Letter

Privacy-Preserving Average Consensus Algorithm Under Round-Robin Scheduling Protocol

Yingjiang Guo, Wenying Xu, Haodong Wang, Jianquan Lu, and Shengli Du

Dear Editor,

Over the past decades, cooperative control and distributed optimization have gained significant research attention due to their broad applications such as signal processing, robotics, and social networks [1], [2]. As a fundamental component of distributed control and optimization, the issue of average consensus has become a recurring topic of interest [3], [4]. To achieve average consensus, it is essential to establish a distributed algorithm with local information under which each node is able to adjust its own behavior by exchanging information with its neighbors instead of relying on a central node.

Until now, various average consensus algorithms are designed for different types of systems, such as continuous-time and discrete-time dynamics. It is worthwhile to mention that most of the existing consensus algorithms are dependent on agents' real and explicit states and thus their privacy is easily leaked and preserving privacy becomes a concern. Recently, there exist several works on privacy-preserving consensus algorithms. One approach is to use differential privacy techniques to add noise to the agents' private inputs before transmitting them to neighbors. This can help protect the privacy of individual agents at the expense of the exact convergence [5]−[9]. Another approach is to use secure multi-party computation (MPC) techniques to enable agents to collaboratively compute the consensus without revealing their private information to others. This can be done using cryptographic protocols such as homomorphic encryption or secret sharing [10], [11]. Such an approach often come with additional-and-overloaded computational cost and complexity.

Based on the above discussion, this letter proposes a privacy-preserving average consensus algorithm for directed graphs that preserve the initial value of each agent without incurring a lot of computation overhead. Motivated by [12], we adopt the round-robin scheduling protocol and establish a novel push-sum algorithm for privacy protection based on the state decomposition. To be specific, the state of each agent is divided into two components: the one is only kept by itself, and the other one is transmitted to one of its neighboring agent under the scheduling of round-robin protocol. Compared to [13], [14], the adoption of round-robin protocol makes less information transmitted over the network at each instant, which not only reduce communication burden but also makes it difficult for attackers to obtain enough valuable information to estimate initial values of each node, thereby exhibiting high potential for privacy protection. Moreover, while the introduction of round-robin protocol inevitably destroys the connectivity of communication network, we prove that our algorithm is able to guarantee the exact average consensus and maintain all agents' privacy.

Corresponding author: Wenying Xu.

Citation: Y. Guo, W. Xu, H. Wang, J. Lu, and S. Du, "Privacy-preserving average consensus algorithm under round-robin scheduling protocol," *IEEE/CAA J. Autom. Sinica*, vol. 11, no. 7, pp. 1705–1707, Jul. 2024.

Y. Guo, W. Xu, and H. Wang are the School of Mathematics, Southeast University, Nanjing 21189, China (e-mail: 213200411@seu.edu.cn; wyxu@seu.edu.cn; wanghd039@avic.com).

J. Lu is the School of Mathematics, Southeast University, Nanjing 21189, and also with the School of Electronic Information and Electrical Engineering, Chengdu University, Chengdu 610106, China (e-mail: jqlu ma@seu.edu.cn).

S. Du is with the School of Artificial Intelligence and Automation, Beijing University of Technology, Beijing 100124, and also with the Engineering Research Center of Intelligent Perception and Autonomous Control, Ministry of Education, Beijing 100124, China (e-mail: shenglidu@bjut.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.123921

Problem statement: Consider a directed graph structure $G := \{\mathcal{V}, \mathcal{E}\}$ with the node set $\mathcal{V} := \{v_1, v_2, ..., v_N\}$ and the edge set $\mathcal{E} \in \mathcal{V} \times \mathcal{V}$. $(v_j, v_i) \in \mathcal{E}$ means that a directed edge exists from v_i to v_j. Let $\mathcal{N}_j^- = \{v_i \in \mathcal{V} | (v_j, v_i) \in \mathcal{E}\}$ and $\mathcal{N}_j^+ = \{v_l \in \mathcal{V} | (v_l, v_j) \in \mathcal{E}\}$ include in-neighbors and out-neighbors of node v_i, and D_j^- and D_j^+ mean its in-degree and out-degree.

Assumption 1: Suppose that G is directed and strongly connected.

