Automatica 153 (2023) 111025

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Distributed encryption fusion estimation against full eavesdropping☆

Xinhao Yan, Bo Chen *, Yuchen Zhang, Li Yu

Department of Automation, Zhejiang University of Technology, Hangzhou 310023, PR China
Zhejiang Provincial United Key Laboratory of Embedded Systems, Hangzhou 310023, PR China

ARTICLE INFO

Article history:
Received 21 April 2022
Received in revised form 30 January 2023
Accepted 15 February 2023
Available online xxxx

Keywords:
Distributed fusion estimation
Eavesdropping attack
Fusion-based encryption
Artificial noise
Differential privacy

ABSTRACT

This paper is concerned with the privacy-preserving distributed fusion estimation problem against full eavesdropping, where the eavesdropper can completely and precisely obtain the information transmitted from local sensors to legitimate user. To depict the privacy-preservation level, we propose novel confidentiality index and rank based on the estimation performances of both eavesdropper and legitimate user. Then, a new encryption approach, which is composed of two-step sequential noise injections, is developed such that the highest confidentiality rank can be achieved. It is rather remarkable that the weighting fusion matrix, which is unique in the distributed fusion estimation field, is utilized to design perturbation noises. In this case, the compensating fusion estimator of legitimate user can effectively reduce the adverse impact of disturbance with null space design in the proposed approach. Moreover, the probability distribution of inserted noises simultaneously satisfies the differential privacy, which strongly enhances the confidentiality level of local state estimates. Finally, an illustrative example is provided to verify the effectiveness and advantages of the proposed methods.

1. Introduction

In recent years, networked multi-sensor fusion estimation has become a key issue in information fusion (Chen, Ho, Zhang, & Yu, 2017), since the introduction of communication networks can efficiently increase scalability and reduce wiring complexity. The networked multi-sensor fusion systems (NMFSs) have been widely discussed and applied in a great number of scenarios, such as target tracking (Bar-Shalom, Li, & Kirubarajan, 2001), cyber–physical systems (Chen, Hu, Ho and Yu, 2016) and sensor networks (Zhang & Shi, 2018). However, because of the openness to networks and the remote connection among sensors and fusion centers (FCs), NMFSs are susceptible to a series of cyber-attacks (Ding, Han, Xiang, Ge, & Zhang, 2018), including man-in-the-middle attacks (Huang, Ho, Li, Yang, & Tang, 2022), stealthy attacks (Shang, Zhou, & Chen, 2022), and eavesdropping attacks (Yang, Li, Zhang, Tang, & Zheng, 2020), etc. Notice that wire-tapping transmission will cause serious privacy leakage, and the intercepted information can make other attacks more aggressive. Therefore, one of the most significant research objects is the privacy-preservation for NMFSs. Generally, there exist two primary fusion structures: the centralized fusion structure (Chen & Hu, 2018) and the distributed fusion structure (Sun & Deng, 2004; Yan, Chen and Hu, 2022; Zhang, Chen, & Yu, 2020). Compared with centralized fusion structure, where raw measurements are directly transmitted from sensors to legitimate user's FC, the distributed fusion structure is more robust and fault-tolerant attributed to the calculation of local state estimates (LSEs) (Roecker & McGillem, 1988). As a result, the distributed fusion estimation acquires more attractions on privacy-preserving approaches, which is going to be discussed in this paper.

For the sake of countering unauthorized eavesdroppers, privacy-preserving techniques are mainly studied from anonymization (Yin & Li, 2020), cryptography (Lu & Zhu, 2018), data perturbation (Mo & Murray, 2017) and trust framework (Basudan, Lin, & Sankaranarayanan, 2017). It should be pointed out that the sensors in NMFSs are usually equipped with master chips of general performance, which are only utilized for simple algorithm realization, control and communication. This indicates that their computation ability is very limited in most cases. Hence, adopting data perturbation methods is more practical for protecting privacy of NMFSs, where the transmitted values are modified simply. Among plenty of encryption methods, communication over packet drop links is an essential premise (Ding, Ren, Leong, Quevedo, & Shi, 2021; Goel & Negi, 2008; Huang, Ding, Leong, Quevedo, & Shi, 2021; Leong, Quevedo, Dolz, & Dey, 2019; Leong, Redder, Danie, & Dey, 2018; Tsiamis, Gatsis, & Pappas, 2018, 2020;

☆ The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Luca Schenato under the direction of Editor Christos G. Cassandras.

* Corresponding author at: Department of Automation, Zhejiang University of Technology, Hangzhou 310023, PR China.
E-mail addresses: yanxinhao1998@aliyun.com (X. Yan), bchen@aliyun.com (B. Chen), YuchenZhang95@163.com (Y. Zhang), lyu@zjut.edu.cn (L. Yu).

https://doi.org/10.1016/j.automatica.2023.111025
0005-1098/

Wang, Cao, Zhang, Sun, & Zheng, 2022; Xu, Yan, Chen, & Yu, 2022). The main approaches consist of transmission scheduling (Huang et al., 2021; Leong et al., 2019; Wang et al., 2022), state-secrecy code (Tsiamis et al., 2018, 2020) and complex noise injection (Goel & Negi, 2008; Leong et al., 2018; Xu et al., 2022). It is impractical to employ complex noise insertion strategy for NMFSs, since sensors are generally powered by mobile energies such as lithium batteries, and creating complex noise will reduce their working hours. On the other hand, the furtive channels constructed by eavesdroppers are always unknown, which makes the assumption of packet drop links not appropriate enough. Therefore, it is significant to design encryption approaches against the full eavesdropping, where all the transmitted data are precisely overheard without other uncertain factors, including packet dropping and complex noise perturbation.

Most recently and relevantly, the active contamination method was proposed (Yan, Zhang, Xu and Chen, 2022) by replacing certain components of transmitted estimates with random noises. However, it can be noted that the effectiveness of state-secrecy code (Tsiamis et al., 2020) and active contamination (Yan, Zhang et al., 2022) are both on the basis of unstable systems. The unboundedness of eavesdropper's estimator is related to that of system state, which limits the scope for applying algorithms. In this case, how to diverge the eavesdropper's estimator independently of system stability requires to be studied. Moreover, differential privacy is known as a classical method (Dwork, McSherry, Nissim, & Smith, 2006), where the artificial noise is inserted to perturb the statistical information of a great number of elements in a database. Due to its rigorous statistical modeling and powerful performance, the notion of differential privacy has been extended to many areas, such as control theory (Kawano, Kashima, & Cao, 2021), filtering theory (Le Ny & Pappas, 2014; Yan, Chen, Zhang and Yu, 2022) and consensus (Fiore & Russo, 2019). Nonetheless, the introduction of differential privacy into information fusion area has a fatal disadvantage, i.e., the legitimate user will receive disturbed data. This perturbation will degrade the estimation performance of legitimate fusion estimator, which serves an important index in multi-sensor fusion. Thus, it is of great significance to reduce such adverse impact occurs in legitimate user's FC.

It can be found from above methods that the confidentiality techniques for state estimation are generally based on single sensor. To the authors' knowledge, encryption approaches for multi-sensor fusion estimation have rarely been investigated, especially using fusion knowledge which is unique in this field. After designing fusion-based encryption method, not only the estimation performance can be improved, but also the privacy preservation level can be further enhanced. Therefore, we concern the distributed encryption fusion estimation problem and design encryption approach with fusion information for increasing the confidentiality and reliability of NMFSs. On the other hand, qualitative analysis for secure estimation against eavesdropper is less discussed. Thus, we propose novel confidentiality index and rank by combining the estimation performances of eavesdropper and legitimate user. The main contributions of this paper are summarized as follows.

(1) A novel fusion-based encryption approach, which consists of two-step sequential noise perturbation, is designed by resorting to the weighting fusion matrix that is unique in the distributed fusion estimation literature.
(2) The high confidentiality index is achieved, which is independent of system stability and does not require extra energy consumption. Meanwhile, the covariance of designed noises satisfies the differential privacy.

The notations and abbreviations that are frequently used throughout the paper are summarized in Table 1.

Table 1
Notations.

