Differentially Private Discrete-Time Second-Order Consensus under Directed Topologies

Mengzhou Ma, Chengcheng Zhao, and Jianping He

Abstract— **This paper considers the privacy protection of discrete-time second-order consensus under a directed communication topology in multi-agent systems. To protect the initial states of agents, random noise with exponentially decaying variance is added to the communication states at each iteration. We provide sufficient and necessary conditions under which consensus can be maintained, and specify the convergence rate. We analyze the level of privacy protection based on differential privacy and derive certain boundaries of privacy degrees when Laplacian or Gaussian noise is added. The definition of (b, r)-accuracy shows the lower bound $1 - b$ of probability that the absolute position deviation from the original trajectory without noise is within r. It is used to characterize the system accuracy, and then the accuracy level is given. Simulations are conducted to validate the correctness of the obtained results.**

I. Introduction

Over the past decades, consensus problems in multi-agent systems have attracted great attention for various applications and theoretical challenges. Early works on consensus with first-order dynamics can be found in [1], [2]. Also, there have been increasing interests in the second-order consensus [3]. Existing researches include the performance analysis and controller design for different situations such as convergence evaluation, adaptive controller design and consensus validation under a dynamic topology [4]–[7]. Typically, to reach consensus, each agent follows a time-invariant update algorithm and updates the next state with a combination of information transmitted from neighbour nodes. Complex interaction and communication between agents will bring the risk of private information leakage with undesired consequences. Even if agents are trustworthy, a potential malicious attacker eavesdropping on the messages exchange among agents can estimate the topology and other important system information [8], [9].

Therefore, privacy protection has been focused on in consensus-based network systems [10]–[12]. For example, Huang et al. introduced the private consensus by presenting a server-based and a completely distributed randomized mechanism respectively [13]. [14] proposed an algorithm to guarantee the privacy of the initial condition in the first-order consensus, and meanwhile this algorithm was proved to achieve minimum privacy breach. [15] presented a novel approach that enabled secure and privacy-preserving average consensus in a decentralized architecture in the absence of any trusted third-party. In addition to the first-order consensus, a PPMC algorithm which protected the privacy of maximum consensus was proposed and its convergence time and privacy degree were given in [16].

Although there have been numerous researches on privacy-preserving first-order consensus, privacy concerns about the second-order consensus remain to be a challenging problem. It is noted that second-order consensus has higher dimensions of state space. Besides, the input of second-order consensus is acceleration rather than the velocity, which means the privacy mechanisms' influence is coupled in velocity, position and acceleration. Considering the challenges above, we focus on the privacy protection of second-order consensus. [17] explored a Paillier encryption for consensus-based systems with second-order dynamics. A privacy-preserving second-order consensus(PPSC) protocol was proposed in [18], and its asymptotic convergence rate and privacy level based on (ε, δ)- data-privacy were given. In addition to the privacy notions in the literature, differential privacy with rigorous properties including resilience to postprocessing and side information is well-suited for multi-agent scenarios. And adding noise is a better option than encryption algorithms considering the additional computational complexity introduced by calculating keys. Thus, A privacy-preserving second-order consensus algorithm based on differential privacy is proposed in this paper. However, noise adding mechanism in this approach will influence the certainty of state information and result in the trajectory deviation. Then evaluating the necessary and sufficient conditions of convergence, privacy degree and accuracy to guarantee the effectiveness of this method is significant and challenging.

In this paper, we aim to study the privacy protection of second-order consensus under a directed topology. A privacy-preserving second-order consensus algorithm is proposed. And its properties such as convergence, privacy, and accuracy of the algorithm are explored. Specifically, the main contributions of this work are summarized as follows.

- We consider the problem of privacy protection in discrete-time second-order consensus. Random noise is added to preserve initial states. Sufficient and necessary conditions to guarantee the convergence are provided, and the convergence rate is specified.
- Based on differential privacy, the privacy protection

This work was supported by in part by the Natural Science Foundation of China (NSFC) under Grants 61973218 and 61903328, and in part by the China Postdoctoral Science Foundation under Grant 2019M652082.

Mengzhou Ma and Jianping He are with the Department of Automation, Shanghai Jiao Tong University, and Key Laboratory of System Control and Signal Processing, Ministry of Education of China, Shanghai 200240, China. E-mail: mamengzhou@sjtu.edu.cn, jphe@sjtu.edu.cn.

Chengcheng Zhao is with The State Key Laboratory of Industrial Control Technology and Institute of Cyberspace Research, Zhejiang University, China, and the Department of Electrical and Computer Engineering, University of Victoria, BC, Canada. E-mail: zccsq90@gmail.com.

978-1-7281-9093-8/20/$31.00 ©2020 IEEE

level of privacy-preserving second-order consensus algorithm is analyzed. Certain boundaries of privacy degrees are given when Gaussian or Laplacian noise is added.