Consider a multi-agent system comprising of N agents and the initial value of each agent v_j is I_j. The ultimate goal of each agent v_j is to guarantee the average consensus through a directed communication graph, that is, $\frac{\sum_{j=1}^N I_j}{N}$.

Consider a matrix P with dimensions $N \times N$, denoted as $[p_{ji}]_{N\times N}$, where p_{ji} is positive if node v_i is an in-neighbor of node v_j, or if $v_i = v_j$. In all other cases, p_{ji} equals to zero. The weights p_{ji} also have to satisfy $\sum_{j=1}^N p_{ji} = 1$. Obviously, P is column stochastic. According to Perron-Frobenius Theorem [15], the equation shown below holding true:

$$\lim_{\nu\to\infty} P^\nu = \pi 1^T \tag{1}$$

where π is a vector with positive elements such that $1^T\pi = 1$. Also, the product of the matrix P and the vector π is equal to π, i.e., $P\pi = \pi$. Note that 1^T denotes the transpose of a row vector of ones.

We consider the push-sum algorithm, which is given below:

$$\begin{aligned} u_j[\nu+1] &= p_{jj}[\nu]u_j[\nu] + \sum_{v_i\in\mathcal{N}_j^-} p_{ji}[\nu]u_j[\nu] \\ w_j[\nu+1] &= p_{jj}[\nu]w_j[\nu] + \sum_{v_i\in\mathcal{N}_j^-} p_{ji}[\nu]w_j[\nu] \\ r_j[\nu+1] &= \frac{u_j[\nu+1]}{w_j[\nu+1]},\ \ \nu = 1,2,\dots \end{aligned} \tag{2}$$

At each ν, two operations need to be performed by each node v_j: the calculation of the ratio $r_j[\nu]$ and the transmission of relevant information to its neighbors. Here, $u_j[0] = I_j$ and $w_j[0] = 1$ for $j = 1,2,\dots$ For convenience, the iterations of Algorithm (2) can be expressed more concisely as follows:

$$u[\nu+1] = P[\nu]u[\nu],\ \ w[\nu+1] = P[\nu]w[\nu] \tag{3}$$

where $u[\nu] = [u_1[\nu], u_2[\nu], \dots, u_N[\nu]]^T$ and $w[\nu] = [w_1[\nu], w_2[\nu], \dots, w_N[\nu]]^T$. It follows from (3) for each agent $v_j \in \mathcal{V}$ that:

$$\lim_{\nu\to\infty} r_j[\nu] = \frac{\sum_{j=1}^N u_j[0]}{\sum_{j=1}^N w_j[0]} = \frac{\sum_{j=1}^N I_j}{N}. \tag{4}$$

Equation (4) implies that $r_j[\nu]$ approaches $\frac{\sum_{j=1}^N I_j}{N}$ as $\nu \to \infty$.

Attack model: Two typical attackers, an honest-but-curious adversary and an eavesdropper, are considered in this letter. The honest-but-curious adversary is quite interested in information of other nodes, and is assumed to have access to the exact information of its neighbors and attempts to collect them. The eavesdropper does not belong to the network but has a good understanding of the network topology and can observe messages transmitted over the network.

In this letter, we aim to developing a privacy-preserving algorithm for average consensus through a directed graph to protect node privacy from attackers on the basis of ensuring average consensus.

Main results: In this letter, we propose a privacy-preserving algorithm based on state decomposition under the round-robin protocol, where a directed network (not necessarily balanced) is considered.

Round-robin scheduling protocol: To avoid the privacy leakage and reduce the burden of network communication, we use round-robin protocol to schedule the network communication, under which each agent sends information to only one of its out-neighbor. Here, we take any node v_k in the graph as an example to explain the transmission rules under the round-robin protocol:

1) All out-neighbors of v_k can be represented as $\mathcal{N}_k^+ = \{v_{k_1}, v_{k_2}, \dots,$

$v_{k_m}\}$, where m equals to D_k^+, which is the total number of v_k's neighbors.

2) We arrange all nodes in $\mathcal{N}_k^+$ in an arbitrary but fixed order, in other words, make these nodes form a non-repetitive ordered sequence. We label this sequence as $T_k := \{v_{k_1'}, v_{k_2'}, \ldots, v_{k_m'}\}$ and for any $k_i', i \in \{1,2,\ldots,m\}$, there is always $n \in \{1,2,\ldots,m\}$ satisfying $v_{k_i'} = v_{k_n}$. In fact, T_k is a permutation of $\{v_{k_1}, v_{k_2}, \ldots, v_{k_m}\}$. We can regard T_k as the transmission sequence under round-robin protocol.