$\triangleq$	Define
x'	Adjacent vector of x
$\mathbb{A}^{\mathrm{T}}$	Transpose of matrix A
I_n	Identity matrix with dimension n
$\mathbb{Z}$	Set of integers
$\mathbb{R}^n$	Set of n-dimensional real vectors
$\mathbb{R}^{n\times m}$	Set of $n \times m$ real matrices
$\mathbb{E}\{\cdot\}$	Mathematical expectation
$\mathbb{P}\{\cdot\}$	Probability function
diag$\{\cdot\}$	Block diagonal matrix
col$\{\cdot\}$	Column vector
Tr$\{\cdot\}$	Trace of a matrix
rank$\{\cdot\}$	Rank of a matrix
$X > (<)0$	Positive-definite (negative-definite)
$X \geq (\leq)0$	Non-negative definite (non-positive definite)
$\|\cdot\|_2$	2-norm of a matrix
$\sigma_{\max}(\cdot)$	Maximum singular
$\rho_{\max}(\cdot)$	Maximum eigenvalue
$\lfloor x \rfloor$	Floor function: $\max\{a \in \mathbb{Z} : a < x\}$
$\mathcal{G}(x)$	Gaussian right tail function: $\frac{\int_x^\infty e^{-\frac{t^2}{2}} dt}{\sqrt{2\pi}}$
$\mathcal{V}(\mathrm{x})$	Variation between x and its adjacency x'
LSE	Local state estimate
DFE	Distributed fusion estimate
PLSE	Perturbed local state estimate
PLRE	Perturbed local released estimate
WLSE	Wiretapped local state estimate
WDFE	Wiretapped distributed fusion estimate
CDFE	Compensated distributed fusion estimate
ODFE	Optimal distributed fusion estimate
CI	Confidentiality index
CR	Confidentiality rank
i.i.d.	Independently and identically distributed
iff	If and only if

2. Problem formulation

Consider a NMFS described by the following discrete-time state–space model:

$$\mathrm{x}(t+1) = \mathrm{A}\mathrm{x}(t) + \mathrm{B}\mathrm{w}(t) \tag{1}$$

$$\mathrm{y}_i(t) = \mathrm{C}_i\mathrm{x}(t) + \mathrm{v}_i(t)(i = 1, \ldots, L) \tag{2}$$

where $\mathrm{x}(t) \in \mathbb{R}^n$ represents the system state at time t, and $\mathrm{y}_i(t) \in \mathbb{R}^{m_i}$ denotes the measurement of sensor i. Matrices $\mathrm{A} \in \mathbb{R}^{n\times n}$, $\mathrm{B} \in \mathbb{R}^{n\times n_{\mathrm{w}}}$ and $\mathrm{C}_i \in \mathbb{R}^{m_i\times n}$ are time-invariant with appropriate dimensions, while $\mathrm{w}(t) \in \mathbb{R}^{n_{\mathrm{w}}}$ and $\mathrm{v}_i(t) \in \mathbb{R}^{m_i}$ are i.i.d. white Gaussian noises (WGNs) satisfying

$$\begin{aligned}\mathbb{E}\{[\mathrm{w}^{\mathrm{T}}(t_1)\ \mathrm{v}_i^{\mathrm{T}}(t_1)]^{\mathrm{T}}[\mathrm{w}^{\mathrm{T}}(t_2)\ \mathrm{v}_j^{\mathrm{T}}(t_2)]\} \\ = \delta(t_1, t_2)\mathrm{diag}\{\mathrm{Q}_{\mathrm{w}}, \delta(i,j)\mathrm{Q}_{\mathrm{v}_i}\}\end{aligned} \tag{3}$$

where Q_{w} and $\mathrm{Q}_{\mathrm{v}_i}$ are respectively constant covariances for noises $\mathrm{w}(t)$ and $\mathrm{v}_i(t)$. $\delta(i,j)$ is the delta function such that $\delta(i,j) = 1$ if $i = j$; otherwise, $\delta(i,j) = 0$. Then, we make the following assumption about given NMFS.

Assumption 1 (*Controllability & Observability*)**.** The pair (A, B) is controllable and the pairs $(\mathrm{A}, \mathrm{C}_i)(\forall\ i)$ are observable.

In distributed fusion structure, LSE $\hat{\mathrm{x}}_i(t)$ should be calculated at each sensor and then transmitted to legitimate user. Since Kalman filter converges quickly and only in a few steps under Assumption 1, we directly apply steady-state Kalman filter for the calculation of LSE, which means that each estimator gain is time-invariant. With such steady-state design, the computation amount can be effectively decreased due to the reduction of some high-dimensional inverse matrices and time-varying recursion. Therefore, this steady-state estimation method will provide sufficient time for encryption process and make engineering application more convenient. For increasing the reliability of the

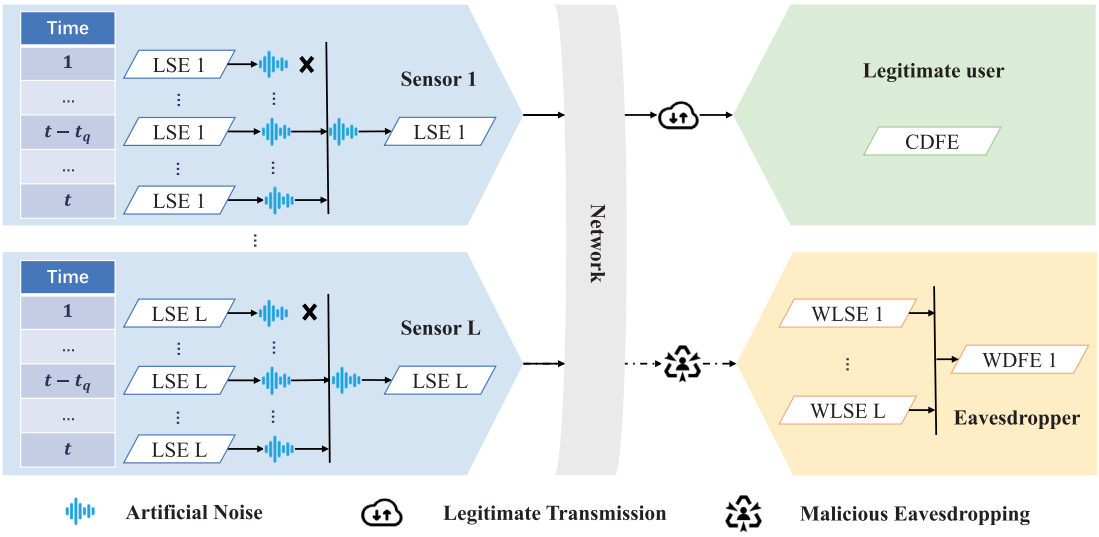


Fig. 1. The encryption fusion structure under eavesdropping.

encryption methods, we set the defense object as a strong wiretapping model called full eavesdropping, which is defined as follows.

Definition 1 (*Full Eavesdropping*)**.** The full eavesdropping is a passive wiretapping that silently monitors the communication channels without modification. Except for the encryption scheme, it can acquire the same information as legitimate user, which can be divided by the following two sets: (1) Accurate and real-time transmitted data over network layer without uncertain factors. (2) Estimator parameters and fusion criterion related to physical layer.

Aiming at ensuring confidentiality, the finally transmitted estimate at each sensor is set as the perturbed local released estimate (PLRE), which is denoted as $\hat{\mathrm{x}}_i^s(t) \triangleq \mathrm{M}(\hat{\mathrm{x}}_i^m(t))$, where M is a random mechanism and $\hat{\mathrm{x}}_i^m(t) \triangleq \mathrm{col}\{\hat{\mathrm{x}}_i(t-t_q), \ldots, \hat{\mathrm{x}}_i(t)\}$ with index $\tau = t - t_q, \ldots, t$. Let us define its adjacent vector as $[\hat{\mathrm{x}}_i^s(t)]' \triangleq \mathrm{M}([\hat{\mathrm{x}}_i^m(t)]')$, where $[\hat{\mathrm{x}}_i^m(t)]' \triangleq \mathrm{col}\{\hat{\mathrm{x}}_i(t-t_q), \ldots, \hat{\mathrm{x}}_i(t-1), [\hat{\mathrm{x}}_i(t)]'\}$, and the distance between $[\hat{\mathrm{x}}_i(t)]'$ and $\hat{\mathrm{x}}_i(t)$ is bounded. If PLREs are not encrypted, the eavesdropper can obtain $\hat{\mathrm{x}}_i(t)$ by resorting to the difference operation between $\hat{\mathrm{x}}_i^s(t)$ and $[\hat{\mathrm{x}}_i^s(t)]'$. For countering such eavesdropping approach, the mechanism M should be designed to achieve the following differential privacy index (Dwork et al., 2006):

$$\mathbb{P}(\hat{\mathrm{x}}_i^s(t) = \bar{\mathrm{x}}_i) \leq e^{\epsilon}\mathbb{P}([\hat{\mathrm{x}}_i^s(t)]' = \bar{\mathrm{x}}_i) + \delta, \ \forall\, \bar{\mathrm{x}}_i \in \mathcal{M} \tag{4}$$

where $\mathcal{M} = \mathrm{range}(\mathrm{M})$ represents the domain of observation under mechanism M, the parameters ϵ and δ are constants and determined in line with practical privacy demand. According to the existing differentially private mechanism (Le Ny & Pappas, 2014), the bound of variation $\mathcal{V}(\hat{\mathrm{x}}_i(t)) \triangleq \hat{\mathrm{x}}_i(t) - [\hat{\mathrm{x}}_i(t)]'$ should be obtained. Since the boundary between PLREs cannot be directly found due to multiple operations of estimators, we give the adjacency relation between corresponding states instead.