- The system accuracy is characterized by exploring the definition of (b, r)-accuracy. The lower bound of probability that the position deviation of agents under privacy-preserving second-order consensus algorithm from the original position is within a certain range depends on the variance parameters of noise.

The remainder of this paper is organized as follows. Section II gives some preliminaries on second-order consensus and the privacy mechanism. Section III shows the main results. Simulations to validate our results are given in Section IV. Section V provides the conclusion.

II. Preliminaries

Consider a multi-agent system with $n+1$ nodes having unique ID $1, 2, \cdots, n+1$. A digraph $\mathcal{G} = (\mathcal{V}, \mathcal{A})$ is used to model a multi-agent system, where $\mathcal{V}=\{1, 2, \cdots, n+1\}$ is the set of nodes and $\mathcal{A} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges. We have $(i, j) \subset \mathcal{A}$ if and only if(iff) agent i can get information from agent j. Let A and D be the adjacent matrix and degree matrix of the graph respectively. The elements of A is defined as a_{ij}.If the node i can obtain information from the node j, $a_{ij} = 1$, and $a_{ij} = 0$ otherwise. Then, we can denote the Laplacian matrix by $L = D - A$.

A. Leader-following Second-order Consensus

The second-order dynamic of each node i, $\forall i \in \mathcal{V}$, is

$$\dot{x}_i = v_i, \dot{v}_i = u_i \tag{1}$$

with position $x_i \in \mathbb{R}$, speed $v_i \in \mathbb{R}$, and the acceleration input $u_i \in \mathbb{R}$. Given the sampling time τ, by first-order holder, we get the discrete-time model of (1) as

$$\begin{cases} x_i(k+1) = x_i(k) + \tau v_i(k), \\ v_i(k+1) = v_i(k) + \tau u_i(k). \end{cases}$$

We consider the second-order consensus in leader-following formation control, which has wide applications [19]. Assume that there are n followers and 1 leader in the system. Let the desired relative position that node i should keep to the leader (node $n+1$) in formation as $\Delta x_i = x_i - x_{n+1}$. To simplify the model, we assume the acceleration of the leader is zero. Referring to [20], the second-order consensus control law for agent i ($i \in \mathcal{V}$, $i \neq n+1$) is

$$\begin{aligned} u_i(k) = -\sum_{j=1}^{n+1} a_{ij}[&\gamma_1(v_i(k) - v_j(k)) + \gamma_0(x_i(k) - x_j(k)) \\ &-\gamma_0(\Delta x_i - \Delta x_j)], \end{aligned} \tag{2}$$

where γ_0 and γ_1 are positive control gains. Let $\otimes$ denote Kronecker product, I_y be the y-dimensional identity matrix. We denote the state vector of agent i be $z_i(k) = [\; x_i(k) \quad v_i(k) \;]^\top$ and $z = [\; z_1^\top \quad z_2^\top \quad \cdots \quad z_{n+1}^\top \;]^\top$, where $\cdot^\top$ denotes the tranpose of a vector or matrix. Then, the leader-following second-order consensus algorithm is described by

$$z(k+1) = Qz(k) + \Phi, \tag{3}$$

where $Q = I_{2n+2} + \tau[(I_{n+1} \otimes \tilde{A}) - \gamma_0 L \otimes \tilde{B}K]$, $K = [\; 1 \quad \frac{\gamma_1}{\gamma_0} \;]$, and

$$\tilde{A} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \tilde{B} = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

$$\Phi = [\; 1 \quad \cdots \quad 1 \;]_{n+1}^\top \otimes \left[\tau\gamma_0 \cdot \tilde{B} \sum_{j=1}^{n+1} a_{ij}(\Delta x_i - \Delta x_j) \right].$$

If adversaries are able to eavesdrop the communicated information, and get to know the updated rule (3), the initial states of agents will be disclosed and then trajectory will be tracked by adversaries. Therefore, we try to keep the initial states secret from others during the evolution of networks.

B. Differential Privacy and Accuracy

We introduce the notion of differential privacy proposed by Dwork et al. [21], [22]. In the definition, we have a symmetric binary relation Adj on a space of datasets, called adjacency. Intuitively $\mathrm{Adj}(\theta, \theta')$ iff two datasets θ and θ' differ by the data of a single participant.

Definition 1: (Adjacency). Let $\mathcal{D}$ represent $n+1$-dimensional data space, two datasets θ, $\theta' \in \mathcal{D}$ are adjacent, if there exists one $i \in \{1, 2, \cdots, n+1\}$ such that $\theta_i \neq \theta'_i$, but for all $j \neq i$, $\theta_j = \theta'_j$.

