2014 Conference on Decision and Control (CDC)
http://www.cds.caltech.edu/~murray/papers/mm14-cdc.html

Privacy Preserving Average Consensus

Yilin Mo*, Richard M. Murray*

***Abstract*— Average consensus is a widely used algorithm for distributed computing and control, where all the agents in the network constantly communicate and update their states in order to achieve an agreement. This approach could result in an undesirable disclosure of information on the initial state of agent i to the other agents. In this paper, we propose a privacy preserving average consensus algorithm to guarantee the privacy of the initial state and the convergence of the algorithm to the exact average of the initial values, by adding and subtracting random noises to the consensus process. We characterize the mean square convergence rate of our consensus algorithm and derive upper and lower bounds for the covariance matrix of the maximum likelihood estimate on the initial state. A numerical example is provided to illustrate the effectiveness of the proposed design.**

I. Introduction

Consensus has been an active research area over the past decades. Early researches use consensus to model and analyze phenomena such as agreement of opinions by a group of individuals [1] and decision making by decentralized processors [2]. Applications of distributed averaging algorithms include dynamic load balancing [3], coordination of groups of mobile autonomous agents [4] and cooperative control of vehicle formations [5]. A survey of theory and applications of consensus problems in networked systems can be found in [6]. Consensus problems in the context of distributed signal processing applications, such as distributed parameter estimation, source localization and distributed compression have been reviewed in [7].

One commonly adopted consensus scheme is the deterministic average consensus algorithm, where each agent communicates with a fixed set of neighbors and follows a time-invariant update algorithm to reach the average of their initial values. In this approach, if one agent knows the update rules of all the other agents, then under some observability conditions, it can infer the entire trajectory of state of the others. This may turn out to be desirable for some applications, such as malicious intrusion detection and identification [8] and finite-step consensus [9], [10]. However, it also implies that the exact initial value of one agent may be computable by the other agents, which results in a disclosure of information. For privacy concerns, the participating agents may not want to release more information on its initial value than strictly necessary to reach the average consensus. For example, in social networks, a group of individuals can employ consensus algorithm to compute the common opinion on a subject [1]. However, they may not want to reveal their exact personal opinion on the subject. Another application is the multi-agent rendezvous problem [11], where a group of agents want to eventually rendezvous at a certain location. In this application, the participating agents may want to keep their initial location secret to the others.

In the database literature, the concept of differential privacy [12] has been extensively studied in the recent years. A widely adopted differentially private mechanism is to return a randomized answer to any database query to guarantee that the data from any individual participant of the database will only marginally change the distribution of the randomized answer [13]. Recently, the concept of differential privacy has been applied in dynamical systems. In [14], the authors consider the design of differentially private filters for dynamical system by adding white Gaussian perturbations to the system. Xue et al. [15] consider the privacy problem autonomous vehicle networks with a canonical Double-Integrator-Network model. In the context of consensus problem, Huang et al. [16] propose a differentially private consensus algorithm, where an independent and exponentially decaying Laplacian noise process is added to the consensus computation. However, their consensus algorithm does not converge to the *exact* average of the initial value, but to a randomized value. As a result, it cannot be applied to the case where the exact average consensus is required. Manitara and Hadjicostis [17] propose a privacy preserving average consensus scheme by adding correlated noise and discuss whether the initial state of one agent can be perfectly inferred by the other agents. However, they do not provide a quantitative result on how good the initial state can be estimated.

In this paper, we propose a privacy preserving average consensus algorithm, which computes the *exact* average of the initial values and ensures that the initial value of an agent cannot be perfectly inferred by the other participating agents. We further derive upper and lower bounds on the estimation performance of any agent on the initial states.

The rest of the paper is organized as follows: in Section II, we provide a brief introduction of the average consensus algorithm. A privacy preserving average consensus algorithm is proposed in Section III and its properties are proved in Section IV.An illustrative example on a simple network is presented in Section V. Finally, Section VI concludes the paper.

Notations: $\mathbb{N}_0$ is the set of non-negative integers. $\mathbb{R}^{n\times m}$ is the set of n by m matrices. $\mathbb{S}^n$ is the set of n by n symmetric matrices. The ith diagonal entry of the matrix X is denoted as X_{ii}. All the comparisons between matrices in this article are in positive semidefinite sense. range(X) is

*: Yilin Mo and Richard M. Murray are with the Control and Dynamical Systems Department of California Institute of Technology. Email: yilinmo@caltech.edu, murray@cds.caltech.edu

This work is supported in part by IBM and UTC through iCyPhy consortium.

the column space of the matrix X. $\|v\|$ indicates the 2-norm of the vector v, while $\|X\|$ is the largest singular value of the matrix X. For a matrix-valued function $X(k) : \mathbb{N}_0 \to \mathbb{S}^n$, $X(k) = O(f(k)I)$ if there exists an $M > 0$, such that $X(k) \leq Mf(k)I$ for large enough ks. Furthermore, $X(k) = \Theta(f(k)I)$ if there exist $M_1, M_2 > 0$, such that $M_1 f(k)I \leq X(k) \leq M_2 f(k)I$ for large enough ks.

