Distributed Dimensionality Reduction Fusion Estimation for Cyber-Physical Systems under DoS Attacks

Bo Chen, *Member, IEEE*, Daniel W. C. Ho, *Fellow, IEEE*, Wen-An Zhang, *Member, IEEE*, Li Yu, *Member, IEEE*

***Abstract*—This paper studies the distributed dimensionality reduction fusion estimation problem for a class of cyber-physical systems (CPSs) under denial-of-service (DoS) attacks. The problem is modeled under the resource constraints (i.e. bandwidth or energy) for the defender and attacker. Based on a new attack and compensation model, a recursive distributed Kalman fusion estimator (DKFE) is designed for the addressed CPSs. Though the optimization objects of the defender and attacker are opposite, the corresponding optimization problems are established based on different available information. In this case, an explicit form of suboptimal dimensionality reduction is given against DoS attacks, while an effective attack strategy is proposed for the attacker. A stability condition is derived such that the mean square error of the designed DKFE is bounded. Two illustrative examples are given to show the effectiveness of the proposed methods.**

***Index Terms*—Fusion estimation, Kalman filtering, DoS attacks, Dimensionality reduction, Stability analysis, Cyber-physical systems**

I. Introduction

As cyber-physical systems (CPSs) are being widely integrated in various critical infrastructure and running on wired or wireless communication networks, however, these critical infrastructures are vulnerable to cyber security threats [1]–[4]. Since state estimation plays an essential role in the monitoring and supervision of CPSs, its importance has made the security and estimation performance a major concern [5]–[9]. As is known, multi-sensor information fusion estimation, which is one of the important issues in information fusion, utilizes useful information contained in multiple sets of data for the purpose of *estimating* a quantity/a parameter in a process [10]. Thus, fusion estimation provides an attractive alternative to study secure estimation problem under attacks, and the approach leads to improvement of estimation accuracy and enhancement of reliability and robustness against faults [10]–[16]. Moreover, distributed fusion structure is generally more robust, reliable, and fault-tolerant than centralized fusion framework [11], [12], [17], while the denial-of-service (DoS) attack (which can congest the communication channel) is the most reachable attack pattern in the attack space [18] and the most financially expensive security incidents [19]. In this sense, the distributed information fusion estimation problem is investigated in this paper for a class of CPS architecture (see Fig.1) under DoS attacks, where the sensor node only measures the target information, and the sink node is a gateway node, which is responsible for receiving measurements, computing the local estimate and sending the estimate to an information fusion center. A typical example of such CPS is the smart grid communication systems [20], [21].

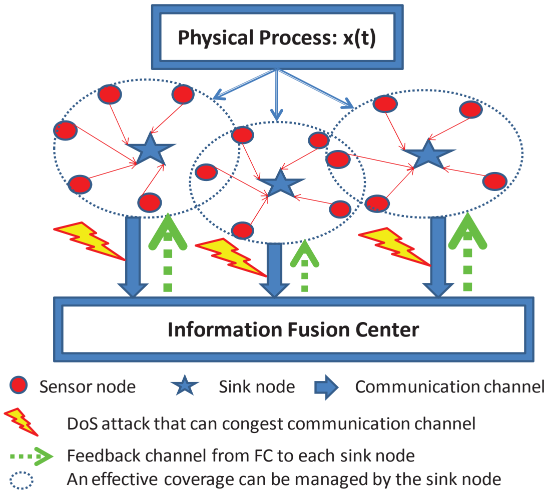

Physical Process: x(t)
Information Fusion Center
● Sensor node
★ Sink node
Communication channel
DoS attack that can congest communication channel
Feedback channel from FC to each sink node
An effective coverage can be managed by the sink node

Fig. 1. Distributed information fusion estimation for a class of spatially distributed physical systems under DoS attacks.

When each local estimate with the same dimension of system state "x(t)" is sent to the fusion center (FC) through a communication channel, it may suffer communication bandwidth constraints, particularly, for large-scale CPSs with high-dimension state "x(t)". This is because any communication network can only carry a finite amount of information per unit of time. It has been pointed out in [8] that, for a multi-dimensional local estimate of "x(t)" in CPSs, the dimensionality reduction method (see [22]–[24]) is more suitable to solve the problem of bandwidth constraint as compared with the vector quantization method (see [25], [26]). On the other hand, when considering the state estimation under attacks, the false data injection attack, which affects the data integrity of packets, has been studied in [27]–[32] to design different secure estimation strategies. Meanwhile, the problem of estimating a deterministic mean-shift parameter was investigated in [33] in the presence of Byzantine attacks, and a data driven approach was proposed in [34] to study the state estimation problem under subspace attacks. Since attacks may run out of energy very fast when their energy budget is limited [35], a random DoS attack strategy was introduced in [36] to save energy by intermittently launching attacks. Then, an optimal energy-constrained attack strategy was proposed in [37] to maximize

This work was supported in part by Research grants Council of the Hong Kong Special Administrative Region, China (CityU 11204514, CityU 11300415) and CityU Strategic Research Grant (7004672), in part by the National Natural Science Funds of China (Nos. 61403345, 61573319, 61673351), in part by the Hong Kong Scholars Program (No. XJ2014013), and in part by the China Post-Doctoral Science Foundation (No. 2016M590547).