Definition 2: (Sensitivity). Let $\mathcal{D}$ be a data space equipped with an adjacency relation Adj. For any query $\mathrm{que} : \mathcal{D} \to \mathbb{R}^k$, the ℓ_μ-sensitivity of que is

$$\Delta_\mu^{sen}\mathrm{que} = \max_{\theta, \theta'} ||\mathrm{que}(\theta) - \mathrm{que}(\theta')||_\mu.$$

Definition 3: (Differential Privacy). The mechanism $\mathcal{M}$ guarantees (ε, δ)-differential privacy if for any two adjacent sets of initial positions of all agents $\theta = \{x_1(0), x_2(0), \cdots, x_{n+1}(0)\}$ and $\theta' = \{x'_1(0), x'_2(0), \cdots, x'_{n+1}(0)\}$ and for all $\mathbb{S} \subseteq \mathrm{Range}(\mathcal{M})$,

$$\Pr\{\mathcal{M}(\mathrm{que}(\theta)) \in \mathbb{S}\} \leq e^\varepsilon \Pr\{\mathcal{M}(\mathrm{que}(\theta')) \in \mathbb{S}\} + \delta,$$

where $\mathrm{Range}(\mathcal{M})$ denotes the range of $\mathcal{M}$, and $\Pr\{\cdot\}$ denotes the probability of some event.

The definition of (b, r)-accuracy given by Huang et al. [13]. Because in the leader-follower scenario, all nodes' state vectors do not converge to an average value, but follow the leader to follow a certain trajectory. An extended definition is explored in this work to characterize the system accuracy.

Definition 4: ((b, r)-accuracy). For any initial position state $x(0)$, $b \in [0, 1]$ and $r \in \mathbb{R}_{\geq 0}$, a randomized mechanism is said to achieve (b, r)-accuracy if every execution starting from $x(0)$ converges to a trajectory within r from the original one, with the probability at least $1 - b$, i.e.,

$$\lim_{k \to \infty} \Pr\{|\tilde{x}_i(k) - x_i(k)| \leq r\} \geq 1 - b,$$

where $\tilde{x}_i(k)$ is the position of node i at time k after the randomized mechanism and $x_i(k)$ is the original one without any randomized mechanism.

C. Problem of Interests

We consider a mechanism to hide positions of the agents by adding noise to the position. The mechanism is

$$\mathcal{M}: \tilde{x}_i(k) = x_i(k) + \eta_i(k), \forall i \in \mathcal{V},$$

where $\eta_i(k)$ is the independent noise variable with zero mean, i.e., $\mathbb{E}(\eta_i(k)) = 0$, and exponentially decaying variance $\mathrm{Var}(\eta_i(k)) = \varphi^k \sigma^2$, $\varphi \in (0,1)$. Let $\tilde{z}(k)$ be the state of agents after adding noise. Then, the noise vector is

$$\Gamma(k) = [\ \eta_1(k) \quad 0 \quad \eta_2(k) \quad 0 \quad \cdots \quad \eta_{n+1}(k) \quad 0\ ]^\top.$$

Thus, the privacy preserving second-order consensus algorithm is given by

$$\begin{cases} \tilde{z}(k+1) = Q\tilde{z}(k) + \Phi + \Gamma(k+1), \\ \tilde{z}(0) = z(0) + \Gamma(0). \end{cases} \tag{4}$$

There are acceleration, velocity, and position coupled in the system and information flow in a directed topology is not symmetric. How noise affects convergence of the system under directed topology will be explored. Besides, little work has been done about the privacy protection of second-order consensus by adding random noise based on differential privacy. The system accuracy is also focused on in our work considering the noise for privacy concerns.

III. Main Results

A. Convergence Analysis

The algorithm (4) needs to guarantee that $x_i(k) \to x_{n+1}(k) + \Delta x_i$, $v_i(k) \to v_{n+1}(k)$ asymptotically. And after adding noise the trajectories of agents should still converge.

Lemma 1: Real symmetric matrices can be always orthogonally similar to diagonal matrix.

Let the eigenvalues of L be λ_i^L, $i \in \{1, 2, \cdots, n+1\}$, where $0 = \lambda_1^L \leq \lambda_2^L \leq \cdots \leq \lambda_{n+1}^L$. Let $\tilde{Q} = Q^\top Q$. And $\lambda_1^{\tilde{Q}}, \lambda_2^{\tilde{Q}}, \cdots, \lambda_{2n+2}^{\tilde{Q}}$ denote the eigenvalues of the real symmetric matrix $\tilde{Q}$, where $\lambda_1^{\tilde{Q}} \leq \lambda_2^{\tilde{Q}} \leq \cdots \leq \lambda_{2n+2}^{\tilde{Q}}$. From Lemma 1, it follows that

$$\tilde{Q} = P^{-1}\Lambda P = P^{-1}\mathrm{diag}(\lambda_i^{\tilde{Q}})P, i = 1, \cdot\cdot\cdot, 2n+2, \tag{5}$$

which is a unit orthogonal similar diagonalization of $\tilde{Q}$. P is a unit orthogonal matrix with elements p_{ij}, for all $i, j = 1, \cdot\cdot\cdot, 2n+2$ and $P^{-1} = P^\top$.

