2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Preserving Data-Privacy Cooperative Control of Discrete-Time Multi-Agent Systems

Lingying Huang, Rong Su, Maode Ma, Yun Lu, Bohui Wang, Zhijian Hu

Abstract— **With the rapid advancements of communication technology, distributed cooperative control has emerged as a promising approach, enabling participants to perform control based on their neighbouring agents, thereby facilitating a faster response and more flexibility. However, the privacy concerns must be addressed not only on the external adversaries but also on the internal adversaries, to encourage the participant to join this cooperative network. In contrast to existing literature, our study considers the scenario where participating agents are unaware of whether their neighbouring nodes inject noises, leading them to directly use the received data in control. We first design the noise injection scheme to ensure the mean-square consensus while preserving privacy in discrete-time multi-agent systems (MASs) and then derive the upper and lower bounds of the convergence rate. After that, we study the covariance matrix of the maximum likelihood estimate on the initial state of other agents based on the internal adversary's local information. The feasibility of (ε, δ)-differential privacy is characterized. Simulations of a practical cooperative adaptive cruise control illustrate the effectiveness of the Privacy-Preserving Cooperative Control (PPCC).**

I. Introduction

Distributed cooperative control between multi-agent systems (MASs) has been widely used. A general principle of distributed cooperative control is that all the participating agents aim to achieve an identical dynamic state via this control based on their neighbouring information. This kind of control could reach a faster response and more flexibility compared with a centralized one, therefore, has been extensively used in distributed sensor networks [1], formation control [2], and etc. However, directly sending the participants' sensitive data to their neighbouring agents may deter them from joining this cooperative control manner. In addition, under some observability conditions, the sensitive data may even be inferred perfectly by the curious nodes in the MASs which are not neighbours of the current node by leveraging the update rule of all the other agents. Due to the above two problems, the study for exploring privacy-preserving mechanisms is encouraged.

In the context of distributed cooperative control, achieving consensus implies that all participating agents' states become identical, thereby eliminating the need for privacy preservation once consensus is reached. However, our focus lies in preserving the initial state of each participating agent throughout the cooperative consensus process. This is crucial, as the initial state may reveal sensitive information such as position and velocity, which can disclose personal details like home address or driving behaviour. Mo and Murray [3] design a time-correlated noise process to conceal the transmitted state while guarantee cooperative consensus. Then the estimation error with respect to the maximum likelihood of the initial state based on the received noised data trajectories and the actual one is derived which further characterizes the privacy level. Huang et al. [4] study agents with scalar outputs to reach a neighbourhood of the actual consensus with probability subject to differential privacy (DP). In their mechanism, the consensus accuracy is sacrificed in order to improve the privacy level. Note that DP has been defined and applied to preserve individual privacy in a dataset [5], where are discussed more to solve the first-order consensus problems in MASs [6], [7]. The optimal distributed estimation based on the local received noised data is derived by He et al. [8] and the resilient estimation is derived by Fiore and Russo [9] using (ε, δ)-DP. Wang et al. [10] extend the above setup to multivariable dynamic MASs. We only make review based on the work on discrete-time MASs since the individual agent will update its state after receiving neighbour's measurements and then inject noise for next communication, in which both require processing time and it is unrealistic and costly to inject noise all the time. It is shown in the literature that the stabilization problem for the discrete-time is essentially more difficult than that of the continuous-time counterpart [11].

Note that in the above literature, the agents not only transmit the noised data to their neighbouring node, but also use the noised data to make control. This simplifies the study, since the average state of the closed-loop systems can then evolve as an open-loop system [12]. However, in practice, they may not have knowledge of whether the transmitted information has been perturbed to preserve privacy. Therefore, they will directly interpret the received data from their neighbours as the "actual states" of their neighbours, and the control is then made based on both the "actual states" of their neighbours and themselves. It should be emphasized that, in this scenario, the control of each node is based on the noised neighbouring information along with the actual own state information. In addition, to preserve its own state information, a noise will be added before sharing to neighbours. The main difficulty is that due to the mismatch of the control signal in MASs, the noise influence will always be injected into the average side. Without careful design, it

L. Huang, R. Su, Y. Lu, B. Wang, and Z. Hu are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mails:lingying.huang@ntu.edu.sg, RSu@ntu.edu.sg, yun.lu@ntu.edu.sg, bhwang@ntu.edu.sg, zhijian.hu@ntu.edu.sg).

M. Ma is with the College of Engineering, Qatar University, Qatar (e-mail: mamaode@qu.edu.qa).

This research is supported by A*STAR under its RIE2020 Advanced Manufacturing and Engineering (AME) Industry Alignment Fund C Pre Positioning (IAF-PP) (Award A19D6a0053).

is shown in Li et al. [13] that the consensus may not be reached. On the other hand, [10] only considers the privacy analysis for the external adversaries with full knowledge of transmitted data, while how the internal adversary which is a curious node to derive estimates of other nodes based on its local information set is not studied.

The two problems are tackled in this paper. We first study the impact of the added noise on the consensus side. We derive the conditions to ensure mean-square consensus and then obtain the lower and upper bounds of the mean-square convergence rate (**Theorem 1**). Later, since a better guess can be obtained giving the whole trajectory, we derive a maximum likelihood initial state estimate of other node given the local observation information set that is shown to be a sufficient statistic for estimating (**Theorem 2**). Therefore, the error covariance with respect to the maximal estimate and the initial state to the internal adversary can be derived. At last, given the error covariance, we characterize the possible $(\varepsilon, \delta)-$DP that could be achieved by this control (**Theorem 3**).

The rest of the paper is organized as follows. The problem formulation is given in Section II. The main results are shown in Section III. Simulation results are shown in Section IV and the conclusions are summarized in Section V.

