Algorithm-Level Confidentiality for Average Consensus on Time-Varying Directed Graphs

Huan Gao, Member, IEEE, and Yongqiang Wang, Senior Member, IEEE

Abstract—Average consensus plays a key role in distributed networks, with applications ranging from time synchronization, information fusion, load balancing, to decentralized control. Existing average consensus algorithms require individual agents to exchange explicit state values with their neighbors, which leads to the undesirable disclosure of sensitive information in the state. In this paper, we propose a novel average consensus algorithm for time-varying directed graphs that can protect the confidentiality of a participating agent against other participating agents. The algorithm injects randomness in interaction to obfuscate information on the algorithm-level and can ensure information-theoretic privacy without the assistance of any trusted third party or data aggregator. By leveraging the inherent robustness of consensus dynamics against random variations in interaction, our proposed algorithm can also guarantee the accuracy of average consensus. The algorithm is distinctly different from differential-privacy based average consensus approaches which enable confidentiality through compromising accuracy in obtained consensus value. Numerical simulations confirm the effectiveness and efficiency of our proposed approach.

Index Terms—Average consensus, confidentiality, time-varying directed graphs.

I. INTRODUCTION

Averaging consensus is an important tool in distributed computing. For a network of $N$ agents interacting on a graph, average consensus can enable the states of all agents to converge to the average of their initial values through local interactions between neighboring agents.

Recently, average consensus is finding increased applications in load balancing [2], [3], network synchronization [4], distributed information fusion [5], [6], and decentralized control [7], [8]. To ensure all agents converge to the average value of their initial values, conventional average consensus approaches require individual agents to exchange explicit state values with their neighbors. This results in the disclosure of sensitive state information, which is sometimes undesirable in terms of confidentiality. In fact, in many applications such as the smart grid, health-care or banking networks, confidentiality is crucial for promoting participation in collaboration since individual agents tend not to trade confidentiality for performance [9]–[11]. For instance, a group of people using average consensus to reach a common opinion may want to keep their individual opinions secret [12]. Another typical example is power systems in which multiple generators have to reach agreement on cost while maintaining their individual generation information confidential [13].

To achieve confidentiality in average consensus, recently results have started to emerge. A commonly used confidentiality mechanism is differential privacy from the database literature [14]–[20] (and its variants [21], [22]) which injects independent (and hence uncorrelated) noises directly to agents’ states in order to achieve confidentiality in average consensus. However, the use of independent noises on the states in these approaches prevents converging to the exact average value [23]. To improve consensus accuracy, which is crucial in cyber-physical systems and sensor networks, [24]–[31] inject carefully calculated correlated additive noises to agents’ states, instead of independent (and hence uncorrelated) noises used in differential-privacy based approaches. (A similar approach was proposed in [32] to achieve maximum consensus.) However, these prior works only consider average consensus under balanced and static network topologies. Different from injecting noises to agents’ states in the aforementioned approaches, [33] employed carefully designed mask maps to protect the actual states. Observability based approaches have also been reported to protect the confidentiality of multi-agent consensus [34]–[50]. Its idea is to design the topology of interactions such that the observability from a compromised agent is minimized, which amounts to minimizing the ability of the compromised agent to infer the initial states of other agents. Recently, encryption based approaches have been proposed to protect the confidentiality by encrypting exchanged messages with the assistance of additive homomorphic encryption [37]–[40], with the price of increasing computation and communication overhead. Another confidentiality approach was proposed in [41] where each agent’s confidentiality is protected by decomposing its state into two sub-states. However, [41] relies on undirected interactions and is inapplicable to time-varying directed graphs considered in this paper.

This paper has been accepted to IEEE Transactions on Network Science and Engineering as a regular paper. Please cite this paper as: Huan Gao and Yongqiang Wang, “Algorithm-Level Confidentiality for Average Consensus on Time-Varying Directed Graphs,” in IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2022.3140274.

Part of the results was presented at 2018 IEEE Conference on Communications and Network Security (CNS) [1]. The work was supported in part by the National Science Foundation under Grants ECCS-1912702 and CCF-2106293.

Huan Gao was with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA. He is now with the School of Automation, Northwestern Polytechnical University, Xi’an 710129, China (email: huangao@nwpu.edu.cn). The work was done when Huan Gao was with Clemson University.

Yongqiang Wang is with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA (email: yongqiw@clemson.edu).
update rule such that the randomness added in the first several iterations does not affect the final convergence result. Different from approaches injecting correlated additive noises directly to agents’ states, our approach adds independent (and hence uncorrelated in time) randomness directly to the average consensus dynamics, which makes it applicable to time-varying directed graphs. Compared with our prior work in [40] which employs homomorphic encryption to preserve confidentiality and [41] which protects each agent’s confidentiality by decomposing its state into two sub-states, this paper proposes a different approach that enables confidentiality by judiciously adding randomness in interaction dynamics. More importantly, both [40] and [41] rely on undirected interactions and hence are inapplicable to time-varying directed graphs considered in this paper. Some of the results here were presented at the 2018 IEEE Conference on Communications and Network Security (CNS) [1]. Compared with the conference version, the journal version has the following significant differences: 1) the journal version extends the results for constant directed graphs in [1] to time-varying directed graphs; 2) the journal version provides formal and rigorous analysis of convergence rate that does not exist in the conference version; 3) the journal version allows multiple adversaries to collude to infer the sensitive value a target agent, which is not addressed in our conference version; and 4) the journal version revises and enhances the proposed confidential average consensus algorithm to guarantee information-theoretic privacy, which is stronger than the confidentiality achieved in the conference version.

II. PRELIMINARIES AND PROBLEM FORMULATION

A. Graph Representation

We represent a network of $N$ agents as a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, \mathcal{E}(k))\}$ where $\mathcal{V} = \{1, 2, \ldots, N\}$ is the set of agents and $k = 0, 1, \ldots$ is the time index. $\mathcal{E}(k) \subset \mathcal{V} \times \mathcal{V}$ is the edge set at time $k$, whose elements are such that $(i, j) \in \mathcal{E}(k)$ holds if and only if there exists a directed edge from agent $j$ to agent $i$ at time $k$, i.e., agent $j$ can send messages to agent $i$ at time $k$. For notational convenience, we assume that there are no self edges, i.e., $(i, i) \notin \mathcal{E}(k)$ for all $k$ and $i \in \mathcal{V}$. At time $k$, each edge $(i, j) \in \mathcal{E}(k)$ has an associated weight, $w_{ij}(k) > 0$. The out-neighbor set of agent $i$ at time $k$, which represents the set of agents that can receive messages from agent $i$ at time $k$, is denoted as $N^{\text{out}}_i(k) = \{j \in \mathcal{V} : (j, i) \in \mathcal{E}(k)\}$. Similarly, at time $k$, the in-neighbor set of agent $i$, which represents the set of agents that can send messages to agent $i$ at time $k$, is denoted as $N^{\text{in}}_i(k) = \{j \in \mathcal{V} : (i, j) \in \mathcal{E}(k)\}$. From the above definitions, it can be obtained that $i \in N^{\text{out}}_j(k)$ and $j \in N^{\text{in}}_i(k)$ are equivalent. Agent $i$’s out-degree at time instant $k$ is represented by $D^{\text{out}}_i(k) = |N^{\text{out}}_i(k)|$ and its indegree is represented by $D^{\text{in}}_i(k) = |N^{\text{in}}_i(k)|$, where $|S|$ is the cardinality of the set $S$.

For graph $G(k) = (\mathcal{V}, \mathcal{E}(k))$ is defined as

$$c_{ij}(k) = \begin{cases} 
1 & \text{if the } l\text{-th edge in } \mathcal{E}(k) \text{ is } (i, j) \\
-1 & \text{if the } l\text{-th edge in } \mathcal{E}(k) \text{ is } (j, i) \\
0 & \text{otherwise}
\end{cases}$$

where $E(k) = |\mathcal{E}(k)|$ represents the number of edges in $\mathcal{E}(k)$. Note that the $l$-th column of $C(k)$ is corresponding to the $l$-th edge in $\mathcal{E}(k)$, and the sum of each column of $C(k)$ is 0, i.e., $1^T C(k) = 0^T$.

For a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, \mathcal{E}(k))\}$, we define $E_\infty$ as the set of directed edges $(i, j)$ that exist for infinitely many time instants, i.e.,

$$E_\infty = \{(i, j) | (i, j) \in \mathcal{E}(k) \text{ for infinitely many indices } k\}$$

We focus on time-varying directed graphs which satisfy the following assumptions:

Assumption 1: For a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, \mathcal{E}(k))\}$, for any $i, j \in \mathcal{V}$ with $i \neq j$, there exists at least one directed path from $i$ to $j$ in $(\mathcal{V}, E_\infty)$, i.e., $(\mathcal{V}, E_\infty)$ is strongly connected.

Assumption 2: For a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, \mathcal{E}(k))\}$, there exists an integer $T \geq 1$ such that for every $(i, j) \in E_\infty$, agent $j$ directly communicates with agent $i$ at least once in every $T$ consecutive time instants. $T$ is called intercommunication interval bound.

Assumption 3: We assume that each agent $i$ has access to its out-degree $D^{\text{out}}_i(k)$ at each iteration $k$.

Remark 1: Assumption 3 is widely used in existing literature on time-varying directed graphs such as [42]–[44]. In fact, in many directed graphs, it is feasible for a node to know its out-neighbors. For example, in many safety-critical systems such as industrial control systems, the exchange of data occurs in a directed way due to unidirectional gateways (aka data diode) whereas control messages (a special type of messages used to configure network connections) can be exchanged in a bidirectional manner to establish connections [45].

