Correspondence

Guaranteeing Differential Privacy in Distributed Fusion Estimation

With the increasing openness of networked sensor systems, information leakage has become an ever-critical issue due to the malicious eavesdropping attacks on privately available data. The distributed fusion estimates (DFEs), which perform well by combining local state estimates (LSEs) supplied by multiple sensors, imperatively require privacy preserving. Note that the eavesdropper can acquire DFEs by wiretapping fusion information from fusion center and weighting LSEs from sensors. For countering such dual eavesdropping, we introduce the idea called differential privacy from database literature. Basically, the publicly released estimates (PREs), which gather statistical information about DFEs, are considered to be disturbed with stochastic noises. The lower bounds of noise covariances can be designed with the privacy parameters and estimation systems. Furthermore, we disperse the location of noise insertion from PREs to LSEs. In this case, the eavesdropper cannot obtain optimal estimate even if it fuses local data by using original criterion, while the differential privacy is still satisfied. Finally, a target tracking system with multisensor observation is given to verify the effectiveness of the proposed methods.

I. INTRODUCTION

Networked sensor systems (NSSs) are a collection of autonomous sensors that are geographically dispersed and connected via networks. After gathering measured information provided by local sensors in NSSs, fusion center (FC) can provide powerful supervision on the dynamics of real-world systems by resorting to multisensor information fusion methods [1]. Compared with traditional sensor systems, NSSs can effectively reduce wiring complexities and enhance scalability. As a result, they have been investigated for a variety of industries, such as cyber-physical systems [2], target tracking systems [3], and multirobot systems [4]. A practical application of NSSs is shown in Fig. 1, where laser, camera, and radar deployed in a quadrotor simultaneously observe the changing environment. The measurements of these sensors are packaged and transmitted to cloud server over networks, and subsequently

Manuscript received 18 June 2022; revised 6 September 2022; accepted 27 October 2022. Date of publication 7 November 2022; date of current version 9 June 2023.

DOI. No. 10.1109/TAES.2022.3219799

Refereeing of this contribution was handled by T. Wewelwala.

This work was supported in part by the National Natural Science Funds of China under Grant 61973277 and Grant 62073292, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR20F030004, and in part by the Major Key Project of PCL under Grant PCL2021A09.

Authors' addresses: The authors are with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China, and also with Zhejiang Provincial United Key Laboratory of Embedded Systems, Hangzhou 310032, China, E-mail: (yanxinhao1998@aliyun.com; bchen@aliyun.com; YuchenZhang95@163.com; lyu@zjut.edu.cn). *(Corresponding author: Bo Chen.)*

utilized for state estimation based upon certain fusion criteria. However, due to the wide distribution of sensors and the openness to network, NSSs are susceptible to a series of attacks [5], including denial-of-service attacks [6], false data injection attacks [7], replay attacks [8], and eavesdropping attacks [9], [10]. Note that the information leakage can make other attacks more aggressive. Therefore, one of the most significant research topics is protecting the privacy of NSSs against eavesdroppers.

For countering eavesdropping, many confidentiality techniques have been studied from the aspects of information theory, cryptography, signal processing, and control theory. In particular, the usage of stochastic noise is viewed as an effective strategy, since the introduced unpredictability can confound eavesdroppers. The noises have been considered as a means of reaching some performance goals, such as ensuring sufficient randomness [9] and disturbing transmission information [11], [12], which relies on channel estimation [13]. As a basic mechanism, noises with certain distributions are considered to affect the probability of publicly released estimates (PREs) after statistical query in differential privacy [14], [15]. Attributed to its powerful performance and rigorous mathematical models, differential privacy has been expanded to a wide range of fields, such as machine learning [16], optimization [17], consensus [18], game theory [19], and control theory [20]. Particularly in filtering and estimation areas, differentially private filters were discussed in [21]. Table I gives the part of related works about differential privacy that are categorized by their study problems. In this correspondence, the idea of differential privacy is introduced for guaranteeing strong confidentiality of fusion estimates. It provides the probability sense to the confidentiality assessment, which differs from traditional covariance index in estimation [9]. Besides, the combination of existing strategies under several senses expands the possibility of future works.

In the subject of information fusion, there exist two primary estimation structures: centralized fusion structure [22], [23], [24] and distributed fusion structure [25], [26], [27]. It can be noted that distributed fusion is more robust and has higher fault tolerance owing to its local preprocessing on measurements [28], [29]. Therefore, we study the distributed confidentiality fusion estimation problem by resorting to the differentially private mechanism. The main contributions of this correspondence are summarized as follows:

1) Differential privacy is introduced for guaranteeing the confidentiality of distributed fusion estimates (DFEs), where the PREs that contain statistical information about DFEs are perturbed by Gaussian noises.
2) Local perturbation framework is proposed for achieving the differential privacy on same level, in which the noise injection process is dispersed from PREs to LSEs. Then, the eavesdropper cannot obtain DFEs by fusing local transmitted data, since the covariances of LSEs are inaccurate.

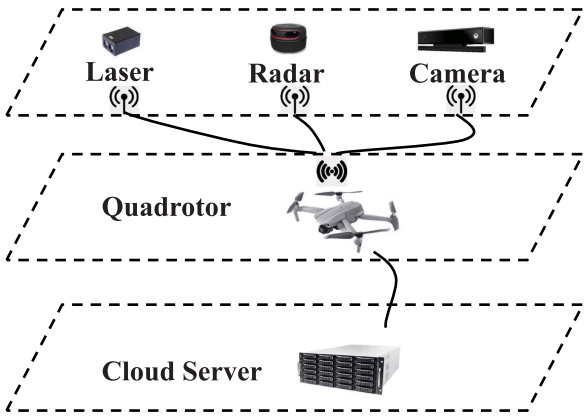

Fig. 1. Practical application of NSSs.

