Distributed Fusion Estimation with Protecting Exogenous Inputs

Liping Guo, *Member, IEEE*, Jimin Wang, *Member, IEEE*, Yanlong Zhao, *Senior Member, IEEE*, and Ji-Feng Zhang, *Fellow, IEEE*

***Abstract*—In distributed fusion estimation, directly transmitting local estimates to the fusion center may cause a privacy leakage concerning exogenous inputs. Thus, it is crucial to protect exogenous inputs against full eavesdropping while achieving distributed fusion estimation. To address this issue, a noise injection strategy is provided by injecting mutually independent noises into the local estimates transmitted to the fusion center. To determine the covariance matrices of the injected noises, a constrained minimization problem is constructed by minimizing the sum of mean square errors of the local estimates while ensuring (ϵ, δ)-differential privacy. Suffering from the non-convexity of the minimization problem, an approach of relaxation is proposed, which efficiently solves the minimization problem without sacrificing differential privacy level. Then, a differentially private distributed fusion estimation algorithm based on the covariance intersection approach is developed. Further, by introducing a feedback mechanism, the fusion estimation accuracy is enhanced on the premise of the same (ϵ, δ)-differential privacy. Finally, an illustrative example is provided to demonstrate the effectiveness of the proposed algorithms, and the trade-off between privacy level and estimation accuracy.**

***Index Terms*—Differential privacy, distributed fusion estimation, constrained optimization, exogenous inputs, full eavesdropping**

I. Introduction

The real-time state estimation problem aims at estimating system state from noisy measurements and plays an important role in many areas, such as target tracking and aerospace engineering [1]–[3]. In contrast to single-sensor state estimation, multi-sensor fusion estimation employing multi-source data improves accuracy and robustness simultaneously, thereby attracting significant attention in recent years [2]–[5]. There are two basic networks for multi-sensor fusion estimation, i.e., centralized and distributed networks. Compared with the former, the latter stands out due to better robustness and system feasibility. However, distributed networks are susceptible to many different types of attacks, such as denial-of-service attacks [6] and false data injection attacks [7]. To defend against these attacks, many meaningful works about distributed fusion estimation have been proposed (see, e.g., [8]–[14]). In these studies, the attackers should acquire some privacy information by eavesdropping before launching a strategic attack [15]. Under this case, it is essential to protect privacy information against eavesdropping at its source. Thus, it is of great significance to study privacy preservation problem against eavesdropping in distributed fusion estimation.

To defend against eavesdropping, some distributed fusion estimation approaches have been developed in [2], [3], [15]. Specifically, encryption-based distributed fusion estimation approaches are presented in [2], [15]. In [3], a differentially private distributed fusion estimation algorithm is provided, where the publicly released estimates defined by fusion estimates averaged over time are protected. Attributed to its powerful performance and rigorous mathematical models, differential privacy stands out from its competitors and is studied in a wide range of fields, such as federated learning [16], consensus [17], optimization [18]–[20], game theory [21], [22] and control theory [23], [24]. Particularly in state estimation fields, differentially private filtering has been firstly discussed in [25]. In addition to measurements and state estimates, exogenous inputs may also contain private information, as demonstrated in applications such as smart grids [26] and building automation [27]–[29]. Therefore, protecting exogenous inputs is critically important, yet it introduces distinct theoretical challenges, including establishing privacy condition, designing optimal noise, and co-optimizing privacy and estimation accuracy. To our best knowledge, research on protecting exogenous inputs in fusion estimation is still lacking.

Motivated by the above analysis, in this paper, we study the differentially private distributed fusion estimation to protect the exogenous inputs against full eavesdropping. To ensure differential privacy of these exogenous inputs, we have to sacrifice some fusion estimation accuracy due to the noise injection strategy adopted at the sensor side. Particularly, we aim at minimizing the sum of mean square errors (MSEs) of local estimates and ensuring (ϵ, δ)-differential privacy simultaneously, which is the main purpose of this paper. Unfortunately, there exist some substantial difficulties in achieving this goal: i) To ensure (ϵ, δ)-differential privacy, a joint consideration of all the local sensors is necessary; under this case,

The work was supported by National Natural Science Foundation of China under Grants 62588101, 62433020, 62603311, 62673047 and T2293770, and the Talent Scientific Fund of Lanzhou University under Grant 561120225. The material in this paper was not presented at any conference. *(Corresponding author: Ji-Feng Zhang)*

Liping Guo is with the School of Mathematics and Statistics, Lanzhou University, Lanzhou 730000, China. (e-mail: lipguo@outlook.com)

Jimin Wang is with the School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, and also with the Key Laboratory of Knowledge Automation for Industrial Processes, Ministry of Education, Beijing 100083, China. (e-mail: jimwang@ustb.edu.cn)

Yanlong Zhao is with the State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. (e-mail: ylzhao@amss.ac.cn)

Ji-Feng Zhang is with the School of Automation and Electrical Engineering, Zhongyuan University of Technology, Zheng Zhou 450007; and also with the State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. (e-mail: jif@iss.ac.cn)

minimizing the sum of MSEs of local estimates is challenging, especially when the correlation among the measurement noises of local sensors is unknown. ii) Computational efficiency is critically important in real-time state estimation, but the minimization problem is non-convex with the optimization variables being matrices, greatly increasing the difficulty of solving it efficiently. iii) Accurate fusion can foster optimal resource utilization and stability in estimation algorithms; thus, is it possible to enhance fusion estimation accuracy while ensuring (ϵ, δ)-differential privacy? These difficulties are properly solved in this paper, and the main contributions are summarized as follows:

- We achieve distributed fusion estimation while protecting exogenous inputs against full eavesdropping. Unlike common differentially private approaches that often inject simple isotropic or scalar noise (see, e.g., [3], [16]–[19], [21], [22], [25]), we propose an optimized anisotropic noise injection strategy tailored to system uncertainties. This strategy introduces less noise along directions where the state is already uncertain, thereby improving estimation accuracy without compromising privacy. The noise covariance matrix is obtained by solving a constrained minimization problem that minimizes the sum of MSEs of local estimates while ensuring (ϵ, δ)-differential privacy. Furthermore, we solve this problem efficiently via a semi-definite programming (SDP) relaxation and establish an explicit upper bound on the relaxation gap. The proposed SDP not only preserves the privacy guarantee but also meets real-time computation requirements.
- We develop two differentially private distributed fusion estimation algorithms based on covariance intersection, balancing low-complexity and high-accuracy requirements. For the first algorithm, we provide an analytical characterization of the estimation accuracy loss, which rigorously quantifies the privacy-accuracy trade-off. For the second algorithm, we incorporate a feedback mechanism that is theoretically guaranteed to enhance estimation accuracy without compromising the (ϵ, δ)-differential privacy, but at the expense of increased computational complexity, thereby establishing a complexity-accuracy trade-off.

Notations. Scalars, vectors and matrices are denoted by lowercase letters, bold lowercase letters, and bold capital letters, respectively. Scalar 0, zero vector, and zero matrix are all denoted by 0 for simplicity. All the vectors are column vectors. The set of all n-dimensional real vectors and all $n \times m$ real matrices are denoted by $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$, respectively. For a vector $\mathbf{a}$, $\|\mathbf{a}\|$ denotes its Euclidean norm, further, $\|\mathbf{a}\|_{\mathbf{A}}$ denotes its Euclidean norm weighted with $\mathbf{A} > 0$, i.e., $\sqrt{\mathbf{a}^{\mathrm{T}}\mathbf{A}\mathbf{a}}$. $\mathrm{diag}(\mathbf{a})$ represents the diagonal matrix with $\mathbf{a}$ on the principal diagonal. In particular, $\mathbf{1}$ represents the vector with all entries one. For a square matrix $\mathbf{A}$, $\mathbf{A} \geq 0$ (or $\mathbf{A} > 0$) means that $\mathbf{A}$ is positive semi-definite (or positive definite). $\mathrm{tr}(\mathbf{A})$ represents the trace of $\mathbf{A}$. $\lambda_{\min}(\mathbf{A})$ denotes the minimum eigenvalue of $\mathbf{A}$. The $\mathrm{block\text{-}diag}(\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n)$ represents the block diagonal matrix with matrices $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_n$ on the principal diagonal. $\mathbf{A}\otimes\mathbf{B}$ represents the Kronecker product operation between matrices $\mathbf{A}$ and $\mathbf{B}$. $\mathbf{I}_n$ represents the $n \times n$ identity matrix. $\mathbb{E}[\cdot]$ is the mathematical expectation operator.