B. The Conventional Push-Sum

The conventional push-sum considers $N$ agents interacting on a constant directed graph $G = (\mathcal{V}, \mathcal{E})$, with each agent having an initial state $x_i^0$ ($i = 1, 2, \ldots, N$) [46], [47]. Represent the average value of all initial states as $x^0 = \sum_{j=1}^{N} x_j^0 / N$. The conventional push-sum algorithm conducts two iterative computations simultaneously, and allows each agent to obtain the exact average of the initial values $x^0$ in an asymptotic way. This mechanism is summarized in Algorithm 0 below:

Algorithm 0: The conventional push-sum algorithm

1) $N$ agents interact on a constant directed graph $G = (\mathcal{V}, \mathcal{E})$. Each agent $i$ is initialized with $s_i(0) = x_i^0$, $w_i(0) = 1$, and $p_i(0) = s_i(0) / w_i(0)$. The weight $p_{ij}$ associated with the edge $(i, j) \in \mathcal{E}$ satisfies $p_{ij} \in (0, 1)$ if $j \in N^{\text{in}}_i \cup \{i\}$ is true and $p_{ij} = 0$ otherwise. For any given $j = 1, 2, \ldots, N$, $p_{ij}$ satisfies $\sum_{i=1}^{N} p_{ij} = 1$.

2) At iteration step $k$:
a) Agent $i$ calculates $p_{ji}s_j(k)$ and $p_{ji}w_j(k)$, and sends both values to all of its out-neighbors $j \in \mathcal{N}_{i}^{\text{out}}$.
b) After receiving the values of $p_{ji}s_j(k)$ and $p_{ji}w_j(k)$ from all its in-neighbors $j \in \mathcal{N}_{i}^{\text{in}}$, agent $i$ updates $s_i$ and $w_i$ as follows:

\[
\begin{align*}
    s_i(k+1) &= \sum_{j \in \mathcal{N}_{i}^{\text{in}} \cup \{i\}} p_{ji}s_j(k) \\
    w_i(k+1) &= \sum_{j \in \mathcal{N}_{i}^{\text{in}} \cup \{i\}} p_{ji}w_j(k)
\end{align*}
\]  

(c) Agent $i$ uses the ratio $\pi_i(k+1) = s_i(k+1)/w_i(k+1)$ to estimate the average value $\bar{x}^0 = \sum_{j=1}^{N} x_j^0/N$.

For the sake of notational simplicity, we rewrite (3) in the following more compact form:

\[
\begin{align*}
    s(k+1) &= \mathbf{P}s(k) \\
    w(k+1) &= \mathbf{P}w(k)
\end{align*}
\]  

where $s(k) = [s_1(k), s_2(k), \ldots, s_N(k)]^T$ and $w(k) = [w_1(k), w_2(k), \ldots, w_N(k)]^T$, and $\mathbf{P} = [p_{ij}]$. From Algorithm 0, we have $s(0) = [s_1^{(0)}, s_2^{(0)}, \ldots, s_N^{(0)}]^T$ and $w(0) = 1$. We can also obtain that the matrix $\mathbf{P}$ is column-stochastic, i.e., $\sum_{i=1}^{N} p_{ij} = 1$ holds for $j = 1, 2, \ldots, N$.

At iteration step $k$, each agent updates the ratio $\pi_i(k+1) = s_i(k+1)/w_i(k+1)$ to estimate the average value $\bar{x}^0 = \sum_{j=1}^{N} x_j^0/N$. Since $\mathcal{G}$ is assumed to be a strongly connected directed graph, $\mathbf{P}^k$ will converge to a rank-1 matrix exponentially fast [48, 49]. Defining $\mathbf{P}^\infty$ as the limit of $\mathbf{P}^k$ as $k \to \infty$, we can obtain the form of $\mathbf{P}^\infty = \mathbf{v}\mathbf{w}^T$ where $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$. Using the facts $s(k) = \mathbf{P}^k s(0)$ and $w(k) = \mathbf{P}^k w(0)$, we can further have [50]:

\[
\begin{align*}
    \pi_i(\infty) &= \frac{s_i(\infty)}{w_i(\infty)} = \frac{[\mathbf{P}^\infty s(0)]_i}{[\mathbf{P}^\infty w(0)]_i} = \frac{\sum_{j=1}^{N} s_j(0)}{\sum_{j=1}^{N} w_j(0)} = \bar{x}^0
\end{align*}
\]  

where $[\mathbf{P}^\infty s(0)]_i$ and $[\mathbf{P}^\infty w(0)]_i$ represent the $i$-th element of vector $\mathbf{P}^\infty s(0)$ and vector $\mathbf{P}^\infty w(0)$, respectively. Hence, all estimates $\pi_1(k), \pi_2(k), \ldots, \pi_N(k)$ will asymptotically converge to the average $\bar{x}^0 = \sum_{j=1}^{N} x_j^0/N$.

C. Problem Formulation

In this paper, we will address average consensus under time-varying directed graphs while protecting the confidentiality of participating agents against adversaries. To this end, we first present some assumptions and definitions.

**Assumption 4:** We assume that all agents’ initial states $x_i^0$ are bounded. Without loss of generality, the lower bound and upper bound are denoted as $a$ and $b$, respectively. Both $a$ and $b$ are assumed known to all agents.

**Remark 2:** It is worth noting that although the bounds $a$ and $b$ are assumed known to all agents, this does not mean that the minimum and maximum of all agents’ initial states are known to all agents. In fact, $a$ (resp. $b$) can be arbitrarily small (resp. large) compared with the actual minimum (resp. maximum) of agents’ initial states.

**Definition 1:** We define an honest-but-curious adversary as an agent who follows all protocol steps correctly but collects received messages in an attempt to infer the initial value of other participating agents.

**Assumption 5:** We assume that agents can collude, i.e., a set of honest-but-curious agents $\mathcal{A}$ can share information with each other to infer the initial value $x_i^0$ of a target agent $i \notin \mathcal{A}$.

**Definition 2:** We define that confidentiality (privacy) of the initial value $x_i^0$ of agent $i$ is preserved if $x_i^0$ is indistinguishable from the viewpoint of honest-but-curious adversaries $\mathcal{A}$. By “indistinguishable,” we mean that the probability distribution of information set accessible to $\mathcal{A}$ does not change when agent $i$’s initial state $x_i^0$ is altered to any $x_i^0 \neq x_i^0$ under the constraint that the sum of the initial states of all nodes not in $\mathcal{A}$ (i.e., $\sum_{j \in \mathcal{V} \setminus \mathcal{A}} x_j^0$) is unchanged.

Our definition of confidentiality requires perfect indistinguishability of a target agent’s different initial states from the viewpoint of honest-but-curious adversaries $\mathcal{A}$, and, therefore, is more stringent than the confidentiality definition in [31], [32], [51]–[53] which defines confidentiality as the inability of an adversary to uniquely determine the sensitive value.

We next show that the conventional push-sum is not confidential. From (3) and (4), an honest-but-curious agent can receive $p_{ij}s_j(0)$ and $p_{ij}w_j(0)$ from its in-neighbor agent $j$ after the first iteration step $k = 0$. Then agent $i$ is able to uniquely determine $x_j^0$ by $x_j^0 = s_j(0)/w_j(0)$ using the fact $w_j(0) = 1$. Therefore, an honest-but-curious agent can always infer the initial values of all its in-neighbors, and hence the conventional push-sum algorithm cannot provide confidentiality against honest-but-curious adversaries. It is worth noting that using a similar argument, we can also obtain that the conventional push-sum is not confidential even when the weight is allowed to be time-varying (e.g., [47]).

III. THE CONFIDENTIALITY ALGORITHM AND PERFORMANCE ANALYSIS

In this section, we will propose a confidential average consensus algorithm for time-varying directed graphs, and then provide rigorous analysis of its convergence rate and enabled strength of confidentiality.

A. Confidential Average Consensus Algorithm

The analysis above reveals that using the same weight $p_{ij}$ for both $p_{ij}s_j(0)$ and $p_{ij}w_j(0)$ discloses the initial state value. Motivated by this observation and the work in [29], here we introduce a novel confidential average consensus algorithm which injects randomness in the dynamics of interactions in iterations $k = 0, \ldots, K$. Note that here $K$ is a non-negative integer and is known to every agent. Its influence will be discussed in detail in Remark [11] and Remark [12].

**Algorithm 1:** Confidential average consensus algorithm

1) $N$ agents interact on a sequence of time-varying directed graphs $\{\mathcal{G}(k) = (\mathcal{V}, \mathcal{E}(k))\}$. Each agent $i$ is initialized with $s_i(0) = N/(N^2) + \frac{1}{(N-2)(N-2)} \in [1/N^2, N/(N^2-1)]$, $w_i(0) = 1$, and $\pi_i(0) = \frac{b-a}{N} + \frac{N-a}{N^2} \lfloor N \times \text{frac}(N s_i(0)/w_i(0)) - 1 \rfloor + a$ where the function $\text{frac}(x) = x - \lfloor x \rfloor$ denotes the fractional part of
a real number $x$ (here $\lfloor x \rfloor$ represents the largest integer not greater than $x$).

2) At iteration step $k$:
   a) Agent $i$ generates a set of random weights $\{p_{ji}(k) \in (\epsilon, 1) \mid j \in N^\text{out}_i(k) \cup \{i\}\}$ with the sum of this set equal to 1, and sets $\Delta w_{ij}(k) = p_{ji}(k)w_i(k)$ for $j \in N^\text{out}_i(k) \cup \{i\}$.
   b) If $k \leq K$, agent $i$ independently generates uniformly distributed values $\Delta s_{ij}(k) \in [0, 1)$ for its out-neighbors $j \in N^\text{out}_i(k)$, and sets $\Delta s_{ij}(k) = \frac{\text{frac}(s_{ij}(k) - \sum_{j \in N^\text{out}_i(k)} \Delta s_{ij}(k))}{\epsilon}$; otherwise, agent $i$ sets $\Delta s_{ij}(k) = p_{ji}(k)s_i(k)$ for $j \in N^\text{out}_i(k) \cup \{i\}$.
   c) Agent $i$ sends $\Delta s_{ij}(k)$ and $\Delta w_{ij}(k)$ from its in-neighbors $j \in N_i^{\text{in}}(k)$, agent $i$ updates $s_i$ and $w_i$ as

$$s_i(k + 1) = \begin{cases} \frac{\sum_{j \in N_i^{\text{in}}(k) \cup \{i\}} \Delta s_{ij}(k)}{\sum_{j \in N_i^{\text{out}}(k) \cup \{i\}} \Delta s_{ij}(k)} & \text{for } k \leq K \\ \sum_{j \in N_i^{\text{out}}(k) \cup \{i\}} \Delta s_{ij}(k) & \text{for } k \geq K + 1 \end{cases}$$

(6)

and

$$w_i(k + 1) = \sum_{j \in N_i^{\text{out}}(k) \cup \{i\}} \Delta w_{ij}(k) \text{ for } k \geq 0$$

(7)

respectively.
   e) Agent $i$ uses the ratio $\pi_i(k + 1) = \frac{b - a}{x_i - x_i^0} + a$ to estimate the average value $\bar{x}^0 = \sum_{j = 1}^{N} x_j^0/N$.