The rest of this article is organized as follows. Section II describes the preliminaries, including system and estimation models, and then discusses the interests of proposed problems. In Section III, the differential privacy problem is first solved with traditional Gaussian mechanism. In the sequel, we propose two specific noise perturbation approach for distributed fusion structure. Then, in Section IV, we simulate the differentially private algorithms on a target tracking system and show the effects of some parameters. Finally, Section VI concludes this article.

Notations: $\mathbb{R}^n$ is the set of n-dimensional vectors and $\mathbb{R}^{n\times m}$ is the set of all $n \times m$ real matrices. The superscript "T" represents the transpose and "I_n" represents the identity matrix with n dimension. Let $\text{diag}\{a_1, \ldots, a_n\}$ and $\text{col}\{a_1, \ldots, a_n\}$, respectively, stand for a diagonal matrix and column vector whose elements are $\{a_1, \ldots, a_n\}$. $\mathbb{E}(\cdot)$ means mathematical expectation and $\mathbb{P}(\cdot)$ means probability. $X > (<)0$ denotes a positive-definite (negative-definite) matrix and $X \geq (\leq)0$ denotes a nonnegative-definite (nonpositive-definite) matrix. $\|\cdot\|$ represents the 2-norm, and $\sigma_{\max}(\cdot)$ represents the maximum singular value. The abbreviation "i.i.d." means independent and identically distributed, while "iff" means if and only if.

II. PROBLEM FORMULATION

A. System Models

Consider an NSS that observes a dynamic object with multiple sensors described by the discrete-time state-space model. In this case, the state transition equation is written as

$$x(t+1) = Ax(t) + w(t) \tag{1}$$

where $x(t) \in \mathbb{R}^n$ denotes the system state and $A \in \mathbb{R}^{n\times n}$ is the state transition matrix. To monitor this object, several sensors are spatially deployed with their measurement equations given by

$$y_i(t) = C_i x(t) + v_i(t)\ (i = 1, \ldots, L) \tag{2}$$

where $y_i(t) \in \mathbb{R}^{m_i}$ represents the measured output and $C_i \in \mathbb{R}^{m_i\times n}$ is the measurement matrix of sensor i. Here, $w(t)$ and $v_i(t)$ in (1) and (2) are i.i.d. white Gaussian noises (WGNs)

TABLE I
Part of Related Work About Differential Privacy

Problem	Learning	Optimization	Consensus	Game	Control	Filtering
Literature	Han *et al.* [16]	Han *et al.* [17]	Liu *et al.* [18]	Ye *et al.* [19]	Kawano and Cao [20]	Ny and Pappas [21]
Mechanism	Laplace	Laplace	Laplace	Laplace	Gaussian	Gaussian, Laplace

that satisfy

$$\begin{cases} \mathbb{E}(w(t_1)w^{\mathrm{T}}(t_2)) = \delta(t_1,t_2)Q_w \\ \mathbb{E}(v_i(t_1)v_j^{\mathrm{T}}(t_2)) = \delta(i,\ j)\delta(t_1,t_2)Q_{v_i} \\ \mathbb{E}(w(t_1)v_i^{\mathrm{T}}(t_2)) = 0,\ \forall\ i,t_1,t_2 \end{cases} \tag{3}$$

where $\delta(i,\ j)$ is the delta function such that $\delta(i,\ j) = 1$ if $i = j$; otherwise, $\delta(i,\ j) = 0$. Moreover, the pair $(A, \sqrt{Q_w})$ is stabilizable and (A, C_i) $(\forall i)$ are detectable.

In distributed fusion structure, each sensor should first calculate the local state estimates (LSEs) $\hat{x}_i(t)$ with the measurements $\{y_i(1), \ldots, y_i(t)\}$. Then, LSEs will be sent to FC through communication networks. After receiving the transmitted estimates, FC will fuse them for obtaining a better performed estimate by means of weighted sum as follows:

$$\hat{x}_f(t) = \sum_{i=1}^{L} W_i\hat{x}_i(t) \tag{4}$$

where $\hat{x}_f(t)$ denotes DFE and $\sum_{i=1}^{L} W_i = I$ guarantees the unbiasedness of $\hat{x}_f(t)$. After defining an augmented estimate $\hat{x}_d(t) \triangleq \mathrm{col}\{\hat{x}_1(t), \ldots, \hat{x}_L(t)\}$, fusion process (4) can be rewritten as $\hat{x}_f(t) = W\hat{x}_d(t)$, where $W \triangleq [W_1 \ldots W_L]$.

In order to reduce storage and improve efficiency, received LSEs will be dropped after fusion, and only DFEs $\{\hat{x}_f(1), \ldots, \hat{x}_f(t)\}$ are retained in FC. However, there exist passive eavesdropping attacks when FC broadcasts information to legitimate users. Thus, it is considered to send PRE instead of single DFE to legitimate user at each time. In this correspondence, PRE represents the average of DFEs at different times, which is expressed as

$$\hat{x}_u(t) = \frac{1}{\kappa}\sum_{k\in\Phi(t)} \hat{x}_f(k) \tag{5}$$

where the constant κ is the number of elements in time index set $\Phi(t)$, and the choice of $\Phi(t)$ is based on the requirement of legitimate user.