Notation: $\mathbb{N}$ ($\mathbb{N}_+$) is the set of (positive) natural numbers. $\mathbb{R}$ and $\mathbb{R}^n$ ($\mathbb{C}^n$) represent the set of real numbers and $n-$dimensional real (complex) column vectors, respectively. We use $(\cdot)^\top$, $\|\cdot\|$ to represent the transpose and 2-norm of $(\cdot)$, respectively. For the matrices $A \in \mathbb{R}^{n\times m}$ and $B \in \mathbb{R}^{p\times q}$, $A \otimes B \in \mathbb{R}^{np\times mq}$ represents their Kronecker product. Let $\rho(A)$ and $\|A\|_F$ the spectral radius and Frobenius norm of matrix A, respectively. The identity column vector and matrix are $\mathbf{1}_m$ and I_m, respectively, and their sizes are m.

II. Problem Formulation

A. Network topology

We model the network composed of N agents as a graph $\mathcal{G} = \{V, E\}$, where $V = \{1, 2, \ldots, N\}$ is the set of vertices representing the agents, $E \subseteq V \times V$ represents the set of edges, and $(i, j) \in E$ if and only if (iif) agent i and j can communicate directly with each other. In this paper, we start with the undirected and connected graph $\mathcal{G}$, i.e., $a_{ij} = a_{ji}$. The neighbourhood of sensor i is defined as $\mathcal{N}_i \triangleq \{j \in V : (i, j) \in E, j \neq i\}$.

B. Privacy-Preserving Cooperative Control (PPCC)

To prevent the local information from leaking to its neighbours, each agent will add random noise at each iteration for local data exchange. Let $x_i^+(k) \in \mathbb{R}^n$ be the data sent out by node i in iteration k:

$$x_i(k+1) = Ax_i(k) + Bu_i(k), x_i^+(k) = x_i(k) + w_i(k), \quad (1)$$

where

$$u_i(k) = K \sum_{j\in\mathcal{N}_i} a_{ij}(x_j^+(k) - x_i(k)). \quad (2)$$

We assume that $w_i(k)$ are some predefined noises with zero mean, and $\mathbb{E}[w_j(k)w_i^\top(k)] = 0, \forall j, i \in V$ and $j \neq i$.

Remark 1. *As an important application, the consensus algorithm can be easily extended to study privacy-preserving cooperative adaptive cruise control to reach formationability. Specially, given the formation vector $h = [h_1^\top, h_2^\top, \ldots, h_N^\top]^\top \in \mathbb{R}^{Nn}$, the following control protocol is adopted to study the formation problem of the discrete-time MAS* (1)*:*

$$u_i(k) = K \sum_{j\in\mathcal{N}_i} a_{ij}((x_j^+(k) - h_j) - (x_i(k) - h_i)), \quad (3)$$

where $h_i - h_j$ is the desired distance vector between agent i and agent j. In addition, we assume $A(h_i - h_j) = h_i - h_j, \forall i, j \in V$, which represents the physical requirement of cruise control that all the agents aim to have the same velocity. Therefore, by letting a new variable $\tilde{x}_i(k) = x_i(k) - h_i$, the formation consensus problem will be equivalent to study the consensus problem in the previous system setup (1)-(2)*.*

Define

$$\begin{aligned} x(k) &\triangleq [x_1^\top(k), x_2^\top(k), \ldots, x_N^\top(k)]^\top \in \mathbb{R}^{Nn}, \\ x^+(k) &\triangleq [x_1^{+\top}(k), x_2^{+\top}(k), \ldots, x_N^{+\top}(k)]^\top \in \mathbb{R}^{Nn}, \\ w(k) &\triangleq [w_1^\top(k), w_2^\top(k), \ldots, w_N^\top(k)]^\top \in \mathbb{R}^{Nn}. \end{aligned} \quad (4)$$

Then the evolution (1)-(2) can be written in a compact form:

$$\begin{aligned} x(k+1) =& \mathcal{A}x(k) + W(k), \\ W(k) \triangleq& \begin{bmatrix} BK\sum_{j\in\mathcal{N}_1} a_{1j}w_j(k) \\ BK\sum_{j\in\mathcal{N}_2} a_{2j}w_j(k) \\ \vdots \\ BK\sum_{j\in\mathcal{N}_N} a_{Nj}w_j(k) \end{bmatrix}, \end{aligned} \quad (5)$$

where $\mathcal{A} = I_N \otimes A - L \otimes BK$ and $L = [l_{ij}] \in \mathbb{R}^{N\times N}$ is the Laplacian matrix where $l_{ij} = \begin{cases} \sum_{l\in\mathcal{N}_i} a_{il}, & \text{if } j = i \\ -a_{ij}, & \text{otherwise} \end{cases}$.

If $w(t) = 0, \forall t \leq k \in \mathbb{N}$, $x(k)$ is deterministically determined by $x(0)$. We denote the state without privacy-preserving protocol as $\theta(k)$. The recursion of $\theta(k)$ follows:

$$\theta(0) = x(0), \theta(k+1) = \mathcal{A}\theta(k). \quad (6)$$

For external adversaries which may have access to all the transmitted information, $x(0)$ will be leaked.

In addition, we also consider the internal adversaries which are curious but honest nodes aiming to infer the other agents' initial state. Without loss of generality, we only consider the case for agent $i = N$. Denote the 1-hop neighbour of agent N as $\mathcal{N}_N = \{j_1, \ldots, j_m\}$. Define

$$C \triangleq [\ e_{j_1} \quad \ldots \quad e_{j_m} \quad e_N\ ]^\top \otimes I_n \in \mathbb{R}^{(m+1)n\times Nn} \quad (7)$$

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 k can be defined as

$$\mathcal{I}(k) = \{x_N(0), y(0), \ldots, y(k)\}, \quad (8)$$

where $y(k) = Cx^+(k) = Cx(k) + Cw(k)$. We assume that $(\mathcal{A}, C)$ is observable and $(\mathcal{A}, C)$ is known by agent N. It is worth noting that node N can perfectly infer $x(0)$ if $(\mathcal{A}, C)$ is observable and $w(k) = 0$, $\forall k \in \mathbb{N}$.

