Correspondence

Distributed Confidentiality Fusion Estimation Against Eavesdroppers

This article is concerned with the distributed confidentiality fusion estimation problem for cyber-physical systems in the presence of eavesdroppers. A novel active contamination strategy is proposed to guarantee the confidentiality of local state estimates (LSEs) that are transmitted to the fusion center (FC) over communication channels. Here, the LSEs are actively contaminated by the contaminating vectors, which are related to the weighting fusion process. Meanwhile, the selecting matrices that denote whether the components are contaminated are, respectively, designed for linear and nonlinear systems by maximizing the mean square errors of eavesdropper's estimator. Under this contamination strategy, the confidentiality of systems can be effectively guaranteed when the eavesdropper tries to obtain the real state by fusing the contaminated estimates, because the estimation error covariance of the eavesdropper is large. At the same time, the corresponding compensation strategy is employed in the FC to compensate the performance loss caused by the proposed contamination method. Finally, two illustrative examples are exploited to demonstrate the effectiveness of the proposed methods.

I. INTRODUCTION

Cyber-physical systems (CPSs) are engineering systems, which coordinate, control, and integrate sensing, computing, and physical environments. These systems have found applications in a wide range of fields, such as smart grid communication systems [1], multirobot systems [2], and intelligent transportation systems [3]. As one of the essential issues in CPSs, real-time state estimation based on sensor measurements receives increasing attention, because it can provide a CPS with real-time monitoring and supervision capability. As is known, multisensor fusion estimation, which uses multiple groups of measurement data to better reconstruct the real states, is an effective method to monitor the operation of CPSs [4]. It can effectively improve estimation accuracy and enhance reliability by designing certain fusion criteria. Moreover, with the increasing openness of systems and communication channels, CPSs are exposed to the risks of eavesdropping. After intercepting and correctly decoding the transmitted information through

Manuscript received March 21, 2021; revised July 19, 2021; released for publication October 17, 2021. Date of publication November 11, 2021; date of current version August 9, 2022.

DOI. No. 10.1109/TAES.2021.3124194

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 and in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR20F030004.

Authors' address: The authors are with the Department of Automation and the Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou 310023, China, E-mail: (yanxinhao1998@aliyun.com; YuchenZhang95@163.com; dxxu@qzc.edu.cn). *(Corresponding author: Bo Chen.)*

communication channels, eavesdroppers can tamper with the obtained packets and carry out network attacks, including denial-of-service attacks, deception attacks, and replay attacks [5], [6]. For example, after the transmitted messages of a smart grid are bugged by the eavesdropper, the wrong voltage that is out of the safe range may be delivered to the control terminal and cause serious accidents. Therefore, a significant research direction in fusion estimation for CPSs is the privacy protection against eavesdroppers.

In general, there are two fundamental fusion structures: the centralized fusion structure [7]–[9] and the distributed fusion structure [10]–[13]. Notice that the distributed fusion structure is more robust and has higher fault tolerance when compared with the centralized fusion structure [14]–[16], and thus, the distributed fusion estimation attracts more attention on security investigation. In fact, traditional confidentiality techniques are studied from the perspective of information theory, where original data are encoded in certain criteria to achieve privacy [17]. However, it is difficult to directly utilize conventional encryption techniques at sensors due to possible heavy computation load. Under this constraint, confidentiality problems have been studied recently from the perspectives of signal processing and control theory, where information of physical layer and systems is employed for achieving privacy protection. In this case, a secrecy mechanism was proposed in [18] by randomly withholding sensor information, which guaranteed the perfect expected secrecy defined in [15]. In addition to maximizing the estimation error covariance at an eavesdropper, the negative at remote estimator was also considered in [19] as part of the performance target. Moreover, it is worth noting that the insertion of artificial noise is an efficient approach to implementing confidentiality. Differential privacy is a typical mechanism to provide strong privacy guarantee by resorting to artificial noise [20], [21], and the filtering algorithms based on differential privacy have been employed in many fields, such as road traffic estimation [22] and the Internet of Things within the fifth generation [23]. Additionally, artificial noises can also be inserted into null spaces to guarantee the confidentiality [24]. For instance, artificial noise was injected into the eavesdropper's channel null space in [25], and thus, only the noise eavesdropper could receive. On the contrary, artificial noise was also injected into the null space lying in the legitimate user's communication channel in [26], and the perfect expected secrecy was also achieved under certain noise energy.

Motivated by the aforementioned analysis, the confidentiality in this article shall be implemented by combining the distributed fusion estimation and the physical layer information. Notice that the existing works mainly discuss the remote confidentiality state estimation problems [18], [19], and the confidentiality techniques are based on the distributed sensors and communication channels. It is rather remarkable that the fusion process is also an important issue of distributed fusion estimation but is less utilized for confidentiality. Hence, different from the null spaces in [25] and [26] that lay in the communication channels, the proposed null spaces in this article are related to the weighting matrices of the optimal fusion criterion. On the other hand, additive artificial noises were injected in [18]–[26] for disturbing transmitted messages and confusing eavesdroppers. However, the probability distribution of contaminated data can be identified by the eavesdropper when the quantity of data is large, and the confidentiality cannot be effectively achieved. Alternatively, the multiplicative noise is considered in this article, where the dealing for eavesdroppers is more difficult and the energy consumption is lower when compared with additive noise. The main contributions of this article are summarized as follows:

1) A novel contamination strategy is proposed to impair the estimation performance of the eavesdropper, where the specific selecting matrices are, respectively, designed for linear and nonlinear systems in the sense of maximizing the estimation error covariance of the eavesdropper.
2) Based on the contamination strategy, distributed confidentiality fusion Kalman estimators (DCFKEs) are designed, respectively, for linear and nonlinear systems by combining the fusion criterion and the compensation strategy.

TABLE I
Notation

$\triangleq$	define
$\mathrm{E}\{\}$	mathematical expectation
$\mathrm{diag}\{\}$	block diagonal matrix
$\mathrm{col}\{\}$	column vector
$\mathrm{Tr}\{\}$	trace of the matrix
$\mathrm{rank}\{\}$	rank of the matrix
$\mathbb{R}^n$	n-dimensional real Euclidean space
$\mathbb{R}^{n\times m}$	set of $n \times m$ real matrix
I	identity matrix
$X > (<)0$	positive-definite (negative-definite) matrix
$X \geq (\leq)0$	non-negative definite (non-positive definite) matrix
$\|\cdot\|$	Matrix norm
$\tilde{x}_i(t)$	estimation error of LSE
$\tilde{x}_i^r(t)$	estimation error of ACLE
$\tilde{x}_i^c(t)$	estimation error of CLE
$\tilde{x}_f(t)$	fusion estimation error of fusion center
$\tilde{x}_e(t)$	fusion estimation error of eavesdropper

Table I summarizes the notations most frequently used throughout the remainder of this article.

II. PROBLEM FORMULATION

In this section, the forms of systems and estimators are, respectively, described by the state-space models and Kalman-like filtering structures. Then, the distributed confidentiality fusion structure is given, and the interest of the formulated problem is proposed.