Assumption 2 (*Adjacency Relation*)**.** The adjacency relation between state vectors $\mathrm{x}^m(t) \triangleq \mathrm{col}\{\mathrm{x}(t-t_q), \ldots, \mathrm{x}(t)\}$ and $[\mathrm{x}^m(t)]' \triangleq \mathrm{col}\{\mathrm{x}'(t-t_q), \ldots, \mathrm{x}'(t)\}$ is defined as:

$$\begin{aligned}&\mathrm{Adj}_{\zeta}(\mathrm{x}^m(t), [\mathrm{x}^m(t)]'):\\ &\text{iff for time } t: \|\mathrm{Hx}(t) - \mathrm{Hx}'(t)\|_2 \leq \zeta,\\ &\text{while } (\mathrm{I}_n - \mathrm{H})\mathrm{x}(t) = (\mathrm{I}_n - \mathrm{H})\mathrm{x}'(t);\\ &\text{for time } \mu = t - t_q, \ldots, t-1: \mathrm{x}(\mu) = \mathrm{x}'(\mu)\end{aligned} \tag{5}$$

where $\mathrm{H} \in \mathbb{R}^{n\times n}$ is a binary diagonal matrix that denotes adjacent components and $\zeta \in \mathbb{R}$ is non-negative.

Based on this assumption, the variation $\mathcal{V}(\mathrm{x}(t)) \triangleq \mathrm{x}(t) - \mathrm{x}'(t)$ can be bounded as $\|\mathcal{V}(\mathrm{x}(t))\|_2 \leq \zeta$. Here, a numerical example is given to simply explain this assumption.

Example 1. Let the state $\mathrm{x}(t)$ represent the three-dimensional coordinate of an engine system as described in Section 4, i.e., $\mathrm{x}(t) \triangleq \{\mathrm{s_x}(t), \mathrm{s_y}(t), \mathrm{s_z}(t)\}$, where $\mathrm{s_x}(t)$, $\mathrm{s_x}(t)$ and $\mathrm{s_x}(t)$ respectively denote the coordinates of "x", "y" and "z" axes. Then, we assume the height $\mathrm{s_z}(t)$ cannot be obtained by the eavesdropper, but the distance between two adjacent vectors related to height can be reduced to one meter. In this case, the binary diagonal matrix becomes $\mathrm{H} = \mathrm{diag}\{0, 0, 1\}$, and the boundary is $\zeta = 1$.

Traditionally, distributed fusion estimate (DFE) $\hat{\mathrm{x}}_f(t)$ is calculated by means of weighted sum on LSEs:

$$\hat{\mathrm{x}}_f(t) = \sum_{i=1}^{L} \bar{\mathrm{W}}_i \hat{\mathrm{x}}_i(t) \tag{6}$$

where $\bar{\mathrm{W}} \triangleq [\bar{\mathrm{W}}_1 \cdots \bar{\mathrm{W}}_L]$ is the optimal weighting fusion matrix. In order to capture the system information as much as possible, the eavesdropper will calculate the wiretapped LSE (WLSE) $\hat{\mathrm{x}}_i^w(t)$ and wiretapped DFE (WDFE) $\hat{\mathrm{x}}_f^w(t)$ by combining weighting fusion matrix $\mathrm{W}(t)$ and overheard PLREs $\hat{\mathrm{x}}_i^s(t)$. The eavesdropper will not consider calculating one-step prediction or trivial estimate to compensate the loss of its estimation performance. This is because the eavesdropper cannot acquire the system matrix and judge the system stability correctly. Besides, the covariances of inserted noises are unknown to the eavesdropper. Then, the covariances of WLSEs and WDFE cannot be calculated, and their divergence cannot be realized. Instead, the expected covariances of estimates are all time-invariant and optimal in the view of eavesdropper. On the other hand, legitimate user will compute the compensated DFE (CDFE) $\hat{\mathrm{x}}_f^c(t)$ based upon designed compensating weighting fusion matrix W^c and received PLREs $\hat{\mathrm{x}}_i^s(t)$. The proposed encryption fusion structure under eavesdropping is shown in Fig. 1.

Let us define the estimation error covariances of CDFE as $\mathrm{P}_f^c(t) \triangleq \mathbb{E}\{\tilde{\mathrm{x}}_f^c(t)[\tilde{\mathrm{x}}_f^c(t)]^{\mathrm{T}}\}(\tilde{\mathrm{x}}_f^c(t) \triangleq \mathrm{x}(t) - \hat{\mathrm{x}}_f^c(t))$, and that of WLSEs and WDFE are $\mathrm{P}_{ii}^w(t) \triangleq \mathbb{E}\{\tilde{\mathrm{x}}_{ii}^w(t)[\tilde{\mathrm{x}}_{ii}^w(t)]^{\mathrm{T}}\}(\forall\, i,\ \tilde{\mathrm{x}}_{ii}^w(t) \triangleq \mathrm{x}(t) - \hat{\mathrm{x}}_{ii}^w(t))$ and $\mathrm{P}_f^w(t) \triangleq \mathbb{E}\{\tilde{\mathrm{x}}_f^w(t)[\tilde{\mathrm{x}}_f^w(t)]^{\mathrm{T}}\}(\tilde{\mathrm{x}}_f^w(t) \triangleq \mathrm{x}(t) - \hat{\mathrm{x}}_f^w(t))$. Then, we propose novel index and rank to depict the privacy-preservation level in the sense of secure estimation against eavesdroppers.

Definition 2 (*Confidentiality Index*)**.** The non-negative confidentiality index (CI) $\mathcal{CI}(t) \in \mathbb{R}$ in privacy-preserving estimation field is defined as

$$\mathcal{CI}(t) \triangleq \log_2 \frac{\mathrm{Tr}\{\mathrm{P}_f^w(t)\}}{\mathrm{Tr}\{\mathrm{P}_f^c(t)\}}. \tag{7}$$

It can be noted that the larger the CI is, the stronger the confidentiality is. Then, for achieving high CI, the general approach is to maximize $\mathrm{Tr}\{\mathrm{P}_f^w(t)\}$ while simultaneously minimize $\mathrm{Tr}\{\mathrm{P}_f^c(t)\}$. Particularly, the unboundedness of eavesdropper's estimators can take CI to infinity when the legitimate user's estimators keep bounded. In this case, it is recommended to diverge WDFE even if the estimation performance of CDFE is slightly jeopardized. Consequently, the problems to be tackled in this paper are described as follows:

(1) The first aim is to design the fusion-based encryption approach such that the highest CR is achieved as time goes to infinity.
(2) The second aim is to design random mechanism M with Assumption 2 such that the differential privacy index (4) is satisfied.

Remark 1. Instead of distributed estimation, where each local system may only acquire its neighboring information, it is multi-sensor fusion estimation that is studied in this paper. Here, data from multiple sensors will be transmitted to the FC for estimation, and the estimation performance can be improved by combining redundant and complementary information. In centralized fusion estimation, the measurements will be sent and then augmented into a high-dimensional vector. This causes the vulnerability to the cyber-attacks, because the modification on measurements will be magnified due to recursion of estimation approaches. On the contrary, since the DFE is only affected by current LSEs in distributed fusion estimation, the outlier caused by cyber-attacks will not be introduced into estimator recursion, which makes DFE more robust, fault-tolerant and better for privacy preservation.

Remark 2. Notice that only using the covariance of eavesdropper cannot precisely show the privacy level. In most random perturbation methods, such as Le Ny and Pappas (2014) and Yan, Zhang et al. (2022), the data received by legitimate user cannot be completely decrypted, and the estimation performance will also be impaired. In such case, it is inappropriate to say that the systems are sufficiently confidential just according to the index of eavesdropper, because the legitimate user may have equally poor performance. Therefore, CI should be a relative quantity which simultaneously depends on the estimation performances of both eavesdropper and legitimate user.

Remark 3. In addition to the division operation on two traces, the logarithm base "2" is introduced to further depict CI. The reasons can be summarized as follows: (1) As a breadth, it is a reasonable necessity to describe CI as non-negative. Since the eavesdropper always has worse estimation performance than legitimate user, i.e., $\mathrm{Tr}\{\mathrm{P}_f^w(t)\}/\mathrm{Tr}\{\mathrm{P}_f^c(t)\} \geq 1$, the logarithmic form is a appropriate operation to achieve non-negativity. (2) When $\mathrm{Tr}\{\mathrm{P}_f^w(t)\} = \mathrm{Tr}\{\mathrm{P}_f^c(t)\}$, the CI becomes 0, which is a clear event to demonstrate no-confidentiality. Meanwhile, two times of legitimate user's performance is a common demarcation of rank. Thus, it is intuitive to analyze systems using logarithm base "2".