II. Preliminaries

In this section we briefly introduce the average consensus algorithm, the notation of which will be used later in the paper.

We model a network composed of n agents as a graph $G = \{V, E\}$. $V = \{1, 2, \ldots, n\}$ is the set of vertices representing the agents. $E \subseteq V \times V$ is the set of edges. $(i, j) \in E$ if and only if agent i and j can communicate directly with each other. In this paper we always assume that G is *undirected and connected*. The neighborhood of agent i is defined as

$$\mathcal{N}(i) \triangleq \{j \in V : (i, j) \in E,\, j \neq i\}.$$

Suppose that each agent has an initial scalar state $x_i(0)$. At each iteration, agent i will communicate with its neighbors and update its state according to the following equation:

$$x_i(k+1) = a_{ii}x_i(k) + \sum_{j \in \mathcal{N}(i)} a_{ij}x_j(k). \tag{1}$$

Define $x(k) \triangleq [x_1(k), \ldots, x_n(k)]' \in \mathbb{R}^n$ and $A \triangleq [a_{ij}] \in \mathbb{R}^{n \times n}$. The update equation (1) can be written in matrix form as

$$x(k+1) = Ax(k). \tag{2}$$

In the rest of the paper, A is assumed to be *symmetric*. Define the essential neighborhood $\mathcal{N}_e(i)$ of an agent i to be the set of neighboring agents whose information is used to compute (1), i.e.,

$$\mathcal{N}_e(i) \triangleq \{j \in \mathcal{N}(i) : a_{ij} \neq 0\}. \tag{3}$$

Furthermore, define the average vector and the error vector to be

$$\bar{x} \triangleq \frac{\mathbf{1}'x(0)}{n}\mathbf{1},\; z(k) \triangleq x(k) - \bar{x}.$$

where $\mathbf{1} \in \mathbb{R}^n$ is a vector whose elements are all ones. The goal of the average consensus is to guarantee that $z(k) \to 0$ as $k \to \infty$ through the update equation (2). Let us arrange the eigenvalues of A in the decreasing order as $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n$. It is well known that the following conditions are necessary and sufficient in order to achieve average consensus from any initial condition $x(0)$:

(A1) $\lambda_1 = 1$ and $|\lambda_i| < 1$ for all $i = 2, \ldots, n$.
(A2) $A\mathbf{1} = \mathbf{1}$, i.e., $\mathbf{1}$ is an eigenvector of A.

For the rest of the paper, we assume that A satisfies assumption (A1) and (A2).

III. Problem Formulation

One issue for the average consensus algorithm is that an agent in the network could potentially infer the other agents' exact initial condition $x_i(0)$s, which may not be desirable when privacy is of concern.

To avoid privacy breaches while enforcing that $x(k)$ converges to $\bar{x}$, we propose the following privacy preserving average consensus algorithm:

1) At time k, each agent generates a standard normal distributed random variable $v_i(k)$ with mean 0 and variance 1. We assume that all the random variables $\{v_i(k)\}_{i=1,\ldots,n,\, k=0,1,\ldots}$ are jointly independent.
2) Each agent then adds a random noise $w_i(k)$ to its state $x_i(k)$, where

$$w_i(k) = \begin{cases} v_i(0) & \text{, if } k = 0 \\ \varphi^k v_i(k) - \varphi^{k-1} v_i(k-1) & \text{, otherwise} \end{cases}, \tag{4}$$

where $0 < |\varphi| < 1$ is a constant for all agents. Define the new state to be $x_i^+(k)$, i.e.,

$$x_i^+(k) = x_i(k) + w_i(k). \tag{5}$$

3) Each agent then communicates with its neighbors and update its state to the average value, i.e.,

$$x_i(k+1) = a_{ii}x_i^+(k) + \sum_{j \in \mathcal{N}(i)} a_{ij}x_j^+(k). \tag{6}$$

Define

$$w(k) \triangleq [w_1(k), \ldots, w_n(k)]' \in \mathbb{R}^n, \tag{7}$$
$$v(k) \triangleq [v_1(k), \ldots, v_n(k)]' \in \mathbb{R}^n, \tag{8}$$
$$x^+(k) \triangleq [x_1^+(k), \ldots, x_n^+(k)]' \in \mathbb{R}^n. \tag{9}$$

We can write (5) and (6) in matrix form as

$$x(k+1) = Ax^+(k) = A(x(k) + w(k)). \tag{10}$$

Remark 1. *We choose the variance of $v_i(k)$ to be 1 to simplify the notations. With proper scaling, all the results in this article hold when Var$(v_i(k)) = \sigma^2$.*