A. Models of Systems and Estimators

Consider a physical process described by the following nonlinear state-space model:

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

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

where $x(t) \in \mathbb{R}^n$ denotes the system state at time t and $w(t)$ is the system noise. $y_i(t) \in \mathbb{R}^{m_i}$ denotes the measurement

of the ith sensor and $v_i(t)$ is the measurement noise. L represents the number of sensors. Meanwhile, $f(x(t)) \in \mathbb{R}^n$ and $h_i(x(t)) \in \mathbb{R}^{m_i}$ are nonlinear vector functions that are assumed to be continuously differentiable. $B(t)$ is a time-varying matrix with appropriate dimension. $w(t)$ and $v_i(t)$ are uncorrelated white Gaussian noises (WGNs) satisfying

$$\begin{aligned}\mathrm{E}\{[w^{\mathrm{T}}(t)\ v_i^{\mathrm{T}}(t)]^{\mathrm{T}}[w^{\mathrm{T}}(t_1)\ v_j^{\mathrm{T}}(t_1)]\} \\ = \delta(t,t_1)\mathrm{diag}\{Q, \delta(i,j)R_i\}\end{aligned} \tag{3}$$

where $\delta(t,t_1)$ is the delta function, i.e., $\delta(t,t_1)=0$ if $t \neq t_1$; otherwise, $\delta(t,t_1)=1$.

Then, based on the measurements $\{y_i(1),\ldots,y_i(t)\}$, the local state estimate (LSE) $\hat{x}_i(t)$ at each sensor for nonlinear systems (1) and (2) is described by

$$\begin{cases}\hat{x}_i^p(t) = f(\hat{x}_i(t-1)) \\ \hat{x}_i(t) = \hat{x}_i^p(t) + K_i^N(t)(y_i(t) - h_i(\hat{x}_i^p(t)))\end{cases} \tag{4}$$

where $\hat{x}_i^p(t)$ denotes the one-step prediction and an optimal gain $K_i^N(t)$ will be given in Section III.

Generally, the nonlinear systems (1) and (2) can be reduced to the following linear systems:

$$x(t+1) = A(t)x(t) + B(t)w(t) \tag{5}$$

$$y_i(t) = C_i(t)x(t) + v_i(t)\ (i=1,\ldots,L) \tag{6}$$

where $A(t)$ and $C_i(t)$ are time-varying matrices with appropriate dimensions. Similarly, the ith LSE $\hat{x}_i(t)$ for linear systems (5) and (6) is given as follows:

$$\begin{cases}\hat{x}_i^p(t) = A(t-1)\hat{x}_i(t-1) \\ \hat{x}_i(t) = \hat{x}_i^p(t) + K_i(t)(y_i(t) - C_i(t)\hat{x}_i^p(t))\end{cases} \tag{7}$$

where an optimal gain $K_i(t)$ will be given in Section III. Furthermore, it is considered that the linear systems (5) and (6) are uniformly completely controllable and observable, i.e., there exist positive scalars ρ_i $(i=1,2,3,4)$ and an integer $N>0$ such that the inequalities (8) and (9) hold for all $t>N$ [27]

$$\rho_1 I_n \le \sum_{j=t-N+1}^{t} \Pi(t,j)B(j)QB^{\mathrm{T}}(j)\Pi^{\mathrm{T}}(t,j) \le \rho_2 I_n \tag{8}$$

$$\rho_3 I_n \le \sum_{j=t-N+1}^{t} \Pi^{\mathrm{T}}(j,t)C_i^{\mathrm{T}}(j)R_i^{-1}C_i(j)\Pi(j,t) \le \rho_4 I_n \tag{9}$$

where

$$\begin{cases}\Pi(j,j) = I_n \\ \Pi(t,j) = \prod_{l=1}^{t-j} A(t-l)(t>j). \\ \Pi(j,t) = \Pi^{-1}(t,j)(t<j)\end{cases} \tag{10}$$

B. Problem of Interest

We consider the distributed confidentiality fusion structure based on the contamination strategy as shown in Fig. 1, where the local estimates are subjected to the eavesdropping when they are transmitted to the fusion center (FC). Before transmission, the LSEs will be actively contaminated by the contaminating vectors, and the actively contaminated local estimates (ACLEs) $\hat{x}_i^r(t)$ are constructed. The detailed contamination criterion will be designed in Section III.

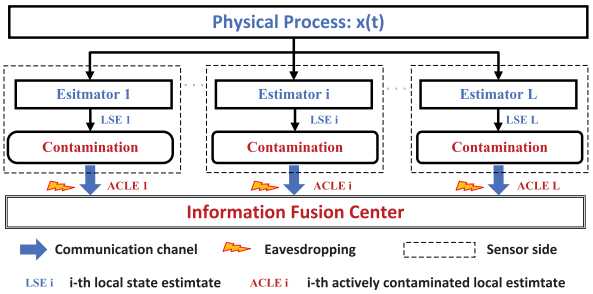

Fig. 1. Distributed confidentiality fusion structure based on the contamination strategy.

After bugging the transmitted estimates (i.e., ACLEs), the eavesdropper can calculate its fusion estimate $\hat{x}_e(t)$ by using the optimal fusion criterion in [10]

$$\hat{x}_e(t) = \sum_{i=1}^{L} W_i(t)\hat{x}_i^r(t) \tag{11}$$

where

$$\begin{cases}W(t) \triangleq [W_1(t), W_2(t), \ldots, W_L(t)] \\ \quad = (I_a^{\mathrm{T}}P^{-1}(t)I_a)^{-1}I_a^{\mathrm{T}}P^{-1}(t) \\ I_a \triangleq [I_n^{\mathrm{T}}\cdots I_n^{\mathrm{T}}] \in \mathbb{R}^{nL\times n} \\ P(t) \triangleq \mathrm{E}\{[\tilde{x}_1^{\mathrm{T}}(t)\cdots\tilde{x}_L^{\mathrm{T}}(t)]^{\mathrm{T}}[\tilde{x}_1^{\mathrm{T}}(t)\cdots\tilde{x}_L^{\mathrm{T}}(t)]\}\end{cases}. \tag{12}$$

Note that the larger the fusion estimation error covariance is, the worse the performance of fusion estimator of eavesdropper is. Thus, the performance target of contamination method in this article is to maximize the estimation error covariance of the eavesdropper.

Since it is also the ACLEs that are received by the FC, the contamination strategy will simultaneously affect the estimation performance of the FC. On the basis of the already-known contamination criterion in FC, the compensation strategies can be applied to reduce the performance loss, and the compensated local estimates (CLEs) $\hat{x}_i^c(t)$ can be constructed. The details of compensation are to be designed in Section III. As such, based on the compensation strategy and the optimal weighting fusion criterion, the distributed fusion estimate (DFE) $\hat{x}_f(t)$ in the FC can be calculated as

$$\hat{x}_f(t) = \sum_{i=1}^{L} W_{fi}(t)\hat{x}_i^c(t) \tag{13}$$

where

$$\begin{cases}W_f(t) \triangleq [W_{f1}(t), W_{f2}(t), \ldots, W_{fL}(t)] \\ \quad = (I_a^{\mathrm{T}}\Sigma_f^{-1}(t)I_a)^{-1}I_a^{\mathrm{T}}\Sigma_f^{-1}(t) \\ \Sigma_f(t) \triangleq \mathrm{E}\{[(\tilde{x}_1^c(t))^{\mathrm{T}}\cdots(\tilde{x}_L^c(t))^{\mathrm{T}}]^{\mathrm{T}} \\ \quad \times[(\tilde{x}_1^c(t))^{\mathrm{T}}\cdots(\tilde{x}_L^c(t))^{\mathrm{T}}]\}\end{cases}. \tag{14}$$

Consequently, the problems to be solved in this article can be described as follows:

1) Design an effective contamination criterion to ensure the confidentiality of the fusion estimation process by encrypting the transmitted estimates and impairing the estimation performance of the eavesdropper.