3. Main results

3.1. Fusion-Based encryption

In distributed fusion structure, LSEs are created at sensors with raw measurements. Here, measurements $\{\mathrm{y}_i(1), \ldots, \mathrm{y}_i(t)\}$ are considered for estimation at time t instead of $\{\mathrm{y}_i(1), \ldots, \mathrm{y}_i(t-1)\}$, since it can provide more useful information according to the projection theory. Based on Assumption 1, the steady-state Kalman filter (Deng, Gao, Mao, Li, & Hao, 2005) is adopted for computing each LSE:

$$\hat{\mathrm{x}}_i(t) = \bar{\Psi}_i \hat{\mathrm{x}}_i(t-1) + \bar{\mathrm{K}}_i \mathrm{y}_i(t) \tag{8}$$

where $\bar{\Psi}_i \triangleq (\mathrm{I}_n - \bar{\mathrm{K}}_i \mathrm{C}_i)\mathrm{A}$, and the optimal local Kalman gain $\bar{\mathrm{K}}_i \in \mathbb{R}^{n \times m_i}$ is recursively calculated by

$$\begin{cases} \bar{\mathrm{P}}_{ii} = (\mathrm{I}_n - \bar{\mathrm{K}}_i \mathrm{C}_i)\bar{\mathrm{P}}_{ii}^z \\ \bar{\mathrm{P}}_{ii}^z = \mathrm{A}\bar{\mathrm{P}}_{ii}\mathrm{A}^{\mathrm{T}} + \bar{\mathrm{Q}}_{\mathrm{w}} \\ \bar{\mathrm{K}}_i = \bar{\mathrm{P}}_{ii}^z \mathrm{C}_i^{\mathrm{T}} \left(\mathrm{C}_i \bar{\mathrm{P}}_{ii}^z \mathrm{C}_i^{\mathrm{T}} + \mathrm{Q}_{v_i}\right)^{-1} \end{cases} \tag{9}$$

where $\bar{\mathrm{Q}}_{\mathrm{w}} \triangleq \mathrm{B}\mathrm{Q}_{\mathrm{w}}\mathrm{B}^{\mathrm{T}}$. In this case, the steady-state prediction covariance $\bar{\mathrm{P}}_{ii}^z$ is the positive semidefinite solution of the following discrete Riccati equation:

$$\begin{aligned} \bar{\mathrm{P}}_{ii}^z =& \mathrm{A}\bar{\mathrm{P}}_{ii}^z \mathrm{A}^{\mathrm{T}} + \bar{\mathrm{Q}}_{\mathrm{w}} - \mathrm{A}\bar{\mathrm{P}}_{ii}^z \mathrm{C}_i^{\mathrm{T}} \\ & \times (\mathrm{C}_i \bar{\mathrm{P}}_{ii}^z \mathrm{C}_i^{\mathrm{T}} + \mathrm{Q}_{v_i})\mathrm{C}_i \bar{\mathrm{P}}_{ii}^z \mathrm{A}^{\mathrm{T}} \end{aligned} \tag{10}$$

while the steady-state estimation covariance $\bar{\mathrm{P}}_{ii}$ is the symmetric positive definite solution of the following Lyapunov equation (Deng et al., 2005):

$$\begin{aligned} \bar{\mathrm{P}}_{ii} =& \bar{\Psi}_i \bar{\mathrm{P}}_{ii} \bar{\Psi}_i^{\mathrm{T}} + (\mathrm{I}_n - \bar{\mathrm{K}}_i \mathrm{C}_i)\bar{\mathrm{Q}}_{\mathrm{w}} \\ & \times (\mathrm{I}_n - \bar{\mathrm{K}}_i \mathrm{C}_i)^{\mathrm{T}} + \bar{\mathrm{K}}_i \mathrm{Q}_{v_i} \bar{\mathrm{K}}_i^{\mathrm{T}}. \end{aligned} \tag{11}$$

Moreover, the cross-covariance between ith and jth LSEs also satisfies the Lyapunov equation:

$$\bar{\mathrm{P}}_{ij} = \bar{\Psi}_i \bar{\mathrm{P}}_{ij} \bar{\Psi}_j^{\mathrm{T}} + (\mathrm{I}_n - \bar{\mathrm{K}}_i \mathrm{C}_i)\bar{\mathrm{Q}}_{\mathrm{w}} (\mathrm{I}_n - \bar{\mathrm{K}}_j \mathrm{C}_j)^{\mathrm{T}}. \tag{12}$$

Then, to obtain the best estimation performance with LSEs, the steady-state weighting fusion matrix is calculated in the linear minimum variance (LMV) sense (Deng et al., 2005):

$$\bar{\mathrm{W}} = (\mathrm{e}^{\mathrm{T}} \bar{\mathrm{P}}^{-1} \mathrm{e})^{-1} \mathrm{e}^{\mathrm{T}} \bar{\mathrm{P}}^{-1}, \tag{13}$$

where $\bar{\mathrm{P}} \triangleq (\bar{\mathrm{P}}_{ij}) \in \mathbb{R}^{nL \times nL}$ and $\mathrm{e} \triangleq [\mathrm{I}_n^{\mathrm{T}} \cdots \mathrm{I}_n^{\mathrm{T}}]^{\mathrm{T}} \in \mathbb{R}^{nL \times n}$. Then, the optimal DFE (ODFE) can be computed by substituting (13) into (6).

Under above fusion structure, the LSEs calculated by steady-state Kalman filters are transmitted from sensors to legitimate user through communication channels. Under such simple transmission, communicated data is transparent to the eavesdropper, which makes serious information leakage. Thus, we propose privacy-preserving fusion estimation by designing fusion-based encryption approach. This approach is mainly based on artificial noise insertion, and the entire process is divided into two steps:

(1) Inserting first part of artificial noise into LSE, that constructs perturbed LSE (PLSE).
(2) Inserting second part of artificial noise into local released estimate (LRE) which contains statistical information about PLSEs, that constructs PLRE for transmission.

The detailed operations are given as follows.

Step 1: Firstly, we construct the PLSE $\hat{\mathrm{x}}_i^p(t)$ by adding stochastic noise on the calculated steady-state LSE:

$$\hat{\mathrm{x}}_i^p(t) = \hat{\mathrm{x}}_i(t) + \mathrm{R}_i \xi_i(t) \tag{14}$$

where $\xi_i(t) \in \mathbb{R}^b$ is an i.i.d. WGN with covariance Q_{ξ_i} and $\mathrm{R}_i \in \mathbb{R}^{n \times b}$ is noise scaling matrix.

Step 2: Secondly, we establish LRE by gathering statistical information of PLSEs, i.e., $\hat{\mathrm{x}}_i^r(t) \triangleq \sum_{\tau=t-t_q}^{t} \hat{\mathrm{x}}_i^p(\tau)(t > t_q)$ while $\hat{\mathrm{x}}_i^r(t) \triangleq (t_q - t)\hat{\mathrm{x}}_i^p(0) + \sum_{\tau=1}^{t} \hat{\mathrm{x}}_i^p(\tau)(0 < t \leq t_q)$. Then, we construct

the PLRE $\hat{x}_i^s(t)$ for secure transmission by adding stochastic noise on LRE:

$$\hat{x}_i^s(t) = \begin{cases} (t_q - t)\hat{x}_i^p(0) + \sum_{\tau=1}^{t} \hat{x}_i^p(\tau) + N_i\alpha(t), \\ \qquad\qquad \text{for time } 0 < t \le t_q \\ \sum_{\tau=t-t_q}^{t} \hat{x}_i^p(\tau) + N_i\alpha(t), \\ \qquad\qquad \text{for time } t > t_q \end{cases} \tag{15}$$

where $\alpha(t) \in \mathbb{R}^a$ is an i.i.d. WGN with covariance Q_α, and $N_i \in \mathbb{R}^{n\times a}$ is the null space of steady-state compensating weighting fusion matrix, which means

$$\bar{W}^c N = 0, \ \ N^T N = I_a \tag{16}$$

with $N \triangleq \text{col}\{N_1, \ldots, N_L\}$.

In Step 1, the covariances of PLSEs defined as $P_{ii}^p(t) \triangleq \mathbb{E}\{\tilde{x}_i^p(t)[\tilde{x}_i^p(t)]^T\}$ and $P_{ij}^p(t) \triangleq \mathbb{E}\{\tilde{x}_i^p(t)[\tilde{x}_j^p(t)]^T\}(\tilde{x}_i^p(t) \triangleq x(t) - \hat{x}_i^p(t))$, have the following steady-state forms:

$$\bar{P}_{ii}^p = \bar{P}_{ii} + R_i Q_{\xi_i} R_i^T, \ \ \bar{P}_{ij}^p = \bar{P}_{ij} (i \ne j).$$

In Step 2, the dimension "a" must satisfy $a = nL - \text{rank}\{\bar{W}^c\}$ $(0 < a \le n)$. Generally, the compensating weighting fusion matrix $\bar{W}^c$ has rank "n", and the dimension "a" is chosen as $n(L-1)$. Besides, we can also directly denote N as a null vector with $a = 1$.

Remark 4. The distributed fusion process is independent of time due to the steady-state weighting fusion matrix design in (13). This means that directly adding random noises into LSEs cannot diverge DFE, which also indicates the robustness of distributed fusion structure. Thus, the summation on PLSEs in different time steps is considered for introducing noises into recursion and creating the possibility for divergence. The time indexes of these PLSEs are not limited from t_q to t, and they can be arbitrary as long as they satisfy recursive computation. Moreover, the form (15) under fixed length is chosen in this paper, because it has been widely utilized (such as moving average models) and is easy to be comprehended.

Remark 5. The artificial noise $R_i\xi_i(t)$ is applied to impair the optimal fusion criterion of eavesdropper by changing the covariances of LSEs. Although this noise is extra inserted, the adverse impact can be reduced by fusing in the LMV sense with its covariance. On the other hand, considering noise injection only on summation, i.e.,

$$\hat{x}_i^s(t) = \sum_{\tau=t-t_q}^{t} \hat{x}_i(\tau) + \hat{\alpha}_i(t)$$

with $\hat{\alpha}_i(t) = R_i\xi_i(t) + N_i\alpha(t)$, is inappropriate and will lead to noise accumulation in legitimate user. Hence, two-step sequential noise insertion method in this paper is proposed.