Without loss of generality, we only consider the case where agent n wants to infer the other agents' initial conditions. Denote the neighborhood of agent n as

$$\mathcal{N}(n) = \{j_1, \ldots, j_m\}.$$

Define

$$C \triangleq \begin{bmatrix} e_{j_1} & \ldots & e_{j_m} & e_n \end{bmatrix}' \in \mathbb{R}^{(m+1) \times n}, \tag{11}$$

where e_i denotes the ith canonical basis vector in $\mathbb{R}^n$ with a 1 in the ith entry and zeros elsewhere. The information set of agent n at time k can be defined as

$$\mathcal{I}(k) \triangleq \{x_n(0), y(0), \ldots, y(k)\}, \tag{12}$$

where

$$y(k) \triangleq Cx^+(k) = C(x(k) + w(k)). \tag{13}$$

Notice that $x_n(k+1), k = 0, 1, \ldots$ is not included in the information set since it can be directly computed from $y(k)$

using (6). We assume that agent n knows the A and C matrices and all the variables in $\mathcal{I}(k)$ at time k.

Remark 2. *Without the additional noise, i.e., $w(k) = 0$, the consensus algorithm is deterministic and agent n can perfectly infer $\zeta' x(0)$, given that $\zeta \in \mathbb{R}^n$ lies in the observable space of (A, C), which illustrates the necessity of the added noise.*

Denote the maximum likelihood estimate of $x(0)$ given $\mathcal{I}(k)$ as $\hat{x}(0|k)$, the variance of which is defined as $P(k)$. Since $\mathcal{I}(k) \subset \mathcal{I}(k+1)$, we have the following proposition:

Proposition 1. *$P(k)$ is monotonically non-increasing, i.e., $P(k_2) \leq P(k_1)$ if $k_1 \leq k_2$.*

Hence, the following limit is well defined:

$$P \triangleq \lim_{k\to\infty} P(k). \tag{14}$$

Since the noises $v_i(k)$ are independently Gaussian distributed, the maximum likelihood estimator is the minimum variance unbiased estimator. As a result, the matrix P determines the fundamental limit on how accurate $x(0)$ can be estimated by agent n. Thus, to preserve the privacy of the initial condition $x(0)$, we need to ensure that P is sufficiently large.

IV. Main Results

In this section, we first characterize the convergence rate of the privacy preserving average consensus algorithm. We then provide upper and lower bounds on the estimation performance P.

A. Convergence Rate

We consider the impact of the added noise $w(k)$ on the performance of the consensus algorithm. Let us define the mean square convergence rate ρ of our consensus algorithm as

$$\rho \triangleq \lim_{k\to\infty} \left(\sup_{z(0)\neq 0} \frac{\mathbb{E}_v z(k)'z(k)}{z(0)'z(0)} \right)^{1/k}, \tag{15}$$

whenever the limit on the RHS exists. The notation $\mathbb{E}_v$ indicates the expectation over noise process $\{v_i(k)\}$. The following theorem establish the convergence properties of $x(k)$:

Theorem 1. *For any initial condition $x(0)$, $x(k)$ converges to $\bar{x}$ in the mean square sense. Furthermore, the mean square convergence rate ρ equals*

$$\rho = \max(|\varphi|^2, |\lambda_2|^2, |\lambda_n|^2). \tag{16}$$

The following lemma is needed to prove Theorem 1:

Lemma 1. *Define matrix $\mathcal{A}$ to be*

$$\mathcal{A} \triangleq A - \mathbf{1}\mathbf{1}'/n.$$

The following equalities hold for all $k \geq 0$

$$A^k(A - I) = \mathcal{A}^k(A - I), \tag{17}$$

$$A^k - \mathbf{1}\mathbf{1}'/n = \mathcal{A}^k(I - \mathbf{1}\mathbf{1}'/n). \tag{18}$$

Proof. The lemma can be proved by diagonalizing A and $\mathcal{A}$. The detailed proof is omitted due to space limit. □

Proof of Theorem 1. Since $\max(|\varphi|^2, |\lambda_2|^2, |\lambda_n|^2) < 1$, we only need to prove (16). By (10),

$$x(k) = A^k x(0) + \sum_{t=0}^{k-1} A^{k-t} w(t)$$

$$= A^k x(0) + \sum_{t=0}^{k-2} \varphi^t A^{k-t-1}(A - I)v(t) + A\varphi^{k-1} v(k-1).$$

Since $\bar{x} = (\mathbf{1}\mathbf{1}'/n)x(0)$, by Lemma 1, we have

$$z(k) = \mathcal{A}^k z(0) + \sum_{t=0}^{k-2} \varphi^t \mathcal{A}^{k-t-1}(A-I)v(t) + A\varphi^{k-1}v(k-1). \tag{19}$$

The result of the proof can be derived by analyzing the RHS of (19) and is omitted due to space limit. □

B. Estimation Performance

In this subsection, we provide upper and lower bounds on P. Notice that our goal is not to design an estimator for agent n, but rather to prove a fundamental limitation on the performance for all possible unbiased estimators, which guarantees the privacy of $x(0)$. We first reduce the state space by removing $x_n(k)$, since it is always known to agent n. To this end, let us define $\tilde{A} \in \mathbb{R}^{(n-1)\times(n-1)}$ as a principal minor of A by removing the last row and column. As a result, the matrix A can be written as

$$A = \begin{bmatrix} \tilde{A} & \zeta \\ \zeta' & a_{nn} \end{bmatrix}, \tag{20}$$

where $\zeta \in \mathbb{R}^{n-1}$. The following lemma characterize the stability of $\tilde{A}$, which can be proved using Cauchy's interlacing theorem. The detailed proof is omitted due to space limit.