2) Design DCFKEs based on the optimal fusion criterion and the compensation strategy to reduce the negative effect caused by the proposed contamination strategy.

Remark 1: As is well known, the eavesdropper can intercept and correctly decode the transmitted data through the communication channels in a practical scenario. In most cases, the eavesdropping process just appears in certain and finite time horizon due to the limitation of eavesdropper's equipment, such as computation power, transmission energy, and sampling period. In other words, such eavesdroppers have limited access to the transmitted information, and they can only obtain partial messages. Meanwhile, there still exist some powerful eavesdroppers, which have enough capacity to obtain all the transmitted messages. Therefore, to prevent eavesdropping as much as possible, the eavesdroppers are considered to be able to obtain real-time transmitted information. Under this background, the proposed algorithm can be suitable for most confidentiality scenarios, and the main work in this article has more practical and important significance.

III. MAIN RESULTS

This section proposes a novel confidentiality scheme called contamination, and the detailed design is given in Section III-A. Based on the above contamination strategy, the DCFKEs and the selecting matrices in contamination criterion are, respectively, designed for linear and nonlinear systems.

A. Contamination Criterion

Notice that the transmitted estimates may be subject to the risk of eavesdropping in communication channels. Hence, it is necessary to appropriately modify the LSE to achieve confidentiality. Inspired by the compression strategy in [28], the LSE will be contaminated by the following form:

$$\hat{x}_i^r(t) = H_i(t)\hat{x}_i(t) + [I_n - H_i(t)]\phi_i(t) \tag{15}$$

where $H_i(t)$ is the selecting matrix and $\phi_i(t)$ is the contaminating vector. More concretely, the selecting matrix $H_i(t)$ is a binary diagonal matrix, which can be described as

$$H_i(t) \triangleq \text{diag}\{\gamma_{i1}(t), \ldots, \gamma_{in}(t)\} \tag{16}$$

where $\gamma_{ij}(t) \in \{0, 1\}$ are binary variables that represent whether the jth component of the LSE is going to be contaminated. Meanwhile, the diagonal elements in (16) satisfy $\sum_{j=1}^{n} \gamma_{ij}(t) = s_i(t)(0 \le s_i(t) \le n)$. It can be noted that the smaller $s_0(t) = \sum_{i=1}^{L} s_i(t)$, the more information of local estimation is lost. Under this trend, though the estimation performance of the eavesdropper will become worse, the performance of the DFE will be impaired simultaneously. In other words, there exists a game between the confidentiality and the accuracy. For the sake of brevity in this article, we postulate $s_0(t)$ to be a constant number $\bar{s}_0$. Then, all the possible selecting matrices will construct the following set with finite elements:

$$\hat{H}_F(t) = \{H_F^1(t), \ldots, H_F^k(t), \ldots, H_F^{\bar{k}}(t)\} \tag{17}$$

where $\bar{k} = C_{nL}^{\bar{s}_0}$ denotes the number of elements in the set. In this case, selecting matrices can only choose elements from the set (17).

Let us define

$$\begin{cases} H_F(t) \triangleq \text{diag}\{H_1(t), \ldots, H_L(t)\} \\ \bar{H}_F(t) \triangleq \text{diag}\{I_n - H_1(t), \ldots, I_n - H_L(t)\}. \\ \bar{W}(t) = W(t)\bar{H}_F(t) \end{cases} \tag{18}$$

Then, the null space of $\bar{W}(t)$ can be described as

$$\Psi(t) = [\varphi_1(t) \cdots \varphi_{nL-r(t)}(t)],\ r(t) = \text{rank}\{\bar{W}(t)\} \tag{19}$$

where $\{\varphi_1(t), \ldots, \varphi_{nL-r(t)}(t)\}$ are the null vectors of $\bar{W}(t)$, and the null space $\Psi(t)$ satisfies

$$\bar{W}(t)\Psi(t) = 0,\ \Psi^{\mathrm{T}}(t)\Psi(t) = I_{nL-r(t)}. \tag{20}$$

Define the WGN $a_F(t) = \text{col}\{a_f(t), \ldots, a_f(t)\} \in \mathbb{R}^{nL-r(t)}$, which is utilized for inserting into the null space, where $a_f(t)$ is the random scalar with covariance $Q_a \triangleq \text{E}\{a_f(t)a_f^{\mathrm{T}}(t)\}$. Then, the contaminating vector $\phi_i(t)$ can be obtained as

$$\phi(t) \triangleq \text{col}\{\phi_1(t) \cdots \phi_L(t)\} = \Psi(t)a_F(t). \tag{21}$$

Remark 2. To enhance the reliability of the proposed contamination strategy, the multiplicative WGN is inserted into $\Psi(t)$ to guarantee the randomness of the transmitted estimates (i.e., ACLEs) such that the contaminated components of ACLEs are random enough and the eavesdropper will not suspect it. Meanwhile, it can be noted that the random vector $\phi(t)$ still lies in the null space of $\bar{W}(t)$, and the contamination strategy can still work during the fusion estimation process of the eavesdropper.

B. DCFKE Design for Linear Systems

For linear systems (5) and (6) under assumption (3), the standard Kalman filter is employed to estimate the real state at each sensor [30], where the optimal gain $K_i(t)$ in (7) is calculated by

$$\begin{cases} K_i(t) = P_{ii}^p(t)C_i^{\mathrm{T}}(t)[C_i(t)P_{ii}^p(t)C_i^{\mathrm{T}}(t) + R_i]^{-1} \\ P_{ii}^p(t) = A(t-1)P_{ii}(t-1)A^{\mathrm{T}}(t-1) \\ \quad\quad +B(t-1)QB^{\mathrm{T}}(t-1) \\ P_{ii}(t) = P_{ii}^p(t) - K_i(t)C_i(t)P_{ii}^p(t) \end{cases}. \tag{22}$$

Meanwhile, the estimation error cross covariance between ith and jth sensors is recursively calculated as follows [31]:

$$\begin{aligned} P_{ij}(t) = [I_n - K_i(t)C_i(t)][A(t-1)P_{ij}(t-1)A^T(t-1) \\ + B(t-1)QB^T(t-1)][I_n - K_j(t)C_j(t)]^T. \end{aligned} \tag{23}$$

Before deriving the results of Theorem 1, let us define

$$\begin{cases} \Lambda(t) \triangleq \text{E}\{x(t)x^{\mathrm{T}}(t)\} \\ \quad = A(t-1)\Lambda(t-1)A^{\mathrm{T}}(t-1) \\ \quad +B(t-1)QB^{\mathrm{T}}(t-1) \\ x_F(t) \triangleq \text{col}\{x(t), \ldots, x(t)\},\ \Lambda_F(t) \triangleq \text{E}\{x_F(t)x_F^{\mathrm{T}}(t)\} \end{cases} \tag{24}$$

where $\Lambda(t)$ represents the second moment of the system state (5).