Then, the covariance of these noises is considered to achieve the differential privacy for enhancing the confidentiality level. We give the following theorem to design noise covariances for satisfying differential privacy index (4).

Theorem 1. *The mechanism (14)–(15) is (ϵ, δ)-differentially private for adjacency relation (5) if the covariances of noises satisfy the following condition:*

$$Q_{\phi_i} \ge \Gamma^2(\epsilon, \delta)\sigma_{\max}^2(\bar{K}_i C_i H)\zeta^2 I_n. \tag{17}$$

where $Q_{\phi_i} = t_q R_i Q_{\xi_i} R_i^T + N_i Q_\alpha N_i^T$ *and* $\Gamma(\epsilon, \delta) = \left(\mathcal{G}^{-1}(\delta) + \sqrt{(\mathcal{G}^{-1}(\delta))^2 + 2\epsilon}\right)/2\epsilon$.

Proof. The fundamental aim of introducing differential privacy is to protect the confidentiality of LSEs instead of PLSEs. Therefore, not only $\alpha(t)$ but also $\xi_i(t)$ are considered for achieving differential privacy index (4). Then, we express the noise addition form about LSEs:

$$\hat{x}_i^s(t) = \sum_{\tau=t-t_q}^{t} \hat{x}_i(\tau) + \phi_i(t)$$

where $\phi_i(t) = \sum_{\tau=t-t_q}^{t} R_i\xi_i(\tau) + N_i\alpha(t)$. The covariance $Q_{\phi_i} \triangleq \mathbb{E}\{\phi_i(t)\phi_i^T(t)\}$ can be easily derived as shown in theorem.

As previous discussion, the key to realizing differentially private mechanism is obtaining the bound of $\mathcal{V}(\hat{x}_i(t))$. According to steady-state Kalman filter (8) and the variation $\mathcal{V}(x(t))$ for states, we can describe $\mathcal{V}(\hat{x}_i(t))$ by

$$\mathcal{V}(\hat{x}_i(t)) = \bar{K}_i C_i H \mathcal{V}(x(t)). \tag{18}$$

By resorting to Cauchy–Schwarz inequality, the variation between LSEs can be bounded as $\|\mathcal{V}(\hat{x}_i(t))\|_2 \le \|\bar{K}_i C_i H\|_2 \|\mathcal{V}(x(t))\|_2$. Then, combining the boundary of $\mathcal{V}(x(t))$ in Assumption 2, the sensitivity $\Delta(\mathcal{V}(\hat{x}_i(t))) \triangleq \sup_{\text{Adj}(x(t),x'(t))} \|\mathcal{V}(\hat{x}_i(t))\|_2$ can be obtained:

$$\Delta(\mathcal{V}(\hat{x}_i(t))) = \sigma_{\max}(\bar{K}_i C_i H)\zeta. \tag{19}$$

Finally, by directly utilizing the Gaussian mechanism in Le Ny and Pappas (2014), we can easily derive the condition (17) in the theorem. This completes the proof.

Remark 6. Although WLSEs diverge under the proposed encryption approach, differentially private mechanism is still needed for protecting local confidentiality due to the diversity of eavesdropping. For example, some eavesdroppers need LSE at a special time merely, which is sensitive and fragile for certain aims. In this case, the eavesdroppers will not calculate recursive estimates. Instead, they will acquire LSEs by computing differences based on transmitted estimates and other adjacent information. To confront such kind of eavesdropping, differential privacy is known as an effective approach and thus is applied in this paper. Besides, the differentially private mechanism is compatible and not in conflict with the design about covariance divergence. More specifically, the divergence of WLSE requires the existence of noise, while the differential privacy needs to design the lower bound of covariance.

3.2. Confidentiality analysis

For legitimate user, the CDFE is designed by the following decryption form:

$$\hat{x}_f^c(t) = \sum_{i=1}^{L} \bar{W}_i^c(\hat{x}_i^s(t) - \hat{x}_i^s(t-1)) + \hat{x}_f^c(t - t_q) \tag{20}$$

where steady-state compensating weighting fusion matrix $\bar{W}^c \triangleq [\bar{W}_1^c \ \cdots \ \bar{W}_L^c]$ is computed as

$$\bar{W}^c = (e^T(\bar{P}^p)^{-1}e)^{-1}e^T(\bar{P}^p)^{-1} \tag{21}$$

with $\bar{P}^p \triangleq (\bar{P}_{ij}^p) \in \mathbb{R}^{nL\times nL}$. On the other hand, the eavesdropper only knows the steady-state gain $\bar{W}$ in (13) based on eavesdropping model in Definition 1, while the knowledge of extra inserted noises is unknown, including Q_{ξ_i} and Q_α during encryption. Hence, it just makes available for traditionally distributed fusion estimation. Then, the WLSE is calculated by operating difference on transmitted estimates:

$$\hat{x}_i^w(t) = \hat{x}_i^s(t) - \hat{x}_i^s(t-1) + \hat{x}_i^w(t - t_q) \tag{22}$$

In the sequel, the WDFE will be obtained by combining WLSE and steady-state weighting fusion matrix (13):

$$\hat{\mathrm{x}}_f^w(t) = \sum_{i=1}^{L} \bar{\mathrm{W}}_i \hat{\mathrm{x}}_i^w(t) \tag{23}$$

Based on above models, we give the following theorem to show the confidentiality achievement by analyzing the covariances of CDFE and WDFE.

Theorem 2. *Consider systems (1)–(2), legitimate estimation (20) with encryption (14)–(15) and eavesdropping estimation (23). The proposed CI (7) will achieve infinity, which means*

$$\mathcal{CI}(t) \to \infty, \text{ as } t \to \infty.$$

Proof. Firstly, we shall prove the stability of CDFE. Based on the null space design in (15), the CDFE (20) is equivalent to $\hat{\mathrm{x}}_f^c(t) = \sum_{i=1}^{L} \bar{\mathrm{W}}_i^c \hat{\mathrm{x}}_i^p(t)$. To calculate the fusion estimate in LMV sense under perturbed covariances, the weighting fusion matrix is designed as (21), which is motivated by (13). Then, the covariance $\mathrm{P}_f^c(t)$ can be described as steady-state form $\bar{\mathrm{P}}_f^c = (\mathrm{e}^{\mathrm{T}}(\bar{\mathrm{P}}^p)^{-1}\mathrm{e})^{-1}$. According to the LMV criterion, the fusion covariance satisfies $\bar{\mathrm{P}}_f^c \le \bar{\mathrm{P}}_{ii}^p$ $(\forall\ i)$, where the equality holds when $\bar{\mathrm{W}}_i^c = \mathrm{I}_n, \bar{\mathrm{W}}_j^c = 0 (j \neq i)$. With trace operation, we can easily have $\mathrm{Tr}\{\mathrm{P}_f^c(t)\} \le \min_{i=1,\ldots,L} \mathrm{Tr}\{\bar{\mathrm{P}}_{ii} + \mathrm{R}_i \mathrm{Q}_{\xi_i} \mathrm{R}_i^{\mathrm{T}}\}$.

Secondly, we demonstrate the divergence of WDFE. According to transmission model (15) and local wiretapping model (22), the WLSE can be expanded as $\hat{\mathrm{x}}_i^w(t) = \hat{\mathrm{x}}_i^w(t-t_q) + \hat{\mathrm{x}}_i^p(t) + \mathrm{N}_i\alpha(t) - \mathrm{N}_i\alpha(t-1) - \hat{\mathrm{x}}_i^p(t-t_q)$. Then, the estimation error $\tilde{\mathrm{x}}_i^w(t) \triangleq \mathrm{x}(t) - \hat{\mathrm{x}}_i^w(t)$ can be expressed by

$$\tilde{\mathrm{x}}_i^w(t) = \begin{cases} \tilde{\mathrm{x}}_i^p(t) + \mathrm{N}_i\alpha(t), & \text{for time } 0 < t \le t_q \\ \tilde{\mathrm{x}}_i^w(t-t_q) + \theta_i(t), & \text{for time } t > t_q \end{cases} \tag{24}$$

where $\theta_i(t) = \mathrm{N}_i\alpha(t) - \mathrm{N}_i\alpha(t-1) + \tilde{\mathrm{x}}_i^p(t) - \tilde{\mathrm{x}}_i^p(t-t_q)$. When $t \ge t_q$, the covariance can be obtained as the following recursive form:

$$\bar{\mathrm{P}}_{ii}^w(t) = \bar{\mathrm{P}}_{ii}^w(t \bmod t_q) + \lfloor t/t_q \rfloor \bar{\mathrm{P}}_{\theta_{ii}}.$$

with $\bar{\mathrm{P}}_{\theta_{ii}} \triangleq \mathbb{E}\{\theta_i(t)\theta_i^{\mathrm{T}}(t)\}$ computed by

$$\bar{\mathrm{P}}_{\theta_{ii}} = (2\mathrm{I}_n - \bar{\Psi}_i^{t_q})\bar{\mathrm{P}}_{ii} - \bar{\mathrm{P}}_{ii}[\bar{\Psi}_i^{t_q}]^{\mathrm{T}} + 2\mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_i^{\mathrm{T}} + 2\mathrm{R}_i\mathrm{Q}_{\xi_i}\mathrm{R}_i^{\mathrm{T}}.$$