B. Problems of Interests

Although the transmission method (5) can protect data privacy on certain level, the system information can also be stolen with other strong eavesdropping methods. Once the eavesdropper realizes the scheme of average, it can calculate DFE with the difference operation on $\hat{x}'_u(t)$ and $\hat{x}_u(t)$, where $\hat{x}'_u(t)$ is the adjacent vector of $\hat{x}_u(t)$, and they only differ by $\hat{x}_f(t)$. Achieving differential privacy by adding noise on PRE is an effective method against such difference eavesdropping, which yields the following traditional mechanism:

$$\hat{x}^p_u(t) \triangleq M(\hat{x}_u(t)) = \hat{x}_u(t) + a(t) \tag{6}$$

where $a(t) \in \mathbb{R}^n$ is an i.i.d. WGN with covariance Q_aI_n. The privacy target about differential privacy can be described by [14]

$$\mathbb{P}(M(\hat{x}_u(t)) \in \mathcal{O}) \le e^{\epsilon}\mathbb{P}(M(\hat{x}'_u(t)) \in \mathcal{O}) + \delta, \forall \mathcal{O} \subseteq \mathcal{M} \tag{7}$$

where $\mathcal{M} \triangleq \mathrm{Range}(M)$ is the domain of the observation under mechanism M. It ensures that two distributions on adjacent perturbed PREs (PPREs) are close to some extent such that the eavesdropper cannot distinguish. Besides, parameters ϵ and δ are presumed as known in the rest of correspondence, since they are constant and generally chosen in accordance with practical privacy demand. On the other hand, the networked transmission between each sensor and FC also has the risks of wiretapping. If the true LSEs are overheard, DFE will be precisely speculated by weighting them as (4) with optimal fusion criterion. Hence, how to guarantee the confidentiality under such potential attack is the problem required to be further concerned.

According to the preliminary of mechanism in [21], a key aim is obtaining the boundary of variation $\mathcal{V}_{\hat{x}_u}(t) \triangleq \hat{x}_u(t) - \hat{x}'_u(t)$. However, it cannot be easily derived due to the possible uncertainties and instabilities of estimators. On the contrary, the boundary of variation between adjacent system states, $\mathcal{V}_x(t) \triangleq x(t) - x'(t)$, is easy to be acquired. Then, we consider that two original states $x(t)$ and $x'(t)$ are equipped by the following adjacency relation [21]:

$$\begin{aligned} &\mathrm{Adj}_\lambda(x(t), x'(t)) : \\ &\|Hx(t) - Hx'(t)\|_2 \le \lambda \\ &\text{while } (I_n - H)x(t) = (I_n - H)x'(t) \end{aligned} \tag{8}$$

where $H \in \mathbb{R}^{n\times n}$ is a binary diagonal matrix whose ith diagonal element indicates whether the ith component of vectors $x(t)$ and $x'(t)$ is adjacent. In this case, how to derive the boundary of variation $\mathcal{V}_{\hat{x}_u}(t)$ based on that of $\mathcal{V}_x(t)$ is a fundamental issue.

Consequently, the problem to be tackled in this correspondence is mainly related to designing the inserted noises for satisfying differential privacy. Moreover, since eavesdroppers can obtain DFEs by calculating difference of PREs and fusing LSEs, the improved noise perturbation framework should be further studied for simultaneously countering both types of wiretapping.

III. MAIN RESULTS

A. Output Perturbation Mechanism

Sensors in distributed fusion systems are autonomous and responsible for local state estimation. Here, LSE at each sensor is considered to be calculated by the standard Kalman

filter [30]

$$\hat{x}_i(t) = A\hat{x}_i(t-1) + K_i(t)(y_i(t) - C_iA\hat{x}_i(t-1)) \quad (9)$$

where the optimal local Kalman gain $K_i(t) \in \mathbb{R}^{n\times m_i}$ is recursively computed as

$$\begin{cases} P_i^-(t) = AP_i(t-1)A^{\mathrm{T}} + Q_w \\ P_i(t) = (I_n - K_i(t)C_i)P_i^-(t) \\ K_i(t) = P_i^-(t)C_i^{\mathrm{T}}\left(C_iP_i^-(t)C_i^{\mathrm{T}} + Q_{v_i}\right)^{-1}. \end{cases} \quad (10)$$

Besides, the cross covariance between ith and jth LSEs can also be computed in a recursive way

$$P_{ij}(t) = (I_n - K_i(t)C_i)(AP_{ij}(t-1)A^{\mathrm{T}} + Q_w) \times (I_n - K_j(t)C_j)^{\mathrm{T}}. \quad (11)$$

Under the stabilization and detection characteristics of systems (1) and (2), Kalman filter (9) will exponentially converge to steady state in a few steps, which yields

$$\bar{P}_{ii} \triangleq \lim_{t\to\infty} P_i(t), \bar{P}_{ij} \triangleq \lim_{t\to\infty} P_{ij}(t), \bar{K}_i \triangleq \lim_{t\to\infty} K_i(t). \quad (12)$$

Furthermore, the weighting matrices in (4) can be calculated by resorting to the optimal fusion criterion [1]

$$\begin{cases} W = (I_a^{\mathrm{T}}\bar{P}^{-1}I_a)^{-1}I_a^{\mathrm{T}}\bar{P}^{-1} \\ I_a \triangleq [I_n^{\mathrm{T}}\cdots I_n^{\mathrm{T}}] \in \mathbb{R}^{nL\times n}, \bar{P} \triangleq (\bar{P}_{ij})_{nL\times nL}. \end{cases} \quad (13)$$

Meanwhile, the fusion covariance can be obtained as $P_f \triangleq \mathbb{E}((x(t) - \hat{x}_f(t))(x(t) - \hat{x}_f(t))^{\mathrm{T}}) = (I_a^{\mathrm{T}}\bar{P}^{-1}I_a)^{-1}$. On the basis of abovementioned fusion estimator design, the Gaussian noise in traditional output perturbation mechanism (6) is going to be designed by the following theorem.