Theorem 1: Considering the active contamination strategy (15), the selecting matrix for linear systems is given by

$$H_F^L(t) = \arg\max_{H_F^k(t)} ||H_F^k(t) - H_F^m(t)|| \tag{25}$$

where

$$H_F^m(t) = \Lambda_F(t)(\Lambda_F(t) + P(t))^{-1}. \tag{26}$$

Moreover, the selecting matrix $H_F^L(t)$ is independent of the initial covariances $P(0)$ under the conditions (8) and (9). Meanwhile, the one-step prediction is employed to compensate the performance loss in the FC

$$\hat{x}_i^c(t) = H_i(t)\hat{x}_i^r(t) + [I_n - H_i(t)]A(t-1)\hat{x}_f(t-1). \tag{27}$$

Proof: Based on the aforementioned contamination criterion, the derivation process of the selecting matrix $H_F^L(t)$ can be summarized by two steps. First, the selecting matrix that minimizes the estimation error covariance of the eavesdropper (i.e., $H_F^m(t)$) is computed in the linear minimum variance sense. It can be deduced from (5) and (15) that the estimation error $\tilde{x}_i^r(t)$ is described as follows:

$$\tilde{x}_i^r(t) = H_i(t)\tilde{x}_i(t) + [I_n - H_i(t)](x(t) - \phi_i(t)). \tag{28}$$

After obtaining the transmitted estimates (i.e., ACLEs), the eavesdropper will directly weight them as (11) and (12). Then, the corresponding fusion estimation error can be described by combining (20) and (28) as

$$\tilde{x}_e(t) = W(t)H_F(t)\tilde{x}_F(t) + \bar{W}(t)x_F(t). \tag{29}$$

Next, the estimation error covariance $P_e(t) \triangleq \mathrm{E}\{\tilde{x}_e(t)\tilde{x}_e^{\mathrm{T}}(t)\}$ can be calculated by

$$\begin{aligned} P_e(t) = W(t)[&H_F(t)P(t)H_F(t) \\ &+ \bar{H}_F(t)\Lambda_F(t)\bar{H}_F(t)]W^{\mathrm{T}}(t). \end{aligned} \tag{30}$$

For minimizing the covariance $P_e(t)$ in (30), the first-order partial derivative of $\mathrm{Tr}\{P_e(t)\}$ about $H_F(t)$ is introduced as

$$\begin{aligned} \frac{\partial \mathrm{Tr}\{P_e(t)\}}{\partial H_F(t)} = W^{\mathrm{T}}(t)W(t)[&2H_F(t)P(t) \\ &- 2\Lambda_F(t) + 2H_F(t)\Lambda_F(t)]. \end{aligned} \tag{31}$$

Then, $H_F^m(t)$ is derived as (26) when the first-order partial derivative (31) equals zero. To demonstrate the minimality under above scenario, $H_F^m(t)$ is substituted into (30), and the extremum of $P_e(t)$ can be obtained as

$$P_e^m(t) = W(t)(I - H_F^m(t))\Lambda_F(t)W^T(t). \tag{32}$$

On the other hand, when $H_F = 0$, (i.e., all the components are contaminated), $P_e(t)$ can be described by

$$P_e^0(t) = W(t)\Lambda_F(t)W^T(t). \tag{33}$$

Since $H_F^m(t)$ is positive definite, one has $\mathrm{Tr}\{P_e^0(t)\} > \mathrm{Tr}\{P_e^m(t)\}$ according to (32) and (33), and this means that $P_e^m(t)$ is the minimum of $P_e(t)$. Second, the fusion estimation error covariance of eavesdropper needs to be maximized to derive the selecting matrix $H_F^L(t)$. In this sense, the matrix norm is maximized as (25), where $H_F^k(t)$ is a matrix selected from the set (17).

At the same time, the contamination strategy will impair the estimation performance in the FC. Therefore, the DFE needs to be compensated to reduce the performance loss. Notice that the one-step prediction compensation strategy in [28] is an effective method to compensate the contaminated components, i.e., the contaminating vector will be replaced by the one-step prediction of the last-time DFE. Then, the CLE will be derived as (27), and the corresponding estimation error of the CLE can be described as

$$\begin{aligned} \tilde{x}_i^c(t) = &H_i(t)\tilde{x}_i(t) + [I_n - H_i(t)]A(t-1)\tilde{x}_f(t-1) \\ &+ [I_n - H_i(t)]B(t-1)w(t-1) \end{aligned} \tag{34}$$

where $\tilde{x}_f(t-1) \triangleq x(t-1) - \hat{x}_f(t-1)$ denotes the estimation error of the DFE, and it can be recursively calculated by the following form:

$$\begin{aligned} \tilde{x}_f(t-1) = &W_f(t-1)H_F(t-1)\tilde{x}_F(t-1) \\ &+ W_f(t-1)\bar{H}_F(t-1)A(t-2)\tilde{x}_f(t-2) \\ &+ W_f(t-1)\bar{H}_F(t-1)B(t-2)w(t-2) \end{aligned} \tag{35}$$

with $\tilde{x}_F^{\mathrm{T}}(t-1) \triangleq [x(t-1) - \hat{x}_1(t-1) \cdots x(t-1) - \hat{x}_L(t-1)]$. Combining (34) and (35), the estimation error covariance $\Sigma_{ij}(t) \triangleq \mathrm{E}\{\tilde{x}_i^c(t)[\tilde{x}_j^c(t)]^{\mathrm{T}}\}$ can be recursively computed by [28]

$$\begin{aligned} \Sigma_{ij}(t) = &H_i(t)P_{ij}(t)H_i(t) + H_i(t)[\Phi_i^{\mathrm{T}}(t)A^{\mathrm{T}}(t-1) \\ &+ (I_n - K_i(t)C_i(t))B(t-1)QB^{\mathrm{T}}(t-1)] \\ &\times (I_n - H_j(t)) + (I_n - H_j(t))[A(t-1)\Phi_j(t) \\ &+ B(t-1)QB^{\mathrm{T}}(t-1)(I_n - K_j(t)C_j(t))^{\mathrm{T}}]H_i(t) \\ &+ (I_n - H_i(t))[A(t-1)P_f(t-1)A^{\mathrm{T}}(t-1) \\ &+ B(t-1)QB^{\mathrm{T}}(t-1)](I_n - H_j(t)) \end{aligned} \tag{36}$$

where

$$\begin{cases} \Phi_i(t) = [W_f(t-1)\bar{H}(t)A(t-2)\Phi_i(t-1) \\ \quad +W_f(t-1)H_F(t)\hat{P}_i(t-1) \\ \quad +W_f(t-1)\bar{H}(t)B(t-2)QB^{\mathrm{T}}(t-2) \\ \quad \times(I_n - K_i(t-1)C_i(t-1))^{\mathrm{T}}] \\ \quad \times[A(t-1) - K_i(t)C_i(t)A(t-1)]^{\mathrm{T}} \\ \hat{P}_i(t) \triangleq col\{P_{1i}^{\mathrm{T}}(t) \dots P_{Li}^{\mathrm{T}}(t)\} \end{cases}. \tag{37}$$

Furthermore, the fusion estimation error covariance $P_f(t) \triangleq \mathrm{E}\{(x(t) - \hat{x}_f(t))(x(t) - \hat{x}_f(t))^{\mathrm{T}}\}$ can be derived according to the optimal fusion criterion

$$P_f(t) = (I_a^{\mathrm{T}}\Sigma_f^{-1}(t)I_a)^{-1}.$$

Finally, the weighting matrices and the DFE can be obtained by (13) and (14).