Remark 3: Compared to the conventional confidentiality-violating push-sum algorithm which broadcasts messages, Algorithm 1 needs agent $i$ to send different random numbers to different out-neighbors in iterations $k \leq K$. This is a price of obtaining confidentiality without losing accuracy in the time-varying directed topology case.

Remark 4: The way of injecting randomness in $\Delta s_{ij}(k)$ is different in iterations $k \leq K$ from $k > K$. In fact, in iterations $k \leq K$, $\Delta s_{ij}(k)$ can be nonzero even when $s_i(k)$ is zero. This is crucial in enabling strong confidentiality as receiving $\Delta s_{ij}(k)$ of a value zero will not allow the recipient to infer information about $s_i(k)$.

Remark 5: In Algorithm 1, the coupling weights are randomly chosen at every iteration. Compared with the commonly used deterministic setting in which the weights are set as $p_{ji}(k) = 1/(D_{out}(k) + 1)$ for all $j \in N^\text{out}(k) \cup \{i\}$, our setting is more general since it includes the commonly used setting as a special case by fixing $p_{ji}(k)$ to deterministic values. Furthermore, the random weights beyond step $K$ in Algorithm 1 can provide additional confidentiality protection for intermediate states $s_i(k)$ after iteration $K$. Given $\Delta s_{ij}(k) = p_{ji}(k)s_i(k)$ for $k \geq K + 1$, we can see that using random weights $p_{ji}(k)$ makes the intermediate state $s_i(k)$ more difficult to infer than using deterministic weights $p_{ji}(k)$.

Setting $\Delta s_{ij}(k), \Delta w_{ij}(k)$, and $p_{ji}(k)$ to 0 for $j \notin N^\text{out}_i(k) \cup \{i\}$, we can rewrite the update rules of $s(k)$ for $k \geq K + 1$ and $w(k)$ for $k \geq 0$ as

$$s_i(k + 1) = \sum_{j = 1}^{N} \Delta s_{ij}(k) = \sum_{j = 1}^{N} p_{ij}(k)s_j(k) \text{ for } k \geq K + 1$$

$$w_i(k + 1) = \sum_{j = 1}^{N} \Delta w_{ij}(k) = \sum_{j = 1}^{N} p_{ij}(k)w_j(k) \text{ for } k \geq 0$$

(8)

Denoting $s(k), w(k)$, and $P(k)$ as $s(k) = [s_1(k) \ldots s_N(k)]^T$, $w(k) = [w_1(k) \ldots w_N(k)]^T$, and $P(k) = [p_{ij}(k)]_{N \times N}$, we can further rewrite (8) into a matrix form

$$s(k + 1) = P(k)s(k) \text{ for } k \geq K + 1$$

$$w(k + 1) = P(k)w(k) \text{ for } k \geq 0$$

(9)

For iteration $k = 0$, we have $s(0) = [x_0^1, x_0^2, \ldots, x_0^N]^T$ and $w(0) = 1$. From Algorithm 1, we know that $P(k)$ in (9) is time-varying and column-stochastic for $k \geq 0$.

Defining the transition matrix as follows

$$\Phi(k : t) = P(k) \cdots P(t)$$

(10)

for all $k$ and $t$ with $k \geq t$, where $\Phi(k : k) = P(k)$, we can rewrite (9) as

$$s(k + 1) = \Phi(k : K + 1)s(K + 1) \text{ for } k \geq K + 1$$

$$w(k + 1) = \Phi(k : 0)w(0) \text{ for } k \geq 0$$

(11)

B. Convergence Analysis

Next we prove that Algorithm 1 can guarantee that the estimates of all agents converge to the exact average value of initial values. We will also analyze the rate of convergence of Algorithm 1. Using the convergence definition in [43] and [54], we define the rate of convergence to be at least $\gamma \in (0, 1)$ if there exists a positive constant value $C$ such that $\|\pi(k) - \bar{x}^0\|_1 \leq C\gamma^k$ is true for all $k$, where $\pi(k) = [\pi_1(k), \ldots, \pi_N(k)]^T$ and $\bar{x}^0 = \sum_{j = 1}^{N} x_j^0/N$ is the average value. Note that this definition means a smaller $\gamma$ corresponding to a faster convergence. To analyze the convergence rate of Algorithm 1, we first introduce Lemma 1 below:

Lemma 1: For a network of $N$ agents represented by a sequence of time-varying directed graphs $\{G(t) = (\mathcal{V}, \mathcal{E}(t))\}$ which satisfy Assumptions 1 and 2 under Algorithm 1, each agent $i$ has $w_i(k) \geq \varepsilon^T(N - 1)$ for $k \geq 1$ where $T$ is defined in Assumption 2.

Proof: For $k \geq 1$, from (11) we have

$$w(k) = \Phi(k - 1 : 0)1$$

(12)

Represent $\delta(k)$ as

$$\delta(k) = \min_{1 \leq i \leq N} w_i(k) = \min_{1 \leq i \leq N} [\Phi(k - 1 : 0)1]_i$$

(13)

for $k \geq 1$. To prove $w_i(k) \geq \varepsilon^T(N - 1)$ for $k \geq 1$, it is sufficient to prove $\delta(k) \geq \varepsilon^T(N - 1)$ for $k \geq 1$. We divide our proof into two parts: $1 \leq k \leq T(N - 1)$ and $k \geq T(N - 1) + 1$. 
Part 1: $\delta(k) \geq \varepsilon^{T(N-1)}$ for $1 \leq k \leq T(N-1)$. One can verify that the following relationship holds

$$
\Phi(k - 1 : 0)_{ii} = [P(k - 1) \cdots P(0)]_{ii} \geq \varepsilon \Phi(k - 2 : 0)_{ii} \geq \varepsilon k \geq \varepsilon^{T(N-1)}
$$

(14)

Given $\Phi(0 : 0)_{ii} = [P(0)]_{ii} \geq \varepsilon$, one can obtain $\Phi(k - 1 : 0)_{ii} \geq \varepsilon k$. Therefore, it follows that

$$
\Phi(k - 1 : k - T(N-1))_{ij} \geq \varepsilon^{T(N-1)}
$$

(16)

for $1 \leq i, j \leq N$. Since $k \geq T(N-1) + 1$ holds and $P(k)$ is a column-stochastic matrix,

$$
\Phi(k - T(N-1) - 1 : 0) = P(k - T(N-1) - 1) \cdots P(0)
$$

(17)

should also be a column-stochastic matrix. Further using the fact $\Phi(k - 1 : 0) = \Phi(k - 1 : k - T(N-1)) \Phi(k - T(N-1) - 1 : 0)$ leads to $\Phi(k - 1 : 0)_{ij} \geq \varepsilon^{T(N-1)}$ for $1 \leq i, j \leq N$. Therefore, we have

$$
\Phi(k - 1 : 0)_{1} \geq N \varepsilon^{T(N-1)} \geq \varepsilon^{T(N-1)}
$$

(18)

for $i = 1, \ldots, N$, meaning $\delta(k) \geq \varepsilon^{T(N-1)}$ for $k \geq T(N-1) + 1$.

Based on $\delta(k) \geq \varepsilon^{T(N-1)}$ for $k \geq 1$, we can obtain $w_i(k) \geq \varepsilon^{T(N-1)}$ for $k \geq 1$. In summary, we always have $w_i(k) \geq \varepsilon^{T(N-1)}$ for $k \geq 1$.

Theorem 1: For a network of $N$ agents represented by a sequence of time-varying directed graphs $\{G(k) = (V, \varepsilon(k))\}$ satisfying Assumptions 1, 2, 3, and 4 under Algorithm 1, the estimate $\pi_i(k) = \frac{1}{N} \sum_{a} \frac{1}{\pi_i(a(k))} + a$ of each agent $i$ will converge to the average $\bar{x}^0 = \frac{1}{N} \sum_{j=1}^{N} x_j^0 / N$. More specifically, the rate of convergence of Algorithm 1 is at least $\gamma = (1 - \varepsilon^{T(N-1)}) \pi(\varepsilon^{T(N-1)}) \in (0, 1)$, meaning that there exists a positive constant $C$ satisfying $\|\pi(k) - \bar{x}^0\| \leq C \gamma^k$ for all $k$.