II. Problem formulation

Consider a distributed multi-sensor network system consisting of M local sensors and a fusion center. For Node $i = 1, 2, \ldots, M$, the following time-varying dynamic system is addressed:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}_k\mathbf{x}_k + \mathbf{B}_k\mathbf{d}_k + \mathbf{w}_k, \\ \mathbf{y}_{i,k} &= \mathbf{C}_{i,k}\mathbf{x}_k + \mathbf{v}_{i,k}, \end{aligned} \tag{1}$$

where $k = 0, 1, 2, \ldots$ is time index, $\mathbf{x}_k \in \mathbb{R}^{n_x}$, $\mathbf{d}_k \in \mathbb{R}^{n_d}$, and $\mathbf{y}_{i,k} \in \mathbb{R}^{n_{y_i}}$ are the state, the exogenous input, and the i-th node's measurement, respectively, $\mathbf{A}_k \in \mathbb{R}^{n_x\times n_x}$, $\mathbf{B}_k \in \mathbb{R}^{n_x\times n_d}$, and $\mathbf{C}_{i,k} \in \mathbb{R}^{n_{y_i}\times n_x}$ are known matrices, $\{\mathbf{w}_k\}$ and $\{\mathbf{v}_{i,k}\}$ are zero-mean Gaussian white noise sequences with covariance matrices $\mathbf{Q}_k$ and $\mathbf{R}_{i,k}$, respectively, and $\mathbf{d}_k$ is regarded as deterministic but unknown [30], [31]. The initial state is independent of the noise sequences. All system parameters, including $\mathbf{A}_k$, $\mathbf{B}_k$, $\mathbf{C}_k$, $\mathbf{Q}_k$ and $\mathbf{R}_{i,k}$, are available to the fusion center. The correlations between the measurement noises of different sensors are typically unknown due to factors such as physical separation and unsynchronized clocks (see, e.g., [1], [32]).

Assumption 1: $\mathrm{rank}(\mathbf{C}_{i,k}\mathbf{B}_{k-1}) = \mathrm{rank}(\mathbf{B}_{k-1}) = n_d$, for all k.

Assumption 2: $(\mathbf{A}_k, \mathbf{C}_{i,k})$ is detectable, for all k.

Remark 1: Assumptions 1 and 2 are standard in the literature (see, e.g., [30], [31]). Assumption 1 ensures $n_x \geq n_d$ and $n_{y_i} \geq n_d$, while Assumption 2 guarantees a bounded error covariance in Kalman filtering.

Distributed fusion estimation aims to produce a fusion estimate and its associated error covariance matrix at each time step k, through the fusion of all local estimates and their error covariance matrices.

At the sensor side, the linear unbiased minimum-variance state estimation proposed in [30] is adopted, which is derived in the minimum mean square error (MSE) sense and comprises two steps. For Node $i = 1, 2, \ldots, M$, let $\hat{\mathbf{x}}_{i,k|k}$ be the estimate of $\mathbf{x}_k$ using the measurements $\mathbf{y}_{i,0}, \mathbf{y}_{i,1}, \ldots, \mathbf{y}_{i,k}$, and $\mathbf{P}_{i,k|k}$ be the associated error covariance matrix.

1) Prediction step. The predicted state estimate, denoted by $\hat{\mathbf{x}}_{i,k|k-1}$, and its error covariance matrix, denoted by $\mathbf{P}_{i,k|k-1}$, are calculated as follows:

$$\hat{\mathbf{x}}_{i,k|k-1} = \mathbf{A}_{k-1}\hat{\mathbf{x}}_{i,k-1|k-1}, \tag{2}$$

$$\mathbf{P}_{i,k|k-1} = \mathbf{A}_{k-1}\mathbf{P}_{i,k-1|k-1}\mathbf{A}_{k-1}^{\mathrm{T}} + \mathbf{Q}_{k-1}. \tag{3}$$

2) Update step. Once receiving the measurement $\mathbf{y}_{i,k}$, the linear unbiased minimum-variance state estimate and its error covariance matrix are given as

$$\hat{\mathbf{x}}_{i,k|k} = \hat{\mathbf{x}}_{i,k|k-1} + \mathbf{G}_{i,k}(\mathbf{y}_{i,k} - \mathbf{C}_{i,k}\hat{\mathbf{x}}_{i,k|k-1}), \tag{4}$$

$$\begin{aligned} \mathbf{P}_{i,k|k} = {} & \mathbf{P}_{i,k|k-1} - \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{P}_{i,k|k-1} \\ & + (\mathbf{B}_{k-1} - \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{B}_{k-1}) \\ & \cdot (\mathbf{B}_{k-1}^{\mathrm{T}}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{B}_{k-1})^{-1} \\ & \cdot (\mathbf{B}_{k-1} - \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{B}_{k-1})^{\mathrm{T}}, \end{aligned} \tag{5}$$

where $\mathbf{G}_{i,k} = \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1} + (\mathbf{B}_{k-1} - \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{B}_{k-1})(\mathbf{B}_{k-1}^{\mathrm{T}}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{B}_{k-1})^{-1}\mathbf{B}_{k-1}^{\mathrm{T}}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}$, and $\mathbf{F}_{i,k} = \mathbf{C}_{i,k}\mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}} + \mathbf{R}_{i,k}$.

Remark 2: The detailed derivations are given in [30], where Eqs. (5) and (19) correspond to (4), and Eq. (21) to (5). The first term of (5), $\mathbf{P}_{i,k|k-1} - \mathbf{P}_{i,k|k-1}\mathbf{C}_{i,k}^{\mathrm{T}}\mathbf{F}_{i,k}^{-1}\mathbf{C}_{i,k}\mathbf{P}_{i,k|k-1}$, is the standard Kalman filter update, while the second is a correction accounting for the unknown input $\mathbf{d}_{k-1}$.

At the fusion center side, after receiving all the local state estimates and error covariance matrices, the fusion estimate, denoted by $\hat{\mathbf{x}}_{k|k}^{\mathrm{umv}}$, and its error covariance matrix, denoted by $\mathbf{P}_{k|k}^{\mathrm{umv}}$, are derived by employing the approach of covariance intersection [32]:

$$\left(\mathbf{P}_{k|k}^{\mathrm{umv}}\right)^{-1}\hat{\mathbf{x}}_{k|k}^{\mathrm{umv}} = \sum_{i=1}^{M} w_i \mathbf{P}_{i,k|k}^{-1}\hat{\mathbf{x}}_{i,k|k}, \left(\mathbf{P}_{k|k}^{\mathrm{umv}}\right)^{-1} = \sum_{i=1}^{M} w_i \mathbf{P}_{i,k|k}^{-1},$$

where the weight vector $\mathbf{w} = [w_1, w_2, \ldots, w_M]^{\mathrm{T}}$ satisfies $w_i \geq 0$ and $\mathbf{w}^{\mathrm{T}}\mathbf{1} = 1$.

Remark 3: The concept of distributed fusion estimation adopted in this work is commonly used [2], [3], [8], [15] and often encountered in radar target tracking and navigation [1]. In our framework, both "distributed" and "fusion" make sense: "distributed" is reflected in each sensor estimating the state from its own measurements, and "fusion" in combining these local estimates at the fusion center. By contrast, in centralized fusion estimation, sensors send raw measurements directly to the fusion center for state estimation; in fully distributed peer-to-peer estimation, sensors exchange local estimates with their neighbors in a network without a fusion center [33].

For the system (1), there may be an eavesdropper, who is external to the system and trying to infer the private information. We assume that the eavesdropper has the following capability, which is referred to as the full eavesdropping hereinafter.