Moreover, to verify the independence of initial values, the error system of local Kalman filter is described by

$$\tilde{x}_i(t+1) = \Omega_i(t)\tilde{x}_i(t) + \delta_i(t) \tag{38}$$

where

$$\begin{cases} \Omega_i(t) = (I_n - K_i(t)C_i(t))A(t) \\ \delta_i(t) = (I_n - K_i(t)C_i(t))B(t)w(t) - K_i(t)v_i(t) \end{cases}.$$

The corresponding covariance of (38) can be expressed by the following form when $t > t_0$:

$$P_{ij}(t) = \Gamma_i(t, t_0)P_{ij}(t_0)\Gamma_j^{\mathrm{T}}(t, t_0) + \hat{\Delta}_{ij}(t, t_0) \tag{39}$$

where

$$\begin{cases} \Gamma_i(t, t_0) = \prod_{l=0}^{t-t_0-1} \Omega_i(t_0 + l) \ (\Gamma_i(t_0, t_0) = I_n) \\ \Delta_{ij}(t) \triangleq \mathrm{E}\{\delta_i(t)\delta_j^{\mathrm{T}}(t)\} \\ \hat{\Delta}_{ij}(t, t_0) = \sum_{l=0}^{t-t_0-1} \Gamma_i(t, t_0 + l + 1) \\ \qquad \times \Delta_{ij}(l + 1)\Gamma_j^{\mathrm{T}}(t, t_0 + l + 1) \end{cases}.$$

When the conditions (8)–(10) hold, the error system (38) will be uniformly stable, and then, the following inequalities will hold [27]:

$$\|\Gamma_i(t, t_0)\| \le c_1 e^{-c_2(t-t_0)} \to 0 \ (t \to \infty, c_1, c_2 > 0) \tag{40}$$

$$\left\|\Gamma_j(t, t_0)\right\| \le c_3 e^{-c_4(t-t_0)} \to 0 \ (t \to \infty, c_3, c_4 > 0). \tag{41}$$

Given initial conditions $P_{ij}^1(t_0)$ and $P_{ij}^2(t_0)$, the following inequality can be obtained by combining (40) and (41):

$$\begin{aligned} \left\|P_{ij}^1(t) - P_{ij}^2(t)\right\| &\le c_1 c_3 e^{-(c_2+c_4)(t-t_0)} \\ &\quad \times \left\|P_{ij}^1(t_0) - P_{ij}^2(t_0)\right\| \\ &\to 0 \ (t \to \infty, c_1, c_2 > 0). \end{aligned} \tag{42}$$

Therefore, the estimation error covariance $P_{ij}(t)$ in (39) will be independent of initial values as t goes to ∞ as the results in (42). As such, the confidentiality will be guaranteed for any initial value of covariance given by the eavesdropper. This completes the proof.

From Theorem 1, the calculation procedures of the proposed DCFKE for linear systems can be presented by Algorithm 1.

Remark 3: The contamination strategy works as follows: when the eavesdropper weights the ACLEs as (11) and (12), the weighting fusion estimate of the contaminated components will be equal to zero due to (20). In this case, the eavesdropper will lost the partial local information, which is related to the corresponding contaminated components, and the fusion estimation error of the eavesdropper will be deduced as (29). On the other hand, the contaminated components are compensated in the FC by utilizing the complementary selecting matrix "$I_n - H_i(t)$," where the contaminated part will be replaced by the compensating estimate as (27). In fact, the performance loss of the DFE is inevitable due to the tradeoff between the confidentiality and the estimation precision. Fortunately, the proposed compensation strategy can reduce the performance loss to some extent in this article.

Remark 4: It can be seen from Theorem 1 that the contamination criterion is composed of certain second moments. To be specific, $W(t)$, $\phi(t)$, $P(t)$, and $\Lambda_F(t)$ are constructed by the corresponding second moments, and thus, they can be calculated in recursive ways by (12); (18)–(21); (22) and (23); and (24), respectively. This implies that the whole contamination process can be done in advance or be independently calculated by sensors and the FC. Hence, the eavesdropper cannot easily obtain the contamination criterion, and it cannot effectively compensate the performance loss.

Algorithm 1 For given $\hat{x}_i(0)$, $i = 1, \ldots, L$

1: Calculate the selecting matrices by (24)–(26);
2: Calculate the contaminating vector by (12) and (19)–(21);
3: Calculate the LSE by (7) and (22);
4: Calculate the ACLE by (15);

Eavesdropper:

5: Calculate the covariances and cross covariances of LSEs by (22) and (23), respectively;
6: Weight the transmitted estimates (i.e., ACLEs) by (8) and (9), output $\hat{x}_e(t)$.

FC:

7: Calculate the selecting matrices by (24)–(26);
8: Calculate the CLEs by (27);
9: Calculate the covariances of CLEs by (36) and (37);
10: Weight the CLEs by (13) and (14), output $\hat{x}_f(t)$.

C. DCFKE Design for Nonlinear Systems

For nonlinear systems (1) and (2), the optimal gain $K_i^N(t)$ in (4) is calculated by the extended Kalman filter [32]

$$\begin{cases} K_i^N(t) = P_{ii}^p(t)C_{J_i}^{\mathrm{T}}(t)[C_{J_i}(t)P_{ii}^p(t)C_{J_i}^{\mathrm{T}}(t) + R_i]^{-1} \\ P_{ii}^p(t) = A_{J_i}(t-1)P_{ii}(t-1)A_{J_i}^{\mathrm{T}}(t-1) \\ \qquad +B(t-1)QB^{\mathrm{T}}(t-1) \\ P_{ii}(t) = P_{ii}^p(t) - K_i^N(t)C_{J_i}(t)P_{ii}^p(t) \end{cases} \tag{43}$$

where $A_{J_i}(t)$ and $C_{J_i}(t)$ are the linearized matrices

$$\begin{cases} A_{J_i}(t) = \left.\frac{\partial f(x(t))}{\partial x(t)}\right|_{x(t)=\hat{x}_i(t)} \\ C_{J_i}(t) = \left.\frac{\partial h_i(x(t))}{\partial x(t)}\right|_{x(t)=f(\hat{x}_i(t))} \end{cases}. \tag{44}$$

At the same time, the estimation error cross covariance can be recursively calculated by

$$\begin{aligned} P_{ij}(t) &= [I_n - K_i^N(t)C_{Ji}(t)][A_{J_i}(t-1)P_{ij}(t-1) \\ &\quad \times A_{J_i}^{\mathrm{T}}(t-1) + B(t-1)QB^{\mathrm{T}}(t-1)] \\ &\quad \times [I_n - K_j(t)C_{J_i}(t)]^{\mathrm{T}}. \end{aligned} \tag{45}$$

Different from the results in linear systems, the second moment of the system state in (1) cannot be directly calculated in a recursive way as (24). In this case, $\Lambda_F(t)$ cannot be recursively calculated and $H_F^m(t)$ cannot be derived as (26) after the derivation of the results for nonlinear systems. In order to maximize the estimation error covariance as much as possible, the following theorem is proposed for nonlinear systems.

Theorem 2: Considering the contamination strategy in (15), the selecting matrix for nonlinear systems is given by

$$H_F^N(t) = \arg\max_{H_F^k(t)} \mathrm{Tr}\{H_F^k(t)P(t)H_F^k(t)\}. \tag{46}$$

Then, the FC reduces the performance loss by taking the nonlinear one-step prediction compensation strategy

$$\hat{x}_i^c(t) = H_i(t)\hat{x}_i^r(t) + [I_n - H_i(t)]f(\hat{x}_f(t-1)). \tag{47}$$

Proof: Similar to the analysis in linear systems, the confidentiality index is maximizing the estimation error covariance of eavesdropper. Since $\Lambda_F(t)$ cannot be directly calculated in a recursive way for nonlinear systems, the selecting matrix $H_F^N(t)$ is computed by (46) to maximize the rest part of (30), i.e., "$H_F(t)P(t)H_F(t)$."