Combining covariances of designed noises and steady-state values, the estimation error covariance of WLSE can be expressed as

$$\mathrm{P}_{ii}^w(t) = \begin{cases} \bar{\mathrm{P}}_{ii} + \mathrm{R}_i\mathrm{Q}_{\xi_i}\mathrm{R}_i^{\mathrm{T}} \\ \quad + \mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_i^{\mathrm{T}}, \text{ for time } 0 < t \le t_q \\ (2\lfloor t/t_q \rfloor + 1)(\mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_i^{\mathrm{T}} + \mathrm{R}_i\mathrm{Q}_{\xi_i}\mathrm{R}_i^{\mathrm{T}}) \\ \quad + (\lfloor t/t_q \rfloor (2\mathrm{I}_n - \bar{\Psi}_i^{t_q}) + \mathrm{I}_n)\bar{\mathrm{P}}_{ii} \\ \quad - \lfloor t/t_q \rfloor \bar{\mathrm{P}}_{ii}[\bar{\Psi}_i^{t_q}]^{\mathrm{T}}, \text{ for time } t > t_q \end{cases} \tag{25}$$

It can be intuitively realized that only t is a variable, thus one has $\mathrm{P}_{ii}^w(t) \to \infty$, as $t \to \infty$.

Analogously, the cross-covariance between WLSEs $(i \neq j)$ is described as follows:

$$\mathrm{P}_{ij}^w(t) = \begin{cases} \bar{\mathrm{P}}_{ij} + \mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_j^{\mathrm{T}}, \text{ for time } 0 < t \le t_q \\ (2\lfloor t/t_q \rfloor + 1)\mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_j^{\mathrm{T}} \\ \quad + (\lfloor t/t_q \rfloor (2\mathrm{I}_n - \bar{\Psi}_i^{t_q}) + \mathrm{I}_n)\bar{\mathrm{P}}_{ij} \\ \quad - \lfloor t/t_q \rfloor \bar{\mathrm{P}}_{ij}[\bar{\Psi}_j^{t_q}]^{\mathrm{T}}, \text{ for time } t > t_q \end{cases} \tag{26}$$

with

$$\bar{\mathrm{P}}_{\theta_{ij}} = 2\mathrm{N}_i\mathrm{Q}_\alpha\mathrm{N}_j^{\mathrm{T}} + (2\mathrm{I}_n - \bar{\Psi}_i^{t_q})\bar{\mathrm{P}}_{ij} - \bar{\mathrm{P}}_{ij}[\bar{\Psi}_j^{t_q}]^{\mathrm{T}}.$$

Its divergence can also be guaranteed as t grows infinity. According to the distributed weighting fusion estimation form (23), we have the estimation error of WDFE as $\tilde{\mathrm{x}}_f^w(t) = \sum_{i=1}^{L} \mathrm{W}_i \tilde{\mathrm{x}}_i^w(t)$, and corresponding covariance is given by

$$\mathrm{P}_f^w(t) = \sum_{i=1}^{L}\sum_{j=1}^{L} \bar{\mathrm{W}}_i \mathrm{P}_{ij}^w(t) \bar{\mathrm{W}}_j^{\mathrm{T}}. \tag{27}$$

Since $\bar{\mathrm{W}}_i (i = 1, \ldots, L)$ are constant matrices computed by (13) and all matrices $\mathrm{P}_{ij}^w(t) (i = 1, \ldots, L; j = 1, \ldots, L)$ diverge, the covariance of WDFE will also grow unbounded, which derives $\mathrm{Tr}\{\mathrm{P}_f^w(t)\} \to \infty$, as $t \to \infty$. Combining Definition 2 and the boundedness of CDFE proved before, the result in this theorem will hold. This completes the proof.

Remark 7. The privacy performance is independent of the calculation order with regard to WLSEs and WDFE. The eavesdropper can directly calculate WDFE without WLSEs as what legitimate user does:

$$\hat{\mathrm{x}}_f^w(t) = \sum_{i=1}^{L} \bar{\mathrm{W}}_i (\hat{\mathrm{x}}_i^s(t) - \hat{\mathrm{x}}_i^s(t-1)) + \hat{\mathrm{x}}_f^w(t-t_q)$$

Through recombining, above estimation can be easily found to be equivalent to (23). Therefore, the estimation error covariances of eavesdropper will diverge regardless of the estimation order.

Remark 8. Different from the proposed wiretapping model, eavesdropper may lose PLSEs at some times under packet drop link assumption in Leong et al. (2019) and Tsiamis et al. (2020). For reducing the estimation error, the eavesdropper will replace empty buffers with following one-step predictions when it misses the transmitted packets:

$$\hat{\mathrm{x}}_i^w(t) = \mathrm{A}\hat{\mathrm{x}}_i^w(t-1) \text{ or } \hat{\mathrm{x}}_i^w(t) = \mathrm{A}\hat{\mathrm{x}}_f^w(t-1).$$

Notice that such information dropping will further increase the covariances of eavesdropper, because the error will be amplified like artificially inserted noises with the proposed encryption approach. Hence, the proposed method can also work under packet drop assumption.

4. Simulation examples

In this section, the effectiveness of proposed fusion-based encryption approach is illustrated by an F-404 aircraft engine system (Eustace, Woodyatt, Merrington, & Runacres, 1994). The real-time states of this engine system imperatively need privacy-preservation, since it must prevent some threatening attacks from third parties, for instance, long-range missile strike, which may cause serious effects on people, economics and politics. The state vector is defined as $\mathrm{x}(t) \triangleq \{\mathrm{s_x}(t), \mathrm{s_y}(t), \mathrm{s_z}(t)\}$, where the pair $(\mathrm{s_x}(t), \mathrm{s_y}(t))$ represents the horizontal position and $\mathrm{s_z}(t)$ denotes the altitude. After setting sampling time $T_0 = 0.1$ s, the matrices in state transition model (1) can be obtained by Chen, Hu, Zhang and Yu (2016):

$$\mathrm{A} = \begin{bmatrix} 0.87 & 0.00 & 0.20 \\ 0.03 & 0.98 & -0.03 \\ 0.03 & 0.00 & 0.80 \end{bmatrix}, \ \mathrm{B} = \begin{bmatrix} 0.1 & 0.0 \\ 0.5 & 0.0 \\ -0.2 & 0.0 \end{bmatrix}.$$

Then, two sensors are considered to observe the above engine system, and the matrices in measurement models (2) are described as

$$\mathrm{C}_1 = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}, \ \mathrm{C}_2 = \begin{bmatrix} 0 & 1 & -1 \end{bmatrix}.$$

Since the operations of aircraft engine and sensors are definitely affected by some factors in practice, including gravity gradients, structural vibrations and mechanical errors, we assume

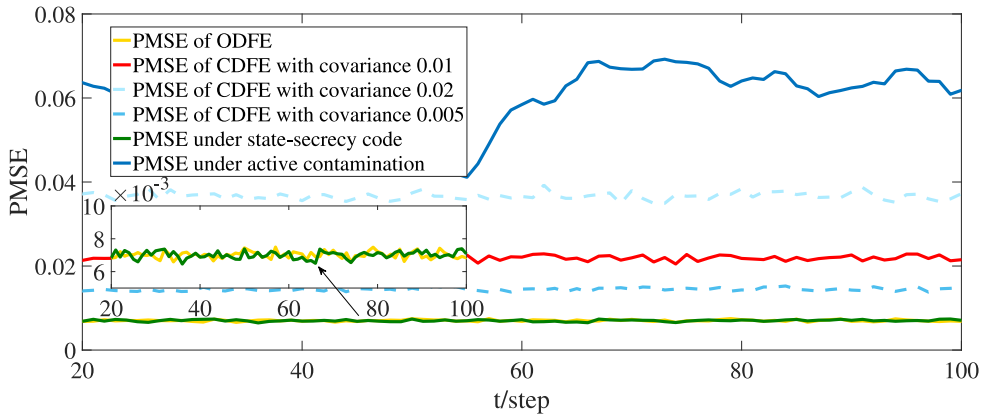


Fig. 2. The comparison of PMSEs in legitimate user under proposed encryption approach, state-secrecy codes in Tsiamis et al. (2018) and Tsiamis et al. (2020) and active contamination in Yan, Zhang et al. (2022).