Definition 1 (Full eavesdropping): The full eavesdropping is a form of passive wiretapping that silently monitors communication channels without modification, and can obtain the same information as the fusion center, which can be classified into two categories: (a) system parameters, including $\mathbf{A}_k$, $\mathbf{B}_k$, $\mathbf{C}_k$, $\mathbf{Q}_k$ and $\mathbf{R}_{i,k}$; (b) real-time transmitted data.

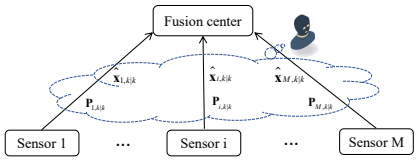


Fig. 1: Architecture of the problem: Each sensor $i = 1, 2, \ldots, M$ completes local estimation task independently, and transmits $\hat{\mathbf{x}}_{i,k|k}$ and $\mathbf{P}_{i,k|k}$ to the fusion center for the fusion estimation task, where all the local estimates $\{\hat{\mathbf{x}}_{i,k|k}\}_{i=1}^{M}$ and their error covariance matrices $\{\mathbf{P}_{i,k|k}\}_{i=1}^{M}$ are available to the full eavesdropper.

The architecture of the problem is depicted in Fig. 1. Note that there is no direct information transmission among the local sensors. In the system (1), the exogenous input $\mathbf{d}_{k-1}$ at time step k contains private information and should be protected against full eavesdropping.

To demonstrate the necessity of protecting $\mathbf{d}_{k-1}$ at time step k, the following two practical examples are representative:

- **Smart grids (see, e.g., [26]):** A household's current power consumption (d_{k-1}) reveals real-time behaviors like appliance usage and occupancy, making its protection a core challenge in smart grids.
- **Building automation (see, e.g., [27]–[29]):** A building's current occupancy (d_{k-1}) is critically private, making its protection a primary objective in building automation.

Remark 4: Our focus on protecting the latest exogenous input, $\mathbf{d}_{k-1}$, at each time step k stems from the high sensitivity of real-time data, such as a household's current power consumption [26] or a building's current occupancy [28], [29], which is of primary interest to an eavesdropper.

Based on the above analysis, we aim to achieve distributed fusion estimation for the system (1), while protecting $\mathbf{d}_{k-1}$ against full eavesdropping at each time step k. Under privacy consideration, the linear unbiased minimum-variance state estimate given by (4) cannot be transmitted to the fusion center directly as it may cause a privacy leakage (see Example 1 in [29]). Therefore, a tailored privacy-preserving local state estimation needs to be designed.

Remark 5: Note that the $\mathbf{P}_{i,k|k}$ given by (5) does not contain any information about $\mathbf{d}_{k-1}$. Therefore, to protect $\mathbf{d}_{k-1}$, we just need to modify the $\hat{\mathbf{x}}_{i,k|k}$ given by (4).

III. Privacy-preserving local state estimation

In this section, we design the privacy-preserving local state estimation based on a noise injection strategy. Particularly, we aim to minimize the sum of MSEs of local estimates while protecting $\mathbf{d}_{k-1}$ against full eavesdropping. To this end, it is not sufficient to consider privacy level for a single sensor; instead, a joint consideration of all the local sensors is necessary. By augmenting all the local estimates together, denoted by $\hat{\mathbf{x}}_{k|k} = [\hat{\mathbf{x}}_{1,k|k}^{\mathrm{T}}, \hat{\mathbf{x}}_{2,k|k}^{\mathrm{T}}, \ldots, \hat{\mathbf{x}}_{M,k|k}^{\mathrm{T}}]^{\mathrm{T}}$, we know that $\hat{\mathbf{x}}_{k|k}$ represents all the transmitted state estimates available to the full eavesdropper at time step k.

Then, we modify $\hat{\mathbf{x}}_{k|k}$ by injecting an independent noise: $\bar{\mathbf{x}}_{k|k} = \hat{\mathbf{x}}_{k|k} + \boldsymbol{\omega}_k$, where $\boldsymbol{\omega}_k \sim \mathcal{N}(0, \boldsymbol{\Sigma}_k)$ and the covariance matrix $\boldsymbol{\Sigma}_k$ need to be determined. Furthermore, to ensure that the local sensors can inject noise independently of each other, we limit the sought-after $\boldsymbol{\Sigma}_k$ into the block-diagonal form: $\boldsymbol{\Sigma}_k = \text{block-diag}(\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k})$. Note that the larger $\boldsymbol{\Sigma}_k$, the higher privacy level, but the lower local and fusion estimation accuracy. As such, an appropriate selection of $\boldsymbol{\Sigma}_k$ is necessary to balance privacy level and fusion estimation accuracy.

To quantified privacy level, we adopt the commonly used (ϵ, δ)-differential privacy (see, e.g., [3], [16]–[19], [21], [22], [25]). Let $(\Omega, \mathcal{F}, P)$ be a probability space. Then, we first introduce the notion of differential privacy, equipped with a symmetric binary adjacency relation, denoted $\mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})$, on the space $\mathbb{R}^{n_d}$.

Definition 2 (Adjacency relation): Let ϵ_0 be a positive real number. Then, $\mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1}) \Leftrightarrow \|\mathbf{d}_{k-1} - \mathbf{d}'_{k-1}\|_2 \leq \epsilon_0$.

Remark 6: Definition 2 is commonly used in the literature (see, e.g., [23], [24]). Notably, the adjacency definition in [20], [25] can also be applied to our framework, denoted as $\mathcal{A}_k = \{(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1}) \mid \mathbf{d}_{k-1}, \mathbf{d}'_{k-1} \in \mathbb{R}^{n_d}, \|\mathbf{d}_{k-1} - \mathbf{d}'_{k-1}\|_0 \leq 1 \text{ and } \|\mathbf{d}_{k-1} - \mathbf{d}'_{k-1}\|_\infty \leq \epsilon_0\}$. Since $\mathcal{A}_k \subset \{(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1}) \mid \mathbf{d}_{k-1}, \mathbf{d}'_{k-1} \in \mathbb{R}^{n_d}, \|\mathbf{d}_{k-1} - \mathbf{d}'_{k-1}\|_2 \leq \epsilon_0\}$, Definition 2

admits a larger set of adjacent pairs than the definition well established in [20], [25].

Definition 3 (Differential privacy, [25]): Let $(\mathbb{R}^{Mn_x}, \mathcal{M})$ be a measurable space, and $\epsilon, \delta \geq 0$. A mechanism $M_q : \mathbb{R}^{n_d} \times \Omega \to \mathbb{R}^{Mn_x}$ is (ϵ, δ)-differentially private if for all $\mathbf{d}_{k-1}, \mathbf{d}'_{k-1} \in \mathbb{R}^{n_d}$ such that $\mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})$, there is $P(M_q(\mathbf{d}_{k-1}) \in \mathbb{S}) \leq e^{\epsilon} P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) + \delta,\ \forall \mathbb{S} \in \mathcal{M}$.

Remark 7: The above inequality is standard in defining the differential privacy. Since it holds for any $\mathbf{d}_{k-1}, \mathbf{d}'_{k-1} \in \mathbb{R}^{n_d}$ satisfying $\mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})$, we can exchange $M_q(\mathbf{d}_{k-1})$ with $M_q(\mathbf{d}'_{k-1})$ and obtain $P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) \leq e^{\epsilon} P(M_q(\mathbf{d}_{k-1}) \in \mathbb{S}) + \delta$. Subtracting the two inequalities yields $1 - e^{\epsilon} - \delta \leq (1 - e^{\epsilon}) P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) - \delta \leq P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) - P(M_q(\mathbf{d}_{k-1}) \in \mathbb{S}) \leq (e^{\epsilon} - 1) P(M_q(\mathbf{d}_{k-1}) + \delta \leq e^{\epsilon} - 1 + \delta$, and hence $|P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) - P(M_q(\mathbf{d}_{k-1}) \in \mathbb{S})| \leq e^{\epsilon} - 1 + \delta$. Since $e^{\epsilon} \approx 1 + \epsilon$ for small $\epsilon > 0$, it means that for sufficiently small $\epsilon, \delta > 0$, the eavesdropper cannot distinguish $\mathbf{d}_{k-1}$ from $\mathbf{d}'_{k-1}$ based on the observation M_q. This means that $\mathbf{d}_{k-1}$ is protected.