From above analysis, the noise is needed either for the external adversaries and the internal adversaries. Denote the maximum likelihood estimate of $x(0)$ given $\mathcal{I}(k)$ as $\hat{\theta}(0|k)$, 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 non-increasing, i.e., $P(k_1) \geq P(k_2)$ if $k_1 \leq k_2$.*

In addition, since $P(k) = \mathbb{E}[(\hat{\theta}(0|k) - x(0))(\hat{\theta}(0|k) - x(0))^\top] \geq 0$, the following limit is well defined:

$$P = [P_{ij}]_{i,j\in\mathcal{N}} \triangleq \lim_{k\to\infty} P(k). \tag{9}$$

As a result, the matrix P_{ii} indicates the optimal estimation performance that agent N can achieve on the initial state $x_i(0)$, where $P_{ij} \in \mathbb{R}^{n\times n}$. To preserve the privacy of the initial condition $x_i(0)$, we need to ensure that P_{ii} is sufficiently large.

III. Main Results

In this section, we first consider the impact of added noise $w(k)$ on the performance of consensus side. Next, we study the estimation performance, and then the (ε, δ)-differential privacy (DP) can be obtained from estimation performance analysis.

A. Convergence Rate

Definition 1 (Mean-square consensus)**.** *The multi-agent system* (1)-(2) *is said to reach mean-square consensus if*

$$\lim_{k\to\infty} \mathbb{E}[\|x_i(k) - x_j(k)\|^2] = 0, \forall i \neq j, i, j \in V, \tag{10}$$

where $\mathbb{E}$ indicates the expectation over noise process $\{w(k)\}$.

Let

$$e(k) \triangleq (I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n x(k) \tag{11}$$

be the error of the MAS. From the fact that $L_G 1_N = 0$, $1_N^\top L_G = 0$, and $\mathbb{E}[w_i(k)] = 0$, it is easy to verify that the mean-square consensus is reached if and only if

$$\lim_{k\to\infty} \mathbb{E}[e^\top(k)e(k)] = 0.$$

Then we define the mean-square convergence rate

$$\gamma \triangleq \lim_{k\to\infty} \left(\sup_{e(0)\neq 0} \frac{\mathbb{E}[e^\top(k)e(k)]}{e^\top(0)e(0)} \right)^{\frac{1}{k}}. \tag{12}$$

We first establish the sufficient conditions to ensure mean-square convergence, i.e., $\gamma < 1$. In preparation, we first introduce a lemma which illustrates the relationship between the upper bound of $\|M\|_F$ and $\rho(M)$ when $\rho(M) < 1$, for M is a square matrix.

Lemma 1. *[10, Lemma 2] Consider a square matrix $M \in \mathbb{R}^{n\times n}$. Assume that $M = Q\mathrm{diag}\{J_1, \ldots, J_m\}Q^{-1}$, where $J_r \in \mathbb{C}^{n_r\times n_r}$ is the Jordan canonical block corresponding to the eigenvalue $\lambda_r(M)$, $r = 1, \ldots, m$. If $\rho(M) < 1$, the following statement is true for $k \in \mathbb{N}_+$:*

$$\|M^k\|_F \leq \beta k^{\hat{n}-1}\rho^k(M), \tag{13}$$

where $\hat{n} \triangleq \max_{1\leq r\leq m}\{n_r\}$ and $\beta \triangleq \sqrt{m}\|Q\|_F\|Q^{-1}\|_F \frac{\rho^{-(\hat{n}+1)}(M)}{\rho^{-2}(M)-1}$.

Theorem 1. *For any initial condition $x(0)$, $x(k)$ reaches mean-square consensus if the following conditions hold:*

1) *The control gain K is designed such that*

$$\begin{aligned} &\rho(\Gamma_m) < 1, m = 2, 3, \ldots, N, \\ &L = U\mathrm{diag}\{0, \lambda_2, \ldots, \lambda_N\}U^\top, \end{aligned} \tag{14}$$

where $\Gamma_m \triangleq A - \lambda_m BK$ for $m = 2, 3, \ldots, N$, $U = [\ u_1 \ \ \ldots \ \ u_N\ ]$ is the orthogonal matrix with $u_i \in \mathbb{R}^N$ for $i \in V$.

2) *The added noises $\{w_i(k)\}, \forall i \in V$ satisfy*

$$\|\mathbb{E}[w_i(k_1)w_i^\top(k_2)]\|_F \leq \mho(k1, k2)\varrho^{k_1+k_2}, \forall k_1, k_2 \in \mathbb{N}, \tag{15}$$

where $\mho(k1, k2) \in \mathcal{F}^+(\alpha, \mathbb{N}\times\mathbb{N})$ is a binary non-negative polynomial, and $\alpha \in \mathbb{N}$ is constant.

Additionally, the convergence rate satisfies

$$\rho_{max}^2 \leq \gamma \leq \max\{\varrho^2, \rho_{max}^2\}, \tag{16}$$

where $\rho_{max} \triangleq \max\{\rho(\Gamma_m), m = 2, 3, \ldots, N\}$.