Proof: From (6), we have

$$
\frac{\sum_{i=1}^{N} s_i(k + 1)}{\sum_{i=1}^{N} s_i(k)} = \frac{\sum_{i=1}^{N} \frac{1}{\pi_i(k + 1)} + a}{\sum_{i=1}^{N} \frac{1}{\pi_i(k)} + a} = \frac{\sum_{i=1}^{N} \Delta s_{ij}(k)}{\sum_{i=1}^{N} \Delta s_{ij}(k)}
$$

(19)

$$
\sum_{i=1}^{N} \Delta s_{ij}(k) = \sum_{i=1}^{N} \Delta s_{ij}(k) + \sum_{i=1}^{N} \Delta s_{ii}(k)
$$

Further combining (19) and (20) yields

$$
\frac{\sum_{i=1}^{N} s_i(k + 1)}{\sum_{i=1}^{N} s_i(k)} = \frac{\sum_{i=1}^{N} s_i(0)}{\sum_{i=1}^{N} s_i(0)} \in \left[\frac{1}{N}, \frac{N - 1}{N}\right] \subset (0, 1)
$$

(20)

Since $P(k)$ is column stochastic, from (9) we have

$$
1^T w(k + 1) = 1^T w(k) = \cdots = 1^T w(0) = N
$$

(22)

for $k \geq 0$. Then we rewrite (11) as

$$
\begin{cases}
    s(K + l + 1) = \Phi(K + l : K + 1) s(K + 1) \\
    w(K + l + 1) = \Phi(K + l : K + 1) w(K + 1)
\end{cases}
$$

(23)

for $l \geq 1$. Under Assumptions 1 and 4, and the requirements on weights $p_{ij}(k)$ in Algorithm 1, following Proposition 1(b) in [55], we know that the transition matrix $\Phi(K + l : K + 1)$ will converge to a stochastic vector $\varphi(K + 1)$ with a geometric rate for all $i$ and $j$, i.e., for all $i, j = 1, \ldots, N$ and $l \geq 1$, we have

$$
\|\Phi(K + l : K + 1)\|_{ij} - \varphi_i(K + l) \leq C_0 \gamma^{l-1}
$$

(24)

with $C_0 = 2(1 - \varepsilon^{T(N-1)})/(1 - \varepsilon^{T(N-1)})$ and $\gamma = (1 - \varepsilon^{T(N-1)}) \pi(\varepsilon^{T(N-1)})$. Defining $M(K + l : K + 1)$ as

$$
M(K + l : K + 1) = \Phi(K + l : K + 1) - \Phi(K + l : K + 1) 1^T
$$

(25)

we have

$$
|M(K + l : K + 1)|_{ij} \leq C_0 \gamma^{l-1}
$$

(26)
for all $i, j = 1, \ldots, N$ and $l \geq 1$. Further combining (23) with (22) leads to

\[
\begin{align*}
\begin{cases}
    s(K + l + 1) &= M(K + l : K + 1)s(K + 1) + \varphi(K + l) 1^T s(K + 1) \\
    w(K + l + 1) &= M(K + l : K + 1)w(K + 1) + N \varphi(K + l)
\end{cases}
\end{align*}
\] (27)

where in the derivation we used $1^T w(K + 1) = N$ from (22). Then from (27), we have

\[
\begin{align*}
    s_i(K + l + 1) &= \frac{\sum_{j=1}^N s_j(K + 1)}{w_i(K + l + 1)} \\
    &= s_i(K + l + 1) - \frac{1^T s(K + 1)i}{w_i(K + l + 1)} \\
    &= s_i(K + l + 1) - \frac{1^T s(K + 1)i}{w_i(K + l + 1)} + \frac{w_i(K + l + 1)}{w_i(K + l + 1)} \\
    &= \frac{[M(K + l : K + 1)s(K + 1)]i + \varphi_i(K + l) 1^T s(K + 1)}{w_i(K + l + 1)} \\
    &= \frac{1^T s(K + 1)[M(K + l : K + 1)w(K + 1)]i}{w_i(K + l + 1)} \\
    &= \frac{1^T s(K + 1)[M(K + l : K + 1)w(K + 1)]i}{w_i(K + l + 1)} + \frac{N w_i(K + l + 1)}{w_i(K + l + 1)} \\
    &= \frac{[M(K + l : K + 1)s(K + 1)]i}{w_i(K + l + 1)} \\
    &= \frac{1^T s(K + 1)[M(K + l : K + 1)w(K + 1)]i}{w_i(K + l + 1)} \\
    &= \frac{1^T s(K + 1)[M(K + l : K + 1)w(K + 1)]i}{w_i(K + l + 1)}.
\end{align*}
\] (28)

Therefore, for $i = 1, \ldots, N$ and $l \geq 1$, we can obtain

\[
\begin{align*}
    &\frac{N s_i(K + l + 1)}{w_i(K + l + 1)} - \sum_{j=1}^N s_j(K + 1) \\
    \leq& \frac{N}{w_i(K + l + 1)} \left[ \max_{j} \left[ \frac{[M(K + l : K + 1)]j}{w_i(K + l + 1)} \right] \right] \|s(K + 1)\|_1 \\
    &+ \frac{N}{w_i(K + l + 1)} \left[ 1^T s(K + 1) \left( \max_{j} \left[ \frac{[M(K + l : K + 1)]j}{w_i(K + l + 1)} \right] \right) \right] \|1^T s(K + 1)\|_1 \\
    \leq& \frac{N}{\varepsilon T(N - 1)} \left[ \max_{j} \left[ \frac{[M(K + l : K + 1)]j}{w_i(K + l + 1)} \right] \right] \|s(K + 1)\|_1 \\
    &+ \frac{N}{\varepsilon T(N - 1)} \left[ 1^T s(K + 1) \left( \max_{j} \left[ \frac{[M(K + l : K + 1)]j}{w_i(K + l + 1)} \right] \right) \right]
\end{align*}
\] (29)

where in the derivation we used $w_i(K + l + 1) \geq \varepsilon T(N - 1)$ from Lemma 1 and $\|w(K + 1)\|_1 = \sum_{j=1}^N w_i(K + 1) = 1^T w(K + 1) = N$ from (22). Further using the relationship $1^T s(K + 1) \leq \|s(K + 1)\|_1$ and (26) yields

\[
\begin{align*}
    \frac{N s_i(k)}{w_i(k)} - \sum_{j=1}^N s_j(K + 1) \leq C_1 \gamma^k 
\end{align*}
\] (30)

for $k \geq K + 2$ with $C_1$ given by

\[
C_1 = 2N C_0 \|s(K + 1)\|_1 \varepsilon^{-T(N - 1)} \gamma^{-K - 2}
\] (31)

Given $s_i(0) = \frac{1}{N} + \frac{(N - 2)(a^0 - a)}{(b - a) N^2}$, we have

\[
\begin{align*}
    \bar{x}^0 &= \frac{1}{N} \sum_{j=1}^N x_j^0 = \frac{b - a}{N - 2} \left( N \sum_{j=1}^N s_j(0) - 1 \right) + a \\
    &= \frac{b - a}{N - 2} \left( N \sum_{j=1}^N s_j(K + 1) - 1 \right) + a \\
    &= \frac{b - a}{N - 2} \left( N \sum_{j=1}^N s_j(K + 1) - 1 \right) + a
\end{align*}
\] (32)

where in the derivation we used $\frac{N s_i(K + 1)}{w_i(K + 1)} = \sum_{j=1}^N s_j(K + 1)$ from (21). Combining (32) with $\pi_i(k) = \frac{b - a}{N - 2} \left( N \frac{s_i(k)}{w_i(k)} - 1 \right) + a$ leads to

\[
\begin{align*}
    \pi_i(k) - \bar{x}^0 &= \frac{b - a}{N - 2} \left( N \frac{s_i(k)}{w_i(k)} - 1 \right) + a \\
    &= \frac{b - a}{N - 2} \left( N \frac{\frac{s_i(k)}{w_i(k)} - 1}{\frac{s_i(k)}{w_i(k)}} \right) + a \\
    &= \frac{b - a}{N - 2} \left( N \frac{s_i(k)}{w_i(k)} - \frac{N s_i(k)}{w_i(k)} \right) + a \\
    &= \frac{b - a}{N - 2} \left( N \frac{\frac{s_i(k)}{w_i(k)} - 1}{\frac{s_i(k)}{w_i(k)}} \right) + a
\end{align*}
\] (33)

From (20) and (21), one can obtain $\frac{N s_i(k)}{w_i(k)} = \sum_{j=1}^N s_j(K + 1)$ from $\frac{N s_i(k)}{w_i(k)} = \sum_{j=1}^N s_j(0) \in \left\{ \frac{1}{N}, \frac{1}{N - 1} \right\}$, then there must exist an integer $Q$ such that $\sum_{j=1}^N s_j(K + 1) = Q + \eta$ holds. From (30), we can see that there must exist a positive integer $K_1 \geq K + 2$ such that

\[
\begin{align*}
    \left| \frac{N s_i(k)}{w_i(k)} - \sum_{j=1}^N s_j(K + 1) \right| \leq C_1 \gamma^k < \frac{1}{N}
\end{align*}
\] (34)

holds for $k \geq K_1$. Then it follows naturally one has

\[
\begin{align*}
    Q < Q + \eta - C_1 \gamma^k \leq \frac{N s_i(k)}{w_i(k)} \leq Q + \eta + C_1 \gamma^k < Q + 1
\end{align*}
\] (35)

for $k \geq K_1$, which leads to

\[
\begin{align*}
    0 < \eta - C_1 \gamma^k \leq \frac{N s_i(k)}{w_i(k)} - \eta \leq + C_1 \gamma^k < 1
\end{align*}
\] (36)

for $k \geq K_1$. Thus, we have

\[
\begin{align*}
    \left| \pi_i(k) - \bar{x}^0 \right| &= \frac{b - a}{N - 2} \left| N \frac{\frac{s_i(k)}{w_i(k)} - 1}{\frac{s_i(k)}{w_i(k)}} \right| \\
    &\leq \frac{b - a}{N - 2} NC_1 \gamma^k
\end{align*}
\] (37)

and further

\[
\begin{align*}
    \left| \pi(k) - \bar{x}^0 1 \right| &\leq C_2 \gamma^k
\end{align*}
\] (38)

for $k \geq K_1$ with $C_2 \leq \frac{b - a}{N - 2} N \sqrt{N} C_1$.

For $k \leq K_1 - 1$, from (33), we have

\[
\begin{align*}
    \left| \pi_i(k) - \bar{x}^0 \right| &< \frac{b - a}{N - 2} N
\end{align*}
\] (39)

which further implies

\[
\begin{align*}
    \left| \pi(k) - \bar{x}^0 1 \right| &< \frac{b - a}{N - 2} N \sqrt{N}
\end{align*}
\] (40)

for $k \leq K_1 - 1$. Defining $C$ as

\[
\begin{align*}
    C &\leq \max \left\{ C_2, \frac{b - a}{N - 2} N \sqrt{N} \gamma^{-k} \right\} \quad 0 \leq k \leq K_1 - 1
\end{align*}
\] (41)

one can obtain

\[
\begin{align*}
    \left| \pi(k) - \bar{x}^0 1 \right| &\leq C \gamma^k
\end{align*}
\] (42)
for all $k$. Therefore, each agent $i$ will converge to the average value $\bar{x}^0 = \frac{\sum_{j=1}^{N} x_j^0}{N}$ with the rate of convergence of at least $\gamma = (1 - \varepsilon^k (N-1)^{\frac{1}{T-1}}) \in (0, 1)$.