On the other hand, the nonlinear one-step prediction compensation strategy is given by (47), and the recursive estimation error covariances of CLEs can be obtained by the similar derivation of (34)–(37)

$$\begin{aligned}\Sigma_{ij}(t) = {} & H_i(t)P_{ij}(t)H_i(t) + H_i(t)[\Phi_i^{\mathrm{T}}(t)A_{J_i}^{\mathrm{T}}(t-1) \\ & + (I_n - K_i^N(t)C_{J_i}(t))B(t-1)QB^{\mathrm{T}}(t-1)] \\ & \times (I_n - H_j(t)) + (I_n - H_j(t))[A_{J_j}(t-1)\Phi_j(t) \\ & + B(t-1)QB^{\mathrm{T}}(t-1)(I_n - K_i^N(t)C_{J_i}(t))^{\mathrm{T}}]H_i(t) \\ & + (I_n - H_i(t))[A_{J_i}(t-1)P_f(t-1)A_{J_j}^{\mathrm{T}}(t-1) \\ & + B(t-1)QB^{\mathrm{T}}(t-1)](I_n - H_j(t))\end{aligned} \tag{48}$$

where

$$\begin{aligned}\Phi_i(t) = {} & [W_f(t-1)\bar{H}(t)A_{J_i}(t-2)\Phi_i(t-1) \\ & + W_f(t-1)H_F(t)\hat{P}_i(t-1) \\ & + W_f(t-1)\bar{H}(t)B(t-2)QB^{\mathrm{T}}(t-2) \\ & \times (I_n - K_i^N(t-1)C_{J_i}(t-1))^{\mathrm{T}}] \\ & \times [A_{J_i}(t-1) - K_i^N(t)C_{J_i}(t)A_{J_i}(t-1)]^{\mathrm{T}}.\end{aligned} \tag{49}$$

Finally, the optimal weighting matrix $W_f(t)$ and the DFE $\hat{x}_f(t)$ can also be calculated by (13) and (14). This completes the proof.

From Theorem 2, the computation procedures of the proposed DCFKE for nonlinear systems can be presented by Algorithm 2.

Remark 5: According to Theorem 2, the selecting matrix is determined by (46) to avoid computing the second moment of the system state. One explanation is that the part "$\bar{H}_F(t)\Lambda_F(t)\bar{H}_F(t)$" cannot be recursively calculated, and thus, the rest part is considered as the maximization target. On the other hand, the maximization problem (46) simultaneously means that the components with the largest covariance are contaminated. Thus, the estimation error covariance of the eavesdropper is maximized for nonlinear systems.

Remark 6: Notice that the maximum of dimension is $nL \times nL$, because some local matrices with dimension n in L sensors are combined to construct an augmented matrix under certain conditions. For instance, the augmented covariance matrix $P(t)$ is constructed by $L \times L$ local estimation error covariance matrices $P_{ij}(t) \in \mathbb{R}^{n\times n}$ $(i = 1, \ldots, L,\ j = 1, \ldots, L)$. Hence, the space complexity of the FC and the eavesdropper is $\mathcal{O}(n^2L^2)$. On the other hand, during the weighting fusion process, the augmented covariance matrices $P(t) \in \mathbb{R}^{nL\times nL}$ and $\Sigma_f(t) \in \mathbb{R}^{nL\times nL}$ will be inverted. Therefore, the time complexity of the FC and the eavesdropper is $\mathcal{O}(n^3L^3)$ due to the inversion of the $nL \times nL$ matrix.

Algorithm 2 For given $\hat{x}_i(0)$, $i = 1, \ldots, L$

1: Calculate the selecting matrices by (46);
2: Calculate the contaminating vector by (12) and (19)–(21);
3: Calculate the LSE by (4), (43), and (44);
4: Calculate the ACLE by (15);

Eavesdropper:

5: Calculate the covariances and cross covariances of LSEs by (43) and (45), respectively;
6: Weight the transmitted estimates (i.e., ACLEs) by (11) and (12), output $\hat{x}_e(t)$.

FC:

7: Calculate the selecting matrices by (46);
8: Calculate the CLEs by (47);
9: Calculate the covariances of CLEs by (48) and (49);
10: Weight the CLEs by (13) and (14), output $\hat{x}_f(t)$.

IV. SIMULATION EXAMPLE

The target tracking system and the robot localization system are utilized to demonstrate the effectiveness of the DCFKEs in this section. Meanwhile, the estimation errors and the corresponding comparisons are plotted to verify the other performances of proposed methods.

A. Target Tracking

Consider a maneuvering target tracking system with two sensors. The system state vector is defined as $x(t) \triangleq \mathrm{col}\{s(t), \dot{s}(t)\}$, where $s(t)$ and $\dot{s}(t)$ denote the position and the velocity of the target, respectively. Then, the system parameters of (5) and (6) can be given by [33]

$$\begin{cases} A = \begin{bmatrix} 1 & f_s(t) \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} \frac{f_s^2(t)}{2} \\ f_s(t) \end{bmatrix} \\ C_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, C_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{cases} \tag{50}$$

where $f_s(t) = 1$ is the sampling period. $w(t)$, $v_1(t)$, and $v_2(t)$ are, respectively, uncorrelated WGNs with covariances

$$Q = 1, R_1 = \begin{bmatrix} 0.9 & 0 \\ 0 & 0.5 \end{bmatrix}, R_2 = \begin{bmatrix} 0.7 & 0 \\ 0 & 0.8 \end{bmatrix}. \tag{51}$$

Moreover, the covariance of the artificial noise is $Q_a = 1$.

To demonstrate the effectiveness of the proposed DCFKE for linear systems, the trajectories of the target and trackings are shown in Fig. 2. It can be seen from this figure that the proposed DCFKE can track the unstable target

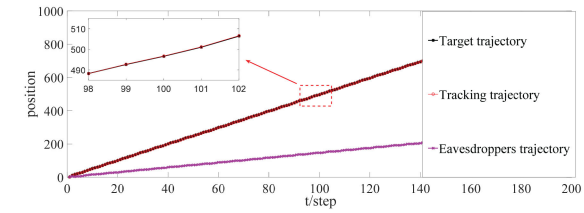

Fig. 2. Trajectories of target, tracking, and eavesdropper for linear systems.

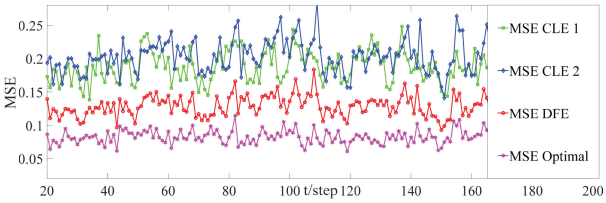

Fig. 3. MSEs of CLEs, DFE, and optimal fusion estimate for linear systems.