Theorem 1: (4) guarantees convergence iff $\mathcal{G}$ contains a spanning tree and the following conditions are satisfied

i)

$$\begin{cases} \tau^2\gamma_0 - 2\tau\gamma_1 > \frac{-4\mathrm{Re}(\lambda_i^L)}{|\lambda_i^L|^2}, \\ \gamma_1 > \tau\gamma_0 > 0, \\ (\tau^2\gamma_0 - 2\tau\gamma_1)|\lambda_i^L|^2 + 4\mathrm{Re}(\lambda_i^L) > \frac{4\gamma_0 \mathrm{Im}^2(\lambda_i^L)}{|\lambda_i^L|^2(\gamma_1 - \tau\gamma_0)^2}, \end{cases} \tag{6}$$

ii) for all $\lambda_j^{\tilde{Q}} \notin (-1, 1]$, there exists a P such that $p_{j(2i-1)} = 0, i = 1, 2, \cdots, n+1, j \in \{1, 2, \cdots, 2n+2\}$.

Proof: First, since $\lim\limits_{k\to\infty} \varphi^k\sigma^2 = 0$, the noise input will exponentially decay to zero overtime, it does not change the consensus of the system. Referring to Theorem 2 in [23], we consider variable sampling time in this paper. It is obtained that agents achieve consensus asymptotically iff the graph contains a spanning tree and the gains are selected to satisfy conditions as (6) for $i = 1, 2, \cdots, n+1$.

Second, we consider whether the error of trajectories converges with the evolution of noise. Define the error vector at time k as $e(k) \triangleq \tilde{z}(k) - z(k)$. Note that here we remove the noise added at time k, because only the real state vector is taken into account at k. Then after adding noise,

$$\tilde{z}(k) = Q^k z(0) + \sum_{i=0}^{k-1} Q^i \Phi + \sum_{s=1}^{k} Q^s \Gamma(k-s). \tag{7}$$

Then the error vector is obtained that $e(k) = \sum\limits_{s=1}^{k} Q^s \Gamma(k-s)$. The expectation of mean square error can be written as

$$\mathbb{E}[e^\top(k)e(k)] = \mathbb{E}\{\sum_{s=1}^{k} \Gamma^\top(k-s)\tilde{Q}^s\Gamma(k-s)\}.$$

Let $\tilde{q}_{ii}(s), i = 1, 2, \cdot\cdot\cdot, 2n+2$ be the diagonal elements of the matrix $\tilde{Q}^s$, we have

$$\mathbb{E}[e^\top(k)e(k)] = \sigma^2 \sum_{i=1}^{n+1}\sum_{s=1}^{k} \varphi^{k-s}\tilde{q}_{(2i-1)(2i-1)}(s).$$

In order to ensure the convergence of the system, it is required that $\lim\limits_{k\to\infty} \mathbb{E}[e^\top(k)e(k)] < \infty$, i.e.

$$\lim_{k\to\infty} \sigma^2 \sum_{i=1}^{n+1}\sum_{s=1}^{k} \varphi^{k-s}\tilde{q}_{(2i-1)(2i-1)}(s) < \infty.$$

According to (5), we have $\tilde{Q}^s = P^\top \mathrm{diag}((\lambda_1^{\tilde{Q}})^s)P$. Therefore, there holds

$$\tilde{q}_{(2i-1)(2i-1)}(s) = \sum_{j=1}^{2n+2} p_{j(2i-1)}^2 (\lambda_j^{\tilde{Q}})^s,$$

and

$$\begin{aligned} &\lim_{k\to\infty} \sigma^2 \sum_{i=1}^{n+1}\sum_{s=1}^{k} \varphi^{k-s}\tilde{q}_{(2i-1)(2i-1)}(s) \\ &= \sigma^2 \lim_{k\to\infty} \varphi^k [\sum_{i=1}^{n+1} p_{1(2i-1)}^2 \frac{\varphi^{-1}\lambda_1^{\tilde{Q}} - (\varphi^{-1}\lambda_1^{\tilde{Q}})^{k+1}}{1 - \varphi^{-1}\lambda_1^{\tilde{Q}}} \\ &+ \cdots + \sum_{i=1}^{n+1} p_{(2n+2)(2i-1)}^2 \frac{\varphi^{-1}\lambda_{2n+2}^{\tilde{Q}} - (\varphi^{-1}\lambda_{2n+2}^{\tilde{Q}})^{k+1}}{1 - \varphi^{-1}\lambda_{2n+2}^{\tilde{Q}}}]. \end{aligned}$$

To ensure that the above limit exists, the limit of each element in the RHS (right hand side) of the last equation must exist. For any $\lambda_m^{\tilde{Q}}$, one can obtain

$$\begin{aligned} &\lim_{k\to\infty} \varphi^k \sum_{i=1}^{n+1} p_{m(2i-1)}^2 \frac{\varphi^{-1}\lambda_m^{\tilde{Q}} - (\varphi^{-1}\lambda_m^{\tilde{Q}})^{k+1}}{1 - \varphi^{-1}\lambda_m^{\tilde{Q}}} \\ &= -\sum_{i=1}^{n+1} p_{m(2i-1)}^2 \cdot \frac{1}{\varphi - \lambda_m^{\tilde{Q}}} \cdot \lim_{k\to\infty} (\lambda_m^{\tilde{Q}})^{k+1}. \end{aligned} \tag{8}$$