Lemma 2. *$\tilde{A}$ is strictly stable, i.e., $\|\tilde{A}\| < 1$. Furthermore, for any i, $\tilde{A}_{ii} < 1$.*

Let us further define

$$\tilde{v}(k) \triangleq \begin{bmatrix} v_1(k) & \dots & v_{n-1}(k) \end{bmatrix}' \in \mathbb{R}^{n-1}, \tag{21}$$

$$\tilde{w}(k) \triangleq \begin{bmatrix} w_1(k) & \dots & w_{n-1}(k) \end{bmatrix}' \in \mathbb{R}^{n-1}, \tag{22}$$

$$\tilde{C} \triangleq \begin{bmatrix} \tilde{e}_{j_1} & \dots & \tilde{e}_{j_m} \end{bmatrix}' \in \mathbb{R}^{m\times(n-1)}, \tag{23}$$

where $\tilde{e}_i$ denotes the ith canonical basis vector in $\mathbb{R}^{n-1}$. We define the reduced state vector $\tilde{x}(k) \in \mathbb{R}^{n-1}$, which satisfies the following update equation:

$$\tilde{x}(k+1) = \tilde{A}(\tilde{x}(k) + \tilde{w}(k)), \tag{24}$$

with initial condition

$$\tilde{x}(0) \triangleq \begin{bmatrix} x_1(0) & \dots & x_{n-1}(0) \end{bmatrix}' \tag{25}$$

Finally, the reduced measurement $\tilde{y}(k) \in \mathbb{R}^m$ is defined as

$$\tilde{y}(k) \triangleq \tilde{C}(\tilde{x}(k) + \tilde{w}(k)). \tag{26}$$

Remark 3. *It is worth noticing that in general,* $\tilde{x}(k) \neq \begin{bmatrix} x_1(k) & \dots & x_{n-1}(k) \end{bmatrix}'$.

Throughout the subsection, we assume that $(\tilde{A}, \tilde{C})$ is *observable*. Otherwise, one can always perform a Kalman decomposition and consider only the observable subspace. Define the information set based on the reduced measurements

$$\tilde{\mathcal{I}}(k) \triangleq \{x_n(0), w_n(0), w_n(k), \tilde{y}(0), \dots, \tilde{y}(k)\}. \tag{27}$$

The following theorem establishes the equivalence between information set $\mathcal{I}(k)$ and $\tilde{\mathcal{I}}(k)$, the proof of which is omitted due to space limit.

Theorem 2. *For any* $k \geq 0$*, there exists an invertible linear transformation from the row vector*

$$\begin{bmatrix} x_n(0) & y(0)' & \dots & y(k)' \end{bmatrix}$$

to the row vector

$$\begin{bmatrix} x_n(0) & w_n(0) & \dots & w_n(k) & \tilde{y}(0)' & \dots & \tilde{y}(k)' \end{bmatrix}.$$

By Theorem 2, $\tilde{\mathcal{I}}(k)$ is a sufficient statistic for estimating $x(0)$. It is easy to see that $\{\tilde{y}(0), \dots, \tilde{y}(k)\}$ is a sufficient statistics for estimating $\tilde{x}(0)$. Therefore, let us define $\tilde{P}(k)$ as the covariance of the maximum likelihood estimate of $\tilde{x}(0)$ given $\tilde{y}(0), \dots, \tilde{y}(k)$. Since $x_n(0)$ is known to agent n, we have the following proposition:

Proposition 2.

$$P(k) = \begin{bmatrix} \tilde{P}(k) & \mathbf{0} \\ \mathbf{0}' & 0 \end{bmatrix},$$

where $\mathbf{0} \in \mathbb{R}^{n-1}$ *is an all zero vector.*

We now try to explicitly write down the relationship between $\tilde{x}(0)$ and $\tilde{y}(k)$. By definition,

$$\tilde{y}(k) = \tilde{C}\left(\tilde{A}^k \tilde{x}(0) + \sum_{t=0}^{k} \tilde{A}^{k-t} \tilde{w}(t)\right).$$