Proof. Define $\hat{W}(k) \triangleq ((I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n)W(k)$. Combining (5) and (11), the recursion of $e(k)$ follows

$$e(k+1) = \mathcal{A}e(k) + \hat{W}(k) = \mathcal{A}^k e(0) + \sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\hat{W}(t). \tag{17}$$

where the first equation holds since $((I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n)\mathcal{A} = \mathcal{A}((I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n)$. Since $\mathbb{E}[\hat{W}(k)] = ((I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n)\mathbb{E}[W(k)] = 0$, we have $\mathbb{E}[e(k+1)] = \mathcal{A}^k e(0) + \sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\mathbb{E}[W(t)] = \mathcal{A}^k e(0)$. Therefore, to ensure the mean-square convergence, one requires $\rho(\mathcal{A}) < 1$ which is equivalent to condition 1) [12, Lemma 3.1].

In addition,

$$\begin{aligned} \mathbb{E}[e(k)^\top e(k)] =& e^\top(0)(\mathcal{A}^k)^\top\mathcal{A}^k e(0) \\ &+ \mathbb{E}[(\sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\hat{W}(t))^\top \sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\hat{W}(t)]. \end{aligned}$$

From (14), using the property of Kronecker product gives that $\mathcal{A} = (U \otimes I_n)\Lambda(U \otimes I_n)^\top$ with $\Lambda = \mathrm{diag}\{A, \Gamma_2, \ldots, \Gamma_N\}$ and $(I_N - \frac{\mathbf{1}_N\mathbf{1}_N^\top}{N}) \otimes I_n = (U \otimes I_n)\mathrm{diag}\{\mathbf{0}_n, \overbrace{I_n, \ldots, I_n}^{N-1}\}(U \otimes I_n)^\top$. Then we derive that

$$\begin{aligned} &\frac{e^\top(0)(\mathcal{A}^k)^\top\mathcal{A}^k e(0)}{e^\top(0)e(0)} \\ =&\frac{\zeta^\top(0)\mathrm{diag}\{\mathbf{0}_n, (\Gamma_2^k)^\top\Gamma_2^k, \ldots, (\Gamma_N^k)^\top\Gamma_N^k)\}\zeta(0)}{\zeta^\top(0)\zeta(0)}, \end{aligned}$$

where $\zeta(0) = (U \otimes I_n)^\top x(0)$. It gives that

$$\sup_{e(0)\neq 0} \frac{\mathbb{E}[e(k)^\top e(k)]}{e(0)^\top e(0)} \geq \sup_{e(0)\neq 0} \frac{e^\top(0)(\mathcal{A}^k)^\top\mathcal{A}^k e(0)}{e^\top(0)e(0)} = \rho_{max}^{2k},$$

which completes the proof of the left inequality in (16).

Meanwhile, let

$$\begin{aligned} \Delta(k) \triangleq& \mathbb{E}[(\sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\hat{W}(t))^\top \sum_{t=0}^{k-1} \mathcal{A}^{k-1-t}\hat{W}(t)] \\ =& \mathbb{E}[\sum_{0\leq s,t\leq k-1} \varpi(t)^\top\Theta(t, s; k)\varpi(s)], \end{aligned} \tag{18}$$

where $\varpi(k) = (U \otimes I_n)^\top W(k)$, and $\Theta(t, s; k) = \mathrm{diag}\{\mathbf{0}_n, (\Gamma_2^{k-t-1})^\top\Gamma_2^{k-s-1}, \ldots, (\Gamma_N^{k-t-1})^\top\Gamma_N^{k-s-1}\}$. Sub-

stituting the expression of $W(k)$ in (5) into (18):

$$\Delta(k)=\sum_{m=2}^{N}\sum_{i,j\in V}\sum_{0\le t,s\le k-1}u_{m,i}u_{m,j}$$
$$\cdot\,\mathbb{E}[(BK\sum_{p=1}^{N}a_{ip}w_p(k))^\top(\Gamma_m^{k-t-1})^\top\Gamma_m^{k-s-1}BK\sum_{q=1}^{N}a_{jq}w_q(k)].$$

Together with the requirements that $\mathbb{E}[w_p(k)w_q^\top(k))]=0,\forall p\neq q\in V$, the above equation further becomes

$$\Delta(k)=\sum_{m=2}^{N}\sum_{i,j\in V}\sum_{p=1}^{N}u_{m,i}u_{m,j}a_{ip}a_{jp}$$
$$\cdot\sum_{0\le t,s\le k-1}\mathbb{E}[w_p^\top(k)(BK)^\top(\Gamma_m^{k-t-1})^\top\Gamma_m^{k-s-1}BKw_p(s)].$$

Since $\mathrm{tr}(M_1^\top M_2)\le(\mathrm{tr}(M_1^\top M_1))^{1/2}(\mathrm{tr}(M_2^\top M_2))^{1/2}=\|M_1\|_F\|M_2\|_F$ for any two compatible square matrices M_1 and M_2, we have

$$\begin{aligned}&\mathbb{E}[w_p^\top(k)(BK)^\top(\Gamma_m^{k-t-1})^\top\Gamma_m^{k-s-1}BKw_p(s)]\\ =&\mathrm{tr}\left((BK)^\top(\Gamma_m^{k-t-1})^\top\Gamma_m^{k-s-1}BK\mathbb{E}[w_p(k)w_p^\top(s)]\right)\quad(19)\\ \le&\|BK\|_2^2\|\Gamma_m^{k-t-1}\|_F\|\Gamma_m^{k-s-1}\|_F\|\mathbb{E}[w_p(k)w_p^\top(s)]\|_F.\end{aligned}$$