THEOREM 3.1 The mechanism (6) is (ϵ, δ)-differentially private for adjacency relation (8) iff the parameter Q_a satisfies

$$Q_a \geq \Gamma^2(\epsilon, \delta)\sigma_{\max}^2(W\bar{K}_dCH)\lambda^2 \quad (14)$$

where $\bar{K}_d \triangleq \mathrm{diag}\{\bar{K}_1, \ldots, \bar{K}_L\}$, $C \triangleq \mathrm{col}\{C_1, \ldots, C_L\}$, and $\Gamma(\epsilon, \delta) = (\mathcal{Q}^{-1}(\delta) + \sqrt{(\mathcal{Q}^{-1}(\delta))^2 + 2\epsilon})/2\epsilon$ with $\mathcal{Q}(x) = (\int_x^\infty e^{-\frac{t^2}{2}})dt/\sqrt{2\pi}$.

PROOF The proof is given in Appendix A. ■

B. Local Perturbation Framework

For simultaneously protecting the privacy against two eavesdropping types, the local perturbation framework is proposed when κ is constant. Such constant model can be used in many scenarios, for example, moving average [31]. Since the eavesdropper can calculate DFE with LSEs, we transfer the noise mechanism from PREs to LSEs for impairing the performance of original fusion approach. The local perturbation framework can be shown in Fig. 2.

To be specific, the perturbed LSE (PLSE) is calculated by the following form:

$$\hat{x}_i^p(t) = \hat{x}_i(t) + a_i(t) \quad (15)$$

where $a_i(t) = G_i\xi_i(t)$ is the inserted noise with $G_i = W_i^{-1}$. In this case, the differential privacy can be achieved after directly fusing the PLSEs without extra noise insertion,

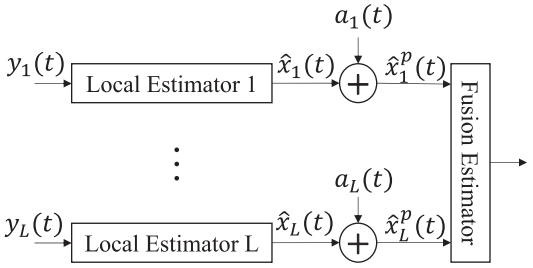

Fig. 2. Local perturbation framework.

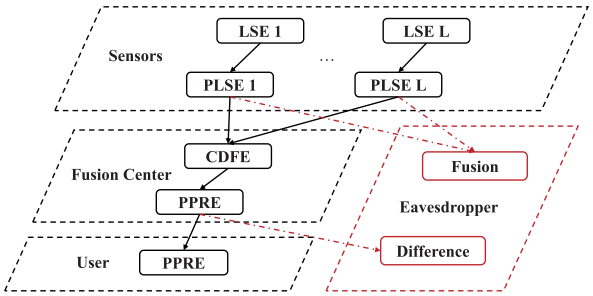

Fig. 3. Distributed fusion structure under local perturbation framework.

where the i.i.d. Gaussian noise ξ_i with covariance $Q_{\xi_i}I_n$ is designed as follows.

THEOREM 3.2 Under local perturbation framework, the mechanism (15) achieves (ϵ, δ)-differential privacy under adjacency relation (8) iff the covariances Q_{ξ_i} $(i = 1, \ldots, L)$ satisfy

$$\sum_{i=1}^{L} Q_{\xi_i} \geq \Gamma^2(\epsilon, \delta)\sigma_{\max}^2(W\bar{K}_dCH)\lambda^2/\kappa. \quad (16)$$

PROOF The proof is given in Appendix B. ■

Under local perturbation framework, original fusion estimation relies on PLSEs, and the perturbed DFE (PDFE) $\hat{x}_f^p(t)$ can be described by $\hat{x}_f^p(t) = W\hat{x}_d^p(t)$, where $\hat{x}_d^p(t) \triangleq \mathrm{col}\{\hat{x}_1^p(t), \ldots, \hat{x}_L^p(t)\}$. Hence, even though the eavesdropper fuses PLSEs with originally optimal weighting matrix (13), it cannot acquire accurate DFEs. The lower bound of covariance of PDFE, i.e., $P_f^p \triangleq \mathbb{E}((x(t) - \hat{x}_f^p(t))(x(t) - \hat{x}_f^p(t))^{\mathrm{T}})$, will become

$$P_f^p = P_f + \Gamma^2(\epsilon, \delta)\sigma_{\max}^2(W\bar{K}_dCH)\lambda^2I_n/\kappa. \quad (17)$$

Unfortunately, it is also PLSEs that FC receives, which degrades the expected estimation performance. In other words, the steady covariances in (12) are unmatched with corresponding PLSEs, and original weighting matrix W is not in the minimum variance sense anymore. To reduce this kind of performance loss, a compensated DFE (CDFE) $\hat{x}_f^c(t)$ is proposed

$$\hat{x}_f^c(t) = W^c\hat{x}_d^p(t). \quad (18)$$

The distributed fusion structure under local perturbation framework is shown in Fig. 3, and the compensating weighting matrix W^c is designed by the following theorem.