From (8), we obtain that the limit exists iff $\lambda_m^{\tilde{Q}} \in (-1, 1]$, or $\sum_{i=1}^{n+1} p_{m(2i-1)}^2 = 0$ that is $p_{m(2i-1)} = 0$, $i = 1, 2, \cdots, n+1$, which completes the proof. ■

Remark 1: Theorem 1 gives the mathematical expression of the sufficient and necessary conditions to guarantee the convergence of the algorithm. Among them, condition i) can be achieved by adjusting control gains γ_0, γ_1 and sampling time τ. And condition ii) can also be satisfied by setting an appropriate communication topology. In simulation, it is easy to find that this condition can be meet for most topologies.

B. Convergence Rate

We consider the impact of the added noise $\Gamma(k)$ on the performance of the consensus algorithm. Let us define the convergence rate β of our privacy preserving second-order consensus algorithm as

$$\beta \triangleq \sup \{\mathbb{E}[||\tilde{z}_i(k) - \tilde{z}_{n+1}(k) - \Delta_i||]\}^{\frac{1}{k}},$$

where $\Delta_i = [\ \Delta x_i \quad 0\ ]^\top$ is a constant vector.

Theorem 2: (Convergence Rate). The convergence rate β of (4) in a discrete-time multi-agent system equals to

$$\beta = \max\{|\lambda^*|, \sqrt{\varphi}\}, \tag{9}$$

where λ^* denotes the maximum of eigenvalues of Q whose moduli are less than 1.

Proof: From (7), we have

$$\tilde{z}(k) = Q^k \tilde{z}(0) + \sum_{i=0}^{k-1} Q^i \Phi + \sum_{s=0}^{k-1} Q^s \Gamma(k-s). \tag{10}$$

Then, we transform the system into a Jordan standard type. Let $J = T^{-1}QT$, $J^k = T^{-1}Q^kT$, where T is the transformation matrix, J is a Jordan standard type of Q, J_i is the Jordan block, and its diagonal elements are eigenvalues of Q. Hence, there holds

$$J = \mathrm{diag}(J_1, J_2, \cdots), J^k = \mathrm{diag}(J_1^k, J_2^k, \cdots).$$

Then, (10) turns into

$$\tilde{z}'(k) = J^k T^{-1} z(0) + \sum_{i=0}^{k-1} J^i T^{-1} \Phi + \sum_{s=0}^{k} J^s T^{-1} \Gamma(k-s).$$

Define eigenvalues of Q as $\lambda(Q) = \{\lambda_1(Q), \cdots, \lambda_{2n+2}(Q)\}$, and $\lambda^k(Q) = \{\lambda_1^k(Q), \cdots, \lambda_{2n+2}^k(Q)\}$. It can be seen that elements of J^k are linear combinations of $\lambda^k(Q), \lambda^{k-1}(Q), \cdots$, and the diagonal elements are exactly $\lambda^k(Q)$. Define the linear combination of $\lambda_i^k(Q), \lambda_i^{k-1}(Q), \cdots, \lambda_i^0(Q)$ as $l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))$, $i = 1, 2, \cdots, 2n+2$. We can derive

$$\begin{aligned}\tilde{z}'(k) =& [l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))]_{(2n+2)\times 1} + \sum_{s=0}^{k} [l(\lambda_i^k(Q), \\ & \cdots, \lambda_i^0(Q))]_{(2n+2)\times(2n+2)} \cdot \begin{bmatrix} \eta_1(k-s) \\ 0 \\ \cdots \\ \eta_{n+1}(k-s) \\ 0 \end{bmatrix},\end{aligned}$$

where $[l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))]_{ij}$ denotes a matrix with i rows and j columns whose elements are $l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))$. Hence, there holds

$$\begin{aligned}\tilde{z}(k) =& [l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))]_{(2n+2)\times 1} + \sum_{s=0}^{k} [l(\lambda_i^s(Q)\eta_j(k-s), \\ & \cdots, \lambda_i^0(Q)\eta_j(k-s))]_{(2n+2)\times 1},\end{aligned}$$

where $i = 1, 2, \cdots, 2n+2$, $j = 1, 2, \cdots, n+1$. Then,

$$\begin{aligned}\tilde{z}_i(k) - \tilde{z}_{n+1}(k) =& [l(\lambda_i^k(Q), \cdots, \lambda_i^0(Q))]_{2\times 1} \\ & + \sum_{s=0}^{k} [l(\lambda_i^s(Q)\eta_j(k-s), \\ & \cdots, \lambda_i^0(Q)\eta_j(k-s))]_{2\times 1}.\end{aligned} \tag{11}$$