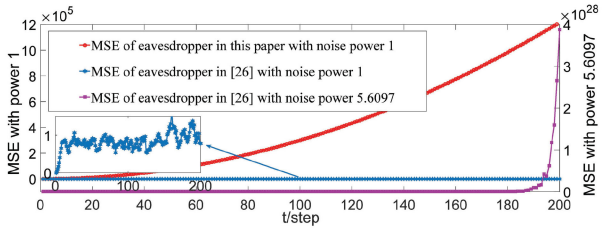

Fig. 4. Comparison of the eavesdropper's performance between the proposed DCFKE and the fusion estimate in [26].

well, while the eavesdropper cannot. Due to the existence of stochastic noises, the estimation performance is assessed by the mean square error (MSE) over an average of 100 runs Monte Carlo method. It is seen from Fig. 3 that all the estimates, including CLEs and DFEs, are bounded. Meanwhile, the MSE of the DFE is smaller when compared with that of each CLE, and thus, the effectiveness of the compensation strategy and the weighting fusion algorithm is illustrated. On the other hand, the MSE of the DFE is a little higher than that of the optimal fusion estimate, where the local estimates used for information fusion are not contaminated. This minor loss implies the tradeoff between the confidentiality and the precision. Then, to illustrate the confidentiality of the proposed DCFKE, the MSE of the fusion estimate of eavesdropper is shown in Fig. 4. It can be seen from Fig. 4 that the MSE of eavesdropper's estimate is large and even diverges under the confidentiality mechanism in Theorem 1. At the same time, the fusion estimate of the eavesdropper in [26] is still bounded under the same noise power "1." Furthermore, only when the power of artificial noise is large enough, e.g., the noise covariance is "5.6097" as given in the simulation of [26], the fusion estimate can diverge as shown in Fig. 4. Hence, the artificial noise insertion method in this article saves the energy to some extent.

B. Mobile Robot Localization

Consider a localization system of mobile robot in planar environments, where the motion model of the robot is given by [34]

$$\begin{cases} S_x(t+1) = S_x(t) + T_0\zeta_v(t)\cos(\Theta(t)) \\ S_y(t+1) = S_y(t) + T_0\zeta_v(t)\sin(\Theta(t)) \\ \Theta(t+1) = \Theta(t) + T_0\zeta_w(t) \end{cases}. \tag{52}$$

Here, $T_0 = 1$ is the sampling period. $(S_x(t), S_y(t))$ are the center Cartesian coordinates of robot in the XY plane, and $\Theta(t)$ is the angular orientation. $\zeta_v(t) = 1$ and $\zeta_w(t) = 0.1$ are the motion commands to, respectively, control the translational velocity and the rotational velocity of the robot. This implies that the robot does the uniform circular motion. Then, let us define the state vector $x(t) = \text{col}\{S_x(t), S_y(t), \Theta(t)\}$, and the nonlinear function $f(x(t))$ in (1) can be described by utilizing the motion model in (52)

$$f(x(t)) = \begin{bmatrix} S_x(t) + T_0\zeta_v(t)\cos(\Theta(t)) \\ S_y(t) + T_0\zeta_v(t)\sin(\Theta(t)) \\ \Theta(t) + T_0\zeta_w(t) \end{bmatrix}. \tag{53}$$

$w(t)$ is a WGN with covariance $Q = 0.01$ and $B = I_2$ for (1).

At the same time, it is considered that four known positions, denoted as $(S_{x_i}, S_{y_i})(i = 1, 2, 3, 4)$, are selected as the landmarks. The distance $d_i(t)$ and the azimuth $\theta_i(t)$ from each landmark to the center Cartesian coordinates of the robot can be described as follows:

$$\begin{cases} d_i(t) = \sqrt{(S_{x_i} - S_x(t))^2 + (S_{y_i} - S_y(t))^2} \\ \theta_i(t) = \Theta(t) - \arctan(\frac{S_{y_i} - S_y(t)}{S_{x_i} - S_x(t)}) \end{cases}. \tag{54}$$

In this case, the measurement equations are given by

$$\begin{cases} y_1(t) = \begin{bmatrix} h_1(x(t)) \\ h_2(x(t)) \end{bmatrix} + v_1(t) \\ y_2(t) = \begin{bmatrix} h_3(x(t)) \\ h_4(x(t)) \end{bmatrix} + v_2(t) \\ h_i(x(t)) = \begin{bmatrix} d_i(t) \\ \theta_i(t) \end{bmatrix} (i = 1, 2, 3, 4) \end{cases} \tag{55}$$

where $v_1(t)$ and $v_2(t)$ are, respectively, uncorrelated WGNs with covariances $R_1 = 0.02$ and $R_2 = 0.04$. By expanding $f(x(t))$ and $h_i(x(t))$ in Taylor series as (44), the linearized matrices $A_{J_i}(t)$ and $C_{J_i}(t)$ near the point $x^* \in \mathbb{R}^3$ can be obtained as

$$\begin{cases} A_{J_i}(t) = \begin{bmatrix} 1 & 0 & -T_0\zeta_v(t)\sin\Theta(t) \\ 0 & 1 & T_0\zeta_v(t)\cos\Theta(t) \\ 0 & 0 & 1 \end{bmatrix}_{x(t)=x^*} \\ D_{J_i}(t) = \begin{bmatrix} \frac{-\tilde{S}_{x_i}(t)}{\sqrt{\tilde{S}_{x_iy_i}(t)}} & \frac{-\tilde{S}_{y_i}(t)}{\sqrt{\tilde{S}_{x_iy_i}(t)}} & 0 \\ \frac{-\tilde{S}_{y_i}(t)}{\tilde{S}_{x_iy_i}(t)} & \frac{-\tilde{S}_{x_i}(t)}{\tilde{S}_{x_iy_i}(t)} & 1 \end{bmatrix}_{x(t)=x^*} \\ C_{J_1}(t) \triangleq \begin{bmatrix} D_{J_1}(t) \\ D_{J_2}(t) \end{bmatrix}, C_{J_2}(t) \triangleq \begin{bmatrix} D_{J_3}(t) \\ D_{J_4}(t) \end{bmatrix} \end{cases} \tag{56}$$

where

$$\begin{cases} \tilde{S}_{x_i}(t) = S_{x_i} - S_x(t) \\ \tilde{S}_{y_i}(t) = S_{y_i} - S_y(t) \\ \tilde{S}_{x_iy_i}(t) = \tilde{S}^2_{x_i}(t) + \tilde{S}^2_{y_i}(t) \end{cases}. \tag{57}$$

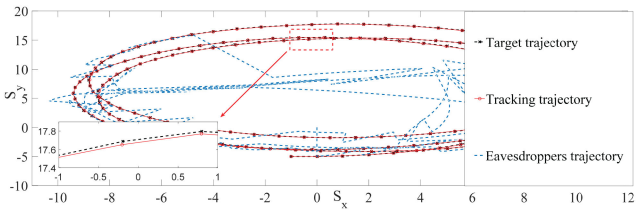

Fig. 5. Trajectories of target, tracking, and eavesdropper for nonlinear systems.

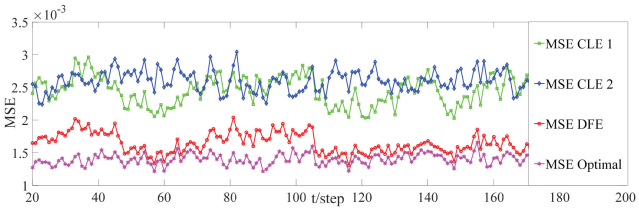

Fig. 6. MSEs of CLEs, DFE, and optimal fusion estimate for nonlinear systems.

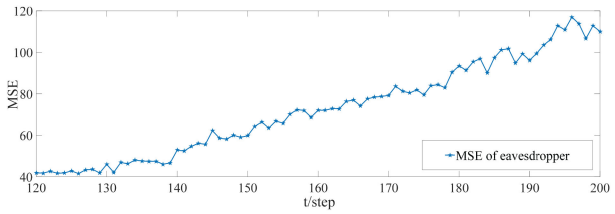

Fig. 7. MSE of the eavesdropper for nonlinear systems.