From Theorem 1, we can see that a smaller $\gamma$ means a faster convergence. Under the relationship $\gamma = (1 - \varepsilon (N-1)^{\frac{1}{T-1}})$, to expedite the convergence, i.e., a smaller $\gamma$, it is sufficient to increase $\varepsilon$, which amounts to reducing the width of the range $(\varepsilon, 1)$ for the random selection of $p_j(k)$. Note that although a reduced range $(\varepsilon, 1)$ enables an honest-but-curious adversary to obtain a better estimation of the range of agent $i$'s intermediate states $s_i(k)$ and $w_i(k)$ for $k \geq K + 1$ from received $p_j(k)s_i(k)$ and $p_j(k)w_i(k)$, it does not affect the confidentiality of agent $i$'s initial state $x_i^0$, as will be shown in the following subsection. It is also worth noting that to meet the requirement of randomly selecting weights in our algorithm, $\varepsilon$ cannot be arbitrarily close to 1. In fact, $\varepsilon$ must satisfy $\varepsilon < 1/\max_{i,k} (D_i^\text{out}(k) + 1)$. An easy way to select $\varepsilon$ is to set $0 < \varepsilon < 1/N$ since $D_i^\text{out}(k) \leq N - 1$ is true for all $k$ and $i \in \mathcal{V}$.

Remark 6: Theorem 1 provides a detailed analysis of the rate of convergence under time-varying directed graphs, the results on which are sparse in the literature on Push-Sum under time-varying random weights.

C. Confidentiality Analysis

Before presenting our main confidentiality result, we first introduce the following lemma.

**Lemma 2:** Consider a network of $N$ agents represented by a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, E(k))\}$ which satisfy Assumptions 1, 2, 3, 4, and 5. Under the proposed Algorithm 1, if at some time instant $0 \leq k^* \leq K$, agent $i \notin \mathcal{A}$ has an in-neighbor or out-neighbor not belonging to $\mathcal{A}$, then under $T_i^* \triangleq \{\Delta s_{mn}(k) \mid (m, n) \in E(k), (m, n) \notin (i, l), (l, m) \notin (i, l), k = 0, 1, \ldots , K\}$, the joint probability distributions of $s_i(K + 1)$ and $s_l(K + 1)$ are identical for any two different initial states $x^0, \bar{x}^0 \in [a, b]^N$ subject to $x_0^0 + x_l^0 = \bar{x}_0^0 + \bar{x}_l^0$ and $x_j^0 = \bar{x}_j^0$ for $j \in \mathcal{V} \setminus \{i, l\}$.

**Proof:** According to [45], we can rewrite the update rule of $s_i(k)$ as follows:

$$s_i(k + 1) = \frac{\sum_{j \in N_i^n(k)} \Delta s_{ij}(k) + s_i(k) - \sum_{j \in N_i^\text{in}(k)} \Delta s_{ji}(k)}{N}$$

for $k \leq K$. We stack all variables $\Delta s_{mn}(k)$ into a vector $\Delta s(k)$ according to indices of edges in $E(k)$, namely, the index of $\Delta s_{mn}(k)$ is determined by the index of the edge $(m, n) \in E(k)$. Then we can further rewrite [45] in the following more compact form:

$$s(k + 1) = \frac{s(k) + C(k) \Delta s(k)}{N}$$

for $k \leq K$, where $C(k)$ is the incidence matrix for graph $\mathcal{G}(k)$ at iteration $k$.

Define the subsets of agents $\mathcal{H}$ and $\mathcal{R}$ as $\mathcal{H} = \{i, l\}$ and $\mathcal{R} = \mathcal{V} \setminus (\mathcal{H} \cup \mathcal{A})$, respectively. Let $N_\mathcal{A} = |\mathcal{A}|$ and $N_\mathcal{R} = |\mathcal{R}|$ represent the number of agents in $\mathcal{A}$ and $\mathcal{R}$, respectively. It is clear that $\mathcal{H}, \mathcal{A}$, and $\mathcal{R}$ are disjoint, and $\mathcal{H} \cup \mathcal{A} \cup \mathcal{R} = \mathcal{V}$ holds. For graph $\mathcal{G}(k) = (\mathcal{V}, \mathcal{E}(k))$, we define the subgraph $\mathcal{G}_k(k)$ as $\mathcal{G}_k(k) = (\mathcal{H}, \mathcal{E}_k(k))$ where $\mathcal{E}_k(k) \subset \mathcal{E}(k)$ is the set of edges entirely within $\mathcal{H}$. The union of subgraphs $\mathcal{G}_k(k)$ for iterations $k = 0, 1, \ldots , K$ is further denoted as $\mathcal{G}_k^* = \bigcup_{k=0}^{K} \mathcal{G}_k(k) = (\mathcal{H}, \mathcal{E}_k^*)$, where $\mathcal{E}_k^* = \bigcup_{k=0}^{K} \mathcal{E}_k(k)$ is the union of edge sets $\mathcal{E}_k(k)$ for iterations $k = 0, 1, \ldots , K$. Denote the edge set $\mathcal{E}_k(k)$ as the collection of edges associated with all agents in $\mathcal{A}$ at iteration $k$, namely, $\mathcal{E}_k(k) = \{(m, n) \mid (m, n) \in \mathcal{E}(k), m \text{ or } n \in \mathcal{A}\}$. Then the set of remaining edges not belonging to $\mathcal{E}_k(k)$ or $\mathcal{E}_k(k)$ can be denoted as $\mathcal{E}_{k}^* = \mathcal{E}(k) \setminus (\mathcal{E}_k(k) \cup \mathcal{E}_k(k))$, which is a collection of edges that are either entirely within $\mathcal{R}$ or between $\mathcal{R}$ and $\mathcal{H}$. Let $\mathcal{E}_k(k) = |\mathcal{E}_k(k)|$, $\mathcal{E}_k(k) = |\mathcal{E}_k(k)|$, and $\mathcal{E}_k(k) = |\mathcal{E}_k(k)|$ represent the number of edges in $\mathcal{E}_k(k)$, $\mathcal{E}_k(k)$, and $\mathcal{E}_k(k)$, respectively. Note that $\mathcal{E}_k(k)$, $\mathcal{E}_k(k)$, and $\mathcal{E}_k(k)$ are disjoint, and we always have $\mathcal{E}_k(k) \cap \mathcal{E}_k(k) \cap \mathcal{E}_k(k) = \mathcal{E}(k)$. Without loss of generality, we can partition the state vector $s(k)$ as $s(k) = [s_h(k)^T \ s_a(k)^T \ s_r(k)^T]^T$ where $s_h(k)$, $s_a(k)$, and $s_r(k)$ denote the state vectors of agents in $\mathcal{H}$, $\mathcal{A}$, and $\mathcal{R}$, respectively. Then we can further rewrite the update rule of $s(k)$ for $k \leq K$ as

$$\begin{bmatrix} s_h(k+1) \\ s_a(k+1) \\ s_r(k+1) \end{bmatrix} = \begin{bmatrix} s_h(k) \\ s_a(k) \\ s_r(k) \end{bmatrix} + \begin{bmatrix} C_h(k) \ C_a(k) \ C_r(k) \\ 0_{N_A \times E_h(k)} \ C_a(k) \ 0_{N_R \times E_h(k)} \\ 0_{N_R \times E_h(k)} \ C_r(k) \ 0_{N_R \times E_h(k)} \end{bmatrix} \begin{bmatrix} \Delta s_h(k) \\ \Delta s_a(k) \\ \Delta s_r(k) \end{bmatrix}$$

where $C_h(k)$ is the incidence matrix for subgraph $\mathcal{G}_h(k) = (\mathcal{H}, \mathcal{E}_h(k))$, and $\Delta s_h(k)$, $\Delta s_a(k)$, and $\Delta s_r(k)$ are vectors stacking $\Delta s_{mn}(k)$ corresponding to edge sets $\mathcal{E}_h(k)$, $\mathcal{E}_a(k)$, and $\mathcal{E}_r(k)$, respectively. It is obvious that $\Delta s_{\mathcal{A}}(k)$ is completely known to agents in $\mathcal{A}$ since every element in $\Delta s_{\mathcal{A}}(k)$ is either sent or received by the agents in $\mathcal{A}$. From [45], we can further obtain

$$\begin{bmatrix} s_h(K+1) \\ s_a(K+1) \\ s_r(K+1) \end{bmatrix} = \begin{bmatrix} s_h(0) \\ s_a(0) \\ s_r(0) \end{bmatrix} + \begin{bmatrix} C_h^T \ C_a^T \ C_r^T \\ 0_{N_A \times E_h^T} \ C_a^T \ 0_{N_R \times E_h^T} \\ 0_{N_R \times E_h^T} \ C_r^T \ 0_{N_R \times E_h^T} \end{bmatrix} \begin{bmatrix} \Delta s_h^* \\ \Delta s_a^* \\ \Delta s_r^* \end{bmatrix}$$

where $E_h^* = \sum_{k=0}^{K} E_h(k)$, $E_r^* = \sum_{k=0}^{K} E_r(k)$, and

$$\begin{bmatrix} C_h^T \\ C_a^T \\ C_r^T \\ 0_{N_A \times E_h^T} \ 0_{N_A \times E_h^T} \ 0_{N_R \times E_h^T} \ \end{bmatrix} \begin{bmatrix} \Delta s_h^* \\ \Delta s_a^* \\ \Delta s_r^* \end{bmatrix}$$

It is worth noting that $C_h^T$ is the incidence matrix for graph
Denoting $v = [v_1, v_2]^T$ as

$$v \equiv \text{frac}(C_{i}^s \Delta s_{i}^s)$$

next we prove that $v$ is uniformly distributed in $[0, 1) \times [0, 1]$ subject to $\text{frac}(v_1 + v_2) = 0$ if at some time instant $0 \leq k^* \leq K$, agent $i$ has an in-neighbor or out-neighbor $l$ not belonging to $\mathcal{A}$.