THEOREM 3.3 Under mechanism (15) for local perturbation framework, the weighting matrix in CDFE (18) is calculated by

$$W^c = (I_a^{\mathrm{T}}(\bar{P}^c)^{-1}I_a)^{-1}I_a^{\mathrm{T}}(\bar{P}^c)^{-1} \tag{19}$$

where $\bar{P}^c \triangleq (\bar{P}_{ij}^c)_{nL\times nL}$, $\bar{P}_{ii}^c = \bar{P}_{ii} + G_iQ_{\xi_i}G_i^{\mathrm{T}}$ and $\bar{P}_{ij}^c = \bar{P}_{ij}(i \neq j)$.

PROOF The proof is given in Appendix C. ■

REMARK 3.1 Instead of directly designing $a_i(t)$ in (15) as i.i.d. WGN, we introduce a multiplier G_i for improving the mechanism. The reasons why we propose this form are summarized by the following two items.

1) One aim is to correspond traditional mechanism (6) such that the noises can be designed with Theorem 3.1. In other words, through designing G_i, the PPRE will become form (31) and the result can be deduced in a straight way with (14) owing to its accordance with (6).
2) Another reason is that the similar mechanism cannot be intuitively derived when $a_i(t)$ is an i.i.d. WGN, since the weighting fusion matrix W will require left inverse. However, as defined in Section II, W is a full row rank matrix which only has right pseudo inverse, and thus, the result cannot be similarly found.

REMARK 3.2 The allocation of covariance under constraint (16) is flexible and always determined with practical demand. In the most widely used background like aforementioned moving average model, all local covariances are considered as identical

$$Q_{\xi_i} = \Gamma^2(\epsilon,\delta)\sigma_{\max}^2(W\bar{K}_dCH)\lambda^2/L\kappa \quad \forall\, i.$$

For slightly general application, where certain sensor denoted as i_0 needs strong confidentiality level, only that sensor is responsible for perturbation, which means

$$Q_{\xi_{i_0}} = \Gamma^2(\epsilon,\delta)\sigma_{\max}^2(W\bar{K}_dCH)\lambda^2/\kappa,\ \exists\, i_0$$

while $Q_{\xi_i} = 0$ for all $i \neq i_0$.

IV. SIMULATION EXAMPLES

Since accurate positions of some individuals, facilities, and objects are secret under specific situations, they require privacy preserving in an ever-increasing demand [32]. Therefore, we assume a target tracking system to quantitatively illustrate the effectiveness of the proposed methods. More concretely, the kinematics of a maneuvering target is described by the following planner (2-D horizontal) curvilinear motion model [33]:

$$\begin{cases} \dot{s}_x(t) = v(t)\cos\theta(t) \\ \dot{s}_y(t) = v(t)\sin\theta(t) \\ \dot{v}(t) = \alpha_t(t) \\ \dot{\theta}(t) = \frac{\alpha_n(t)}{v(t)}. \end{cases} \tag{20}$$

In this kinematic model, the pair $(s_x(t), s_y(t))$ represents the center Cartesian coordinates of target position, whereas $v(t)$ is the velocity and $\theta(t)$ is the heading angle. Moreover, $\alpha_t(t)$ and $\alpha_n(t)$, respectively, denote the tangential and normal accelerations. When $\alpha_t(t) = 0$ and $\alpha_n(t)$ is constant, the general moving model (20) can be reduced to a coordinated turn model, where the velocity and the angular rate are constant, i.e., postulate $\gamma = v(t)$ and $\phi = \dot{\theta}(t)$. After constructing global state vector $x(t) \triangleq \mathrm{col}\{s_x(t), \dot{s}_x(t), s_y(t), \dot{s}_y(t)\}$, the continuous-time state transition equation can be written as

$$\dot{x}(t) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -\phi \\ 0 & 0 & 0 & 1 \\ 0 & \phi & 0 & 0 \end{bmatrix} x(t) + w(t). \tag{21}$$

Accordingly, the system parameters of discrete-time state-space model (1) and (2) can be obtained by utilizing the discretization method

$$\begin{cases} A = \begin{bmatrix} 1 & \sin\phi T_s/\phi & 0 & -(1-\cos\phi T_s)/\phi \\ 0 & \cos\phi T_s & 0 & -\sin\phi T_s \\ 0 & (1-\cos\phi T_s)/\phi & 1 & (\sin\phi T_s)/\phi \\ 0 & \sin\phi T_s & 0 & cos\phi T_s \end{bmatrix} \\ C_1 = \begin{bmatrix} 0.8 & 0.5 & 0 & 0 \\ 0 & 0 & 0.6 & 0.4 \\ 0.4 & 0 & 0.2 & 0 \end{bmatrix}, \\ C_2 = \begin{bmatrix} 0 & 0 & 0.7 & 0.3 \\ 0.6 & 0.2 & 0 & 0 \\ 0 & 0.3 & 0 & 0.8 \end{bmatrix} \end{cases} \tag{22}$$

where $T_s = 1$ is the sampling period of discretization. Meanwhile, the system noises $w(t)$, $v_1(t)$, and $v_2(t)$ are, respectively, i.i.d. WGNs with covariances

$$\begin{cases} Q_{v_1} = \mathrm{diag}\{0.01, 0.04, 0.02\} \\ Q_{v_2} = \mathrm{diag}\{0.03, 0.02, 0.01\} \\ Q_w = \mathrm{diag}\{0.04, 0.01, 0.04, 0.01\}. \end{cases} \tag{23}$$

Let us set $H \triangleq \mathrm{diag}\{0, 1, 0, 1\}$, which means the velocities of both directions are equipped with adjacency relation.