With (14), (15) and Lemma 1, (19) is upper bounded by $\beta^2\|BK\|_2^2(k-t-1)^{\hat{n}-1}(k-s-1)^{\hat{n}-1}\rho_{max}^{2k-t-s-2}\mho(t,s)\varrho^{t+s}$, which is further upper bounded by

$$\beta^2\|BK\|_2^2k^{2\hat{n}-2}\mho(k,k)(\max\{\rho_{max},\varrho\})^{2k-2}.$$

From the above analysis, one has

$$\begin{aligned}&\sup_{e(0)\neq0}\frac{\mathbb{E}[e(k)^\top e(k)]}{e(0)^\top e(0)}\\ \le&\rho_{max}^{2k}+\sup_{e(0)\neq0}\frac{ck^{2\hat{n}}\mho(k,k)(\max\{\rho_{max},\varrho\})^{2k-2}}{e(0)^\top e(0)},\end{aligned}\quad(20)$$

where $c\triangleq\sum_{m=2}^{N}\sum_{i,j\in V}\sum_{p=1}^{N}|u_{m,i}u_{m,j}a_{ip}a_{jp}|>0$. Since $\lim_{k\to\infty}(k^{2\hat{n}}\mho(k,k))^{1/k}=1$, (20) further implies that $\gamma\le\max\{\varrho^2,\rho_{max}^2\}$, which completes the proof. □

Remark 2. *Note that if the noise is selected such that $\varrho\le\rho_{max}$, the mean-square convergence rate is a constant value, i.e., $\gamma=\rho_{max}^2$, which is only related to the communication topology and the choice of the control gain. Therefore, in this case, to ensure a faster convergence rate, one can either tune the communication topology (see possible methods in [14]) or the control gain to make ρ_{max} as small as possible.*

Example 1. *One possible design of added noises $\{w_i(k)\},\forall i\in V$ satisfying* (15) *is as follows:*

1) *At time k, the agent i generates a Gaussian random noise $v_i(k)$ with zero-mean and covariance Σ_i. We assume that $\{v_i(k)\}_{i\in V,k\in\mathbb{N}}$ are jointly independent.*
2) *Each agent then adds a random noise $w_i(k)$ to its state $x_i(k)$, where*

$$w_i(k)=\begin{cases}v_i(0), & \text{if } k=0,\\ \varrho^kv_i(k)-\varrho^{k-1}v_i(k-1), & \text{otherwise.}\end{cases}\quad(21)$$

B. Estimation Performance

We first reduce the state by removing $x_N(k)$, since $x_N(k)$ is known by agent N. Thus, the study on $\hat{\theta}(0|k)$ which lies on $\mathbb{R}^{Nn}$ can be shrunk to the study on $\mathbb{R}^{(N-1)n}$. Let $\tilde{\theta}_i(k)=\theta_i(k)-\theta_N(k)$, for $i=1,\dots,N-1$. By (6), one has $\tilde{\theta}(k)\triangleq[\tilde{\theta}_1^\top(k),\dots,\tilde{\theta}_{N-1}^\top(k),\theta_N^\top(k)]^\top\in\mathbb{R}^{Nn}$, which leads to

$$\tilde{\theta}(k+1)=\begin{bmatrix}\tilde{\mathcal{A}} & 0\\ \tilde{L}_N\otimes BK & A\end{bmatrix}\tilde{\theta}(k),$$

where $\tilde{L}_N=[\ a_{N1}\ \ \dots\ \ a_{N(N-1)}\ ]\in\mathbb{R}^{1\times(N-1)}$, $\tilde{\mathcal{A}}=I_{N-1}\otimes A-\tilde{L}\otimes BK$ and $\tilde{L}=[\tilde{l}_{ij}]\in\mathbb{R}^{(N-1)\times(N-1)}$ with $\tilde{l}_{ij}=l_{ij}-l_{Nj},\forall i,j\in V\setminus\{N\}$.

Let us further define

$$\begin{aligned}\tilde{w}(k)\triangleq&[w_1^\top(k),w_2^\top(k),\dots,w_{N-1}^\top(k)]^\top\in\mathbb{R}^{(N-1)n},\\ \tilde{C}\triangleq&[\ \tilde{e}_{j_1}\ \ \dots\ \ \tilde{e}_{j_m}\ ]^\top\otimes I_n\in\mathbb{R}^{mn\times(N-1)n},\end{aligned}\quad(22)$$

where $\tilde{e}_i$ denotes the ith canonical basis vector in $\mathbb{R}^{N-1}$. Define the reduced state vector $\tilde{x}(k)\in\mathbb{R}^{(N-1)n}$ such that

$$\begin{aligned}\tilde{x}(k+1)=&\tilde{\mathcal{A}}\tilde{x}(k)+\tilde{W}(k),\\ \tilde{W}(k)=&\begin{bmatrix}BK\sum_{j=1}^{N-1}a_{1j}w_j(k)\\ BK\sum_{j=1}^{N-1}a_{2j}w_j(k)\\ :\\ BK\sum_{j=1}^{N-1}a_{Nj}w_j(k)\end{bmatrix},\end{aligned}\quad(23)$$

with initial condition $\tilde{x}(0)=[x_1^\top(0)-x_N^\top(0),\dots,x_{N-1}^\top(0)-x_N^\top(0)]^\top$. Finally, the reduced measurement $\tilde{y}(k)\in\mathbb{R}^{mn}$ is defined as

$$\tilde{y}(k)=\tilde{C}(\tilde{x}(k)+\tilde{w}(k)).\quad(24)$$

Remark 3. *It is worth noticing that in general, $\tilde{x}(k)+\mathbf{1}_{N-1}\otimes x_N(k)\neq[x_1^\top(k),x_2^\top(k),\dots,x_{N-1}^\top(k)]^\top$.*

Since $(\mathcal{A},C)$ is observable, it is not difficult to prove that $(\tilde{\mathcal{A}},\tilde{C})$ is also observable. Define the information set based on the reduced measurements $\tilde{\mathcal{I}}(k)=\{x_N(0),w_N(0),\dots,w_N(k),\tilde{y}(0),\dots,\tilde{y}(k)\}$. The following theorem establishes the equivalence between $\mathcal{I}(k)$ and $\tilde{\mathcal{I}}(k)$.