B. Chen and D. W. C. Ho are with the Department of Mathematics, City University of Hong Kong, Hong Kong, 999077. (email:bchen@aliyun.com; madaniel@cityu.edu.hk).

W.A. Zhang and L. Yu are with the Department of Automation, Zhejiang University of Technology, HangZhou 310023, China (email: wazhang@zjut.edu.cn; lyu@zjut.edu.cn).

the expected average estimation error. By simultaneously considering decision processes of the attacker and defender, the game-theoretic approach was used in [38] to study state estimation problem under attacks. Meanwhile, the resilient control problem has been studied in [39]–[43] for the CPSs under attacks. It should be pointed out that most existing works are focus on the single-sensor state estimation or centralized fusion state estimation under attacks, however, the distributed dimensionality reduction fusion estimation problem under DoS attacks is challenging, and has not yet been fully investigated.

Under the distributed fusion framework, only partial components of each local estimate of "x(t)" can be transmitted to the FC because of bandwidth constraints. At the same time, due to the attacking energy constraints and the spatially distributed sink nodes, the adversary can only intermittently execute DoS attacks, and only κ of the L communication channels can be jammed to cause packet losses when launching a DoS attack. Motivated by the aforementioned analysis, the aims of this paper are i) how to design dimensionality reduction strategy so as to minimize the fusion estimation error by resorting to the feedback channels, and ii) how to design attack strategy so as to maximize the fusion estimation error by the eavesdropped information of the attacker. In summary, the main contributions are as follows:

- By constructing a unified model that can compensate the information loss caused by dimensionality reduction and DoS attacks, the recursive distributed Kalman fusion estimator (DKFE) is designed for the CPSs under attacks.
- A simple judgement criterion is proposed to determine the dimensionality reduction and information compensation strategy for the defender, and an effective attack schedule, which is dependent on the accuracy of the eavesdropped information, is proposed for the attacker.
- Based on the defender's dimensionality reduction and compensation strategy and the attacker's attack strategy, a stability condition is derived such that the mean square error (MSE) of the DKFE is bounded.

Table I summarizes the notation most frequently used throughout the remainder of the paper.

II. Problem Formulation

A. Modeling of Dimensionality Reduction and DoS Attacks

Consider the physical process of Fig.1 modeled by the following discrete state-space model:

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

where $x(t) \in \mathrm{R}^n$ is the current state of the process. It is considered that each sensor can collect information on the partial state components. When the sensor measurements are sent to the corresponding sink nodes, the ith sink node's measurement $y_i(t) \in \mathrm{R}^{q_i}$ is modeled by:

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

where $A \in \mathrm{R}^{n\times n}$ and $C_i \in \mathrm{R}^{q_i\times n}$. $w(t) \in \mathrm{R}^n$ and $v_i(t) \in \mathrm{R}^{q_i}$ are uncorrelated zero-mean Gaussian white noises satisfying

$$\begin{aligned} &\mathrm{E}\{[w^{\mathrm{T}}(t)\ v_i^{\mathrm{T}}(t)]^{\mathrm{T}}[w^{\mathrm{T}}(t_1)\ v_j^{\mathrm{T}}(t_1)]\} \\ &\qquad = \delta_{t,t_1}\mathrm{diag}\{Q_w, \delta_{i,j}Q_{v_i}\} \end{aligned}. \tag{3}$$