Particularly in our problem, the mechanism is given as

$$M_q(\mathbf{d}_{k-1}) = \hat{\mathbf{x}}_{k|k} + \boldsymbol{\omega}_k. \tag{6}$$

We next present what inequality condition does $\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k}$ need to satisfy such that the mechanism (6) is (ϵ, δ)-differentially private. To this end, we first provide the following two lemmas.

Lemma 1: The analytic expression of $\hat{\mathbf{x}}_{k|k}$ with respect to $\mathbf{d}_{k-1}$ is given as $\hat{\mathbf{x}}_{k|k} = q(\mathbf{d}_{k-1}) + \boldsymbol{\nu}_k$, where $q(\mathbf{d}_{k-1}) = \mathbf{M}_k \mathbf{d}_{k-1} + c_k$ with $\mathbf{M}_k = \mathbf{1} \otimes \mathbf{B}_{k-1}$ and c_k being a constant, and $\boldsymbol{\nu}_k$ is a zero-mean Gaussian noise with $\mathrm{Cov}(\boldsymbol{\nu}_k) \geq \boldsymbol{\Upsilon}_k$, where $\boldsymbol{\Upsilon}_k = \bar{\mathbf{G}}_k \mathbf{C}_k \mathbf{Q}_{k-1} \mathbf{C}_k^{\mathrm{T}} \bar{\mathbf{G}}_k^{\mathrm{T}}$, $\bar{\mathbf{G}}_k = \text{block-diag}(\mathbf{G}_{1,k}, \mathbf{G}_{2,k}, \ldots, \mathbf{G}_{M,k})$, and $\mathbf{C}_k = [\mathbf{C}_{1,k}^{\mathrm{T}}, \mathbf{C}_{2,k}^{\mathrm{T}}, \ldots, \mathbf{C}_{M,k}^{\mathrm{T}}]^{\mathrm{T}}$.

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Remark 8: From Lemma 1 and (6), we obtain $M_q(\mathbf{d}_{k-1}) = q(\mathbf{d}_{k-1}) + \boldsymbol{\nu}_k + \boldsymbol{\omega}_k$, where $q(\mathbf{d}_{k-1})$ is the so-called query function. This indicates that the differential privacy level is collectively determined by both noise terms, $\boldsymbol{\nu}_k$ and $\boldsymbol{\omega}_k$.

Lemma 2: Let $\boldsymbol{\mu}_k = q(\mathbf{d}_{k-1}) - q(\mathbf{d}'_{k-1})$ and $\bar{\boldsymbol{\Sigma}}_k = \mathrm{Cov}(\boldsymbol{\nu}_k) + \mathrm{Cov}(\boldsymbol{\omega}_k)$. Then, we have

$$P(M_q(\mathbf{d}_{k-1}) \in \mathbb{S}) \leq e^{\epsilon} P(M_q(\mathbf{d}'_{k-1}) \in \mathbb{S}) + \mathcal{Q}\bigg(\frac{\epsilon}{\|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}}} - \frac{\|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}}}{2} \bigg),$$

where $\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\{-\frac{z^2}{2}\} \mathrm{d}z$ is the $\mathcal{Q}$-function.

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Lemma 2 indicates that the sufficient condition to ensure (ϵ, δ)-differential privacy of the mechanism (6) is

$$\sup_{\mathbf{d}_{k-1}, \mathbf{d}'_{k-1} : \mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})} \mathcal{Q}\bigg(\frac{\epsilon}{\|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}}} - \frac{\|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}}}{2} \bigg) \leq \delta.$$

Unfortunately, the above inequality cannot be directly employed because the analytic computation of $\bar{\boldsymbol{\Sigma}}_k$ is infeasible, owing to the unknown correlations among the measurement noises of the local sensors. To address this, we introduce an analytical lower bound of $\bar{\boldsymbol{\Sigma}}_k$, denoted $\mathbf{S}_k = \boldsymbol{\Upsilon}_k + \text{block-diag}(\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k})$. From $\mathrm{Cov}(\boldsymbol{\nu}_k) \geq \boldsymbol{\Upsilon}_k$ in Lemma 1, we obtain $\mathbf{S}_k \leq \mathrm{Cov}(\boldsymbol{\nu}_k) + \text{block-diag}(\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k}) = \mathrm{Cov}(\boldsymbol{\nu}_k) + \mathrm{Cov}(\boldsymbol{\omega}_k) = \bar{\boldsymbol{\Sigma}}_k$. Then, we have the following theorem.

Theorem 1: Consider the mechanism in (6). Suppose that the injected noise covariances $\{\boldsymbol{\Sigma}_{i,k}\}_{i=1}^{M}$ are chosen such that

$$\sup_{\mathbf{d}_{k-1}, \mathbf{d}'_{k-1} : \mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})} \mathcal{Q}\bigg(\frac{\epsilon}{\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}} - \frac{\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}}{2} \bigg) \leq \delta.$$

Then, the mechanism $M_q(\mathbf{d}_{k-1})$ is (ϵ, δ)-differentially private.

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Remark 9: For any pair of $\mathbf{d}_{k-1}$ and $\mathbf{d}'_{k-1}$ satisfying $\mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})$, Theorem 1 requires that the difference $\boldsymbol{\mu}_k = q(\mathbf{d}_{k-1}) - q(\mathbf{d}'_{k-1})$ satisfies the inequality: $\epsilon / \|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}} - \|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}/2 \geq \mathcal{Q}^{-1}(\delta)$. A smaller Mahalanobis distance $\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}$ indicates that $q(\mathbf{d}_{k-1})$ and $q(\mathbf{d}'_{k-1})$ are statistically closer and thus harder to distinguish, thereby enhancing privacy. Thus, one may reduce $\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}$ by increasing the covariance of the injected noise. This enlarges $\mathbf{S}_k$, thereby reducing $\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}$ since $\mathbf{S}_k^{-1}$ becomes smaller. Observe that the function $f(x) = \epsilon/x - x/2$ is decreasing for $x > 0$. Therefore, reducing $\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}$ increases the value of $f(\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}})$, making Theorem 1's condition easier to meet. Thus, a greater noise covariance leads to a higher (ϵ, δ)-differential privacy level.

Based on Theorem 1, we construct the following constrained minimization problem, aiming at minimizing the sum of MSEs of the local estimates while ensuring (ϵ, δ)-differential privacy:

$$\begin{aligned} \min \quad & \sum_{i=1}^{M} \mathrm{tr}(\boldsymbol{\Sigma}_{i,k}) \\ \text{s.t.} \quad & \sup_{\mathbf{d}_{k-1}, \mathbf{d}'_{k-1} : \mathrm{Adj}(\mathbf{d}_{k-1}, \mathbf{d}'_{k-1})} \mathcal{Q}\bigg(\frac{\epsilon}{\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}} - \frac{\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}}{2} \bigg) \leq \delta \\ & \text{block-diag}(\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k}) \geq 0. \end{aligned} \tag{7}$$

Remark 10: The first constraint of (7) is a joint constraint on the entire block-diagonal noise covariance matrix $\boldsymbol{\Sigma}_k = \text{block-diag}(\boldsymbol{\Sigma}_{1,k}, ..., \boldsymbol{\Sigma}_{M,k})$. The challenge, therefore, is to optimally allocate the privacy budget (in the form of noise covariance) among the different local sensors. Additionally, the optimization variables $\boldsymbol{\Sigma}_{1,k}, \boldsymbol{\Sigma}_{2,k}, \ldots, \boldsymbol{\Sigma}_{M,k}$ are not restricted to being isotropic (i.e., $\boldsymbol{\Sigma}_{i,k} = \sigma_i \mathbf{I}_{n_x}$, $i = 1, 2, \ldots, M$). This is more general than most of the existing works where the parameters to be determined are scalars (see, e.g., [3], [17], [18], [21], [25]). However, this increased generality also results in a greater complexity for the minimization problem.