From (11), the expectation of its norm's square is

$$\begin{aligned}&\mathbb{E}[||\tilde{z}_i(k) - \tilde{z}_{n+1}(k) - \Delta_i||^2] \\ &= \rho_1(k+1)^2\varphi^{k+1} + \rho_2(\lambda^*)^{2k+1} + \rho_3,\end{aligned}$$

where ρ_1, ρ_2 and ρ_3 are constant coefficients. The convergence rate is obtained that

$$\beta = \max\{|\lambda^*|, \sqrt{\varphi}\}.$$

Therefore, the convergence rate of the algorithm is decided by the eigenvalues of the transition matrix and decaying coefficient of the noise variance. ■

C. Privacy Analysis

Let $\{x_1(0), x_2(0), \cdots, x_{n+1}(0)\}$ be the set of initial positions, which is protected to ensure privacy of the system.

Assumption 1: There is only one different element between two sets $\theta = \{x_1(0), x_2(0), \cdots, x_{n+1}(0)\}$ and $\theta' = \{x'_1(0), x'_2(0), \cdots, x'_{n+1}(0)\}$, and

$$||x'_m(0) - x_m(0)|| \leq \Delta,$$

where x_m and x'_m are the different elements in θ and θ' respectively, Δ is a positive real number.

We assume the noise $\eta_i(k)$ is a continuous random variable, and its probability density function (PDF) is $f_k(\eta)$. An adversary has potential access to all group communications. The query from adversaries of position set is the same as the intercommunicating set. Hence, for all $i \in 1, 2, \cdots, n+1$, it holds

$$\begin{aligned}\Pr\{M(\mathrm{que}(\theta)) \in \mathbb{S}\} =& \int_{\mathbb{S}} \prod_{i=1}^{n+1} f_0(u - x_i(0))\mathrm{d}u \\ \leq& e^{\varepsilon} \int_{\mathbb{S}} \prod_{i=1}^{n+1} f_0(u - x'_i(0))\mathrm{d}u + \delta.\end{aligned}$$

The sensitivity, ε and δ are decided by PDF of adding noise. Here, the certain sensitivities and boundaries of ε and δ when adding Gaussian or Laplacian noise are provided. Recall that the Laplace distribution with zero mean and scaled parameter b, denoted by $\mathrm{Lap}(b)$ and Gaussian distribution with zero mean and variance σ^2, denoted by $\mathrm{N}(0, \sigma^2)$.

Lemma 2: Let $\varepsilon > 0$, $0.5 > \delta > 0$, (4) guarantees $(\varepsilon,\delta)-$differential privacy if $\eta_i(k) \sim \mathrm{N}(0, \varphi^k\sigma^2)$ and

$$\varphi^0\sigma^2 \geq \frac{\Delta}{2\varepsilon}(W+\sqrt{W^2+2\varepsilon}), W = \mathcal{Q}^{-1}(\delta),$$

where $\mathcal{Q}(\delta) := \frac{1}{\sqrt{2\pi}}\int_{\delta}^{\infty} e^{-\frac{u^2}{2}}du$.

Lemma 3: (4) guarantees $\varepsilon-$differential privacy if $\eta_i(k) \sim \mathrm{Lap}(\sqrt{\frac{\varphi^k}{2}}\sigma)$ and $\sqrt{\frac{\varphi^0}{2}}\sigma \geq \frac{\Delta}{\varepsilon}$.

Remark 2: Lemma 2 and Lemma 3 can be derived by Theorem 2 and Theorem 3 in [24]. The query of position set is the same as the intercommunicating set. Based on Assumption 1, the sensitivity is upper bounded by Δ.

From Lemma 3 and Lemma 4, it can be seen that the privacy level is decided by the noise variance at the initial time. When ε is smaller, $\varphi^0\sigma^2$ should be correspondingly larger. And for constant variances, ε and δ are inversely proportional. Smaller ε means a higher level of privacy protection and larger variances.

It is worth noting that the "initial state" to be protected is the state eavesdropped by malicious attackers in the beginning. For instance, if an attacker starts observing at time k, it is the noise added at time k that protects privacy. So in order to guarantee the above privacy preserving level, the variance of noise should be $\varphi^k\sigma^2$ instead of $\varphi^0\sigma^2$ in this case. Since the exponential decay is fast, a much larger value of σ^2 is needed to ensure a certain level of privacy.

D. Accuracy Analysis

Due to the influence of noise, the trajectory of agents will fluctuate near the original one. The amplitude of this fluctuation can be considered as a measure of system accuracy.

Theorem 3: (4) achieves $(\frac{\sigma^2}{(1-\varphi)\alpha^2}, \alpha)$-accuracy.