3) v_k selects the same node every D_k^+ times under the sequence T_k, continuing to cycle in this order.

Specifically, at each ν, node v_k follows the following weight rules.

1) The self-weight of v_k is set to $p_{kk}[\nu] > 0$.

2) If its out-neighbor v_l is chosen, and the weight of that connecting edge is set to $p_{lk}[\nu] > 0$, while all other out-going links' weights are set to zero, i.e., $p_{ik} = 0$ for $i \neq l,k$.

It can be seen from the above definition that the period of the round-robin protocol can be defined as the least common multiple of $D_k^+, k = 1,2,\ldots,N$, denoted as $lcm(D_1^+, D_2^+, \ldots, D_N^+)$. During each period of the round-robin protocol, every node transmits information to each of its neighbor at least once, ensuring that all out-neighbors of any v_k are able to receive information. Meanwhile, we denote the communication graph of step ν as $\mathcal{G}_\tau[\nu]$. It is worth noting that $\mathcal{G}_\tau[\nu]$ is a subgraph of G, which reflects the communication of nodes at step ν.

Privacy-preserving algorithm under round-robin scheduling protocol: Let each node decompose its variables u_k and w_k respectively into two sub-states u_k^p, u_k^c and w_k^p, w_k^c with the initial values $u_k^p[0]$, $u_k^c[0]$ and $w_k^p[0]$, $w_k^c[0]$, which are arbitrary real numbers that satisfies $u_k^p[0] + u_k^c[0] = 2u_k[0]$ and $w_k^p[0] + w_k^c[0] = 2w_k[0]$, where $u_k[0] = I_k$, $w_k[0] = 1$ for $k = 0,1,2,\ldots,N$.

By adopting state decomposition and round-robin protocol, a new privacy-preserving algorithm is developed as follows:

$$\begin{aligned}
u_k^p[\nu+1] &= \sum_{v_i \in \mathcal{N}_k^-} p_{ki}[\nu] u_i^c[\nu] + p_{kk}^p[\nu] u_k^p[\nu] \\
u_k^c[\nu+1] &= p_{kk}[\nu] u_k^c[\nu] + p_{kk}^c[\nu] u_k^p[\nu] \\
w_k^p[\nu+1] &= \sum_{v_i \in \mathcal{N}_k^-} p_{ki}[\nu] w_i^c[\nu] + p_{kk}^p[\nu] w_k^p[\nu] \\
w_k^c[\nu+1] &= p_{kk}[\nu] w_k^c[\nu] + p_{kk}^c[\nu] w_k^p[\nu] \\
r_k^p[\nu+1] &= \frac{u_k^p[\nu+1]}{w_k^p[\nu+1]},\ r_k^c[\nu+1] = \frac{u_k^c[\nu+1]}{w_k^c[\nu+1]}
\end{aligned} \tag{5}$$

where $\nu = 0,1,2,\ldots$ The weights need the following requirements: 1) For the initial values $p_{kk}^p[0] > 0$ and $p_{kk}^c[0] > 0$ are randomly selected and satisfy $p_{kk}^p[0] + p_{kk}^c[0] = 1$. Under the round-robin protocol, suppose that v_l is the first node chosen by v_k (where $v_l \in \mathcal{N}_k^-$), and then the weights $p_{kk}[0]$ and $p_{lk}[0]$ can be any real positive numbers which satisfies $p_{kk}[0] + p_{lk}[0] = 1$. The weights $p_{ik}[0]$ $(i \neq l,k)$ are set to 0. 2) For $\nu \geq 1$, Let $p_{kk}^p[\nu] = C_{kk}^p$ and $p_{kk}^c[\nu] = C_{kk}^c$, where C_{kk}^p and C_{kk}^c are positive constants and satisfy $C_{kk}^p + C_{kk}^c = 1$. In addition, under the round-robin protocol, provided that $v_l \in \mathcal{N}_k^-$ and v_l is the node selected by v_k at instant ν, let $p_{kk}[\nu] = C_{kk}$ and $p_{lk}[\nu] = C_{lk}$, where C_{kk} and C_{lk} are positive constants and satisfy $C_{kk} + C_{lk} = 1$. Otherwise, $p_{l'k}[\nu] = 0$ when $l' \neq l,k$. Obviously, $\sum_{i=1}^N C_{ik} = 1$.