As a result

$$\sum_{t=0}^{k} \tilde{y}(k) = \tilde{C}(I - \tilde{A}^{k+1})(I - \tilde{A})^{-1}\tilde{x}(0) + \sum_{t=0}^{k} \tilde{A}^{k-t}\varphi^t \tilde{v}(t),$$

which implies that

$$\begin{bmatrix} \sum_{t=0}^{0} \tilde{y}(t)/\varphi^0 \\ \sum_{t=0}^{1} \tilde{y}(t)/\varphi^1 \\ \vdots \\ \sum_{t=0}^{k} \tilde{y}(t)/\varphi^k \end{bmatrix} = H(k)\tilde{x}(0) + F(k) \begin{bmatrix} \tilde{v}(0) \\ \tilde{v}(1) \\ \vdots \\ \tilde{v}(k) \end{bmatrix}, \tag{28}$$

where

$$H(k) \triangleq \begin{bmatrix} \tilde{C}(I - \tilde{A})^{-1}/\varphi^0 \\ \tilde{C}(I - \tilde{A})^{-1}/\varphi^1 \\ \vdots \\ \tilde{C}(I - \tilde{A})^{-1}/\varphi^k \end{bmatrix} - \begin{bmatrix} \tilde{C}\tilde{A}(\tilde{A}/\varphi)^0(I - \tilde{A})^{-1} \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^1(I - \tilde{A})^{-1} \\ \vdots \\ \tilde{C}\tilde{A}(\tilde{A}/\varphi)^k(I - \tilde{A})^{-1} \end{bmatrix}, \tag{29}$$

and

$$F(k) \triangleq \begin{bmatrix} \tilde{C} & & & \\ \tilde{C}\tilde{A}/\varphi & \tilde{C} & & \\ \vdots & \vdots & \ddots & \\ \tilde{C}(\tilde{A}/\varphi)^k & \tilde{C}(\tilde{A}/\varphi)^{k-1} & \dots & \tilde{C} \end{bmatrix}. \tag{30}$$

Hence, the covariance $\tilde{P}(k)$ of the maximum likelihood estimate [18] is given by

$$\tilde{P}(k) = \left[H(k)'(F(k)F(k)')^{-1}H(k)\right]^{-1}. \tag{31}$$

Assume that the eigenvectors of the symmetric matrix $(I - \tilde{A})^{-1}\tilde{C}'\tilde{C}(I - \tilde{A})^{-1}$ are $\psi_1, \dots, \psi_{n-1} \in \mathbb{R}^{n-1}$. Without loss of generality, we assume that $\{\psi_1, \dots, \psi_{n-1}\}$ forms an orthonormal basis of $\mathbb{R}^{n-1}$. Furthermore, by Lemma 2 and (23), we know that

$$\text{rank}\left[(I - \tilde{A})^{-1}\tilde{C}'\tilde{C}(I - \tilde{A})^{-1}\right] = m.$$

Hence, without loss of generality we assume that the eigenvalues corresponding to the eigenvectors $\{\psi_1, \dots, \psi_m\}$ are non-zero and the eigenvalues corresponding to $\{\psi_{m+1}, \dots, \psi_{n-1}\}$ are zero. Define the orthogonal matrix

$$\mathcal{Q} \triangleq \begin{bmatrix} \mathcal{Q}_1 & \mathcal{Q}_2 \end{bmatrix} \in \mathbb{R}^{(n-1)\times(n-1)}, \tag{32}$$

where

$$\mathcal{Q}_1 \triangleq \begin{bmatrix} \psi_1 & \dots & \psi_m \end{bmatrix} \in \mathbb{R}^{(n-1)\times m}, \tag{33}$$

$$\mathcal{Q}_2 \triangleq \begin{bmatrix} \psi_{m+1} & \dots & \psi_{n-1} \end{bmatrix} \in \mathbb{R}^{(n-1)\times(n-m-1)}. \tag{34}$$

The following theorem provides upper and lower bounds on $\tilde{P}$ by exploring the structure of $F(k)$ and $H(k)$ matrices. The proof is reported in the appendix.

Theorem 3. *If* $1 > \varphi > \|\tilde{A}\|$*, then*

$$\left(1 + \frac{\|\tilde{A}\|}{\varphi}\right)^{-2} \Delta \leq \tilde{P} \leq \left(1 - \frac{\|\tilde{A}\|}{\varphi}\right)^{-2} \Delta \tag{35}$$

where

$$\Delta \triangleq \mathcal{Q}_2\left[\mathcal{Q}_2'(I - \tilde{A})^{-1}\mathcal{X}(I - \tilde{A})^{-1}\mathcal{Q}_2\right]^{-1}\mathcal{Q}_2', \tag{36}$$

and $\mathcal{X}$ *is the unique solution of the following Lyapunov equation*

$$\mathcal{X} = \tilde{A}\mathcal{X}\tilde{A}/\varphi^2 + \tilde{A}\tilde{C}'\tilde{C}\tilde{A}. \tag{37}$$

Combining with Proposition 2, we have the following corollary:

Corollary 1.