Due to the existence of stochastic noises, the estimation performance is assessed by the practical mean square errors (PMSEs) that approximate theoretical MSEs by implementing Monte Carlo method over an average of 1000 runs. It can be seen from Fig. 4 that the PDFE under local perturbation framework performs worse than DFE, which is in line with the desired effects of noises. The high PMSE of

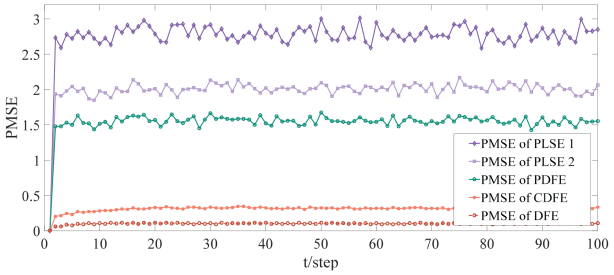

Fig. 4. PMSEs of estimators in distributed fusion structure.

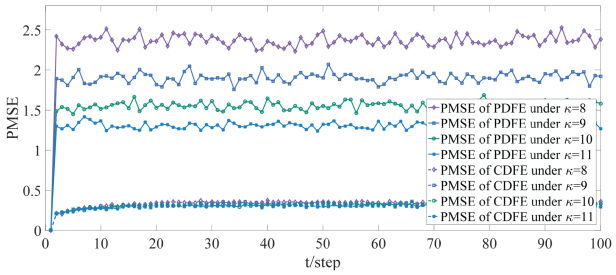

Fig. 5. PMSEs of PDFEs and CDFEs under different κ.

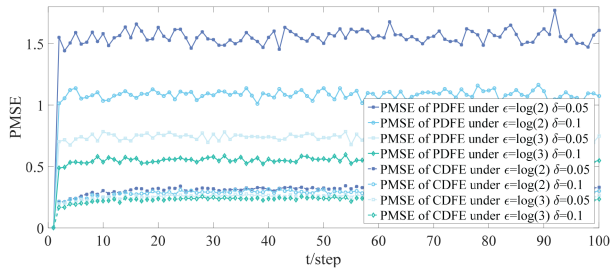

Fig. 6. PMSEs of PDFEs and CDFEs under different ϵ and δ.

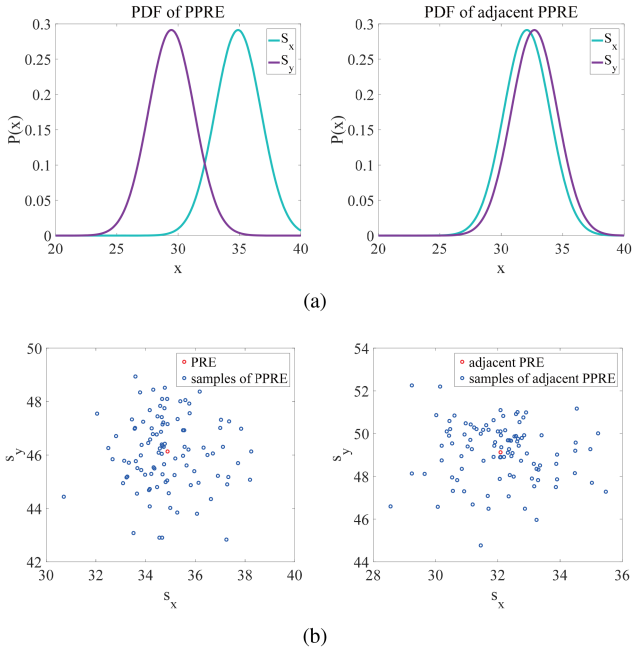

Fig. 7. (a) PDFs of queried outputs after mechanisms. (b) In total, 100 samples of distributed outputs correspond to (a).

PDFE protects the confidentiality of transmission between each sensor and FC, because it indicates the large estimation error of eavesdropper when fusing transmitted PLSEs. Fortunately, the proposed compensation method (19) can effectively improve the estimation performance according to the less performance loss of CDFE.

Then, we plot the curves of PMSEs about PDFEs and CDFEs under different parameters $\kappa = 8, 9, 10, 11$ in Fig. 5. It is observed that PMSE increases as κ increases, which corresponds with the dispersion analysis. At the same time, PMSEs of CDFEs are lower than that of corresponding PDFEs, which indicates the performance improvement of compensation strategy. Next, Fig. 6 depicts the relationship between PMSEs and privacy level parameters ϵ and δ. This figure also implies that the compensation strategy can effectively reduce the performance loss even if some parameters change.

To more specifically show the realization of proposed method, we provide the numerical analysis relying on Theorem 3.1. It is presumed that the position of specific time $t = 10$ is sensitive and needs privacy protection against eavesdropping. By implementing Gaussian mechanism (6), certain probability distribution functions (PDFs) and samples of PPREs are plotted in Fig. 7. Specifically, Fig. 7(a) shows the probability distributions of horizontal positions that eavesdropper has obtained, i.e., PDFs of S_x and S_y of two adjacent PPREs. Moreover, 100 simulation samples of the abovementioned two PPREs are plotted in Fig. 7(b), where we can roughly observe the disturbance under proposed mechanism. It can be illustrated from this figure that PDFs under differentially private mechanism are close to some extent, and thus the eavesdropper cannot easily distinguish accurate position by computing variation.

V. CONCLUSION

In this correspondence, the idea of differential privacy was introduced for guaranteeing the confidentiality of DFE. Basically, we considered traditional implementation of differential privacy, where artificial noises were injected into PREs. The covariances of inserted Gaussian noises were designed based on the privacy parameters and system matrices. Furthermore, we dispersed the location of noise insertion from PREs to LSEs in local perturbation framework, which simultaneously countered eavesdropping with difference and fusion. Then, a compensation approach was designed by recomputing the covariances of PLSEs to reduce the performance loss generated by locally inserted noises. Finally, a maneuvering target tracking system was exploited to demonstrate the effectiveness of the proposed methods.