Given $\mathcal{H} = \{i, l\}$, if at some time instant $0 \leq k^* \leq K$, agent $i$ has an in-neighbor or out-neighbor $l$ not belonging to $\mathcal{A}$, the columns of $C_{i}^s$ are either $[1 - 1]^T$ or $[-1 1]^T$ (l is an in-neighbor of agent $i$) or $[-1 1]^T$ (l is an out-neighbor of agent $i$). Denote the $j$-th column of $C_{i}^s$ as $c_j^s$, then $c_j^s$ can be expressed as

$$c_j^s = r_j c_i^s$$

where $r_j \in \{1, -1\}$ is the corresponding coefficient. Defining $r = [r_1 \cdots r_{|\mathcal{E}_i|}]$, one can obtain

$$v = \text{frac}(C_{i}^s \Delta s_{i}^s) = \text{frac}(c_i^s r \Delta s_i^s) = \text{frac}(c_i^s \cdot \text{frac}(r \Delta s_i^s))$$

Since all the elements in $\Delta s_{i}^s$ are independent of each other and uniformly distributed in $[0, 1)$, we have that $\text{frac}(r \Delta s_i^s)$ is uniformly distributed in $[0, 1)$. As $c_i^s$ is either $[1 - 1]^T$ or $[-1 1]^T$, we have that $v$ is uniformly distributed in $[0, 1) \times [0, 1]$ subject to $\text{frac}(v_1 + v_2) = 0$.

From (48), we have $s_{\mathcal{H}}(K + 1) = \text{frac}(s_{\mathcal{H}}(0) + v + C_{i}^s \Delta s_{i}^s + C_{i}^s \Delta s_{i}^s)$.

Further taking into account the fact that $v$ is uniformly distributed in $[0, 1) \times [0, 1]$ subject to $\text{frac}(v_1 + v_2) = 0$ if at some time instant $0 \leq k^* \leq K$, agent $i$ has an in-neighbor or out-neighbor $l$ not belonging to $\mathcal{A}$, we can obtain that $s_{\mathcal{H}}(K + 1)$ is also uniformly distributed in $[0, 1) \times [0, 1]$ subject to $\text{frac}(1^T s_{\mathcal{H}}(K + 1)) = \text{frac}(1^T s_{\mathcal{H}}(0) + 1^T C_{i}^s \Delta s_{i}^s + 1^T C_{i}^s \Delta s_{i}^s)$.

Now we analyze the probability distributions of $s_{\mathcal{H}}(K + 1)$ under different initial conditions of agent $i$. For any two different initial conditions $\tilde{x}_0^0, \tilde{x}_0^0 \in [a, b]^N$ subject to $x_i^0 + x_j^0 = \tilde{x}_0^0 + \tilde{x}_0^0$ and $x_j^0 = \tilde{x}_0^0$ for $j \in \mathcal{V} \setminus \{i, l\}$, one can obtain $s_i(0) = \tilde{s}_i(0)$.

Theorem 2: Consider a network of $N$ agents represented by a sequence of time-varying directed graphs $\{G(k) = (\mathcal{V}, \mathcal{E}(k))\}$ which satisfy Assumptions 1, 2, 3, 4, and 5. Under the proposed Algorithm 1, the confidentiality of agent $i \notin \mathcal{A}$ can be preserved against $\mathcal{A}$ if at some time instant $0 \leq k^* \leq K$, agent $i$ has an in-neighbor or out-neighbor $l$ not belonging to $\mathcal{A}$.

Proof: To show that the confidentiality of agent $i$ can be protected, we have to show that under different initial values of agent $i$, the probability distributions are identical for honest-but-curious agents $\mathcal{A}$' information set. It suffices to prove that the probability distributions of information sets accessible to $\mathcal{A}$ are identical for all $x^0, \bar{x}^0 \in [a, b]^N$ subject to $x_i^0 + x_j^0 = \tilde{x}_0^0 + \tilde{x}_0^0$ and $x_j^0 = \tilde{x}_0^0$ for $j \in \mathcal{V} \setminus \{i, l\}$, which is an in-neighbor or out-neighbor of agent $i$ at some time instant $0 \leq k^* \leq K$. Thus, given $x^0$ and $\bar{x}^0$, the sum of the initial states of all nodes not in $\mathcal{A}$ keeps unchanged, i.e., $\sum_{j \in \mathcal{V} \setminus \mathcal{A}} x_j^0 = \sum_{j \in \mathcal{V} \setminus \mathcal{A}} \bar{x}_j^0$.

Given $s_i(0) = \frac{1}{N} + \frac{(N-2)(x_0^0 - a)}{(b-a)N^2}$, this is equivalent to proving that the probability distributions of information sets accessible to $\mathcal{A}$ are identical for all $s_i(0), \bar{s}_i(0) \in \left[\frac{1}{N}, \frac{N-1}{N}\right]^N$ subject to $s_i(0) + s_l(0) = \bar{s}_i(0) + \bar{s}_l(0)$ and $s_j(0) = \bar{s}_j(0)$ for $j \in \mathcal{V} \setminus \{i, l\}$. Denoting $I_s(k)$ and $I_{w}(k)$ as

$$I_s(k) = \{s_{\mathcal{A}}(k), \Delta s_{\mathcal{A}}(k)\}$$
$$I_{w}(k) = \{w_{\mathcal{A}}(k), \Delta w_{\mathcal{A}}(k)\}$$

where $s_{\mathcal{A}}(k)$ and $w_{\mathcal{A}}(k)$ are state vectors of agents in $\mathcal{A}$, and $\Delta s_{\mathcal{A}}(k)$ and $\Delta w_{\mathcal{A}}(k)$ are augmented vectors of $\Delta s_{\mathcal{W}}(k)$ and $\Delta w_{\mathcal{W}}(k)$ corresponding to edge set $\mathcal{E}_A(k)$, respectively. We can see that agents in $\mathcal{A}$ have access to both $I_s(k)$ and $I_{w}(k)$ at each iteration $k$. Further denote $I_{11}, I_{1w}, I_{21}, I_{2w}$, and $I_{2w}$ as

$$I_{11} = \bigcup_{k=0}^{\infty} I_s(k), \quad I_{1w} = \bigcup_{k=0}^{\infty} I_{w}(k)$$
$$I_{21} = \bigcup_{k=K+1}^{\infty} I_s(k), \quad I_{2w} = \bigcup_{k=K+1}^{\infty} I_{w}(k)$$

$$I_{11} = I_{11} \cup I_{1w}, \quad I_{21} = I_{21} \cup I_{2w}$$

According to Algorithm 1, $I_s \equiv I_{11} \cup I_{1w}$ represents all the information accessible to $\mathcal{A}$. We denote the conditional probability density of $I_s$ given $s(0)$ as $f(I_s | s(0))$. Thus, to show that the confidentiality of agent $i$ can be protected, it is equivalent to proving $f(I_s | s(0)) = f(I_s | \tilde{s}(0))$ for all $s(0), \tilde{s}(0) \in \left[\frac{1}{N}, \frac{N-1}{N}\right]^N$ subject to $s_i(0) + s_l(0) = \tilde{s}_i(0) + \tilde{s}_l(0)$ and $s_j(0) = \tilde{s}_j(0)$ for $j \in \mathcal{V} \setminus \{i, l\}$.

Since

$$f(I_s | s(0)) = f(I_s | I_{1s}, s(0)) = f(I_{1s} | s(0)) f(I_s | I_{1s}, s(0))$$

holds, to show $f(I_s | s(0)) = f(I_s | \tilde{s}(0))$, it suffices to prove that

$$f(I_{1s} | s(0)) = f(I_{1s} | \tilde{s}(0))$$

and

$$f(I_{2s} | s(0)) = f(I_{2s} | \tilde{s}(0))$$
Similarly, one can also obtain

\[ f(I_1 | s(0)) = f(I_2 | s(0)) = f(I_3 | s(0)) = \ldots = f(I_n | s(0)) \]

which implies

\[ f(I_1 | s(0)) = f(I_2 | s(0)) = f(I_3 | s(0)) = \ldots = f(I_n | s(0)) \]

where we used \( s(A(0)) = \bar{s}_A(0) \) in the derivation.

To show \( f(\mathcal{I}_2 | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2 | \mathcal{I}_1, \bar{s}(0)) \), it suffices to prove

\[ f(\mathcal{I}_2, s(K+1), w(K+1) | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2, w(K+1) | \mathcal{I}_1, \bar{s}(0)) \]

Given \( s(K+1) \) and \( w(K+1) \), \( \mathcal{I}_2 \) is independent of \( \mathcal{I}_1 \), which further leads to

\[ f(\mathcal{I}_2, s(K+1), w(K+1) | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2 | s(K+1), w(K+1) | \mathcal{I}_1, s(0)) \times f(s(K+1), w(K+1) | \mathcal{I}_1, s(0)) \]

Further taking into account the facts that 1) \( s(K+1) \) is conditionally independent of \( w(K+1) \) and \( \mathcal{I}_1 \), and 2) \( w(K+1) \) is conditionally independent of \( \mathcal{I}_1 \) and \( s(0) \), one can obtain

\[ f(\mathcal{I}_2, s(K+1), w(K+1) | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2 | s(K+1), w(K+1) | \mathcal{I}_1, s(0)) \times f(s(K+1), w(K+1) | \mathcal{I}_1, s(0)) \times f(\mathcal{I}_2 | s(K+1), w(K+1) | \mathcal{I}_1, s(0)) \times f(s(K+1) | w(K+1), \mathcal{I}_1, s(0)) | f(w(K+1) | \mathcal{I}_1, s(0)) \]

Similarly, one can also obtain

\[ f(\mathcal{I}_2, s(K+1), w(K+1) | \mathcal{I}_1, \bar{s}(0)) = f(\mathcal{I}_2 | s(K+1), w(K+1) | \mathcal{I}_1, \bar{s}(0)) \times f(s(K+1), w(K+1) | \mathcal{I}_1, \bar{s}(0)) \]

Therefore, to show \( f(\mathcal{I}_2 | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2 | \mathcal{I}_1, \bar{s}(0)) \), it suffices to prove \( f(s(K+1) | \mathcal{I}_1, s(0)) = f(s(K+1) | \mathcal{I}_1, \bar{s}(0)) \).