Under the algorithm (5), each node $v_k \in \mathcal{V}$ transmits its sub-states u_k^c, w_k^c to only one of its out-neighbor v_l which is determined by the round-robin protocol. Let $\boldsymbol{u} = [\boldsymbol{u_1}^T, \ldots, \boldsymbol{u_N}^T]^T \in \mathbb{R}^{2N}$ and $\boldsymbol{w} = [\boldsymbol{w_1}^T, \ldots, \boldsymbol{w_N}^T]^T \in \mathbb{R}^{2N}$, where $\boldsymbol{u_k} = [u_k^p, u_k^c]$ and $\boldsymbol{w_k} = [w_k^p, w_k^c]$. Hence, the iterations (5) are written in matrix-vector form

$$\boldsymbol{u}[\nu+1] = P[\nu]\boldsymbol{u}[\nu], \boldsymbol{w}[\nu+1] = P[\nu]\boldsymbol{w}[\nu] \tag{6}$$

where the weight matrices $P[\nu] = [\boldsymbol{p}_{ki}[\nu]]_{N\times N} \in \mathbb{R}^{2N\times 2N}$ with

$$\boldsymbol{p}_{kk}[\nu] = \begin{bmatrix} p_{kk}^p[\nu] & 0 \\ p_{kk}^c[\nu] & p_{kk}[\nu] \end{bmatrix},\ \boldsymbol{p}_{ik}[\nu] = \begin{bmatrix} 0 & p_{ik}[\nu] \\ 0 & 0 \end{bmatrix} (i \neq k). \tag{7}$$

Average consensus analysis: For the convenience of theorem proof and algorithm analysis, we first present the following lemmas.

Lemma 1: Consider the communication graph $\mathcal{G}_\tau[\nu]$ under the round-robin protocol, and the corresponding matrix $P[\nu]$ with positive diagonal elements and column stochastic property. Let $\mathcal{M}$ be a finite positive real number such that the following set:

$$\begin{aligned}
&\mathcal{G}_\tau[\sigma\mathcal{M}+\mathcal{M}-1] \cup \cdots \cup \mathcal{G}_\tau[\sigma\mathcal{M}+1] \cup \mathcal{G}_\tau[\sigma\mathcal{M}] \\
&\quad := (\mathcal{V}, \mathcal{E}[\sigma\mathcal{M}+\mathcal{M}-1] \cup \cdots \cup \mathcal{E}[\sigma\mathcal{M}+1] \cup \mathcal{E}[\sigma\mathcal{M}])
\end{aligned}$$

$(\sigma = 0,1,2,\ldots)$ is strongly connected. Then, $P[\sigma\mathcal{M}+\mathcal{M}-1]\ldots P[\sigma\mathcal{M}+1]P[\sigma\mathcal{M}]$, $\sigma = 0,1,2,\ldots$, can be a primitive column stochastic matrix.

Proof: Since $\mathcal{G}_\tau[\sigma\mathcal{M}+\mathcal{M}-1] \cup \cdots \cup \mathcal{G}_\tau[\sigma\mathcal{M}+1] \cup \mathcal{G}_\tau[\sigma\mathcal{M}]$ is strongly connected, we can easily prove that $P[\sigma\mathcal{M}+\mathcal{M}-1]\cdots P[\sigma\times\mathcal{M}+1]P[\sigma\mathcal{M}]$ corresponds to a strongly connected graph with stronger connectivity. By the definition of irreducible matrix and $P[\nu]$, $P[\sigma\mathcal{M}+\mathcal{M}-1]\cdots P[\sigma\mathcal{M}+1]P[\sigma\mathcal{M}]$ is irreducible and nonnegative with all its main diagonal entries are positive. Hence, $P[\sigma\mathcal{M}+\mathcal{M}-1]\cdots P[\sigma\mathcal{M}+1]P[\sigma\mathcal{M}]$ is primitive [15]. The column stochastic property of the matrix can be guaranteed because the multiplication of column stochastic matrices is still column stochastic. ■

Lemma 2 [10]: Suppose that Assumption 1 holds, and the weight matrices $P[\nu]$ in (6) $(\nu = 0,1,2,\ldots)$ satisfy.