As mentioned previously, this correspondence only studies the simplest fusion estimation structure about implementing differentially private mechanism. Hence, in the future, other algorithms can consider these perturbation frameworks for achieving differential privacy. Moreover, since differential privacy only guarantees the confidentiality in probability sense, the privacy-preserving studies that combine different senses are also valuable directions.

APPENDIX

A. Proof of Theorem 3.1

According to the differentially private mechanism in [21], the most important issue is to design sensitivity $\Delta(\hat{x}_u(t)) \triangleq \sup \|\hat{x}_u(t) - \hat{x}'_u(t)\|_2$. Thus, we calculate it with given adjacency relation (8).

Under sensed variable (2), the variation between two adjacent measurements, $\mathcal{V}_{y_i}(t) \triangleq y_i(t) - y_i'(t)$, can be easily found with $\mathcal{V}_x(t)$

$$\mathcal{V}_{y_i}(t) = C_i \mathcal{V}_x(t). \tag{24}$$

Then, the variation $\mathcal{V}_{\hat{x}_d}(t) \triangleq \hat{x}_d(t) - \hat{x}_d'(t)$, can be given by combining steady-state Kalman filter

$$\mathcal{V}_{\hat{x}_d}(t) = \bar{K}_d C \mathcal{V}_x(t). \tag{25}$$

In the sequel, we can obtain the variation $\mathcal{V}_{\hat{x}_f}(t)$ with fusion form (4) and variation (25)

$$\mathcal{V}_{\hat{x}_f}(t) = W \bar{K}_d C \mathcal{V}_x(t). \tag{26}$$

Since H is binary and diagonal, one has $H\mathcal{V}_x(t) = \mathcal{V}_x(t)$. Thus, the variation (26) can be further expressed as

$$\mathcal{V}_{\hat{x}_f}(t) = W \bar{K}_d C H \mathcal{V}_x(t). \tag{27}$$

By resorting to Cauchy–Schwarz inequality, the variation between PREs can be bounded from adjacency relation (8) and variation (27)

$$\begin{aligned} \left\| \hat{x}_u(t) - \hat{x}_u'(t) \right\|_2 &= \left\| \mathcal{V}_{\hat{x}_f}(t) \right\|_2 \\ &= \left\| W \bar{K}_d C H \mathcal{V}_x(t) \right\|_2 \\ &\le \left\| W \bar{K}_d C H \right\|_2 \left\| \mathcal{V}_x(t) \right\|_2 \\ &\le \sigma_{\max}(W \bar{K}_d C H) \lambda. \end{aligned} \tag{28}$$

Finally, the sensitivity $\Delta(\hat{x}_u(t))$ is determined with the supremum of (28)

$$\Delta(\hat{x}_u(t)) = \sigma_{\max}(W \bar{K}_d C H) \lambda. \tag{29}$$

On the basis of Gaussian mechanism [21], the condition of covariance Q_a is obtained as (14). This completes the proof.

B. Proof of Theorem 3.2

Combining PLSEs (15) and DFE (4), the PDFE can be described as the following noise insertion form:

$$\hat{x}_f^p(t) = \hat{x}_f(t) + \sum_{i=1}^{L} \xi_i(t). \tag{30}$$

Based on abovementioned noise insertion method, we can derive the following mechanism on PRE:

$$M(\hat{x}_u(t)) = \hat{x}_u(t) + \sum_{k \in \Phi(t)} \sum_{i=1}^{L} \xi_i(k). \tag{31}$$

This modality gives PPRE the equivalent form to (6), and thus, we can easily deduce the following covariance condition by using result (14) in Theorem 3.1:

$$\sum_{k \in \Phi(t)} \sum_{i=1}^{L} Q_{\xi_i} \ge \Gamma^2(\epsilon, \delta) \sigma_{\max}^2(W \bar{K}_d C H) \lambda^2. \tag{32}$$

Since the set $\Phi(t)$ has fixed elements as aforementioned, we have $\sum_{k \in \Phi(t)} \sum_{i=1}^{L} Q_{\xi_i} = \kappa \sum_{i=1}^{L} Q_{\xi_i}$, and the result (16) is derived. This completes the proof.

C. Proof of Theorem 3.3

Motivated by the derivation of (13), the main work of deducing CDFE is calculating the covariances of PLSEs $\hat{x}_i^p(t)$, which are actually utilized for fusion estimation. According to the definition of covariance, one has $P_{ij}^c(t) \triangleq \mathbb{E}((\hat{x}_i^p(t) - \mathbb{E}(\hat{x}_i^p(t)))(\hat{x}_j^p(t) - \mathbb{E}(\hat{x}_j^p(t)))^{\mathrm{T}})$. Since $\mathbb{E}(\hat{x}_i^p(t)) = x(t)$, we have $P_{ij}^v = \mathbb{E}((\tilde{x}_i(t) + a_i(t))(\tilde{x}_i(t) + a_i(t))^{\mathrm{T}})$. Combining $\mathbb{E}(\xi_i(t)\xi_i^{\mathrm{T}}(t)) = Q_{\xi_i}$ and $\mathbb{E}(\xi_i(t)\xi_j^{\mathrm{T}}(t)) = 0$, the compensated covariances $\bar{P}_{ij}^v$ can be easily written as the form given in theorem. Then, the compensating weighting matrix W^c can be calculated as (19) by the identical fusion criterion in (13). This completes the proof.