TABLE I
Table of Notations

$\triangleq$	define
$\mathrm{E}\{\cdot\}$	mathematical expectation
$\mathrm{diag}\{\cdot\}$	block diagonal matrix
$\mathrm{Tr}(\cdot)$	trace of the matrix
$\mathrm{rank}(\cdot)$	rank of the matrix
$\lvert\lvert \cdot \rvert\rvert_2$	2-norm of the matrix
$\mathrm{Prob}\{X\}$	occurrence probability of the event X
X^{T}	transpose of matrix X
$X(i,i)$	the ith diagonal element of the matrix X
$a \perp b$	orthogonal vectors a and b
R^n	n-dimensional real Euclidean space
$\mathrm{R}^{n\times m}$	set of $n \times m$ real matrix
I_n	identity matrix of size $n \times n$
$n!$	$n(n-1)(n-2)\cdots 1$
δ_{t,t_1}	$\delta_{t,t_1} = \begin{cases} 1 & t = t_1 \\ 0 & t \neq t_1 \end{cases}$
A	system matrix of a CPS
$w(t)$	process noise in a CPS
Q_w	covariance of $w(t)$
C_i	measurement matrix
$v_i(t)$	measurement noise from the ith sensor
Q_{v_i}	covariance of $v_i(t)$
L	the number of sensors or communication channels
$x(t)$	state of a CPS
$y_i(t)$	measurement from ith sensor
$\hat{\mathrm{x}}_i(t)$	the ith local state estimate of a CPS based on $y_i(t)$
$\eta(t)$	decision variable is used to determine whether the adversary launches a DoS attack or not at time t
$\eta_i(t)$	decision variable is used to determine whether the ith communication channel is jammed or not by attacks at time t
r_i	only r_i components of $\hat{\mathrm{x}}_i(t)$ are allowed to be transmitted to the FC at each time
$\gamma_{ij}(t)$	decision variable is used to determine whether the jth component of $\hat{\mathrm{x}}_i(t)$ is selected and sent to the FC or not
$H_i(t)$	compression operator: $H_i(t) = \mathrm{diag}\{\gamma_{i1}(t), \gamma_{i2}(t), \cdots, \gamma_{in}(t)\}$
κ	only κ communication channels can be jammed when the adversary launches a DoS attack
$\tilde{\mathrm{x}}_i(t)$	estimation error of $\hat{\mathrm{x}}_i(t)$
$\hat{\mathrm{x}}_{s_i}(t)$	dimensionality reduction signal that is sent to the FC
$\bar{\mathrm{x}}_{s_i}(t)$	local estimation signal received by the FC
$\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$	compensating state estimate of $x(t)$ in the FC
$\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)$	estimation error of $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$
$z_x(t)$	the adversary eavesdrops on the $x(t)$
$z_c^i(t)$	the adversary eavesdrops on the $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$
$\hat{\mathrm{x}}_{\mathrm{A}}(t-1)$	least square estimate of $x(t-1)$ based on $z_x(t)$
$\hat{\mathrm{x}}_{\mathrm{AC}}^i(t-1)$	least square estimate of $\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$ based on $z_c^i(t)$
$\hat{\mathrm{x}}(t)$	DKFE for the CPSs
$\tilde{\mathrm{x}}(t)$	fusion estimation error of $\hat{\mathrm{x}}(t)$
$P_{ij}(t)$	estimation error covariance between $\hat{\mathrm{x}}_i(t)$ and $\hat{\mathrm{x}}_j(t)$: $\mathrm{E}\{\tilde{\mathrm{x}}_i(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\}(\forall i, j)$
$\Sigma_{ij}(t)$	estimation error covariance between $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$ and $\hat{\mathrm{x}}_j^{\mathrm{c}}(t)$: $\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)[\tilde{\mathrm{x}}_j^{\mathrm{c}}(t)]^{\mathrm{T}}\}(\forall i, j)$
$P(t)$	fusion estimation error covariance: $\mathrm{E}\{\tilde{\mathrm{x}}(t)\tilde{\mathrm{x}}^{\mathrm{T}}(t)\}$
$\mathrm{W}_i(t)$	weighting fusion matrix

As pointed out in [6], model (1) is widely adopted for describing state dynamics of power systems, smart gird infrastructures, and build automation systems, etc. Based on the measurements $\{y_i(1), \cdots, y_i(t)\}$, the local optimal estimator at the ith sink node is given by the Kalman filter [44]:

$$\begin{cases} \hat{\mathrm{x}}_i(t) = \Phi_{\mathrm{K}_i}(t)\hat{\mathrm{x}}_i(t-1) + \mathrm{K}_i(t)y_i(t) \\ \mathrm{K}_i(t) = P_{ii}^*(t)C_i^{\mathrm{T}}[C_iP_{ii}^*(t)C_i^{\mathrm{T}} + Q_{v_i}]^{-1} \end{cases}, \tag{4}$$

where $\mathrm{G}_{\mathrm{K}_i}(t) \triangleq I_n - \mathrm{K}_i(t)C_i, \Phi_{\mathrm{K}_i}(t) \triangleq \mathrm{G}_{\mathrm{K}_i}(t)A$, and the local optimal estimation error covariance matrix $P_{ii}(t)$ is computed by:

$$\begin{cases} P_{ii}(t) = \mathrm{G}_{\mathrm{K}_i}(t)P_{ii}^{*}(t) \\ P_{ii}^{*}(t) = AP_{ii}(t-1)A^{\mathrm{T}} + Q_w \end{cases}, \tag{5}$$

where $P_{ii}^{*}(t)$ denotes one-step prediction error covariance matrix. Moreover, it follows from (4–5) that the estimation error cross-covariance matrix $P_{ij}(t)$ is calculated by:

$$P_{ij}(t) = \mathrm{G}_{\mathrm{K}_i}(t)[AP_{ij}(t-1)A^{\mathrm{T}} + Q_w]\mathrm{G}_{\mathrm{K}_j}^{\mathrm{T}}(t). \tag{6}$$

As shown in Fig.1, to design an optimal fusion estimator, each local estimate $\hat{\mathrm{x}}_i(t)$ must be transmitted to the FC through communication channel. In fact, the dimension of the state variable "x(t)" in (1) is high in many large-scale CPSs, however, any communication channel can only carry a finite amount of information per unit time. In this case, it is unrealistic that each sink node can send complete information on the $\hat{\mathrm{x}}_i(t)$ to the FC. To reduce communication traffic, similar to the idea of the dimensionality reduction strategies in [22], [23], only r_i $(1 \leq r_i < n)$ components of the ith local estimate $\hat{\mathrm{x}}_i(t)$ are selected and transmitted to the FC at a particular time. According to this dimensionality reduction strategy, the allowed sending components (ASC) of $\hat{\mathrm{x}}_i(t)$ has Δ_i possible cases, where Δ_i is taken as

$$\Delta_i = \mathrm{C}_n^{r_i} = \frac{n!}{r_i!(n-r_i)!}. \tag{7}$$

Then, at a particular time, only one vector signal, which is taken from one groups of the above Δ_i cases, is selected and transmitted to the FC, and this selected signal is denoted by $\hat{\mathrm{x}}_{s_i}(t)(\in \mathrm{R}^{r_i})$.