Remark 11: It follows from $\mathcal{Q}(\epsilon/\|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}} - \|\boldsymbol{\mu}_k\|_{\bar{\boldsymbol{\Sigma}}_k^{-1}}/2) \leq \mathcal{Q}(\epsilon/\|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}} - \|\boldsymbol{\mu}_k\|_{\mathbf{S}_k^{-1}}/2)$ that the use of $\mathbf{S}_k$ relaxes the privacy constraint in (7), but comes at the cost of increased noise injection. This leads to a larger state estimation covariance, demonstrating a direct trade-off between privacy level and estimation accuracy.

On the one hand, it is not difficult to verify that the first constraint is non-convex. Thus, the problem (7) is non-convex and its analytic solution is hard to obtain. On the other hand,

computational efficiency is critically important in real-time state estimation. Thus, it is of great significance to develop an efficient algorithm to solve the problem (7). To this end, an approach of relaxation is proposed, as presented in the following theorem.

Theorem 2 (SDP relaxation for optimal noise design): Let $b = \frac{\epsilon_0^2 \|\mathbf{M}_k\|_2^2}{(-\mathcal{Q}^{-1}(\delta)+\sqrt{(\mathcal{Q}^{-1}(\delta))^2+2\epsilon})^2}$. Then, the original problem (7) can be relaxed to the following SDP problem:

$$\begin{aligned} \min \quad & \sum_{i=1}^{M} \mathrm{tr}(\mathbf{\Sigma}_{i,k}) \\ \text{s.t.} \quad & \text{block-diag}(\mathbf{\Sigma}_{1,k}, \mathbf{\Sigma}_{2,k}, \ldots, \mathbf{\Sigma}_{M,k}) \\ & + \mathbf{\Upsilon}_k - b\mathbf{I}_{Mn_x} \geq 0, \\ & \text{block-diag}(\mathbf{\Sigma}_{1,k}, \mathbf{\Sigma}_{2,k}, \ldots, \mathbf{\Sigma}_{M,k}) \geq 0. \end{aligned} \tag{8}$$

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Remark 12: The SDP relaxation (8) offers a twofold benefit. First, it is computationally tractable and can be efficiently solved by standard packages like CVX (see [35]). Second, and crucially, any feasible solution to (8) also satisfies the constraints of the original problem (7). This implies that the (ϵ, δ)-differential privacy of (6) is maintained. Thus, this relaxation yields a practical solution method without compromising the privacy guarantee.

To assess the effectiveness of the SDP relaxation (8), the following proposition quantifies the relaxation quality by providing an upper bound on the gap between the SDP relaxation (8) and the original problem (7).

Proposition 1 (Upper bound on the relaxation gap): Let J^*_{orig} and J^*_{relax} be the minimums of the original problem (7) and the SDP problem (8), respectively, and $\mathbf{S}^*_{k,\text{orig}} = \mathbf{\Upsilon}_k + \mathbf{\Sigma}^*_{k,\text{orig}}$ with $\mathbf{\Sigma}^*_{k,\text{orig}}$ being the optimal solution of (7). Then, the relaxation gap is bounded by

$$J^*_{\text{relax}} - J^*_{\text{orig}} \leq \left(\max\left(1, \frac{b}{\lambda_{\min}(\mathbf{S}^*_{k,\text{orig}})}\right) - 1 \right) \mathrm{tr}(\mathbf{S}^*_{k,\text{orig}}).$$

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

According to Proposition 1, the relaxation gap vanishes if $\lambda_{\min}(\mathbf{S}^*_{k,\text{orig}}) \geq b$ (the relaxation is tight); otherwise, its upper bound monotonically increases with the ratio $b/\lambda_{\min}(\mathbf{S}^*_{k,\text{orig}})$.

IV. Privacy-preserving distributed fusion estimation

At the fusion center side, after receiving all the noisy state estimates and error covariance matrices, the fusion estimate, denoted by $\hat{\mathbf{x}}^{\text{cen}}_{k|k}$, and the corresponding error covariance matrix, denoted by $\mathbf{P}_{k|k}$, are derived by utilizing the approach of covariance intersection [32]:

$$\mathbf{P}^{-1}_{k|k}\hat{\mathbf{x}}^{\text{cen}}_{k|k} = \sum_{i=1}^{M} w_i \bar{\mathbf{P}}^{-1}_{i,k|k}\bar{\mathbf{x}}_{i,k|k}, \tag{9}$$

$$\mathbf{P}^{-1}_{k|k} = \sum_{i=1}^{M} w_i \bar{\mathbf{P}}^{-1}_{i,k|k}, \tag{10}$$

where $\bar{\mathbf{x}}_{i,k|k} = \hat{\mathbf{x}}_{i,k|k} + \boldsymbol{\omega}_{i,k}$, $\boldsymbol{\omega}_{i,k} \sim \mathcal{N}(0, \mathbf{\Sigma}^*_{i,k})$, and $\bar{\mathbf{P}}_{i,k|k} = \mathbf{P}_{i,k|k} + \mathbf{\Sigma}^*_{i,k}$.

The proposed differentially private distributed fusion estimation algorithm is summarized in Algorithm 1. It should be noted in Algorithm 1 that the local sensors uses the optimal local state estimates given by (4) for the next prediction step. The noisy local estimates are adopted at the fusion center only. Besides, the process that the fusion center sends $\{\mathbf{\Sigma}^*_{i,k}\}_{i=1}^M$ to the local sensors will not cause a privacy leakage since the full eavesdropper cannot obtain the sampled values of the injected noises from $\{\mathbf{\Sigma}^*_{i,k}\}_{i=1}^M$.

Algorithm 1 Differentially private distributed fusion estimation algorithm

Input: $\hat{\mathbf{x}}_{i,k-1|k-1}$, $\mathbf{P}_{i,k-1|k-1}$

1: **for** $i = 1, 2, \ldots, M$ **do**
2: Node i calculates $\hat{\mathbf{x}}_{i,k|k-1}$ and $\mathbf{P}_{i,k|k-1}$ using (2) and (3).
3: Node i calculates $\hat{\mathbf{x}}_{i,k|k}$ and $\mathbf{P}_{i,k|k}$ using (4) and (5).
4: **end for**
5: Fusion center solves (8) to get

$$\mathbf{\Sigma}^*_k = \text{block-diag}(\mathbf{\Sigma}^*_{1,k}, \mathbf{\Sigma}^*_{2,k}, \ldots, \mathbf{\Sigma}^*_{M,k}),$$

and sends $\mathbf{\Sigma}^*_{i,k}$ to Node i.
6: **for** $i = 1, 2, \ldots, M$ **do**
7: Node i generates $\boldsymbol{\omega}_{i,k} \sim \mathcal{N}(0, \mathbf{\Sigma}^*_{i,k})$.
8: Node i calculates $\bar{\mathbf{x}}_{i,k|k} = \hat{\mathbf{x}}_{i,k|k} + \boldsymbol{\omega}_{i,k}$.
9: Node i calculates $\bar{\mathbf{P}}_{i,k|k} = \mathbf{P}_{i,k|k} + \mathbf{\Sigma}^*_{i,k}$.
10: Node i sends $\bar{\mathbf{x}}_{i,k|k}$ and $\bar{\mathbf{P}}_{i,k|k}$ to the fusion center.
11: **end for**
12: Fusion center calculates $\hat{\mathbf{x}}^{\text{cen}}_{k|k}$ and $\mathbf{P}_{k|k}$ using (9) and (10).

Output: $\hat{\mathbf{x}}^{\text{cen}}_{k|k}$, $\mathbf{P}_{k|k}$

Remark 13: The covariance intersection fusion yields a consistent estimate, that is, the fused covariance matrix $\mathbf{P}_{k|k}$ satisfies $\mathbb{E}[(\hat{\mathbf{x}}^{\text{cen}}_{k|k} - \mathbf{x}_k)(\hat{\mathbf{x}}^{\text{cen}}_{k|k} - \mathbf{x}_k)^{\mathrm{T}}] \leq \mathbf{P}_{k|k}$, conservatively bounding the true error to prevent over-confidence and filter divergence. This holds provided that the covariance matrix from each local sensor upper-bounds its true error [32]. In Algorithm 1, the fusion center receives the noisy state estimate $\bar{\mathbf{x}}_{i,k|k} = \hat{\mathbf{x}}_{i,k|k} + \boldsymbol{\omega}_{i,k}$, whose true error covariance matrix is $\mathbb{E}\left[(\bar{\mathbf{x}}_{i,k|k} - \mathbf{x}_k)(\bar{\mathbf{x}}_{i,k|k} - \mathbf{x}_k)^{\mathrm{T}}\right] = \mathbf{P}_{i,k|k} + \mathbf{\Sigma}^*_{i,k} = \bar{\mathbf{P}}_{i,k|k}$. Therefore, although $\mathbf{P}_{i,k|k}$ contains no information about $\mathbf{d}_{k-1}$ (Remark 5), transmitting the augmented covariance matrix $\bar{\mathbf{P}}_{i,k|k}$ is required for consistency.