$$\left(1 + \frac{\|\tilde{A}\|}{\varphi}\right)^{-2} \begin{bmatrix} \Delta & \mathbf{0} \\ \mathbf{0}' & 0 \end{bmatrix} \leq P \leq \left(1 - \frac{\|\tilde{A}\|}{\varphi}\right)^{-2} \begin{bmatrix} \Delta & \mathbf{0} \\ \mathbf{0}' & 0 \end{bmatrix}$$

It is worth noticing that $\text{rank}(P) = n - m - 1$, which implies that agent n can perfectly infer some linear combinations of the initial state. The following theorem provides a

topological condition on the computability of $x_i(0)$ for agent n:

Theorem 4. *$P_{ii} = 0$ if and only if $i = n$ or $\mathcal{N}_e(i) \bigcup \{i\} \subseteq \mathcal{N}(n) \bigcup \{n\}$.*

Proof. Consider the case where $i \neq n$. By Corollary 1, $P_{ii} = 0$ is equivalent to

$$\tilde{e}_i' \Delta \tilde{e}_i = 0, \tag{38}$$

where $\tilde{e}_i$ is the ith canonical basis vector. Since $(\tilde{A}, \tilde{C})$ is observable, $\mathcal{X}$ is full rank. Hence, (38) is equivalent to $\mathcal{Q}_2' \tilde{e}_i = 0$. As a result, $\tilde{e}_i$ belongs to the null space of $\mathcal{Q}_2'$, which is also the column space of $\mathcal{Q}_1$ and $(I - \tilde{A})^{-1}\tilde{C}'$ matrices. Therefore,

$$\tilde{e}_i - \tilde{A}\tilde{e}_i \in \text{range}(\tilde{C}').$$

By (23), a vector $v \in \text{range}(\tilde{C}')$ if and only if $v_j = 0$ for all $j \notin \mathcal{N}(n)$. By Lemma 2, the jth entry of $\tilde{e}_i - \tilde{A}\tilde{e}_i$ is 0 if and only if $j \notin (\mathcal{N}_e(i) \bigcup \{i\}) \setminus \{n\}$. Hence, $P_{ii} = 0$ is equivalent to $\mathcal{N}_e(i) \bigcup \{i\} \subseteq \mathcal{N}(n) \bigcup \{n\}$. □

By Theorem 4, as long as agent n cannot listen to agent i and all its essential neighbors, agent n cannot estimate the initial condition $x_i(0)$ perfectly. As a result, to enforce privacy, we should enforce that for any pair of agents i and j, the following holds:

$$\mathcal{N}_e(i) \bigcup \{i\} \nsubseteq \mathcal{N}(j) \bigcup \{j\}. \tag{39}$$

V. Numerical Examples

We consider the following network consisted of 4 agents:

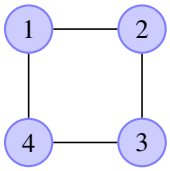

Fig. 1. Network Topology

Assume that $a_{ii} = a_{ij} = 1/3$ for all $j \in \mathcal{N}(i)$. Hence, $\|\tilde{A}\| = 0.805$. As a result, we choose $\varphi = 0.9 > \|\tilde{A}\|$. Fig 2 illustrates the trajectory of $x_i(k)$. It is worth noticing that all $x_i(k)$s converge to the true average of the initial condition $x(0)$.

Fig 3 shows $P_{ii}(k)$ of the maximum likelihood estimate of agent 4. $P_{33}(k)$ is omitted since it equals $P_{11}(k)$ due to symmetry. Notice that both lower bounds of $P_{11}(k)$ and $P_{22}(k)$ are greater than 0. As a result, agent 4 cannot infer the exact initial condition of agent 1 or agent 2, which complies with Theorem 4. It is also worth noticing that the lower bounds are actually quite lose, which we plan to investigate in the future.

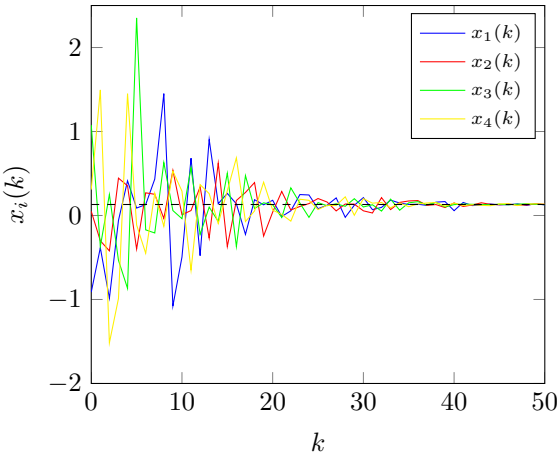

Fig. 2. The trajectory of each state $x_i(k)$. The blue, red, green, yellow lines correspond to $x_1(k), x_2(k), x_3(k), x_4(k)$ respectively. The black dashed line corresponds to the average value of the initial $x(0)$.