When each sink node sends $\hat{\mathrm{x}}_{s_i}(t)$ to the remote FC through communication networks, an adversary can congest the communication channels between the sink nodes and the FC by launching DoS attacks. This means that the FC may not receive $\hat{\mathrm{x}}_{s_i}(t)$ at time t. Notice that the attacker has a limited energy budget and has to determine whether to jam the channels or not at each sampling time [37]. Moreover, due to the limited energy and the spatially distributed sink nodes, when the adversary launches a DoS attack, only κ $(1 \leq \kappa < L)$ channels of the L communication channels can be jammed such that packets are dropped. To model the above attack strategy, let $\eta(t) \in \{0, 1\}$ denote whether the adversary launches a DoS attack or not at time t. Meanwhile, denote $\eta_i(t) = 1$ or $\eta_i(t) = 0$ as the indicator function whether the ith communication channel is jammed by attacks or not at time t, and $\eta_i(t)$ must satisfy:

$$\sum\nolimits_{i=1}^{L} \eta_i(t) = \kappa \; (1 \leq \kappa < L), \tag{8}$$

where $\eta_i(t)(i = 1, \cdots, L)$ are to be designed in Section III for maximizing the performance degradation when the adversary launches a DoS attack at time t. Meanwhile, it is considered that $\eta(t)$ is a Bernoulli random variable with $\mathrm{E}\{\eta(t)\} = \eta$, where η is called the rate of attack.

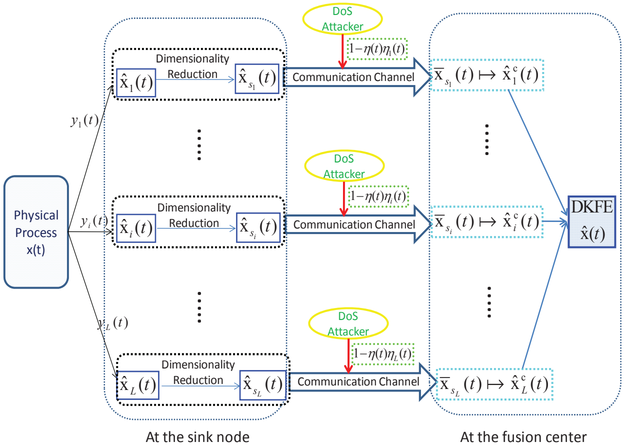


Fig. 2. Block diagram of modeling process.

Let $\bar{\mathrm{x}}_{s_i}(t)$ denote the local estimation signal received by the FC. Then, under DoS attacks, each $\bar{\mathrm{x}}_{s_i}(t)$ is modeled by:

$$\bar{\mathrm{x}}_{s_i}(t) = [1 - \eta(t)\eta_i(t)]\hat{\mathrm{x}}_{s_i}(t), \tag{9}$$

which means that when $\eta(t) = 0$ or $\eta(t) = 1, \eta_i(t) = 0$, the ith communication channel is not jammed by a DoS attack at time t, then one has $\bar{\mathrm{x}}_{s_i}(t) = \hat{\mathrm{x}}_{s_i}(t)$. If the distributed fusion estimator is directly designed based on the signals $\bar{\mathrm{x}}_{s_i}(t)(i = 1, 2, \cdots, L)$, the fusion estimation performance will be degraded seriously. To prevent the rapid performance degradation from attacks, according to (9), the compensating state estimate (CSE) of $x(t)$ in the FC, denoted by $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$, is given by:

$$\begin{aligned} \hat{\mathrm{x}}_i^{\mathrm{c}}(t) &= (1 - \eta(t)\eta_i(t))[H_i(t)\hat{\mathrm{x}}_i(t) \\ &\quad + (I_n - H_i(t))A\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)] + \eta(t)\eta_i(t)A\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1) \end{aligned} \tag{10}$$

where $H_i(t)$ denotes the compression operator, and

$$H_i(t) = \mathrm{diag}\{\gamma_{i1}(t), \gamma_{i2}(t), \cdots, \gamma_{in}(t)\} \tag{11}$$

with $\gamma_{ij}(t) \in \{0, 1\}$. When there is no attack at time t, $\gamma_{ij}(t)$ denotes that the jth component of $\hat{\mathrm{x}}_i(t)$ is sent to the FC or not. Obviously, $H_i(t)$ can determine the selected ASC $\hat{\mathrm{x}}_{s_i}(t)$. Then, the binary variables $\gamma_{ij}(t)(j = 1, \cdots, n)$ must satisfy

$$\sum\nolimits_{j=1}^{n} \gamma_{ij}(t) = r_i \; (i \in \{1, \cdots, L\}), \tag{12}$$

where r_i represents the bandwidth constraint. To clearly show the selection process of $\hat{\mathrm{x}}_{s_i}(t)$, we give the following example:

Let $\hat{x}_i(t) \triangleq \begin{bmatrix} 1.5 \\ 2.7 \\ 3.6 \end{bmatrix}$. Due to bandwidth constraints, only two components of $\hat{x}_i(t)$ are allowed to be transmitted to the FC, i.e., $r_i = 2$. Then, the corresponding compression matrix is $H_i(t) = \mathrm{diag}\{\gamma_{i1}(t), \gamma_{i2}(t), \gamma_{i3}(t)\}$, where $\gamma_{ij}(t) \in \{0, 1\}(j = 1, 2, 3)$ and $\gamma_{i1}(t) + \gamma_{i2}(t) + \gamma_{i3}(t) = 2$. Notice that $\gamma_{ij}(t) = 1$ represents the jth component of $\hat{x}_i(t)$ is sent to the FC; otherwise, this component is not allowed to be sent. From the above analysis, $H_i(t)$ has the following three cases:

$$\begin{cases} \text{Case 1}: & H_i(t) = \mathrm{diag}\{1, 1, 0\} \\ \text{Case 2}: & H_i(t) = \mathrm{diag}\{1, 0, 1\} \\ \text{Case 3}: & H_i(t) = \mathrm{diag}\{0, 1, 1\} \end{cases}$$

This result is in line with (7) (i.e., $\Delta_i = 3$). Under this case, when choosing different $H_i(t)$, the corresponding ASC $\hat{\mathrm{x}}_{s_i}(t)$

is taken as follows:

$$\begin{cases} H_i(t) = \mathrm{diag}\{1,1,0\} \Rightarrow \hat{\mathrm{x}}_{s_i}(t) = \begin{bmatrix} 1.5 \\ 2.7 \end{bmatrix} \\ H_i(t) = \mathrm{diag}\{1,0,1\} \Rightarrow \hat{\mathrm{x}}_{s_i}(t) = \begin{bmatrix} 1.5 \\ 3.6 \end{bmatrix} \\ H_i(t) = \mathrm{diag}\{0,1,1\} \Rightarrow \hat{\mathrm{x}}_{s_i}(t) = \begin{bmatrix} 2.7 \\ 3.6 \end{bmatrix} \end{cases}$$

Up to now, the problem of the dimensionality reduction and DoS attacks has been presented, and the process diagram is shown in Fig.2. Particularly, the proposed CSE model (10) can describe the following two cases:

- For $\eta(t)\eta_i(t) = 0$, the CSE model reduces to $\hat{\mathrm{x}}_i^{\mathrm{c}}(t) = H_i(t)\hat{\mathrm{x}}_i(t) + (I_n - H_i(t))A\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$, which means that though the selected $\hat{\mathrm{x}}_{s_i}(t)$ is successfully transmitted to the FC, the un-transmitted components of $\hat{\mathrm{x}}_i(t)$ are compensated based on $\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$.
- For $\eta(t)\eta_i(t) = 1$, the CSE model reduces to $\hat{\mathrm{x}}_i^{\mathrm{c}}(t) = A\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$, which means that when the ith communication channel is jammed by a DoS attack at time t, the CSE is given by one-step prediction from $\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$.

It is noted that $\eta(t)$ and $\eta_i(t)$ in (10) are determined by the attacker, while $H_i(t)$ in (10) is determined by the defender that includes the function of sink nodes and the FC.

B. Problem of Interest

Based on the CSEs $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$ $(i = 1, 2, \cdots, L)$ (10), the DKFE for the addressed CPSs under DoS attacks is given by:

$$\hat{\mathrm{x}}(t) = \sum\nolimits_{i=1}^{L} \mathrm{W}_i(t)\hat{\mathrm{x}}_i^{\mathrm{c}}(t), \tag{13}$$

where $\sum_{i=1}^{L} \mathrm{W}_i(t) = I_n$. Since the design of $\mathrm{W}_i(t)$ is dependent on the selection of compression operator $H_i(t)$ and attack decision variable $\eta_i(t)$, the key issue for the defender is how to design $H_i(t)$ satisfying (12), while it is a key issue for the attacker to design $\eta_i(t)$ satisfying (8). These are trade-off parameters between the attacker and defender in the proposed model. According to the CSE (10), the estimation precision of $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)$ is dependent on that of $\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$. Under this case, when there are feedback channels from the FC to sink nodes in Fig.1, the order information on the optimal $\hat{\mathrm{x}}_{s_i}(t)$ can be determined at the FC side and fed back to the corresponding sink node. On the other hand, when the attacker decides how to determine κ $(1 \le \kappa < L)$ communication channels to jam, it is difficult for the attacker to know the system completely, but the attacker could eavesdrop on the system information with certain errors. Under this case, when the adversary launches a DoS attack at time t, for the attacker, the eavesdropped information can be expressed as:

$$\begin{cases} z_x(t) = B_x(t)x(t-1) + \varsigma(t-1) \\ z_c^i(t) = B_c^i(t)\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1) + \varepsilon_i(t-1) \end{cases}, \tag{14}$$

where $z_x(t)$ and $z_c^i(t)$, respectively, represent the eavesdropped information from system dynamics and the CSE, while $B_x(t)$ and $B_c^i(t)$ are the observation matrices. $\varsigma(t)$ and $\varepsilon_i(t)$ are zero-mean Gaussian white noises, and they may result from active disturbances of the defender or external disturbances.