The following proposition quantifies the estimation accuracy loss incurred by privacy protection. The loss, defined as $\Delta\mathbf{P}_{k|k} = \mathbf{P}_{k|k} - \mathbf{P}^{\text{umv}}_{k|k} \geq 0$ at time step k, is derived by comparing the error covariance matrix of Algorithm 1 with that of the non-private, linear unbiased minimum-variance estimator.

Proposition 2 (Estimation accuracy loss): The estimation accuracy loss of Algorithm 1 at time step k is given as:

$$\Delta\mathbf{P}_{k|k} = \mathbf{P}_{k|k}\left(\sum_{i=1}^{M} w_i \mathbf{P}^{-1}_{i,k|k}\mathbf{\Sigma}^*_{i,k}(\mathbf{P}_{i,k|k} + \mathbf{\Sigma}^*_{i,k})^{-1}\right)\mathbf{P}^{\text{umv}}_{k|k}.$$

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Remark 14: Based on Proposition 2, we have the following observations: i) Under small injected noise (i.e., $\|\mathbf{\Sigma}_{i,k}^*\|$ is small relative to $\|\mathbf{P}_{i,k|k}\|$), the inverse term admits the approximation $(\mathbf{P}_{i,k|k} + \mathbf{\Sigma}_{i,k}^*)^{-1} \approx \mathbf{P}_{i,k|k}^{-1} - \mathbf{P}_{i,k|k}^{-1}\mathbf{\Sigma}_{i,k}^*\mathbf{P}_{i,k|k}^{-1}$, and thus $\mathbf{P}_{k|k}^{\text{priv}} \approx \mathbf{P}_{k|k}^{\text{umv}}$. Consequently, the estimation accuracy loss can be approximated as $\Delta\mathbf{P}_{k|k} \approx \mathbf{P}_{k|k}^{\text{umv}}\left(\sum_{i=1}^{M} w_i\mathbf{P}_{i,k|k}^{-1}\mathbf{\Sigma}_{i,k}^*\mathbf{P}_{i,k|k}^{-1}\right)\mathbf{P}_{k|k}^{\text{umv}}$, which indicates that $\Delta\mathbf{P}_{k|k}$ is approximately linear in $\mathbf{\Sigma}_k^*$. ii) The result also reveals a trade-off between privacy level and estimation accuracy: a higher privacy level implies a larger noise covariance $\mathbf{\Sigma}_k^*$, which enlarges the estimation accuracy loss $\Delta\mathbf{P}_{k|k}$.

The information transmission in Algorithm 1 is illustrated in Fig. 2. We can see from Fig. 2 that the local sensors send their state estimates $\{\bar{\mathbf{x}}_{i,k|k}\}_{i=1}^M$ and error covariance matrices $\{\bar{\mathbf{P}}_{i,k|k}\}_{i=1}^M$ to the fusion center, but the fusion center does not send the fusion estimate $\hat{\mathbf{x}}_{k|k}^{\text{cen}}$ and error covariance matrix $\mathbf{P}_{k|k}$ back to the local sensors.

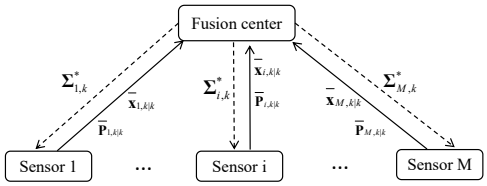


Fig. 2: Information transmission in Algorithm 1

Accuracy is crucial in distributed fusion estimation as it directly improves the reliability of decision-making in various applications. To enhance the fusion estimation accuracy of Algorithm 1 while ensuring the same (ϵ, δ)-differential privacy, we introduce a feedback mechanism. Specifically, after implementing Algorithm 1, the fusion center further sends the fusion estimate $\hat{\mathbf{x}}_{k|k}^{\text{cen}}$ and error covariance matrix $\mathbf{P}_{k|k}$ back to all the local sensors. Then, each node i updates its local estimate and error covariance matrix to $\hat{\mathbf{x}}_{i,k|k}^{\text{update}}$ and $\mathbf{P}_{i,k|k}^{\text{update}}$, by fusing its local estimate $\hat{\mathbf{x}}_{i,k|k}$ and error covariance matrix $\mathbf{P}_{i,k|k}$ with the fusion estimate $\hat{\mathbf{x}}_{k|k}^{\text{cen}}$ and error covariance matrix $\mathbf{P}_{k|k}$. The differentially private distributed fusion estimation algorithm with enhanced accuracy via a feedback mechanism is summarized in Algorithm 2.

Remark 15: By implementing Step 4 and Step 5 in Algorithm 2, each node enhances its local estimation accuracy at time step k. Furthermore, the fusion estimation accuracy for the next time step $k+1$ will be enhanced. Despite an enhanced accuracy, there is always a loss due to the noise injection strategy, which reflects the trade-off between differential privacy level and fusion estimation accuracy.

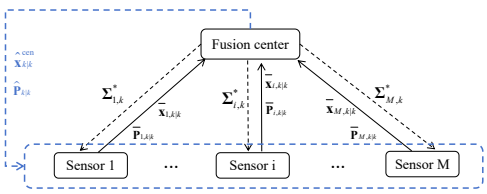


Fig. 3: Information transmission in Algorithm 2

Algorithm 2 Differentially private distributed fusion estimation algorithm with enhanced accuracy via a feedback mechanism

Input: $\hat{\mathbf{x}}_{i,k-1|k-1}^{\text{update}}$, $\mathbf{P}_{i,k-1|k-1}^{\text{update}}$

1: Implement Algorithm 1 to get $\hat{\mathbf{x}}_{k|k}^{\text{cen,(A2)}}$ and $\mathbf{P}_{k|k}^{\text{(A2)}}$ at the fusion center, where $(\hat{\mathbf{x}}_{i,k-1|k-1}, \mathbf{P}_{i,k-1|k-1})$ is replaced by $(\hat{\mathbf{x}}_{i,k-1|k-1}^{\text{update}}, \mathbf{P}_{i,k-1|k-1}^{\text{update}})$.

2: Fusion center sends $\hat{\mathbf{x}}_{k|k}^{\text{cen,(A2)}}$ and $\mathbf{P}_{k|k}^{\text{(A2)}}$ to all the local sensors.

3: **for** $i = 1, 2, \ldots, M$ **do**

4: Node i updates its local estimate and error covariance matrix using the approach of covariance intersection:

$$\left(\mathbf{P}_{i,k|k}^{\text{update}}\right)^{-1}\hat{\mathbf{x}}_{i,k|k}^{\text{update}} = v_1^{(i)}\left(\mathbf{P}_{i,k|k}^{\text{(A2)}}\right)^{-1}\hat{\mathbf{x}}_{i,k|k}^{\text{(A2)}} + v_2^{(i)}\left(\mathbf{P}_{k|k}^{\text{(A2)}}\right)^{-1}\hat{\mathbf{x}}_{k|k}^{\text{cen,(A2)}},$$

$$\left(\mathbf{P}_{i,k|k}^{\text{update}}\right)^{-1} = v_1^{(i)}\left(\mathbf{P}_{i,k|k}^{\text{(A2)}}\right)^{-1} + v_2^{(i)}\left(\mathbf{P}_{k|k}^{\text{(A2)}}\right)^{-1},$$

where the weights $v_1^{(i)}$, $v_2^{(i)}$ are chosen as follows:

- If $\mathbf{P}_{k|k}^{\text{(A2)}} \leq \mathbf{P}_{i,k|k}^{\text{(A2)}}$, set $v_1^{(i)} = 0, v_2^{(i)} = 1$;
- Otherwise, set $v_1^{(i)} = 1, v_2^{(i)} = 0$.