Theorem 2. *For any $k\in\mathbb{N}$, there exists an invertible linear transformation from the row vector $[x_N^\top(0),y^\top(0),\dots,y^\top(k)]$ to the row vector $[x_N^\top(0),w_N^\top(0),\dots,w_N^\top(k),\tilde{y}^\top(0),\dots,\tilde{y}^\top(k)]$.*

Proof. Define

$$x_r(k)\triangleq[x_1^\top(k)-x_N^\top(k),\dots,x_{N-1}^\top(k)-x_N^\top(k)]^\top\in\mathbb{R}^{(N-1)n}.$$

and $e_r(k)=x_r(k)-\tilde{x}(k)$. By (5) and (23), we have that

$$\begin{aligned}e_r(k+1)=&\tilde{\mathcal{A}}e_r(k)+[a_{1N},\dots,a_{(N-1)N}]^\top\otimes(BKw_N(k))\\ =&\tilde{\mathcal{A}}e_r(k)+\tilde{L}_N^\top\otimes BKw_N(k),\end{aligned}$$

where the second equality holds since $a_{ij}=a_{ji}$.Since $e_r(0)=0,\forall k\in\mathbb{N}$,

$$e_r(k+1)=\sum_{t=0}^{k}\tilde{\mathcal{A}}^{k-t}\tilde{L}_N^\top\otimes BKw_N(t).\quad(25)$$

We will then prove Theorem 2 by induction. By (23)-(24), $y^\top(0)=[\tilde{y}(0)^\top+\tilde{C}(\mathbf{1}_{N-1}\otimes x_N(0))^\top,x_N^\top(0)+w_N^\top(0)]$. Hence, Theorem 2 holds when $k=0$. Suppose that Theorem 2 holds when $k=t$, we want to prove that it still holds when $k=t+1$. By induction, we only need to prove that

1) $w_N(t+1)$ and $\tilde{y}(t+1)$ can both be written as linear combination of the variables in $\mathcal{I}(t+1)$;
2) $y(t+1)$ can be written as a linear combination of the

variables in $\tilde{\mathcal{I}}(t+1)$.

It is easy to verify that

$$y(t+1) - \begin{bmatrix} \tilde{y}(t+1) \\ w_N(t+1) \end{bmatrix} = \begin{bmatrix} \tilde{C}(\mathbf{1}_{N-1} \otimes x_N(t+1) + e_r(t+1)) \\ x_N(t+1) \end{bmatrix}.$$

Together with (25) and (5), which states that $e_r(t+1), x_N(t+1)$ can be obtained given $\mathcal{I}(t)$ (or $\tilde{\mathcal{I}}(t)$), the proof is completed. □

By Theorem 2, $\tilde{\mathcal{I}}(k)$ is a sufficient statistic for estimating $x(0)$. Define $\tilde{P}(k)$ as the covariance of the maximum likelihood estimate of $\tilde{x}(0)$ given $\{\tilde{y}(0), \ldots, \tilde{y}(k)\}$. From (23)-(24)

$$\tilde{y}(k) = \tilde{C}(\tilde{\mathcal{A}}^k \tilde{x}(0) + \sum_{t=0}^{k-1-t} \tilde{\mathcal{A}}^{k-1-t} \tilde{W}(t) + \tilde{w}(k)).$$

Let $G : \mathbb{R}^{(N-1)n} \to \mathbb{R}^{(N-1)n}$ be the linear mapping such that $\tilde{W}(t) \triangleq G\tilde{w}(k)$, from (23), G is well-defined. Here, we only consider the added error satisfying Example 1. We will leave the general study of $P(k)$ in the future. By (21), one further has $\sum_{t=0}^{k} \tilde{y}(t) = \tilde{C}\sum_{t=0}^{k} \tilde{\mathcal{A}}^t \tilde{x}(0) + \tilde{C}\sum_{t=0}^{k-1} \varrho^t \tilde{\mathcal{A}}^{k-1-t} G\tilde{v}(t) + \tilde{C}\varrho^k \tilde{v}(k)$, which implies that

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

where $\tilde{v}(k) \triangleq [v_1^\top(k), \ldots, v_{N-1}^\top(k)]^\top \in \mathbb{R}^{(N-1)n}$,

$$H(k) = \begin{bmatrix} \tilde{C}\sum_{t=0}^{0} \tilde{\mathcal{A}}^t/\varrho^0 \\ \vdots \\ \tilde{C}\sum_{t=0}^{k} \tilde{\mathcal{A}}^t/\varrho^k \end{bmatrix},$$

and

$$F(k) = \begin{bmatrix} \tilde{C} & & & \\ \tilde{C}G/\varrho & \tilde{C} & & \\ \vdots & \vdots & \ddots & \\ \tilde{C}\tilde{\mathcal{A}}^{k-1}G/\varrho^k & \tilde{C}\tilde{\mathcal{A}}^{k-2}G/\varrho^{k-1} & \cdots & \tilde{C} \end{bmatrix},$$

then the covariance of the maximum likelihood estimate [15] satisfies

$$\tilde{P}(k) = [H^\top(k)(F(k)(I_k \otimes \mathrm{diag}\{\Sigma_i\}_{i=1}^{N-1})F^\top(k))^{-1}H(k)]^{-1}. \quad (26)$$

The design of noise will affect $\tilde{P}(k)$ which will further influence the differential privacy as studied in the next subsection.