Denote \( \mathcal{T}_K = \{ \Delta s_K(k) | k = 0, 1, \ldots, K \} \). To prove

\[ f(s(K+1) | \mathcal{I}_1, s(0)) = f(s(K+1) | \mathcal{I}_1, \bar{s}(0)) \]

we only need to prove

\[ f(s(K+1), I_R | \mathcal{I}_1, s(0)) = f(s(K+1), I_R | \mathcal{I}_1, \bar{s}(0)) \]

From \([46]\), we can obtain the following facts: 1) \( s_H(K+1) \) is conditionally independent of \( s_A(K+1) \) and \( s_R(K+1) \) given \( I_R, \mathcal{I}_1 \), and \( s(0) \); 2) \( s_A(K+1) \) and \( s_R(K+1) \) are conditionally independent of \( s_H(0) \) given \( I_R, \mathcal{I}_1, s_A(0), s_R(0) \). Taking into account these facts, we have

\[ f(s(K+1), I_R | \mathcal{I}_1, s(0)) = f(s_H(K+1), s_A(K+1), s_R(K+1), I_R | \mathcal{I}_1, s(0)) = f(s_H(K+1), s_R(K+1), I_R | \mathcal{I}_1, s(0)) \]

and

\[ x \times f(s_A(K+1), s_R(K+1) | \mathcal{I}_R, \mathcal{I}_1, s(0)) f(I_R | \mathcal{I}_1, s(0)) \]

where in the derivation we used the independence between \( \mathcal{I}_R \) and \( \{ \mathcal{I}_1, s(0) \} \). Similarly, one can obtain

\[ f(s(K+1), I_R | \mathcal{I}_1, \bar{s}(0)) = f(s_H(K+1), s_A(K+1), s_R(K+1), I_R | \mathcal{I}_1, \bar{s}(0)) = f(s_H(K+1), s_R(K+1), I_R | \mathcal{I}_1, \bar{s}(0)) \]

From Lemma \([2]\), we have that if at some time instant \( 0 \leq k^* \leq K \), agent \( i \) has an in-neighbour or out-neighbour \( l \) not belonging to \( A \), \( f(s_H(K+1) | \mathcal{I}_1, s(0)) = f(s_H(K+1) | \mathcal{I}_1, \bar{s}(0)) \) holds, where \( \mathcal{I}_1 = \{ \Delta s(A(k)) | (m, n) \notin \mathcal{E}_A(k), (m, n) \notin \mathcal{E}_R(k), k = 0, 1, \ldots, K \} \) is the collection of all elements \( \Delta s(A(k)) \) and \( \Delta s_R(k) \) from iteration 0 to iteration \( K \). Given that \( \Delta s(A(k)) \in \mathcal{I}_1 \) and \( \Delta s_R(k) \in \mathcal{I}_1 \) hold for \( k = 0, 1, \ldots, K \), we further have

\[ f(s_H(K+1) | I_R, \mathcal{I}_1, s(0)) = f(s_H(K+1) | I_R, \mathcal{I}_1, \bar{s}(0)) \]

Based on \( s_A(0) = \bar{s}_A(0) \) and \( s_R(0) = s_R(0) \), we have

\[ f(s(K+1), I_R | \mathcal{I}_1, s(0)) = f(s(K+1), I_R | \mathcal{I}_1, \bar{s}(0)) \]

implying \( f(\mathcal{I}_2 | \mathcal{I}_1, s(0)) = f(\mathcal{I}_2 | \mathcal{I}_1, \bar{s}(0)) \) if at some time instant \( 0 \leq k^* \leq K \), agent \( i \) has an in-neighbour or out-neighbour \( l \) that does not belong to \( A \).

**Remark 7:** Compared with our previous work \([1]\) which defines privacy as the positivity of probability that adversaries’ accessible information set being the same under two different initial states, in this work we significantly improved our confidential results by proving that the probability distributions of information sets are identical under different initial states, meaning that the initial states are perfectly indistinguishable from the viewpoint of adversaries.

**Remark 8:** It is worth noting that although the confidential approach in \([30]\) looks similar to ours (both protocols employ random values in the first several iterations), they are in fact significantly different. More specifically, to guarantee the accuracy of average consensus, not only does the confidential protocol in \([30]\) require pairwise local averaging of exchanged random values in the first several iterations, but it also needs to compensate the errors induced by the random values immediately after the first several iterations, which is equivalent to introducing time-correlated additive random noises to agents’ states. To the contrary, our confidential approach exchanges
time-uncorrelated random values for iterations \( k \leq K \). To ensure consensus accuracy, each agent \( i \) uses a carefully-designed \( \Delta s_{i}(k) \) to compensate the errors induced by the random values at each iteration \( k \leq K \). Therefore, the random values used in our approach are space-correlated. As shown in Theorem 2 the space-correlated randomness can make the probability distributions of information sets accessible to adversaries identical under different initial states and hence achieves information-theoretic privacy, which is stronger than the confidentiality achieved using time-correlated noises in [30].

Next we proceed to show that if the conditions in Theorem 2 are not met, then the confidentiality of agent \( i \) may be breached.

**Theorem 3:** Consider a network of \( N \) agents represented by a sequence of time-varying directed graphs \( \{G(k) = (V, E(k))\} \) which satisfy Assumptions 1, 2, 3, 4, and 5. Under the proposed Algorithm 1, the confidentiality of agent \( i \notin A \) cannot be preserved against \( A \) if all in-neighbors and out-neighbors of agent \( i \) belong to \( A \), i.e., \( \{N_{i}^{m}(k) \cup N_{i}^{out}(k) \mid k \geq 0\} \subset A \). In fact, when \( \{N_{i}^{m}(k) \cup N_{i}^{out}(k) \mid k \geq 0\} \subset A \) is true, the initial value \( x_{i}^{0} \) of agent \( i \) can be uniquely determined by honest-but-curious agents in \( A \).

**Proof:** From (43) we have

\[
\frac{\text{frac}(s_{i}(k + 1) - s_{i}(k))}{\text{frac} \left( \sum_{n \in N_{i}^{in}(k)} \Delta s_{in}(k) - \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(k) \right)} \quad (65)
\]

for \( k \leq K \) and further

\[
\frac{\text{frac} \left( \sum_{k=0}^{K} \left[ \sum_{n \in N_{i}^{in}(k)} \Delta s_{in}(k) - \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(k) \right] \right)}{(66)}
\]

Since \( s_{i}(0) \in \left[ \frac{1}{N} s, \frac{N-1}{N} s \right] \) holds, one can obtain

\[
s_{i}(0) = \text{frac} \left( s_{i}(K + 1) \right) - \sum_{k=0}^{K} \left[ \sum_{n \in N_{i}^{in}(k)} \Delta s_{in}(k) - \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(k) \right] \quad (67)
\]

According to the requirements in Algorithm 1, we have

\[
\Delta s_{i}(k) + \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(k) = s_{i}(k) \quad \text{for} \ k \geq K + 1
\]

and

\[
\Delta w_{i}(k) + \sum_{m \in N_{i}^{out}(k)} \Delta w_{mi}(k) = w_{i}(k) \quad \text{for} \ k \geq 0.
\]

Plugging these relationships into (67) and (68), we can obtain

\[
s_{i}(k + 1) - s_{i}(k) = \sum_{n \in N_{i}^{in}(k)} \Delta s_{in}(k) - \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(k) \quad (68)
\]

for \( k \geq K + 1 \) and

\[
w_{i}(k + 1) - w_{i}(k) = \sum_{n \in N_{i}^{in}(k)} \Delta w_{in}(k) - \sum_{m \in N_{i}^{out}(k)} \Delta w_{mi}(k) \quad (69)
\]

for \( k \geq 0 \), which further lead to

\[
s_{i}(k) - s_{i}(K + 1) = \sum_{l=0}^{k-1} \left[ \sum_{n \in N_{i}^{in}(k)} \Delta s_{in}(l) - \sum_{m \in N_{i}^{out}(k)} \Delta s_{im}(l) \right] \quad (70)
\]

for \( k \geq K + 1 \) and

\[
w_{i}(k) - w_{i}(0) = \sum_{l=0}^{k-1} \left[ \sum_{n \in N_{i}^{in}(k)} \Delta w_{in}(l) - \sum_{m \in N_{i}^{out}(k)} \Delta w_{mi}(l) \right] \quad (71)
\]

for \( k \geq 0 \).

Under Assumption 5 if \( \{N_{i}^{out}(k) \cup N_{i}^{in}(k) \mid k \geq 0\} \subset A \) is true, then all terms on the right-hand side of (70) and (71) are known to the honest-but-curious agents in \( A \). Further taking into account \( w_{i}(0) = 1 \), we have that agents in \( A \) can uniquely determine \( w_{i}(k) \) for all \( k \). Under Assumption 1 and \( \{N_{i}^{out}(k) \cup N_{i}^{in}(k) \mid k \geq 0\} \subset A \), there must exist at least one agent \( j \in A \) such that \( j, i \in E_{\infty} \) is true. This is because otherwise graph \( (V, E_{\infty}) \) is not strongly connected, which does not satisfy Assumption 5. According to Assumption 2, agent \( i \) directly communicates with agent \( j \in A \) at least once in every \( T \) consecutive time instants. So there must exist \( k' \geq K + 1 \) at which agent \( i \) directly communicates with agent \( j \), i.e., agent \( i \) sends \( \Delta s_{ji}(k') \) and \( \Delta w_{ji}(k') \) to agent \( j \) at iteration \( k' \). As \( j \in A \), every honest-but-curious agent in \( A \) has access to \( \Delta s_{ji}(k') \) and \( \Delta w_{ji}(k') \). So agents in \( A \) can easily infer \( s_{i}(k') \) by using the following relationship

\[
s_{i}(k') = \frac{\Delta s_{ji}(k')}{\Delta w_{ji}(k')} w_{i}(k') = \frac{p_{ji}(k') s_{i}(k')}{p_{ji}(k') w_{i}(k')} \quad (72)
\]

and then determine the value of \( s_{i}(K + 1) \) using (70). Further making use of (67), agents in \( A \) can infer the value of \( s_{i}(0) \), and then uniquely determine the initial value of agent \( i \) using \( x_{i}^{0} = \frac{b-a}{N} (N^{2}s_{i}(0) - 1) + a \). Therefore, the confidentiality of agent \( i \notin A \) cannot be preserved against \( A \) if all in-neighbors and out-neighbors of agent \( i \) belong to \( A \).