that the system is disturbed by some WGNs, and the covariances of the noises are set as $Q_w = \mathrm{diag}\{0.04, 0.01\}$, $Q_{v_1} = 0.06$, $Q_{v_2} = 0.02$. It can be computed that $\mathrm{rank}\{[B\ AB\ A^2B]\} = 3$ and $\mathrm{rank}\{\mathrm{col}\{C_i, C_iA, C_iA^2\}\} = 3$ $(i = 1, 2)$, and thus Assumption 1 is satisfied. Moreover, the eigenvalues of system matrix A are $\lambda_1(A) = 0.98$, $\lambda_2(A) = 0.92$ and $\lambda_3(A) = 0.75$, and the spectral radius is $\rho(A) = \max_i |\lambda_i(A)| = 0.98 < 1$. This indicates that the system is stable, in which the advantages of proposed methods can be demonstrated more prominently. By solving the discrete algebra Riccati equations and Lyapunov equations, the steady-state values can be obtained:

$$\begin{cases} \bar{K}_1 = \begin{bmatrix} 0.03 \\ 0.32 \\ -0.10 \end{bmatrix}, \bar{K}_2 = \begin{bmatrix} 0.06 \\ 0.44 \\ -0.16 \end{bmatrix}, \\ \bar{W} = \begin{bmatrix} 0.19 & 0.00 & 0.00 & 0.81 & -0.00 & -0.00 \\ 0.16 & 0.21 & 0.12 & -0.16 & 0.79 & -0.12 \\ -0.03 & -0.01 & 0.16 & 0.03 & 0.01 & 0.84 \end{bmatrix}. \end{cases}$$

When sensors send their information through communication networks, the passive eavesdropper wiretaps transmitted data all the time and then calculates their WDFEs. Therefore, the proposed encryption approach is considered, and the summation length is set as $t_q = 3$. Furthermore, in accordance with the size of $\mathcal{CI}(t)$ in (7), five different confidentiality ranks (CRs) are described as follows:

$$\mathcal{CR}(t) = \begin{cases} \text{low, if } 0 \le \mathcal{CI}(t) < 1; \\ \text{relatively low, if } 1 \le \mathcal{CI}(t) < 2; \\ \text{medium, if } 2 \le \mathcal{CI}(t) < 4; \\ \text{relatively high, if } 4 \le \mathcal{CI}(t) < 8; \\ \text{high, otherwise.} \end{cases} \tag{28}$$

When $\mathcal{CI}(t) = 0$, the eavesdropper has the equally optimal fusion performance as legitimate user, which means the confidentiality is low. When $\mathcal{CI}(t) = 1$, the eavesdropper only obtains half the estimation performance of user, and we set this level as relatively low. The medium and relatively high ranks are similarly determined with incremental indexes. Finally, when $\mathcal{CI}(t) \ge 8$, we set the index as highest level, since hundreds times more damage is enough to describe the privacy-preservation level. On the other hand, although the eavesdropper cannot directly acquire LSE, it also tries to roughly calculate it by resorting to some adjacent PLREs. Hence, the values in Example 1 are introduced in this section, and the differential privacy parameters are determined as $\epsilon = \log 2$ and $\delta = 0.1$.

For showing the effectiveness, the results under the state-secrecy code method (Tsiamis et al., 2018, 2020) (critical events occur at time $t = 1$) and the active contamination method (Yan, Zhang et al., 2022) are considered to be compared with proposed encryption approach. The method in Tsiamis et al. (2018) achieves higher CI than Tsiamis et al. (2020) for stable systems, while both of them approach the open loop prediction case. Then, the relationship between the estimation performance and the covariance Q_α is also given. Besides, due to the existence of random noises, the estimation performance is assessed by mean square error (MSE) which is approximated by implementing Monte Carlo method over an average of 1000 runs. Such practical MSEs (PMSEs) of the estimator in legitimate user under different methods are plotted in Fig. 2. It is seen from this figure that the proposed CDFE is stable, and its performance is close to ODFE. Meanwhile, the PMSE of CDFE decreases as the noise covariance Q_{ξ_i} is reduced. Moreover, owing to the perfectly decoding of LSEs, the DFE under state-secrecy code method has equivalent theoretical MSE to ODFE, and thus it performs better. On the other hand, the PMSE of DFE under active contamination method is the highest due to the reduction of valid components. Although the compensation strategy is used to counteract inserted noise similarly to the proposed approach, the estimation performance loss is inevitable. The fundamental difference is that the local information under active contamination method is dropped, while that under proposed approach still exists which is just perturbed.

To demonstrate the privacy level, Fig. 3 shows the PMSEs of eavesdropper under aforementioned methods. It can be intuitively realized from this figure that only the PMSE under proposed fusion-based encryption approach grows unbounded. At the same time, the divergence rate increases with the addition of noise covariance. Furthermore, the PMSEs under other methods cannot achieve unbounded, since their divergences depend heavily on unstable systems. The stability-independent reason of proposed approach is that the artificial noises are introduced into recursion, and it illustrates the advancement of proposed encryption approach. Combining fusion estimation performances of legitimate users and eavesdroppers, the confidentiality indexes and confidentiality ranks proposed in Definition 2 are shown in Table 2. The privacy-preservation level of fusion-based encryption approach is the highest, because the WDFE diverges while CDFE is bounded, while other methods have relatively low levels due to the insufficient divergence on system states.

On the other hand, we assume the eavesdropper has obtained two adjacent vectors to calculate LSE by difference operation. Then, the probability density functions (PDFs) of these two adjacent PLREs are shown in the following figure, where the difference on two expectations of PLREs represents LSE. It can be illustrated from Fig. 4 that the probabilities of two adjacent PLREs are close to some extent. This distance between PDFs means

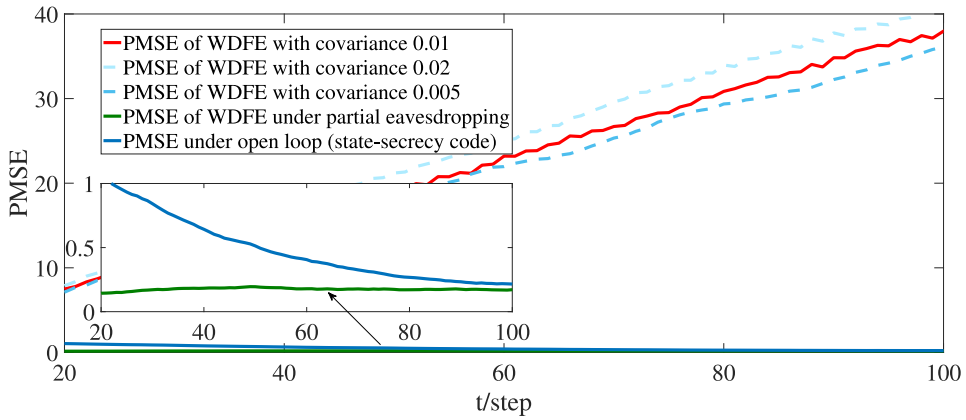


Fig. 3. The comparison of PMSEs in eavesdropper under proposed encryption approach, open loop (state-secrecy codes in Tsiamis et al. (2018, 2020)) and active contamination in Yan, Zhang et al. (2022).

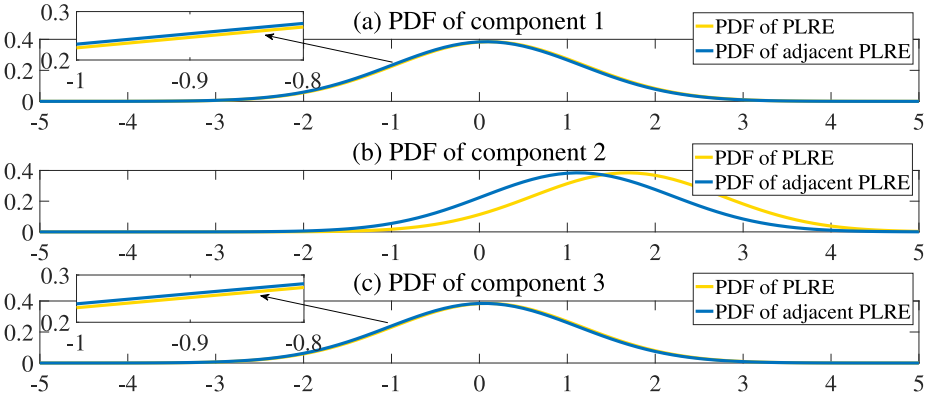


Fig. 4. (a). PDF of component 1. (b). PDF of component 2. (c). PDF of component 3.

Table 2
The comparison of CIs and CRs for different methods.

Encryption methods	Theoretical		t = 2		t = 20		t = 50		t = 100	
	CI	CR	CI	CR	CI	CR	CI	CR	CI	CR
Fusion-based encryption	$\to \infty$	High	3.00	Medium	7.39	High	8.14	High	8.48	High
Open loop (State-secrecy code Tsiamis et al., 2018, 2020)	3.66	Medium	0.76	Low	3.11	Medium	3.26	Medium	3.01	Medium
Active contamination (Yan, Zhang et al., 2022)	1.23	Relatively low	0.56	Low	0.79	Low	1.20	Relatively low	0.23	Low

the certain error of WLSE and the realization of differentially private mechanism. The result for component 2 shows that the conservative performance of mechanism, while the extreme close of other adjacent components' PDFs shows the efficiency.

5. Conclusion

In this paper, the privacy-preservation problem has been investigated for a class of NMFSs against full eavesdropping. New confidentiality index and rank were proposed to depict the privacy-preservation level on secure estimation. On the basis of weighting fusion matrix which is unique in the distributed fusion estimation literature, we designed a fusion-based encryption approach by sequentially inserting two stochastic noises on LSEs. With the null space of compensating weighting fusion matrix in this approach, the adverse impacts of noises in legitimate user were efficiently reduced, which guaranteed the boundedness of CDFE. Moreover, artificial noises were introduced into the recursive computation of eavesdropper's estimators, and then the accumulation of these extra noises diverged the covariance of WDFE. In this case, the CI grew infinity and the highest CR was achieved. At the same time, the differentially private mechanism was realized by designing the lower bound of inserted noises, thus the confidentiality of local information was further enhanced. Finally, the simulation on an aircraft engine system was given to demonstrate the effectiveness of the proposed methods.