C. Differential Privacy

Denote the probability space generated by $\{\tilde{w}(k)\}$ as $(\Omega, \mathcal{F}, \mathbb{P})$ and $D = \mathbb{R}^{(N-1)n}$ is the set of all possible initial conditions $\tilde{x}(0)$. We define a binary "adjacency" relation Adj on D, such that two initial conditions $\tilde{x}^{(1)}(0)$ and $\tilde{x}^{(2)}(0)$ are adjacent iif the Euclidean distance between them is no greater than d, i.e.,

$$Adj(\tilde{x}^{(1)}(0), \tilde{x}^{(2)}(0)) \triangleq \begin{cases} 1, & \text{if } \|\tilde{x}^{(1)}(0) - \tilde{x}^{(2)}(0)\| \le d, \\ 0, & \text{otherwise.} \end{cases}$$

Let us write $\hat{x}(0|k) = [\hat{x}_1(0|k), \ldots, \hat{x}_{N-1}(0|k)]$ be the maximum likelihood estimate of $\tilde{x}(0)$ given $\tilde{\mathcal{I}}(k)$. Clearly, $\hat{x}_i(0|k)$ is a mapping from $D \times \Omega \to \mathbb{R}^n$ written as

$$\hat{x}_i(0|k) = M_{i,k}(\tilde{x}(0), \omega), \quad \tilde{x}(0) \in D, \omega \in \Omega. \quad (27)$$

Definition 2 ((ε, δ)-DP)**.** *The mapping $M_{i,k}$ reaches (ε, δ)-DP for Adj if for all Borel-measurable $S \subseteq \mathbb{R}^n$ and adjacent initial conditions $\tilde{x}^{(1)}(0)$ and $\tilde{x}^{(2)}(0)$, the following inequality holds:*

$$\mathbb{P}[M_{i,k}(\tilde{x}^{(1)}(0), \omega) \in S] \le e^{\varepsilon}\mathbb{P}[M_{i,k}(\tilde{x}^{(2)}(0), \omega) \in S] + \delta.$$

After deriving $\tilde{P}(k)$ by (26), it will converge to $\tilde{P} = [P_{ij}]_{i,j \in \mathcal{N}\setminus\{N\}}$ in (9) when $k \to \infty$.

Theorem 3. *If $P_{ii} > 0$, then for any $k \in \mathbb{N}$, the mapping $M_{i,k}$ achieves $(\varepsilon, \delta)-$differential privacy for Adj, if $\epsilon > 0$, $0 < \delta < 0.5$ and*

$$\frac{(\rho(P_{ii}))^{-\frac{1}{2}} d}{2\varepsilon}(K + \sqrt{K^2 + 2\varepsilon}) \le 1, \quad (28)$$

where $K = \mathcal{Q}^{-1}(\delta)$ and $\mathcal{Q}(x) \triangleq \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-\frac{u^2}{2}) du$.

Proof. From subsection III-B, we know that $\hat{x}_i(0|k) = x_i(0) + \varsigma_i(k)$, where $\varsigma_i(k)$ is a random variable with mean 0 and variance $P_{ii}(k) \in \mathbb{R}^{n \times n}$. In addition, $P_{ii}(k) \ge P_{ii} = TT^\top$. Since $P_{ii} > 0$, one has T is non-singular. Let $\Delta_2 q = \sup_{Adj(x_i(0), x_i'(0))} \|T^{-1}(x_i(0) - x_i'(0))\|_2 = (\rho(P_{ii}))^{-\frac{1}{2}} d$, $\varsigma_i(k) = T\varsigma_i'(k)$, then the variance on each element of $\varsigma_i'(k)$ is no smaller than 1 and each element is independent with each other. By [16, Theorem 3], we can complete the proof. □

Remark 4. *Theorem 3 characterizes multiple choices of (ε, δ) given the added noise mechanism. Note that $\frac{1}{2\varepsilon}(K + \sqrt{K^2 + 2\varepsilon})$ can be bounded by $O(ln(\frac{1}{\delta}))^{\frac{1}{2}}/\varepsilon$ [16]. From Theorem 3, given fixed δ, one has $\varepsilon \ge O(ln(\frac{1}{\delta}))^{\frac{1}{2}}(\rho(P_{ii}))^{-\frac{1}{2}} d$, which means that if P_{ii} is larger, one can have higher privacy level since ε can be smaller given fixed δ.*

IV. Simulations

In this section, we consider the application of cooperative adaptive cruise control where each agent follows [17] with

$$A = \begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} \frac{1}{2}\tau^2 \\ \tau \end{bmatrix}, \quad (29)$$

with a sampling period $\tau > 0$ and $x_i(k)$ is the configuration variable of agent i at time kh, where the first and second element of it represent the position and velocity, respectively. The cooperative adaptive cruise control reaches a fixed formation $h_p = [p_1, \ldots, p_N]^\top \in \mathbb{R}^N$ if the following condition holds

$$\lim_{k \to \infty} \|x_i(k) - [p_i, 0]^\top - x_j(k) - [p_j, 0]^\top\| = 0. \quad (30)$$

It is easy to verify that $A([p_i, 0]^\top - [p_j, 0]^\top) = [p_i, 0]^\top - [p_j, 0]^\top$. By remark 1, for given control (3) and system evolution (1), by letting $x_i(k) \leftarrow x_i(k) - [p_i, 0]^\top$, the cooperative formation consensus can be transformed into the consensus problem considering system (1)-(2). After obtaining $x_i(k)$ from the evolution of (1)-(2), the true state can be realized by setting $x_i(k) \leftarrow x_i(k) + [p_i, 0]^\top$.