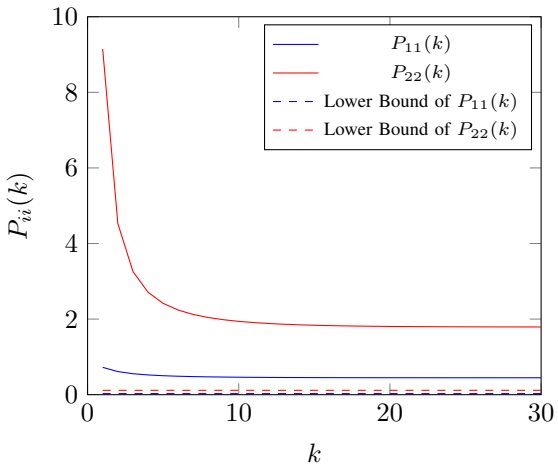

Fig. 3. $P_{ii}(k)$ v.s. k. The blue solid and dashed line correspond to $P_{11}(k)$ and the lower bound of $P_{11}(k)$ respectively. The red solid and dashed line correspond to $P_{22}(k)$ and the lower bound of $P_{22}(k)$ respectively.

VI. Conclusion and Future Work

In this paper, we propose a privacy preserving average consensus algorithm. We compute the exact mean square convergence rate of the proposed algorithm. Furthermore, we derive upper and lower bounds of the covariance matrix of the maximum likelihood estimate, which guarantees the privacy of the initial condition of agent i. Future research includes exploring other possible average consensus algorithms that preserves privacy and proving tighter bounds on the covariance matrix for the proposed algorithm.

Appendix I
Proof of Theorem 3

Several intermediate results are needed to prove Theorem 3:

Lemma 3. *If $\varphi > \|\tilde{A}\|$, then*

$$\left(1 - \frac{\|\tilde{A}\|}{\varphi}\right)^2 I \leq (F(k)F(k)')^{-1} \leq \left(1 + \frac{\|\tilde{A}\|}{\varphi}\right)^2 I.$$

Proof. The lemma can be proved using the same technique in the proof of Lemma 1 in [19] and is hence omitted due to space limit. □

We are now ready to prove Theorem 3

Proof of Theorem 3. By Lemma 3, we only need to prove that

$$\Delta = \lim_{k\to\infty} \left[H(k)'H(k)\right]^{-1}, \tag{40}$$

Let us write $\mathcal{Q}'H(k)'H(k)\mathcal{Q}$ as

$$\mathcal{Q}'H(k)'H(k)\mathcal{Q} = \begin{bmatrix} \mathcal{S}_{11}(k) & \mathcal{S}_{12}(k) \\ \mathcal{S}'_{12}(k) & \mathcal{S}_{22}(k) \end{bmatrix},$$

where

$$\mathcal{S}_{11}(k) = \mathcal{Q}'_1H(k)'H(k)\mathcal{Q}_1,\ \mathcal{S}_{22}(k) = \mathcal{Q}'_2H(k)'H(k)\mathcal{Q}_2,$$
$$\mathcal{S}_{12}(k) = \mathcal{Q}'_1H(k)'H(k)\mathcal{Q}_2.$$

Let us define

$$H_1(k) \triangleq \tilde{C}(I - \tilde{A})^{-1}/\varphi^k\mathcal{Q}_1,$$
$$H_2(k) \triangleq -\tilde{C}\tilde{A}(\tilde{A}/\varphi)^k(I - \tilde{A})^{-1}\mathcal{Q}_1,$$
$$H_3(k) \triangleq -\tilde{C}\tilde{A}(\tilde{A}/\varphi)^k(I - \tilde{A})^{-1}\mathcal{Q}_2.$$

Hence,

$$\mathcal{S}_{11}(k) = \sum_{t=0}^{k}(H_1(t) + H_2(t))'(H_1(t) + H_2(t)),$$
$$\mathcal{S}_{22}(k) = \sum_{t=0}^{k} H_3(t)'H_3(t),$$
$$\mathcal{S}_{12}(k) = \sum_{t=0}^{k}(H_1(t) + H_2(t))'H_3(t).$$

Now by matrix inversion lemma, we have

$$\mathcal{Q}'\left[H'(k)H(k)\right]^{-1}\mathcal{Q} = \begin{bmatrix} \mathcal{R}_{11}(k) & \mathcal{R}_{12}(k) \\ \mathcal{R}'_{12}(k) & \mathcal{R}_{22}(k) \end{bmatrix},$$

where

$$\mathcal{R}_{11}(k) = \left[\mathcal{S}_{11}(k) - \mathcal{S}_{12}(k)\mathcal{S}_{22}^{-1}(k)\mathcal{S}'_{12}(k)\right]^{-1},$$
$$\mathcal{R}_{22}(k) = \left[\mathcal{S}_{22}(k) - \mathcal{S}'_{12}(k)\mathcal{S}_{11}^{-1}(k)\mathcal{S}_{12}(k)\right]^{-1}.$$

