automation Association Council and the Chinese Artificial Intelligence Association Council. He was elevated to IEEE Fellow in 2017. He received the First Prize of Natural Science Award from the Ministry of Education of China in both 2006 and 2016, and the Second Prize of the National Natural Science Award of China in 2008. He was a recipient of the "IEEE Transactions on Fuzzy Systems Outstanding Paper Award" in 2008. He is a "National Outstanding Youth" honored by NSF of China, "Changjiang Scholar" by the Ministry of Education of China and State-level Scholar of New Century Bai Qianwan Talent Program of China.