We consider the communication topology between the 5 vehicles as shown in Fig. 1. In addition, let $\tau = \frac{1}{10}$s,

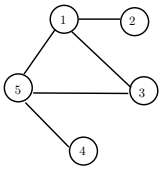

Fig. 1: Communication topology.

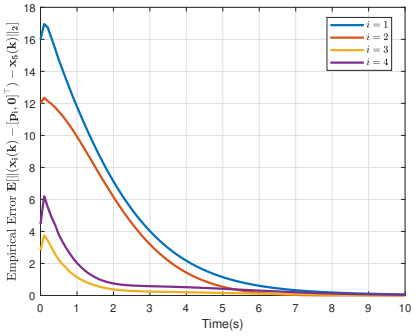

Fig. 2: Demonstration of empirical formation error between node i to node 5.

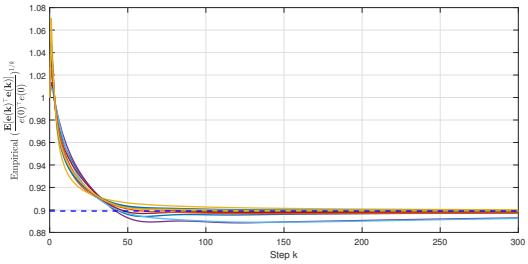

Fig. 3: Demonstration of convergence Rate.

$p_i = (5-i)d_0\text{m}$ with $d_0 = 26\text{m}$, $x_1(0) = [150, 20]^\top$, $x_2(0) = [120, 20]^\top$, $x_3(0) = [80, 22]^\top$, $x_4(0) = [60, 18]^\top$, $x_5(0) = [30, 20]^\top$, and $K = [1, 2]$. Note that the choice of K satisfies the condition 1) in Theorem 1 with $\rho_{max} = 0.9482$. To preserve the initial state not be leaked to the initial adversaries, we design noise following Example 1 with $\Sigma_i = \text{diag}\{1, 10\}$ and $\varrho = 0.8 < \rho_{max}$. Then from Theorem 1, we have $\gamma = \rho_{max}^2 = 0.899$. Without loss of generality, we only plot formation error and the unbaised optimal estimate covariance of other nodes on node 5. The trajectories of empirical $\mathbb{E}[\|(x_i(k) - [p_i, 0]^\top) - x_5(k)\|_2], \forall i \in V \setminus \{5\}$ implementing over 1000 trials are plotted in Fig. 2. We then randomly generate 10 initial state and plot the empirical expectation for $\left(\frac{\mathbb{E}[e(k)^\top e(k)]}{e(0)^\top e(0)}\right)^{\frac{1}{k}}$ over 100 trials. The result is shown in Fig. 3, where for each initial condition, the empirical expectation converges as time goes to infinity, and tends to mean-square convergence rate shown in the blue dashed line as derived from Theorem 1.

V. Conclusion

In this paper, we propose the PPCC which generates the control signal based on the perturbed received neighbour data and the actual state data since the participating node does not know that the received data is perturbed and will take them as the actual state from other agents. We first derive the conditions to ensure the mean-square consensus and then derive the upper and lower bounds of the convergence rate. We then study the covariance matrix of the maximum likelihood estimate on the initial state of other agents based on the internal adversary's local information. The possible (ε, δ)-differential privacy is further characterized. At last, the simulation provides a practical cooperative adaptive cruise control to illustrate the effectiveness of the PPCC. The future work direction includes studying the state with randomness and then designing a privacy-preserving estimator before injecting transmitted noises.

References

[1] J. Cortés and F. Bullo, "Coordination and geometric optimization via distributed dynamical systems," *SIAM journal on control and optimization*, vol. 44, no. 5, pp. 1543–1574, 2005.

[2] Y. Liu, D. Yao, H. Li, and R. Lu, "Distributed cooperative compound tracking control for a platoon of vehicles with adaptive nn," *IEEE Transactions on Cybernetics*, vol. 52, no. 7, pp. 7039–7048, 2021.

[3] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2017.

[4] 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, 2012.

[5] C. Dwork, "Differential privacy," in *Proceedings of Automata, Languages and Programming: 33rd International Colloquium, (ICALP), Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*, pp. 1–12, Springer, 2006.

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

[7] J. He and L. Cai, "Differential private noise adding mechanism: Basic conditions and its application," in *2017 American Control Conference (ACC)*, pp. 1673–1678, IEEE, 2017.

[8] 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.

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

[10] Y. Wang, J. Lam, and H. Lin, "Consensus of linear multivariable discrete-time multiagent systems: Differential privacy perspective," *IEEE Transactions on Cybernetics*, vol. 52, no. 12, pp. 13915–13926, 2022.

[11] C.-Q. Ma and J.-F. Zhang, "Necessary and sufficient conditions for consensusability of linear multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 5, pp. 1263–1268, 2010.

[12] K. You and L. Xie, "Network topology and communication data rate for consensusability of discrete-time multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2262–2275, 2011.

[13] T. Li, M. Fu, L. Xie, and J.-F. Zhang, "Distributed consensus with limited communication data rate," *IEEE Transactions on Automatic Control*, vol. 56, no. 2, pp. 279–292, 2010.

[14] M. Fabris, G. Michieletto, and A. Cenedese, "A general regularized distributed solution for system state estimation from relative measurements," *IEEE Control Systems Letters*, vol. 6, pp. 1580–1585, 2021.

[15] L. L. Scharf and C. Demeure, *Statistical signal processing: detection, estimation, and time series analysis*. Prentice Hall, 1991.

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

[17] W. Ren and E. Atkins, "Distributed multi-vehicle coordinated control via local information exchange," *International Journal of Robust and Nonlinear Control: IFAC-Affiliated Journal*, vol. 17, no. 10-11, pp. 1002–1033, 2007.