Proof: We consider the accuracy of the leader's position state. According to (2) (M_i represents the constant item)

$$u_i(k) = -\sum_{j=1}^{n+1} a_{ij}[\gamma_1(v_i(k)-v_j(k)) \tag{12}$$

$$+\gamma_0(x_i(k)-x_j(k))+M_i]. \tag{13}$$

From (12), the iteration formula of position is given by

$$x_i(k+1) = x_i(k)+\tau v_i(k-1)-\tau^2\sum_{j=1}^{n+1} a_{ij}[\gamma_1(v_i(k-1)$$

$$-v_j(k-1))+\gamma_0(x_i(k-1)-x_j(k-1))+M_i].$$

Since the acceleration of leader is 0, let $v_{n+1}(0) = v_{n+1}(1) = \cdots = v_{n+1}(k) = v_{n+1}$. So without noise

$$x_{n+1}(k) = x_{n+1}(0)+k\tau\cdot v_{n+1}.$$

After adding noise, the position at time k of the leader is

$$\tilde{x}_{n+1}(k) = x_{n+1}(0)+k\tau\cdot v_{n+1}+\sum_{s=0}^{k}\eta_{n+1}(s).$$

By Chebyshev's inequality for any $k \geq 0$

$$\Pr\{|\tilde{x}_{n+1}(k)-x_{n+1}(k)| \leq \alpha\} \geq 1-\frac{\mathrm{Var}(\sum_{s=0}^{k}\eta_{n+1}(s))}{\alpha^2}.$$

From the definition of $\eta_i(t)$, we have

$$\mathrm{Var}(\sum_{s=0}^{k}\eta_{n+1}(s)) = \sigma^2\sum_{s=0}^{k}\varphi^s = \sigma^2\frac{1-\varphi^{k+1}}{1-\varphi}.$$

Let $k \to \infty$, the variance converges to $\frac{\sigma^2}{1-\varphi}$. And since the position errors of the followers and the leader will converge to zero over time, there holds

$$\lim_{k\to\infty}\Pr\{|\tilde{x}_i(k)-x_i(k)| \leq \alpha\} \geq 1-\frac{\sigma^2}{\alpha^2(1-\varphi)},$$

for all $i = 1, \cdots, n+1$. ■

From Theorem 3, it is noted that the accuracy of the position states of agents is influenced by the coefficients φ and σ^2 of the noise variance. If the variance becomes larger, the probability that deviation from the original trajectory within α becomes smaller, which means less accuracy.

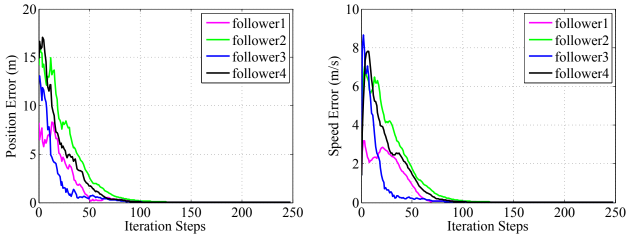
IV. Simulation

We consider the formation of 4 followers and 1 leader in 2-D plane for intuitive. The privacy preserving second-order consensus algorithm is used in $x-$direction and $y-$direction independently. The following adjacent matrix A is applied

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The relative positions that followers keep to the leader in $x-$direction and $y-$direction in the formation are $\{-2,-6,-2,-6,0\}$ and $\{4,4,-4,-4,0\}$ respectively. The initial coordinates of all agents are $\{-10,-4,2,4,0\}$ in $x-$direction and $\{6,-10,8,-15,0\}$ in $y-$direction. The initial velocities in two directions are both 1 m/s for the leader and 0 m/s for followers.

First, let $\gamma_0 = 1$, $\gamma_1 = 2$, $\tau = 0.1$s, and we add Gaussian noise with σ^2=1, $\varphi = 0.9$. Fig. 1 illustrates the position and speed errors of followers relative to the leader while they are reaching consensus over time. The errors gradually decay to zero so that followers can keep up with the leader accurately, and the pre-set formation can still be formed.

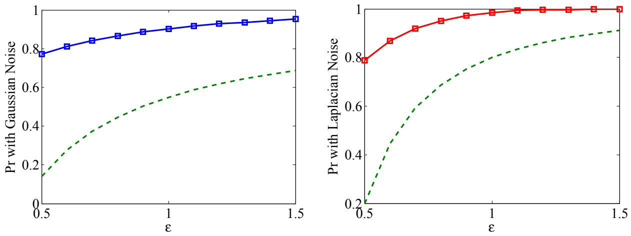


(a) Position error of followers

(b) Speed error of followers

Fig. 1: Relative errors of followers to leader

Then, we investigate the relationship between privacy and accuracy in this system. Gaussian and Laplacian noise are added to the node states separately. We selected $\alpha = 5$, $\varphi = 0.9$, $\Delta = 0.5$ and different ε from 0.5 to 1.5. Let $\delta = 0.02$ in the case of Gaussian noise. We examine the probability that the position deviation was bounded by α. In order to ensure the accuracy as much as possible, each set of parameters was tested 10000 times.