Consequently, the problems to be solved in this paper are described as follows:

P.I) Assume that $\eta_i(t)$ and $H_i(t)$ $(i = 1, 2, \cdots, L)$ are known in priori, and then the aim is to design the optimal weighting matrices $\mathrm{W}_1(t), \cdots, \mathrm{W}_L(t)$ such that the MSE of DKFE $\hat{\mathrm{x}}(t)$ is minimal at each time step, i.e.,

$$\hat{\mathrm{x}}(t) = \arg\min_{\hat{\mathrm{x}}_*(t)} \mathrm{E}\{[x(t) - \hat{\mathrm{x}}_*(t)]^{\mathrm{T}}[x(t) - \hat{\mathrm{x}}_*(t)]\}, \tag{15}$$

where $\hat{\mathrm{x}}_*(t)$ denotes an arbitrary group of convex linear combination with respective to the CSEs $\hat{\mathrm{x}}_i^{\mathrm{c}}(t)(i = 1, 2, \cdots, L)$.

P.II) Utilizing the eavesdropped information (14) and the desired fusion estimation algorithm (15), design an online scheduling strategy for determining $H_i(t)(i = 1, 2, \cdots, L)$ and an attack strategy for determining $\eta_i(t)(i = 1, 2, \cdots, L)$ by solving the following optimization problem:

$$\begin{cases} \min\limits_{\{H_1(t),\cdots,H_L(t)\}} \max\limits_{\{\eta_1(t),\cdots,\eta_L(t)\}} \mathrm{E}\{\tilde{\mathrm{x}}^{\mathrm{T}}(t)\tilde{\mathrm{x}}(t)\} \\ \text{s.t.}: \ (8) \text{ and } (12) \end{cases}, \tag{16}$$

P.III) Find a stability condition, which is dependent on the attack schedule and dimensionality reduction strategy, such that the MSE of DKFE $\hat{\mathrm{x}}(t)$ is bounded, i.e.,

$$\lim_{t\to\infty} \mathrm{E}\{\tilde{\mathrm{x}}^{\mathrm{T}}(t)\tilde{\mathrm{x}}(t)\} = \lim_{t\to\infty} \mathrm{Tr}(P(t)) < p, \tag{17}$$

where p is a positive scalar.

III. Main Results

In this section, the recursive fusion estimator will be first designed in Subsection A, and then Subsection B will design the defender's dimensionality reduction strategy and the attacker's attack strategy. Finally, the stability of the designed fusion estimator will be discussed under the effects of dimensionality reduction and DoS attacks.

A. DKFE Design

According to the fusion criterion in [12], the optimal weighting matrices $\mathrm{W}_1(t), \cdots, \mathrm{W}_L(t)$ are calculated by:

$$[\mathrm{W}_1(t), \cdots, \mathrm{W}_L(t)] = (I^{\mathrm{T}}\Sigma^{-1}(t)I)^{-1}I^{\mathrm{T}}\Sigma^{-1}(t), \tag{18}$$

where $I = [I_n^{\mathrm{T}}, \cdots, I_n^{\mathrm{T}}]^{\mathrm{T}} \in \mathrm{R}^{nL\times n}$, and

$$\begin{aligned} \Sigma(t) = \mathrm{E}\{[(\tilde{\mathrm{x}}_1^{\mathrm{c}}(t))^{\mathrm{T}} \cdots (\tilde{\mathrm{x}}_L^{\mathrm{c}}(t))^{\mathrm{T}}]^{\mathrm{T}} \\ \times[(\tilde{\mathrm{x}}_1^{\mathrm{c}}(t))^{\mathrm{T}} \cdots (\tilde{\mathrm{x}}_L^{\mathrm{c}}(t))^{\mathrm{T}}]\} \end{aligned}. \tag{19}$$

Then, the estimation error covariance matrix $P(t)$ is given by:

$$P(t) = (I^{\mathrm{T}}\Sigma^{-1}(t)I)^{-1}. \tag{20}$$

Therefore, it can be concluded from (13) and (18) that if the computation procedures of $\Sigma(t)$ is obtained, then the design of the DKFE will be completed. Before deriving the main result, we introduce the following Lemma.

Lemma 1: [22] For stochastic matrices U, Q, G, where

$$U \triangleq \mathrm{diag}\{u_1, \cdots, u_n\},\ Q \triangleq \mathrm{diag}\{q_1, \cdots, q_n\}$$

$$G \triangleq \begin{bmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{nn} \end{bmatrix}$$

If each random variable g_{ij} in G is independent of any random variables of u_k and $q_k(k = 1, 2, \cdots, n)$, then

$$\mathrm{E}\{UGQ\} = \mathrm{E}\{U \odot Q\} \otimes \mathrm{E}\{G\}$$

where "$\otimes$" is defined as $[G^1 \otimes G^2]_{ij} = G^1_{ij}G^2_{ij}$, and the product "$\odot$" for the matrices U and B is defined by

$$U \odot Q = \begin{bmatrix} u_1 q_1 & \cdots & u_1 q_n \\ \vdots & \ddots & \vdots \\ u_n q_1 & \cdots & u_n q_n \end{bmatrix}$$

Based on Lemma 1, the recursive form of $\Sigma(t)$ is given in Theorem 1.