**Remark 9:** It is worth noting that in confidential average consensus, topology requirements such as the ones in Theorem 2 are widely used. In fact, to guarantee both accuracy and confidentiality, [26]–[31], [33]–[35], [39]–[41] all rely on similar topology requirements.

**Remark 10:** Our algorithm can protect the confidentiality of an agent even when all its neighbors interact (at least one does not collude) with adversaries, which is not allowed in [27] and [31].

**Remark 11:** From the above analysis, we know that introducing randomness into interaction dynamics by each agent \( i \) for \( k \leq K \) is key to protect confidentiality against honest-but-curious agents. It is worth noting that compared with the conventional push-sum approach which does not take confidentiality into consideration, the introduced randomness in our approach has no influence on the convergence rate \( \gamma \). However, the randomness does delay the convergence process and hence leads to a trade-off between confidentiality preservation and convergence time. This is confirmed in our
numerical simulations in Fig. 2, which shows that convergence only initiates after $k = K + 1$.

Remark 12: If an adversary can obtain side information, then a larger $K$ protects the confidentiality of more intermediate states $s_i(k)$ for $1 \leq k \leq K$. This is because for $k \geq K + 1$, $s_i(k)$ can be easily obtained by its out-neighbor $j$ due to the relationship $s_i(k) = w_i(k)\Delta s_{ji}(k)/\Delta w_{ji}(k)$ if side information about $w_i(k)$ is available to the adversary $j$. Therefore, although a larger $K$ leads to more delay in the convergence process, as discussed in Remark 11, it can protect more intermediate states ($s_i(k)$ for $1 \leq k \leq K$) when an adversary can obtain side information. Of course, if side information is not of concern, a smaller $K$ is preferable to minimize the delay in the convergence process.

Remark 13: Our algorithm can be extended to preserve confidentiality against external eavesdroppers wiretapping all communication links without compromising algorithmic accuracy by patching partially homomorphic encryption. More specifically, using public-key cryptosystems (e.g., Paillier [57], RSA [58], and ElGamal [59]), each agent generates and floods its public key before the consensus iteration starts. Then in decentralized implementation, an agent encrypts its messages to be sent, which can be decrypted by a legitimate recipient without the help of any third party. Note that since public-key cryptosystems can only deal with integers, the final consensus result would be subject to a quantization error. However, as indicated in our previous work [40], the quantization error can be made arbitrarily small in implementation.

IV. RESULTS VALIDATION

We conducted numerical simulations to verify the correctness and the effectiveness of our proposed approach.

We first evaluated our proposed Algorithm 1 under a network of $N = 5$ agents interacting on a time-varying directed graph. More specifically, we used the interaction graph in Fig. 1(a) when $k$ is even and Fig. 1(b) when $k$ is odd. It can be verified that this time-varying directed graph satisfies Assumptions 1 and 2. Parameter $\varepsilon$ was set to 0.05. The initial values $\bar{x}_i^0$ for $i = 1, \ldots, N$ were randomly chosen from $(-50, 50)$. We used $e(k)$ to measure the estimation error between the estimate $\pi_i(k) = s_i(k)/w_i(k)$ and the true average value $\bar{x}^0 = \sum_{j=1}^{N} x_j^0/N$ at iteration $k$, i.e.,

$$e(k) = \|\pi(k) - \bar{x}^0 1\| = \left(\sum_{i=1}^{N} (\pi_i(k) - \bar{x}^0)^2\right)^{1/2} \tag{73}$$

Three experiments were conducted with parameter $K$ being 10, 20, and 30, respectively. The evolution of $e(k)$ is shown in Fig. 2. It can be seen that $e(k)$ approached 0, meaning that every agent converged to the average value $\bar{x}^0 = \sum_{j=1}^{N} x_j^0/N$. From Fig. 2, we can also see that Algorithm 1 did not start to converge in the first $K + 1$ iterations due to the introduced randomness, which confirms our analysis in Remark 11.

We also evaluated the influence of parameter $\varepsilon$ on the convergence rate $\gamma$. The interaction graph was the same as above. $K$ was set to 10. The simulation results are given in Fig. 3 where the mean and variance of $\gamma$ from 1,000 runs of the algorithm are shown under different values of $\varepsilon$. Fig. 3 shows that as $\varepsilon$ increases, the convergence rate $\gamma$ decreases (i.e., the convergence speed increases), which confirms our analysis in Sec. III-B.

We then compared the proposed Algorithm 1 with existing data-obfuscation based approaches, more specifically, the differential-privacy based approach in [14], the decaying-noise approach in [27], and the finite-noise-sequence approach in [31]. Under the same setup as in the previous simulation, we chose the initial values as $\{10, 15, 20, 25, 30\}$, which led to an average value 20. We adopted the weight matrix $W$
from \([14]\), i.e., the \(ij\)-th entry was \(w_{ij} = 1/(|N^\text{out}_j| + 1)\) for \(i \in N^\text{out}_j \cup \{j\}\) and \(w_{ij} = 0\) for \(i \notin N^\text{out}_j \cup \{j\}\). As the graph is directed and imbalanced, and does not meet the undirected or balanced assumption in \([14], [27], [31]\), all three approaches failed to achieve average consensus, as shown in the numerical simulation results in Fig. 4, Fig. 5 and Fig. 6 respectively.

Finally, we conducted numerical simulations to verify the scalability of our proposed Algorithm 1 using a network of \(N = 1,000\) agents. At every iteration \(k\), each agent \(i\) was assumed to have three out-neighbors, i.e.,

\[
N^\text{out}_i(k) = \begin{cases} 
\{i + 1, i + 2, i + 3\} & \text{if } k \text{ is even} \\
\{i - 1, i - 2, i - 3\} & \text{if } k \text{ is odd} 
\end{cases}
\]

where the superscript “−” represents modulo operation on \(N\), i.e., \(\overline{i} \equiv i \mod N\). The initial values \(x^0_i\) for \(i = 1, 2, \ldots, N\) were randomly chosen from \((-50, 50)\). \(\epsilon\) and \(K\) were set to 0.05 and 10, respectively. The evolution of estimation error \(e(k) = \|\pi(k) - \bar{x}^0\|\) is shown in Fig. 7. It can be seen that \(e(k)\) converged to 0, implying that our proposed algorithm can guarantee the convergence of all agents to the actual average value even when the network size is large.

\[
\begin{align*}
\text{Fig. 4: The evolution of } x_1(k) \text{ under the approach in } [14]. \\
\text{Fig. 5: The evolution of } x_i(k) \text{ under the approach in } [27]. \\
\text{Fig. 6: The evolution of } x_i(k) \text{ under the approach in } [31]. \\
\end{align*}
\]

\[
\begin{align*}
\text{Fig. 7: The evolution of error } e(k) \text{ in a network of } N = 1,000 \text{ agents.} \\
\end{align*}
\]

V. Conclusions

We proposed a confidential average consensus algorithm for time-varying directed graphs. In distinct difference from existing differential-privacy based approaches which enable confidentiality through compromising the accuracy of obtained consensus value, we leveraged the inherent robustness of average consensus to embed randomness in interaction dynamics, which guarantees confidentiality of participating agents without sacrificing the accuracy of average consensus. Finally, we provided numerical simulation results to confirm the effectiveness and efficiency of our proposed approach.

References

[1] H. Gao, C. Zhang, M. Ahmad, and Y. Q. Wang, “Privacy-preserving average consensus on directed graphs using push-sum,” in 2018 IEEE Conference on Communications and Network Security (CNS), 2018.
[2] J. E. Boillat, “Load balancing and poisson equation in a graph,” Concurrency and Computation: Practice and Experience, vol. 2, no. 4, pp. 289–313, 1990.
[3] G. Cybenko, “Dynamic load balancing for distributed memory multiprocessors,” J. Parallel Distrib. Comput., vol. 7, no. 2, pp. 279–301, 1989.
[4] N. A. Lynch, Distributed algorithms. San Francisco, CA: Morgan Kaufmann Publishers, 1996.
Huan Gao was born in Shandong, China. He received the B.S. degree in automation and the M.Sc. degree in control theory and control engineering from Northwestern Polytechnical University, Xi’an, Shaanxi, China, in 2011 and 2015, respectively, and the Ph.D. degree in electrical engineering from Clemson University, Clemson, SC, USA, in 2020. He is currently an Associate Professor with the School of Automation, Northwestern Polytechnical University. His research interests include decentralized optimization, cooperative control, and privacy preservation in distributed systems.

Yongqiang Wang was born in Shandong, China. He received the B.S. degree in electrical engineering and automation, the B.S. degree in computer science and technology from Xi’an Jiaotong University, Xi’an, Shaanxi, China, in 2004, and the M.Sc. and Ph.D. degrees in control science and engineering from Tsinghua University, Beijing, China, in 2009. From 2007 to 2008, he was with the University of Duisburg-Essen, Germany, as a Visiting Student. He was a Project Scientist with the University of California at Santa Barbara, Santa Barbara. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Clemson University. His current research interests include distributed control, optimization, and learning, with emphasis on privacy protection. He currently serves as an associate editor for IEEE Transactions on Control of Network systems and IEEE Transactions on Automatic Control.