1) All the elements of $P[\nu]$ are nonnegative integers; especially, $p_{ki}[\nu] = 0$ if $v_i \in \mathcal{N}_k^- \cup \{v_k\}$, while $p_{ki}[\nu] \geq 0$ in other cases.

2) The sum of each column element of $P[\nu]$ equals to 1.

3) The matrix $P[\sigma\mathcal{M}+\mathcal{M}-1]\cdots P[\sigma\mathcal{M}+1]P[\sigma\mathcal{M}]$, $(\sigma = 0,1,2,\ldots,)$ forms a primitive column stochastic matrix.

Then, $\lim_{\nu\to\infty} r_k[\nu] = \frac{\sum_{k=1}^N I_k}{N}$.

Theorem 1: Consider a multi-agent system comprising of N nodes, and suppose that Assumption 1 holds. Under the algorithm (5), the estimated value $r_k^p[\nu]$ and $r_k^c[\nu]$ of node v_k converge to $\frac{\sum_{k=1}^N I_k}{N}$, i.e., $\lim_{\nu\to\infty} r_k^p[\nu] = r_k^c[\nu] = \frac{\sum_{k=1}^N I_k}{N}$, consistent with the average of the initial state values of all nodes.

Proof: To prove the average consensus of algorithm (5), we only have to prove the weight matrix satisfies (1)−(3) in Lemma 2. According to the weight rules, (1) and (2) are obviously satisfied since the column sums of each $P[\nu]$ equals to 1. Then, we just need to prove (3) can be satisfied as well. Let $\mathcal{M} = lcm(D_1^+, D_2^+, ..., D_N^+)$ and we will get the same matrix every $\mathcal{M}$ times. Then, $\mathcal{G}_\tau[\sigma\mathcal{M}+\mathcal{M}-1] \cup \cdots \cup \mathcal{G}_\tau[\sigma\mathcal{M}+1] \cup \mathcal{G}_\tau[\sigma\mathcal{M}]$ is strongly connected, which indicates the corresponding matrix $P[\sigma\mathcal{M}+\mathcal{M}-1]\cdots P[\sigma\mathcal{M}+1]P[\sigma\mathcal{M}]$ is a primitive and column stochastic matrix according to Lemma 1. By Lemma 2, $r_k^p[\nu]$ and $r_k^c[\nu]$ converge to $\frac{\sum_{k=1}^N I_k}{N}$. ■

Privacy-preserving analysis:

Theorem 2: Consider a multi-agent system comprising of N nodes, and suppose that Assumption 1 holds. The proposed privacy-preserving algorithm (5) under the round-robin protocol is able to preserve the privacy of node v_k.

Proof: To prove that node v_j cannot predict I_k of node v_k through only collecting its information, given that v_j is an out-neighbor of v_k. Let $O_j^r(\nu)$ and $O_j^t(\nu)$ mean the information received and transmitted, respectively, by node j at instant ν. $O_j^s(\nu)$ denotes the state of node j at instant ν. The specific forms are given as follows:

$$\begin{aligned}
O_j^r(\nu) &:= \{p_{jl}u_l^c[\nu], p_{jl}w_l^c[\nu] : l \in \mathcal{N}_j^-\} \\
O_j^t(\nu) &:= \{p_{lj}u_j^c[\nu], p_{lj}w_j^c[\nu] : l \in \mathcal{N}_j^+\} \\
O_j^s(\nu) &:= \{p_{jj}^p[\nu], p_{jj}^c[\nu], p_{jj}[\nu], u_j^p[\nu], u_j^c[\nu], w_j^p[\nu], w_j^c[\nu]\}.
\end{aligned} \tag{8}$$

Let O_j denote all information that node j has access to, which is defined as

$$O_j := \bigcup_{\nu=0}^{\infty} \{O_j^r(\nu) \bigcup O_j^t(\nu) \bigcup O_j^s(\nu)\}. \tag{9}$$

Next, we prove that the initial value of node j cannot be accurately estimated by illustrating that there are initial values $\widehat{I}_k \neq I_k$ such that $\widehat{O}_j = O_j$.