Theorem 1: Define

$$\begin{cases} \Lambda_{ij}(t) \triangleq H_i(t) \odot H_j(t) \\ \mathrm{M}_{ij}(t) \triangleq [I_n - H_i(t)] \odot [I_n - H_j(t)] \\ \mathrm{V}_{ij}(t) \triangleq H_i(t) \odot [I_n - H_j(t)] \end{cases}, \tag{21}$$

where the operators "$\odot$" and "$\otimes$" are defined in Lemma 1. Then, the estimation error covariance matrix $\Sigma_{ij}(t)$ is calculated by:

$$\begin{cases} \Sigma_{ij}(t) = (1-\eta(t)\eta_i(t))(1-\eta(t)\eta_j(t))\Sigma^{11}_{ij}(t) \\ \quad +[1-\eta(t)\eta_i(t)]\eta(t)\eta_j(t)\Sigma^{12}_{ij}(t) \\ \quad +[1-\eta(t)\eta_j(t)]\eta(t)\eta_i(t)\Sigma^{21}_{ij}(t) \\ \quad +\eta(t)\eta_i(t)\eta_j(t)\Sigma^{22}_{ij}(t) \\ \Sigma^{11}_{ij}(t) = \Lambda_{ij}(t) \otimes P_{ij}(t) + \mathrm{M}_{ij}(t) \otimes \Sigma^{22}_{ij}(t) \\ \quad +\mathrm{V}_{ij}(t) \otimes [\Phi_{\mathrm{K}_i}(t)\Omega_{ij}(t-1)A^{\mathrm{T}} + \mathrm{G}_{\mathrm{K}_i}(t)Q_w] \\ \quad +\mathrm{V}^{\mathrm{T}}_{ji}(t) \otimes [A\Omega^{\mathrm{T}}_{ji}(t-1)\Phi^{\mathrm{T}}_{\mathrm{K}_j}(t) + Q_w\mathrm{G}^{\mathrm{T}}_{\mathrm{K}_j}(t)] \\ \Sigma^{12}_{ij}(t) = (I_n - H_i(t))\Sigma^{22}_{ij}(t) \\ \quad +H_i(t)[\Phi_{\mathrm{K}_i}(t)\Omega_{ij}(t-1)A^{\mathrm{T}} + \mathrm{G}_{\mathrm{K}_i}(t)Q_w] \\ \Sigma^{21}_{ij}(t) = \Sigma^{22}_{ij}(t)(I_n - H_j(t)) \\ \quad +[A\Omega^{\mathrm{T}}_{ji}(t-1)\Phi^{\mathrm{T}}_{\mathrm{K}_j}(t) + Q_w\mathrm{G}^{\mathrm{T}}_{\mathrm{K}_j}(t)]H_j(t) \\ \Sigma^{22}_{ij}(t) = A\Sigma_{ij}(t-1)A^{\mathrm{T}} + Q_w \end{cases}, \tag{22}$$

where the statistical correlation between the estimations $\tilde{\mathrm{x}}_i(t)$ and $\tilde{\mathrm{x}}^c_j(t)$, denoted as $\Omega_{ij}(t) \triangleq \mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}^{\mathrm{c}}_j(t)]^{\mathrm{T}}\}$, is computed by:

$$\begin{aligned} &\Omega_{ij}(t) = (1-\eta_j(t)\eta(t))P_{ij}(t)H_j(t) + \mathrm{G}_{\mathrm{K}_i}(t)Q_w \\ &+\Phi_{\mathrm{K}_i}(t)\Omega_{ij}(t-1)A^{\mathrm{T}} - (1-\eta_j(t))\eta(t)\Phi_{\mathrm{K}_i}(t) \\ &\times\Omega_{ij}(t-1)A^{\mathrm{T}}H_j(t) - (1-\eta_j(t))\eta(t)\mathrm{G}_{\mathrm{K}_i}(t)Q_wH_j(t) \end{aligned} \tag{23}$$

where $\mathrm{G}_{\mathrm{K}_i}(t)$ and $\Phi_{\mathrm{K}_i}(t)$ are determined by (4), while $P_{ij}(t)$ is calculated by (5–6). Moreover, the relationship between DKFE (10) and each local CSE (13) is given by:

$$\mathrm{Tr}\{P(t)\} \leq \mathrm{Tr}\{\Sigma_{ii}(t)\}. \tag{24}$$

Proof: See A.1 in Appendix. ■

From Theorem 1, when $\Sigma(t)$ is computed by (22), the optimal weighting matrices $\mathrm{W}_1(t), \cdots, \mathrm{W}_L(t)$ in (15) is calculated by (18).