To show the effectiveness of the proposed DCFKE for nonlinear systems, the target's trajectory and the trackings' trajectories are plotted in Fig. 5. It is seen from this figure that the proposed DCFKE can keep up with the nonlinear target under the contamination strategy, while the eavesdropper cannot track well. Similar to the results in linear systems, Fig. 6 shows that the DFE is bounded and performs better than any CLE, while little worse than the optimal fusion estimate. Then, it can be seen from Fig. 7 that the MSE of eavesdropper's fusion estimate becomes large by implementing Theorem 2 when compared with that of the DEF in Fig. 6. This implies that the selecting matrix $H_F^N(t)$ can also effectively impair the estimation performance of the eavesdropper.

V. CONCLUSION

In this article, the distributed confidentiality fusion estimation problem was investigated for a class of CPSs with the existence of eavesdropping. The active contamination strategy was employed to achieve the confidentiality of transmission, where the null spaces lay in the weighting matrices and the WGNs were inserted to guarantee the sufficient randomness. Specifically, the selecting matrices were, respectively, designed for linear and nonlinear systems in the sense of maximizing the estimation error covariance of the eavesdropper. In this case, the eavesdropper's estimator performed bad by directly weighting the transmitted estimates. Nevertheless, the DFE reduced the performance loss by combining the one-step prediction compensation strategy and the corresponding optimal fusion algorithm weighted by matrices. Finally, two illustrative examples were employed to demonstrate the effectiveness of the proposed methods.

XINHAO YAN
YUCHEN ZHANG
DAXING XU
BO CHEN, *Member, IEEE*
Zhejiang University of Technology, Hangzhou, China

REFERENCES

[1] M. Liu, Y. Shi, and H. Gao
Aggregation and charging control of PHEVs in smart grid: A cyber-physical perspective
Proc. IEEE, vol. 104, no. 5, pp. 1071–1085, May 2016, doi: 10.1109/JPROC.2015.2512500.

[2] J. Fink, A. Ribeiro, and V. Kumar
Robust control for mobility and wireless communication in cyber-physical systems with application to robot teams
Proc. IEEE, vol. 100, pp. 164–178, Jan. 2012.

[3] A. Gokhale, M. P. Mcdonald, S. Drager, and W. McKeever
A cyber physical systems perspective on the real-time and reliable dissemination of information in intelligent transportation systems
Netw. Protoc. Algorithms, vol. 2, pp. 116–136, 2010.

[4] 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.

[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] T. Li, B. Chen, L. Yu, and W. A. Zhang
Active security control approach against DoS attacks in cyber-physical systems
IEEE Trans. Autom. Control, vol. 66, no. 9, pp. 4303–4310, Sep. 2021.

[7] Y. Zhang, B. Chen, and L. Yu
Fusion estimation under binary sensors
Automatica, vol. 115, 2020, Art. no. 108861.

[8] S. Deshmukh, B. Natarajan, and A. Pahwa
State estimation over a lossy network in spatially distributed cyber-physical systems
IEEE Trans. Signal Process., vol. 62, no. 15, pp. 3911–3923, Aug. 2014.

[9] X. Wang, A. K. Gostar, T. Rathnayake, B. Xu, A. Bab-Hadiashar, and R. Hoseinnezhad
Centralized multiple-view sensor fusion using labeled multi-Bernoulli filters
Signal Process., vol. 150, pp. 75–84, 2018, doi: 10.1016/j.sigpro.2018.04.010.

[10] S. Sun and Z. Deng
Multi-sensor optimal information fusion Kalman filter
Automatica, vol. 40, pp. 1017–1023, 2005.

[11] 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, to be published, doi: 10.1109/TAC.2021.3075198.

[12] Y. Wang and X. R. Li
Distributed estimation fusion with unavailable cross-correlation
IEEE Trans. Aerosp. Electron. Syst., vol. 48, no. 1, pp. 259–278, Jan. 2012, doi: 10.1109/TAES.2012.6129634.

[13] 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, doi: 10.1109/TAES.2015.130803.

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

[15] 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, doi: 10.1109/TAES.2003.1207252.

[16] J. A. Roecker and C. D. McGillen
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.

[17] C. Shannon
Communication theory of secrecy
system," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[18] A. Tsiamis, K. Gatsis, and G. J. Pappas
State estimation with secrecy against eavesdroppers
IFAC-PapersOnLine, vol. 50, pp. 8385–8392, 2017.

[19] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey
Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper
IEEE Trans. Autom. Control, vol. 64, no. 9, pp. 3732–3739, Sep. 2017.

[20] K. H. Degue and J. Le Ny
On differentially private Kalman filtering
in *Proc. IEEE Glob. Conf. Signal Inf. Process.*, 2017, pp. 487–491.

[21] J. L. Ny and G. J. Pappas
Differentially private filtering
IEEE Trans. Autom. Control, vol. 59, no. 2, pp. 341–354, Feb. 2014, doi: 10.1109/TAC.2013.2283096.

[22] H. Andre and J. Le Ny
A differentially private ensemble Kalman Filter for road traffic estimation
in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, New Orleans, LA, USA, 2017, pp. 6409–6413, doi: 10.1109/ICASSP.2017.7953390.

[23] J. Wang, R. Zhu, and S. Liu
A differentially private unscented Kalman filter for streaming data in IoT
IEEE Access, vol. 6, pp. 6487–6495, 2018, doi: 10.1109/ACCESS.2018.2797159.

[24] S. Goel and R. Negi
Guaranteeing secrecy using artificial noise
IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[25] 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, doi: 10.1109/TAES.2017.2649178.

[26] D. Xu, B. Chen, L. Yu, and W. A. Zhang
Secure dimensionality reduction fusion estimation against eavesdroppers in cyber-physical systems
ISA Trans., vol. 104, pp. 154–161, 2020, doi: 10.1016/j.isatra.2019.11.009.

[27] A. H. Jazwinski
Stochastic Processes and Filtering Theory. New York, NY, USA: Academic, 1970.

[28] B. Chen, W. A. Zhang, L. Yu, G. Hu, and H. Song
Distributed fusion estimation with communication bandwidth constraints
IEEE Trans. Autom. Control, vol. 60, no. 5, pp. 1398–1403, May 2015.

[29] Z. Deng, Y. Gao, L. Mao, Y. Li, and G. Hao
New approach to information fusion steady-state Kalman filtering
Automatica, vol. 41, no. 10, pp. 1695–1707, 2005.

[30] R. E. Kalman
A new approach to linear filtering and prediction problems
J. Basic Eng., vol. 82, pp. 35–45, 1960.

[31] S. L. Sun
Multi-sensor information fusion white noise filter weighted by scalars based on Kalman predictor
Automatica, vol. 40, pp. 1447–1453, 2004, doi: 10.1016/j.automatica.2004.03.012.

[32] K. Reif, S. Gunther, E. Yaz, and R. Unbehauen
Stochastic stability of the discrete-time extended Kalman filter
IEEE Trans. Autom. Control, vol. 44, no. 4, pp. 714–728, 1999, doi: 10.1109/9.754809.

[33] X. R. 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, doi: 10.1109/TAES.2003.1261132.

[34] S. Thrun, W. Burgard, and D. Fox
Probabilistic Robotics. Cambridge, MA, USA: MIT, 2005.