XINHAO YAN
BO CHEN, *Member, IEEE*
YUCHEN ZHANG, *Student Member, IEEE*
LI YU, *Member, IEEE*
Zhejiang University of Technology, Hangzhou, China,
Zhejiang Provincial United Key Laboratory of Embedded Systems, Hangzhou, China

REFERENCES

[1] S. Sun and Z. Deng, "Multi-sensor optimal information fusion Kalman filter," *Automatica*, vol. 40, pp. 1017–1023, Jun. 2004.

[2] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "Distributed covariance intersection fusion estimation for cyber-physical systems with communication Constraints," *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 4020–4026, Dec. 2016.

[3] Y. Bar-Shalom, X. Li, and T. Kirubarajan, *Estimation With Applications to Tracking and Navigation*. New York, NY, USA: Wiley, 2001.

[4] G. Hu, W. P. Tay, and Y. Wen, "Cloud robotics: Architecture, challenges and applications," *IEEE Netw.*, vol. 26, no. 3, pp. 21–28, May/Jun. 2012.

[5] D. Ding, Q. Han, Y. Xiang, X. Ge, and X. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[6] B. Chen, D. W. C. Ho, W. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 2, pp. 455–468, Feb. 2019.

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

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

[9] X. Yan, Y. Zhang, D. Xu, and B. Chen, "Distributed confidentiality fusion estimation against eavesdroppers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 4, pp. 3633–3642, Aug. 2022.

[10] T. Bao, H. Wang, W. J. Wang, H. C. Yang, and M. Hasna, "Secrecy outage performance analysis of UAV-assisted relay communication systems with multiple aerial and ground eavesdroppers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 3, pp. 2592–2600, Jun. 2022.

[11] D. Xu, X. Yan, B. Chen, and L. Yu, "Energy-constrained confidentiality fusion estimation against eavesdroppers," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 2, pp. 624–628, Feb. 2022.

[12] X. Guo, A. S. Leong, and S. Dey, "Estimation in wireless sensor networks with security constraints," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 2, pp. 544–561, Apr. 2017.

[13] M. Rice, C. Hogstrom, M. S. Afran, and M. Saquib, "On sparse channel estimation in aeronautical telemetry," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 5, pp. 2612–2618, Oct. 2019.
[14] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. 3rd Theory Cryptogr. Conf.*, 2006, pp. 265–284.
[15] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Adv. Cryptol.-Eurocrypt*, 2006, pp. 486–503.
[16] D. Han, K. Liu, Y. Lin, and Y. Xia, "Differentially private distributed online learning over time-varying digraphs via dual averaging," *Int J. Robust Nonlinear Control*, vol. 32, no. 5, pp. 2485–2499, 2021.
[17] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Trans. Autom. Control*, vol. 62, no. 1, pp. 50–64, Jan. 2017.
[18] X. Liu, J. Zhang, and J. Wang, "Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems," *Automatica*, vol. 122, 2020, Art. no. 109283.
[19] M. Ye, G. Hu, L. Xie, and S. Xu, "Differentially private distributed Nash equilibrium seeking for aggregative games," *IEEE Trans. Autom. Control*, vol. 67, no. 5, pp. 2451–2458, May 2022.
[20] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3863–3878, Sep. 2020.
[21] J. L. Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.
[22] B. Chen, W. Zhang, G. Hu, and L. Yu, "Networked fusion Kalman filtering with multiple uncertainties," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 51, no. 3, pp. 2232–2249, Jul., 2015.
[23] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "Distributed estimation and control for discrete time-varying interconnected systems," *IEEE Trans. Autom. Control*, vol. 67, no. 5, pp. 2192–2207, May 2022.
[24] X. Yan, B. Chen, Y. Teng, and L. Ge, "Distributed estimation for discrete sequential systems under binary sensors," *Proc. IEEE 30th Int. Symp. Ind. Electron.*, 2021, pp. 1–6.
[25] X. Yan, B. Chen, and Z. Hu, "Distributed estimation for interconnected dynamic systems under binary sensors," *IEEE Sensors J.*, vol. 22, no. 13, pp. 13153–13161, Jul. 2022.
[26] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "A new approach to linear/nonlinear distributed fusion estimation problem," *IEEE Trans. Autom. Control*, vol. 64, no. 3, pp. 1301–1308, Mar. 2019.
[27] X. Yan, B. Chen, and X. Qiu, "Distributed dimensionality reduction fusion Kalman filtering with quantized innovations," *Circuits Syst Signal Process*, vol. 40, pp. 5234–5247, 2021.
[28] H. Chen, T. Kirubarajan, and Y. Bar-Shalom, "Performance limits of track-to-track fusion versus centralized estimation: Theory and application," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 2, pp. 386–400, Apr. 2003.
[29] J. A. Roecker and C. D. McGillem, "Comparison of two-sensor tracking methods based on state vector fusion and measurement fusion," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 24, no. 4, pp. 447–449, Jul. 1988.
[30] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, pp. 35–45, 1960.
[31] S. M. Seong, J. G. Lee, and C. G. Park, "Equivalent ARMA model representation for RLG random errors," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 36, no. 1, pp. 286–290, Jan. 2000.
[32] D. Ciuonzo, P. K. Willett, and Y. Bar-Shalom, "Tracking the tracker from its passive sonar ML-PDA estimates," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 1, pp. 573–590, Jan. 2014.
[33] X. Li and V. P. Jilkov, "Survey of maneuvering target tracking. Part I. Dynamic models," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 39, no. 4, pp. 1333–1364, Oct. 2003.