(a) Gaussian noise

(b) Laplacian noise

Fig. 2: Relationship of privacy and accuracy

In Fig. 2, the blue/red solid line plots the result of the actual simulation, and the dashed line is the theoretically calculated lower bound. We see that actual probabilities and the lower bound have the same trend from Fig. 2(a) and Fig. 2(b). There is a tradeoff between privacy and accuracy level. To guarantee a higher level of privacy, adding larger noise is needed, which makes the system performance worse.

It can be seen that we only need to generate one $n + 1$ dimensional random number matrix once at the beginning, the noise adding mechanism does not bring additional computational overhead. Therefore, the time complexity of the proposed privacy-preserving second-order consensus algorithm is $\mathcal{O}(n^2)$. However, if we use Paillier encryption mechanism in [17] in the actual system, each agent needs to encrypt and decrypt the transmitted state in each iteration. In fact, in the case of a large-scaled network, the computing burden is heavy and may even reach the second delay, then our proposed algorithm will be more advantageous.

V. Conclusion

In this paper, we considered leader-following second-order consensus in multi-agent systems while preserving the privacy of initial positions. A privacy-preserving second-order consensus algorithm was proposed by adding random noise with exponentially decaying variance. The sufficient and necessary conditions of convergence of the algorithm were provided and the convergence rate was specified. In addition, we performed a privacy analysis based on differential privacy and uncovered the certain boundaries of privacy degree when Gaussian or Laplacian noise was added. The system accuracy was characterized to show the boundary of probability that the trajectory deviation was bounded within a certain range.

References

[1] 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, 2007.

[2] W. Shi, Q. Ling, G. Wu, and W. Yin, "Extra: An exact first-order algorithm for decentralized consensus optimization," *SIAM Journal on Optimization*, vol. 25, no. 2, pp. 944–966, 2015.

[3] W. Yu, G. Chen, and M. Cao, "Some necessary and sufficient conditions for second-order consensus in multi-agent dynamical systems," *Automatica*, vol. 46, no. 6, pp. 1089–1095, 2010.

[4] Y. Chen, J. Lu, X. Yu, and Z. Lin, "Consensus of discrete-time second-order multiagent systems based on infinite products of general stochastic matrices," *SIAM Journal on Control and Optimization*, vol. 51, no. 4, pp. 3274–3301, 2013.

[5] H. Su, G. Chen, X. Wang, and Z. Lin, "Adaptive second-order consensus of networked mobile agents with nonlinear dynamics," *Automatica*, vol. 47, no. 2, pp. 368–375, 2011.

[6] H. Li, X. Liao, T. Huang, and W. Zhu, "Event-triggering sampling based leader-following consensus in second-order multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 7, pp. 1998–2003, 2014.

[7] J. Qin, H. Gao, and W. X. Zheng, "Consensus strategy for a class of multi-agents with discrete second-order dynamics," *International Journal of Robust and Nonlinear Control*, vol. 22, no. 4, pp. 437–452, 2012.

[8] R. Olfati-Saber, "Distributed kalman filtering for sensor networks," in *2007 46th IEEE Conference on Decision and Control*, pp. 5492–5498, IEEE, 2007.

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

[10] T. Yin, Y. Lv, and W. Yu, "Accurate privacy preserving average consensus," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2019.

[11] H. Gao, C. Zhang, M. Ahmad, and Y. Wang, "Privacy-preserving average consensus on directed graphs using push-sum," in *2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, IEEE, 2018.

[12] C. Zhao, J. Chen, J. He, and P. Cheng, "Privacy-preserving consensus-based energy management in smart grids," *IEEE Transactions on Signal Processing*, vol. 66, no. 23, pp. 6162–6176, 2018.

[13] 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*, pp. 81–90, ACM, 2012.

[14] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2016.

[15] M. Ruan, M. Ahmad, and Y. Wang, "Secure and privacy-preserving average consensus," in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy*, pp. 123–129, ACM, 2017.

[16] X. Duan, J. He, P. Cheng, Y. Mo, and J. Chen, "Privacy preserving maximum consensus," in *2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 4517–4522, IEEE, 2015.

[17] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on paillier encryption," *arXiv preprint arXiv:1805.01065*, 2018.

[18] Z. Chen, B. Fu, Z. Wu, and Q. Xu, "Privacy preserving second-order consensus for wasns," in *2018 37th Chinese Control Conference (CCC)*, pp. 7236–7241, IEEE, 2018.

[19] Q. Song, J. Cao, and W. Yu, "Second-order leader-following consensus of nonlinear multi-agent systems via pinning control," *Systems & Control Letters*, vol. 59, no. 9, pp. 553–562, 2010.

[20] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative control of multi-agent systems: optimal and adaptive design approaches*. Springer Science & Business Media, 2013.

[21] C. Dwork, "Differential privacy," *Encyclopedia of Cryptography and Security*, pp. 338–340, 2011.

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

[23] D. Xie and S. Wang, "Consensus of second-order discrete-time multi-agent systems with fixed topology," *Journal of Mathematical Analysis and Applications*, vol. 387, no. 1, pp. 8–16, 2012.

[24] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2013.