5: **end for**

Output: $\hat{\mathbf{x}}_{k|k}^{\text{cen,(A2)}}$, $\mathbf{P}_{k|k}^{\text{(A2)}}$

The information transmission in Algorithm 2 is illustrated in Fig. 3. We can see from Figs. 2 and 3 that Algorithm 2 needs to transmit $\hat{\mathbf{x}}_{k|k}^{\text{cen}}$ and $\mathbf{P}_{k|k}$, but Algorithm 1 does not. This implies that the full eavesdropper can acquire more data in Algorithm 2. Then, a natural question is whether Algorithm 2 can ensure the same (ϵ, δ)-differential privacy while achieving enhanced estimation accuracy over Algorithm 1? The following two propositions give the answer.

Proposition 3: Algorithm 2 ensures the same (ϵ, δ)-differential privacy as Algorithm 1.

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Proposition 4: Algorithm 2 enhances the fusion and local estimation accuracy of Algorithm 1, i.e., $\mathbf{P}_{k|k}^{\text{(A2)}} \leq \mathbf{P}_{k|k}$, $\mathbf{P}_{i,k|k}^{\text{update}} \leq \mathbf{P}_{i,k|k}$, for all k.

Proof. Due to space limitation, we leave the proof to the extended version [34] of this paper (arXiv:2512.22914). ■

Remark 16: Propositions 3 and 4 indicate that Algorithm 2 enhances the fusion estimation accuracy of Algorithm 1 while ensuring the same (ϵ, δ)-differential privacy. However, more computational cost is needed in Algorithm 2. Specifically, the computational complexity of Algorithm 2 is $\mathcal{O}(Mn_x^3)$ more than that of Algorithm 1. Overall, Algorithm 1 prefers to a scenario with low-complexity requirements, while Algorithm 2 prefers to a scenario with high-accuracy requirements.

Remark 17: Compared to encryption-based methods (see, e.g., [2], [3], [15]), the proposed algorithms are more efficient. Specifically, the computational cost is lower because it primarily involves solving an SDP, which can be performed efficiently using interior-point methods (see, e.g., [36]). Moreover, the communication overhead is lower because only noisy

estimates and their covariance matrices should be transmitted. Beyond efficiency, a further distinction lies in the privacy guarantee: while encryption provides a binary guarantee reliant on computational assumptions, our differential privacy framework ensures a probabilistic guarantee.

Remark 18: In implementing the proposed algorithms, two practical issues are addressed as follows: i) numerical stability, which is ensured via square-root filtering techniques (see, e.g., [37]); and ii) potential model uncertainty, which is ensured via robust filtering techniques (see, e.g., [37]).

V. Example

Consider the dynamic model in [1] as follows:

$$\mathbf{x}_{k+1} = \mathbf{A}_k \mathbf{x}_k + \mathbf{B}_k \mathbf{d}_k + \mathbf{w}_k,$$

where

$$\mathbf{A}_k = \begin{bmatrix} 1 & \Delta t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \Delta t \\ 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{B}_k = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \mathbf{d}_k = \begin{bmatrix} 5\cos k \\ 5\cos k \end{bmatrix},$$

and $\mathbf{w}_k \sim \mathcal{N}(0, \mathbf{Q}_k)$ with $\mathbf{Q}_k = \mathrm{diag}([1, 0.1, 1, 0.1]^{\mathrm{T}})$. The initial state is generated from $\mathcal{N}(\hat{\mathbf{x}}_0, \mathbf{P}_0)$ with $\hat{\mathbf{x}}_0 = [0, 5, 0, 5]^{\mathrm{T}}$ and $\mathbf{P}_0 = \mathrm{diag}([10, 10, 10, 10]^{\mathrm{T}})$. The distributed multi-sensor network system consists of two local sensors with their measurement model being

$$\mathbf{y}_{i,k} = \mathbf{C}_{i,k} \mathbf{x}_k + \mathbf{v}_{i,k}, \ i = 1, 2,$$

where $\mathbf{C}_{1,k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$, $\mathbf{C}_{2,k} = \mathbf{I}_4$, and $\mathbf{v}_{i,k} \sim \mathcal{N}(0, \mathbf{R}_i)$ with $\mathbf{R}_1 = 0.1\mathbf{I}_2$ and $\mathbf{R}_2 = 20\mathbf{I}_4$.

Set $\epsilon_0 = 0.1$, $\epsilon = \delta = 10^{-3}$ for differential privacy level (see Definition 3). In the covariance intersection fusion (9) and (10), uniform weights ($w_1 = w_2 = 0.5$) are adopted for simplicity. To demonstrate the effectiveness of the proposed two algorithms, the MSEs of local and fusion estimates over 50 time steps and 50 Monte Carlo runs for Algorithm 1 (legends labeled A1) and Algorithm 2 (legends labeled A2) are depicted in Fig. 4. We have the following observations and explanations:

1) Under the same differential privacy level, the MSEs of local and fusion estimates in Algorithm 2 are smaller than those in Algorithm 1 consistently. Intuitively, for the same line shape, the red lines are all below the black lines. This demonstrates that Algorithm 2 does enhance the local and fusion estimation accuracy of Algorithm 1.

2) For Algorithm 1, the MSEs of fusion estimates are smaller than those of local estimates consistently. Intuitively, the black solid line is below the other two black marked lines consistently. This is due to the effectiveness of the covariance intersection approach adopted at the fusion center.

3) For Algorithm 2, however, the MSE of fusion estimate is smaller than that of Sensor 2 and larger than that of Sensor 1 at each time step. Intuitively, the red solid line is between the other two red marked lines. This is because the covariance intersection approach is inherently conservative to ensure consistency (Remark 13). As a result, Sensor 2 may not trust the feedback from the fusion center, leading to a lower local estimation accuracy compared with the fusion center.

Table I lists the averaged MSEs for different weight selections in covariance intersection. The results show that Algorithm 2 outperforms Algorithm 1 across all weighting schemes. Moreover, the MSEs of both algorithms decrease as the weight w_1 increases. This trend is consistent with the higher measurement accuracy of Node 1 compared to Node 2, as reflected by the smaller order of magnitude of its measurement noise covariance $\mathbf{R}_1$.

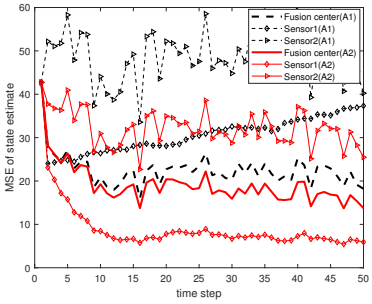
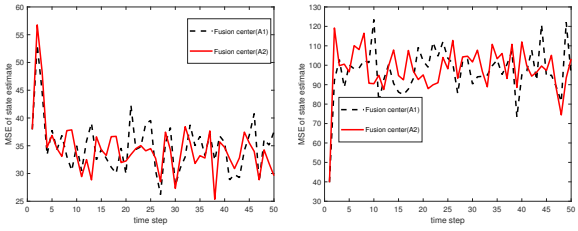


Fig. 4: MSEs of local and fusion estimates for Algorithm 1 and Algorithm 2.

TABLE I: Comparison of averaged MSEs under different weight selections for covariance intersection.

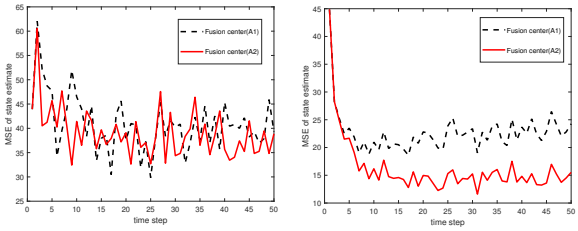
MSE / Algorithm \ (w_1, w_2)	$(0.4, 0.6)$	$(0.5, 0.5)$	$(0.6, 0.4)$
Algorithm 1	34.36	26.12	24.67
Algorithm 2	22.43	16.86	11.85

To show the trade-off between differential privacy level and fusion estimation accuracy, the MSEs of fusion estimates for different parameter settings are presented in Figs. 5 and 6.