Suppose $v_\eta \in \mathcal{N}_k^+ \cup \mathcal{N}_k^-, (\eta \neq j)$. The initial values are set to be

$$\begin{aligned}
&\widehat{I}_\eta = I_\eta - \xi, \widehat{I}_k = I_k + \xi \\
&\widehat{I}_l = I_l, v_l \in \mathcal{V} \setminus \{v_k, v_\eta\} \\
&\widehat{u}_l^p[0] = u_l^p, v_l \in \mathcal{V} \\
&\widehat{u}_l^c[0] = 2\widehat{I}_k - \widehat{u}_l^p[0] \\
&\widehat{u}_\eta^c[0] = 2\widehat{I}_\eta - \widehat{u}_\eta^p[0]
\end{aligned} \tag{10}$$

where ξ is not equal to zero and also not equal to $u_k^p[0] - 2I_k$ and $2I_\eta - u_\eta^p[0]$. We just need to change the initial coupling weights and keep other weights constant at each step $\nu (\nu = 1, 2, \ldots)$.

When $\eta \in \mathcal{N}_k^+$, it is easy to have $\widehat{O}_j = O_j$ with the newly-defined weights below:

$$\begin{aligned}
&\widehat{p}_{lk}[0] = p_{lk}[0]u_k^c[0]/\widehat{u}_k^c[0], \ v_l \in \mathcal{V} \setminus \{v_k\} \\
&\widehat{p}_{lq}[0] = p_{lq}[0], \ v_l, v_q \in \mathcal{V}, \ q \neq k, \eta \\
&\widehat{p}_{l\eta}[0] = p_{l\eta}[0]u_\eta^c[0]/\widehat{u}_\eta^c[0], \ v_l \in \mathcal{V} \setminus \{v_k\} \\
&\widehat{p}_{kk}[0] = (p_{kk}[0]u_k^c[0] + 2\xi)/\widehat{u}_k^c[0] \\
&\widehat{p}_{k\eta}[0] = (p_{k\eta}[0]u_\eta^c[0] - 2\xi)/\widehat{u}_\eta^c[0].
\end{aligned} \tag{11}$$

When $\eta \in \mathcal{N}_k^-$, similarly, we obtain $\widehat{O}_j = O_j$ with the newly-defined weights below:

$$\begin{aligned}
&\widehat{p}_{lk}[0] = p_{lk}[0]u_k^c[0]/\widehat{u}_k^c[0], \ v_l \in \mathcal{V} \setminus \{v_\eta\} \\
&\widehat{p}_{lq}[0] = p_{lq}[0], \ v_l, v_q \in \mathcal{V}, \ q \neq j, \eta \\
&\widehat{p}_{l\eta}[0] = p_{l\eta}[0]u_\eta^c[0]/\widehat{u}_\eta^c[0], \ v_l \in \mathcal{V} \setminus \{v_k\} \\
&\widehat{p}_{\eta k}[0] = (p_{\eta k}[0]u_k^c[0] + 2\xi)/\widehat{u}_k^c[0] \\
&\widehat{p}_{\eta\eta}[0] = (p_{\eta\eta}[0]u_\eta^c[0] - 2\xi)/\widehat{u}_\eta^c[0].
\end{aligned} \tag{12}$$

■

Numerical example: Consider a five-agent network that exchange information via a strongly connected graph (see Fig. 1(a)). Let the initial value of each node k be $I_k = k$ and then the average value is 3. By the upper part of Fig. 1(b), the exact average consensus is guaranteed by our proposed privacy-preserving algorithm (5). Node 1 arbitrarily selects the weight $p_{21}[0]$, which is not accessible to other nodes. If node 2 is an attacker who is honest-but-curious, it can receive information $\{p_{21}[\nu]u_1^c[\nu], p_{21}[\nu]u_1^c[\nu]\}$ from node 1 at instant ν. To evaluate initial value of $u_1[0]$ using the algorithm (5), node 2 firstly has to predict the weights which are unknown to it. It is noteworthy that the weights are arbitrarily selected, node 2 is impossible to predict $u_1[0]$ correctly and exactly. The estimate $u_1[0]$ of node 2 over 20 times is shown in the lower part of Fig. 1(b).