Acknowledgments

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, in part by the Key Research and Development Program of Zhejiang Province under Grant 2023C01144, and in part by the Major Key Project of PCL under Grant PCL2021A09.

References

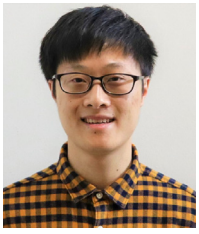
Bar-Shalom, Y., Li, X. R., & Kirubarajan, T. (2001). *Estimation with applications to tracking and navigation*. Hoboken, NJ, USA: Wiley.

Basudan, S., Lin, X., & Sankaranarayanan, K. (2017). A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing. *IEEE Internet of Things Journal*, *4*(3), 772–782.

Chen, B., Ho, D. W. C., Zhang, W., & Yu, L. (2017). Networked fusion estimation with bounded noises. *IEEE Transactions on Automatic Control*, *62*(10), 5415–5421.
Chen, B., & Hu, G. (2018). Nonlinear state estimation under bounded noises. *Automatica*, *98*, 159–168.
Chen, B., Hu, G., Ho, D. W. C., & Yu, L. (2016). Distributed covariance intersection fusion estimation for cyber–physical systems with communication constraints. *IEEE Transactions on Automatic Control*, *61*(12), 4020–4026.
Chen, B., Hu, G., Zhang, W., & Yu, L. (2016). Distributed mixed H_2/H_∞ fusion estimation with limited communication capacity. *IEEE Transactions on Automatic Control*, *61*(3), 805–810.
Deng, Z., Gao, Y., Mao, L., Li, Y., & Hao, G. (2005). New approach to information fusion steady-state Kalman filtering. *Automatica*, *41*(10), 1695–1707.
Ding, D., Han, Q., Xiang, Y., Ge, X., & Zhang, X. (2018). A survey on security control and attack detection for industrial cyber–physical systems. *Neurocomputing*, *275*, 1674–1683.
Ding, K., Ren, X., Leong, A. S., Quevedo, D. E., & Shi, L. (2021). Remote state estimation in the presence of an active eavesdropper. *IEEE Transactions on Automatic Control*, *66*(1), 229–244.
Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Proc. 3rd theory of cryptogr. conf.* (pp. 265–284).
Eustace, R. W., Woodyatt, B. A., Merrington, G. L., & Runacres, A. (1994). Fault signatures obtained from fault implant tests on an F404 engine. *Transactions of the ASME. Journal of Engineering for Gas Turbines and Power*, *116*(1), 178–183.
Fiore, D., & Russo, G. (2019). Resilient consensus for multi-agent systems subject to differential privacy requirements. *Automatica*, *106*, 18–26.
Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communication*, *7*(6), 2180–2189.
Huang, L., Ding, K., Leong, A. S., Quevedo, D. E., & Shi, L. (2021). Encryption scheduling for remote state estimation under an operation constraint. *Automatica*, *127*, Article 109537.
Huang, J., Ho, D. W. C., Li, F., Yang, W., & Tang, Y. (2022). Secure remote state estimation against linear man-in-the-middle attacks using watermarking. *Automatica*, *121*, Article 109182.
Kawano, Y., Kashima, K., & Cao, M. (2021). Modular control under privacy protection: Fundamental trade-offs. *Automatica*, *127*, Article 109518.
Le Ny, J., & Pappas, G. J. (2014). Differentially private filtering. *IEEE Transactions on Automatic Control*, *59*(2), 341–354.
Leong, A. S., Quevedo, D. E., Dolz, D., & Dey, S. (2019). Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper. *IEEE Transactions on Automatic Control*, *64*(9), 3732–3739.
Leong, A. S., Redder, A., Danie, E., & Dey, S. (2018). On the use of artificial noise for secure state estimation in the presence of eavesdroppers. In *2018 European control conference* ECC, (pp. 325–330).
Lu, Y., & Zhu, M. (2018). Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, *96*, 314–325.
Mo, Y., & Murray, R. M. (2017). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, *62*(2), 753–765.
Roecker, J. A., & McGillem, C. D. (1988). Comparison of two-sensor tracking methods based on state vector fusion and measurement fusion. *IEEE Transactions on Aerospace and Electronic Systems*, *24*(4), 447–449.
Shang, J., Zhou, J., & Chen, T. (2022). Single-dimensional encryption against innovation-based stealthy attacks on remote state estimation. *Automatica*, *136*, Article 110015.
Sun, S., & Deng, Z. (2004). Multi-sensor optimal information fusion Kalman filter. *Automatica*, *40*(6), 1017–1023.
Tsiamis, A., Gatsis, K., & Pappas, G. J. (2018). State-secrecy codes for stable systems. In *2018 Annual American control conference* ACC, (pp. 171–177).
Tsiamis, A., Gatsis, K., & Pappas, G. J. (2020). State-secrecy codes for networked linear systems. *IEEE Transactions on Automatic Control*, *65*(5), 2001–2015.
Wang, L., Cao, X., Zhang, H., Sun, C., & Zheng, W. X. (2022). Transmission scheduling for privacy-optimal encryption against eavesdropping attacks on remote state estimation. *Automatica*, *137*, Article 110145.
Xu, D., Yan, X., Chen, B., & Yu, L. (2022). Energy-constrained confidentiality fusion estimation against eavesdroppers. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *69*(2), 624–628.
Yan, X., Chen, B., & Hu, Z. (2022). Distributed estimation for interconnected dynamic systems under binary sensors. *IEEE Sensors Journal*, *22*(13), 13153–13161.
Yan, X., Chen, B., Zhang, Y., & Yu, L. (2022). Guaranteeing differential privacy in distributed fusion estimation. *IEEE Transactions on Aerospace and Electronic Systems*, http://dx.doi.org/10.1109/TAES.2022.3219799.
Yan, X., Zhang, Y., Xu, D., & Chen, B. (2022). Distributed confidentiality fusion estimation against eavesdroppers. *IEEE Transactions on Aerospace and Electronic Systems*, *58*(4).
Yang, W., Li, D., Zhang, H., Tang, Y., & Zheng, W. X. (2020). An encoding mechanism for secrecy of remote state estimation. *Automatica*, *120*, Article 109116.
Yin, X., & Li, S. (2020). Synthesis of dynamic masks for infinite-step opacity. *IEEE Transactions on Automatic Control*, *65*(4), 1429–1441.
Zhang, Y., Chen, B., & Yu, L. (2020). Fusion estimation under binary sensors. *Automatica*, *115*, Article 108861.
Zhang, W., & Shi, L. (2018). Sequential fusion estimation for clustered sensor networks. *Automatica*, *89*, 358–363.

Xinhao Yan received the B.E. degree in communication engineering from Zhejiang University of Technology, Hangzhou, China, in 2020, where he is currently pursuing the M.Sc. degree in control science and engineering. He was also a visiting scholar with The Hong Kong Polytechnic University, Hong Kong, China, in 2022. His current research interests include distributed estimation, information fusion, machine learning, networked systems, privacy and security.

Bo Chen received the B.S. degree in information and computing science from Jiangxi University of Science and Technology, Ganzhou, China, in 2008, and the Ph.D degree in Control Theory and Control Engineering from Zhejiang University of Technology, Hangzhou, China, in 2014. He jointed the Department of Automation, Zhejiang University of Technology in 2018, where he is currently a Professor. He was a Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2014 to 2015 and from 2017 to 2018. He was also a Postdoctoral Research Fellow with the Department of Mathematics, City University of Hong Kong, Hong Kong, from 2015 to 2017. His current research interests include information fusion, distributed estimation and control, networked fusion systems, and secure estimation of cyber–physical systems. Prof. Chen was a recipient of the Outstanding Thesis Award of Chinese Association of Automation in 2015 and also was a recipient of the First Prize of Natural Science of Ministry of Education in 2020. He serves as Associate Editor for IET Control Theory and Applications, Journal of the Franklin Institute and Frontiers in Control Engineering.



Yuchen Zhang received the B.E. degree in automation from the Zhejiang University of Technology, Hangzhou, China, in 2017. He is currently working toward the Ph.D. degree in control science and engineering from Zhejiang University of Technology, Hangzhou, China. His current research interests include distributed estimation of interconnected systems, fusion estimation of binary sensor systems.

Li Yu received the B.S. degree in control theory from Nankai University, Tianjin, China, in 1982, and the M.S. and Ph.D. degrees from Zhejiang University, Hangzhou, China. He is currently a Professor at College of Information Engineering, Zhejiang University of Technology, China. He has successively presided over 20 research projects. He has published 5 academic monographs, 1 textbook and over 300 journal papers. He has also been authorized over 100 patents for invention and granted 5 scientific and technological awards. His current research interests include robust control, networked control systems, cyber–physical systems security and information fusion.