By definition, $\mathcal{S}_{11}(k) = \Theta(\varphi^{-2k}I)$, $\mathcal{S}_{22}(k) = \Theta(I)$. Furthermore

$$\mathcal{S}_{12}(k)\mathcal{S}_{22}^{-1}(k)\mathcal{S}'_{12}(k) = \begin{cases} O\left[\left(\frac{\|\tilde{A}\|}{\varphi^2}\right)^{2k} I\right] & \text{, if } \|\tilde{A}\| > \varphi^2 \\ O(k^2 I) & \text{, if } \|\tilde{A}\| = \varphi^2 \\ O(I) & \text{, if } \|\tilde{A}\| < \varphi^2 \end{cases},$$

and $\lim_{k\to\infty} \mathcal{S}'_{12}(k)\mathcal{S}_{11}^{-1}(k)\mathcal{S}_{12}(k) = 0$. Therefore

$$\lim_{k\to\infty} \mathcal{R}_{11}(k) = 0,\ \lim_{k\to\infty} \mathcal{R}_{22}(k) = \left[\lim_{k\to\infty} \mathcal{S}_{22}(k)\right]^{-1}. \tag{41}$$

Since $\mathcal{Q}'\left[H'(k)H(k)\right]^{-1}\mathcal{Q} \geq 0$, by (41) we know that

$$\lim_{k\to\infty} \mathcal{R}_{12}(k) = 0.$$

One can verify that

$$\lim_{k\to\infty} \mathcal{S}_{22}(k) = \mathcal{Q}'_2(I - \tilde{A})^{-1}\mathcal{X}(I - \tilde{A})^{-1}\mathcal{Q}_2.$$

On the other hand, by (32), (36) is equivalent to

$$\mathcal{Q}'\Delta\mathcal{Q} = \begin{bmatrix} 0 & 0 \\ 0 & \left(\mathcal{Q}'_2(I - \tilde{A})^{-1}\mathcal{X}(I - \tilde{A})^{-1}\mathcal{Q}_2\right)^{-1} \end{bmatrix},$$

which finishes the proof. □

REFERENCES

[1] M. DeGroot, "Reaching a consensus," *Journal of the American Statistical Association*, vol. 69, no. 345, pp. 118–121, March 1974.

[2] J. Tsitsiklis, "Problems in decentralized decision making and computation," *Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge*, November 1984.

[3] G. Cybenko, "Dynamic load balancing for distributed memory multiprocessors," *Journal of parallel and distributed computing*, vol. 7, pp. 279–301, 1989.

[4] A. Jadbabaie, J. Lin, and A. S. Morse, "Coordination of groups of mobile autonomous agents using nearest neighbor rules," *IEEE Transactions on automatic control*, vol. 48, no. 6, pp. 988–1001, June 2003.

[5] W. Ren, R. Beard, and E. Atkins, "A survey of consensus problems in multi-agent coordination," in *American Control Conference*, June 2005, pp. 1859–1864.

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

[7] A. G. Dimakis, S. Kar, J. M. F. Moura, M. G. Rabbat, and A. Scaglione, "Gossip algorithms for distributed signal processing," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1847–1864, November 2010.

[8] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," vol. 57, no. 1, pp. 90–104, 2012.

[9] S. Sundaram and C. Hadjicostis, "Finite-time distributed consensus in graphs with time-invariant topologies," in *American Control Conference*, 2007, pp. 711–716.

[10] Y. Yuan, G.-B. Stan, L. Shi, M. Barahona, and J. Goncalves, "Decentralised minimum-time consensus," *Automatica*, vol. 49, no. 5, pp. 1227 – 1235, 2013.

[11] J. Lin, A. S. Morse, and B. D. Anderson, "The multi-agent rendezvous problem," in *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, vol. 2. IEEE, 2003, pp. 1508–1513.

[12] C. Dwork, "Differential privacy," in *Automata, languages and programming*. Springer, 2006, pp. 1–12.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Springer, 2006, pp. 265–284.

[14] J. Le Ny and G. Pappas, "Differentially private filtering," *Automatic Control, IEEE Transactions on*, vol. 59, no. 2, pp. 341–354, Feb 2014.

[15] M. Xue, W. Wang, and S. Roy, "Security concepts for the dynamics of autonomous vehicle networks," *Automatica*, vol. 50, no. 3, pp. 852–857, 2014.

[16] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*. ACM, 2012, pp. 81–90.

[17] N. Manitara and C. Hadjicostis, "Privacy-preserving asymptotic average consensus," in *Control Conference (ECC), 2013 European*, 2013, pp. 760–765.

[18] L. L. Scharf, *Statistical signal processing*. Addison-Wesley Reading, MA, 1991, vol. 98.

[19] Y. Mo and B. Sinopoli, "Kalman filtering with intermittent observations: Tail distribution and critical value," vol. 57, no. 3, pp. 677–689, 2012.