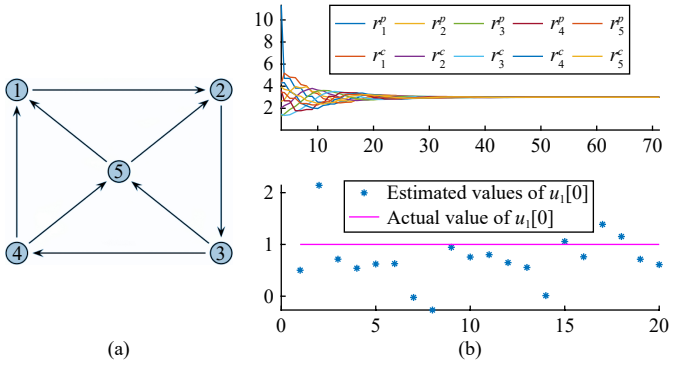

Fig. 1. The Simulation of convergence and privacy on a directed graph with five nodes. (a) Five nodes are connected by a strongly connected graph; and (b) The trajectory of r_i^p and r_i^c under the algorithm (5) and the actual value of $u_1[0]$ and its estimate generated by the agent 2.

Conclusion: This letter has proposed a privacy-preserving average consensus algorithm for multi-agent systems through directed graphs under round-robin protocol and state decomposition. It has been proved that the proposed algorithm guarantees the average consensus while preserving the privacy of every agent. A numerical example has been presented finally to show the efficiency of the proposed algorithm. Future research directions would include the extension of the privacy-preserving methods to more general systems (such as linear/nonlinear systems [4], [16]−[18]) and collaborative tasks (such as formation and leader-following consensus [19], [20]).

Acknowledgments: This work was supported in part by the National Natural Science Foundation of China (62173087), the Fundamental Research Funds for the Central Universities, and the Alexander von Humboldt Foundation of Germany.

References

[1] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 988–1001, 2003.

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

[3] Q. Xu, C. Yu, X. Yuan, Z. Fu, and H. Liu, "A privacy-preserving distributed subgradient algorithm for the economic dispatch problem in smart grid," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 7, pp. 1625–1627, 2023.

[4] W. Xu, W. He, D. W. C. Ho, and J. Kurths, "Fully distributed observer-based consensus protocol: Adaptive dynamic event-triggered schemes," *Automatica*, vol. 139, p. 110188, 2022.

[5] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — The new and improved power grid: A survey," *IEEE Communi. Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[6] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus with optimal noise selection," *IFAC PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[7] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed Nash equilibrium seeking for aggregative games," *IEEE Trans. Automa. Control*, vol. 67, no. 5, pp. 2451–2458, 2022.

[8] A. Wang, X. Liao, and H. He, "Event-triggered differentially private average consensus for multi-agent network," *IEEE/CAA J. Autom. Sinica*, vol. 6, no. 1, pp. 75–83, 2019.

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

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

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

[12] L. Zou, Z. Wang, Q.-L. Han, and D. Zhou, "Moving horizon estimation for networked time-delay systems under round-robin protocol," *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 5191–5198, 2019.

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

[14] H. Wang, W. Xu, and J. Lu, "Privacy-preserving push-sum average consensus algorithm over directed graph via state decomposition," in *Proc. 3rd Int. Conf. Industrial Artificial Intelligence*, Shenyang, China, 2021, pp. 1–6.

[15] Horn, A. Roger, and C. R. Johnson, *Matrix Analysis*. Cambridge, UK: Cambridge University Press, 2013.

[16] X. Li, D. Ho, and J. Cao, "Event-triggered impulsive control for nonlinear delay systems," *Automatica*, vol. 150, pp. 213–221, 2020.

[17] X. Li, D. Ho, and J. Cao, "Finite-time stability and settling-time estimation of nonlinear impulsive systems," *Automatica*, vol. 99, pp. 361–368, 2019.

[18] Q. Zhang and Y. Zhou, "Recent advances in non-gaussian stochastic systems control theory and its applications," *Int. J. Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 111–119, 2022.

[19] Y. Su, H. Cai, and J. Huang, "The cooperative output regulation by the distributed observer approach," *Int. J. Network Dynamics and Intelligence*, vol. 1, no. 1, pp. 20–35, 2022.

[20] W. Xu, D. Ho, J. Zhong, and B. Chen, "Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Networks and Learning Systems*, vol. 30, no. 10, pp. 3137–3149, 2019.