(a) $\epsilon_0 = 0.5, \epsilon = \delta = 10^{-3}$. (b) $\epsilon_0 = 1, \epsilon = \delta = 10^{-3}$.

Fig. 5: MSEs of fusion estimates for different ϵ_0.



(a) $\epsilon_0 = 0.1, \epsilon = \delta = 10^{-6}$. (b) $\epsilon_0 = 0.1, \epsilon = \delta = 0.1$.

Fig. 6: MSEs of fusion estimates for different ϵ, δ.

For different ϵ_0, the MSEs of fusion estimates are compared in Fig. 5. Specifically, from Fig. 5(a) to Fig. 5(b), the ϵ_0 becomes larger, and thus the differential privacy level gets higher. Nevertheless, the fusion estimation accuracy gets lower, as confirmed in Fig. 5(b). For different ϵ, δ, the MSEs of fusion estimates are compared in Fig. 6. Specifically, from Fig. 6(a) to Fig. 6(b), the ϵ and δ becomes larger, and thus the differential privacy level gets lower. As expected, the fusion estimation accuracy in Fig. 6(b) is superior to that in Fig. 6(a). Overall, Figs. 5 and 6 illustrate the trade-off between differential privacy level and fusion estimation accuracy.

VI. Conclusion

In this paper, we have achieved distributed fusion estimation while protecting the exogenous inputs against full eavesdropping. By solving a constrained minimization problem, the (ϵ, δ)-differential privacy is ensured and the sum of MSEs of local estimates is minimized simultaneously. We relax the non-convex minimization problem to an SDP for efficient real-time state estimation. We develop two differentially private distributed fusion estimation algorithms emphasizing low complexity and high accuracy, respectively. Particularly, the second algorithm with the feedback mechanism enhances the fusion estimation accuracy of the first algorithm while ensuring the same (ϵ, δ)-differential privacy, despite sacrificing some acceptable computational complexity. Given that protecting a sequence of inputs is more general than protecting only the latest one, a promising future direction is to generalize our approach to protect the latest k_1 inputs ($k_1 \geq 2$).

References

[1] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation: Theory, Algorithms, and Software*. New York, NY, USA: Wiley, 2001.

[2] X. Yan, B. Chen, Y. Zhang, and L. Yu, "Distributed encryption fusion estimation against full eavesdropping," *Automatica*, vol. 153, Article 111025, 2023.

[3] X. Yan, B. Chen, Y. Zhang, and L. Yu, "Guaranteeing differential privacy in distributed fusion estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 3, pp. 3416–3423, 2023.

[4] G. Cao and J. Wang, "Distributed unknown input observer," *IEEE Transactions on Automatic Control*, vol. 68, no. 12, pp. 8244–8251, 2023.

[5] G. Yang, A. Barboni, H. Rezaee, and T. Parisini, "State estimation using a network of distributed observers with unknown inputs," *Automatica*, vol. 146, Article 110631, 2022.

[6] Y. Tian, X. Li, B. Dong, Y. Gao, and L. Wu, "Event-based sliding mode control under denial-of-service attacks," *Science China Information Sciences*, vol. 65, Article 162203, 2022.

[7] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A stackelberg game analysis," *IEEE Transactions on Automatic Control*, vol. 63, no. 10, pp. 3503–3509, 2018.

[8] B. Chen, D. W. C. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 2, pp. 455–468, 2019.

[9] B. Chen, D. W. C. Ho, G. Hu, and L. Yu, "Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks," *IEEE Transactions on Cybernetics*, vol. 48, no. 6, pp. 1862–1876, 2018.

[10] Y. Liu and G.-H. Yang, "Event-triggered distributed state estimation for cyber-physical systems under DoS attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 5, pp. 3620–3631, 2022.

[11] X. Ren, Y. Mo, J. Chen, and K. H. Johansson, "Secure state estimation with byzantine sensors: A probabilistic approach," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3742–3757, 2020.

[12] W.-A. Zhang, L. Yu, and D. He, "Sequential fusion estimation for sensor networks with deceptive attacks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 3, pp. 1829–1843, 2020.

[13] H. Song, P. Shi, C.-C. Lim, W.-A. Zhang, and L. Yu, "Attack and estimator design for multi-sensor systems with undetectable adversary," *Automatica*, vol. 109, Article 108545, 2019.

[14] J. Chen, C. Dou, L. Xiao, and Z. Wang, "Fusion state estimation for power systems under DoS attacks: A switched system approach," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1679–1687, 2019.

[15] D. Xu, B. Chen, Y. Zhang, and L. Yu, "Distributed anti-eavesdropping fusion estimation under energy constraints," *IEEE Transactions on Automatic Control*, vol. 68, no. 12, pp. 7795–7802, 2023.

[16] K. Wei, J. Li, C. Ma, M. Ding, F. Shu, H. Zhao, W. Chen, and H. Zhu, "Gradient sparsification for efficient wireless federated learning with differential privacy," *Science China Information Sciences*, vol. 67, Article 142303, 2024.

[17] J. Wang, J. Ke, and J. F. Zhang, "Differentially private bipartite consensus over signed networks with time-varying noises," *IEEE Transactions on Automatic Control*, vol. 69, no. 9, pp. 5788–5803, 2024.

[18] T. Ding, S. Zhu, J. He, C. Chen, and X. Guan, "Differentially private distributed optimization via state and direction perturbation in multiagent systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 2, pp. 722–737, 2022.

[19] Y. Wang and A. Nedić, "Tailoring gradient methods for differentially private distributed optimization," *IEEE Transactions on Automatic Control*, vol. 69, no. 2, pp. 872–887, 2024.

[20] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2017.

[21] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed nash equilibrium seeking for aggregative games," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2451–2458, 2022.

[22] Y. Wang and A. Nedić, "Differentially private distributed algorithms for aggregative games with guaranteed convergence," *IEEE Transactions on Automatic Control*, vol. 69, no. 8, pp. 5168–5183, 2024.

[23] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3863–3878, 2020.

[24] K. Yazdani, A. Jones, K. Leahy, and M. Hale, "Differentially private LQ control," *IEEE Transactions on Automatic Control*, vol. 68, no. 2, pp. 1061–1068, 2023.

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

[26] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3679–3695, 2018.

[27] E. Nekouei, H. Sandberg, M. Skoglund, and K. H. Johansson, "Optimal privacy-aware estimation," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2253–2266, 2022.

[28] C. Weng, E. Nekouei, and K. H. Johansson, "Optimal privacy-aware dynamic estimation," *IEEE Transactions on Automatic Control*, vol. 70, no. 11, pp. 7095–7108, 2025.

[29] L. Guo, J. Wang, Y. Zhao, and J. F. Zhang, "State estimation with protecting exogenous inputs via Cramér-Rao lower bound approach," *Science China Information Sciences*, vol. 69, no. 9, Article 192207, 2026.

[30] P. K. Kitanidis, "Unbiased minimum-variance linear state estimation," *Automatica*, vol. 23, no. 6, pp. 775–778, 1987.

[31] M. Darouach and M. Zasadzinski, "Unbiased minimum variance estimation for systems with unknown exogenous inputs," *Automatica*, vol. 33, no. 4, pp. 717–719, 1997.

[32] S. Julier and J. Uhlmann, "A non-divergent estimation algorithm in the presence of unknown correlations," in *American Control Conference*, Albuquerque, NM, USA, Jun. 6, 1997.

[33] F. S. Cattivelli and A. H. Sayed, "Diffusion strategies for distributed Kalman filtering and smoothing," *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2069–2084, 2010.

[34] L. Guo, J. Wang, Y. Zhao, and J. F. Zhang, "Distributed fusion estimation with protecting exogenous inputs," *arXiv:2512.22914*, 2025.

[35] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," https://cvxr.com/cvx, Mar. 2014.

[36] S. J. Wright, *Primal-Dual Interior-Point Methods*. Philadelphia, PA, USA: SIAM, 1997.

[37] D. Simon, *Optimal State Estimation: Kalman, H∞, and Nonlinear Approaches*. New York, NY, USA: Wiley, 2006.