Remark 1. At time t, an attack schedule is determined by the attacker, and the selected ASC $\bar{\mathrm{x}}_{s_i}(t)$ is determined by the sink node. However, the FC can know the variables $\eta(t)$, $\eta_i(t)$ and $H_i(t)$ according to the signal $\bar{\mathrm{x}}_{s_i}(t)$ (9). Moreover, it is concluded from (22) that the computation procedure for the $\Sigma_{ij}(t)$ is independent of the sensor measurements, and thus $\Sigma_{ij}(t)$ can be separately computed in the FC. Notice that this subsection does not concern the determining process of $\eta(t)$, $\eta_i(t)$ and $H_i(t)$. Since the binary variable $\eta(t)$ obeying the Bernoulli distribution is randomly generated from the attacker, how to design the attacker's decision variable $\eta_i(t)$ and the defender's compression matrix $H_i(t)$ to achieve the opposite goals will be solved in Subsection B.

B. Design of Dimensionality Reduction Strategy and Attack Strategy

First, we consider the following two facts:

- **(F1)**: For each sink node, it is unable to know whether the signal $\hat{\mathrm{x}}_{s_i}(t)$ is dropped by attacks or not at time t, and thus the optimal dimensionality reduction strategy at time t is only designed based on the the CSEs $\hat{\mathrm{x}}^{\mathrm{c}}_i(t-1)(i = 1, 2, \cdots, L)$.
- **(F2)**: For the attacker, it is unable to know $\hat{\mathrm{x}}_{s_i}(t)$ at time t, and thus the optimal attack strategy at time t is only designed based on the CSEs $\hat{\mathrm{x}}^{\mathrm{c}}_i(t-1)(i = 1, 2, \cdots, L)$.

Therefore, the design of dimensionality reduction strategy is independent of attack strategy at time t, which means that the optimization problem (16) is equivalent to two problems:

$$\min_{\{H_1(t),\cdots,H_L(t),\forall\eta_i(t)\}} \mathrm{Tr}\{P(t)\} \ \text{ s.t. : (12)} \tag{25}$$

$$\max_{\{\eta_1(t),\cdots,\eta_L(t),\forall H_i(t)\}} \mathrm{Tr}\{P(t)\} \ \text{ s.t. : (8)} \tag{26}$$

Notice that the optimal solutions to (25–26) are difficult to be obtained because: i) The objection function $\mathrm{Tr}\{P(t)\}$ is nonlinear with respective to $H_1(t), \cdots, H_L(t)$ and $\eta_1(t), \cdots, \eta_L(t)$; ii) For the attacker, the covariance matrix $P(t)$ is unknown, and each decision variable $\eta_i(t)$ in (26) is only designed by the eavesdropped information (14). In this case, under certain relaxation conditions, suboptimal solutions to (25–26) will be given in Theorem 2.

Theorem 2: From the persecutive of the attacker, let $\hat{\mathrm{x}}_{\mathrm{A}}(t)$ and $\hat{\mathrm{x}}^i_{\mathrm{AC}}(t)$ denote state estimates of $x(t)$ and $\hat{\mathrm{x}}^{\mathrm{c}}_i(t)$ based on the eavesdropped information. Then, one has

$$\begin{cases} \hat{\mathrm{x}}_{\mathrm{A}}(t-1) = (B^{\mathrm{T}}_x(t)B_x(t))^{-1}B^{\mathrm{T}}_x(t)z_x(t) \\ \hat{\mathrm{x}}^i_{\mathrm{AC}}(t-1) = ((B^i_c(t))^{\mathrm{T}}B^i_c(t))^{-1}(B^i_c(t))^{\mathrm{T}}z^i_c(t) \end{cases}, \tag{27}$$

where $z_x(t)$ and $z^i_c(t)$ are given by (14). Define

$$\begin{cases} \tilde{\Sigma}_{ii}(t-1) = [\hat{\mathrm{x}}_{\mathrm{A}}(t-1) - \hat{\mathrm{x}}^i_{\mathrm{AC}}(t-1)] \\ \qquad\qquad \times[\hat{\mathrm{x}}_{\mathrm{A}}(t-1) - \hat{\mathrm{x}}^i_{\mathrm{AC}}(t-1)]^{\mathrm{T}} \\ \mathrm{c}^i_j(t) = P_{ii}(t)(j,j) - \Sigma^{22}_{ii}(t)(j,j) \\ \mathrm{d}_i(t) = \mathrm{Tr}\{A\tilde{\Sigma}_{ii}(t-1)A^{\mathrm{T}}\} \\ \Theta^s_i(t) = \{\mathrm{c}^i_1(t), \cdots, \mathrm{c}^i_n(t)\} \\ \Theta^a(t) = \{\mathrm{d}_1(t), \cdots, \mathrm{d}_L(t)\} \end{cases}, \tag{28}$$

where $\Sigma^{22}_{ii}(t)$ is computed by (22). Then, the elements of the set $\Theta^s_i(t)$ are listed from the minimum to maximum as follows:

$$\mathrm{c}^i_{\chi_1}(t) \leq \cdots \leq \mathrm{c}^i_{\chi_{r_i}}(t) \leq \mathrm{c}^i_{\chi_{(r_i+1)}}(t) \leq \cdots \leq \mathrm{c}^i_{\chi_n}(t), \tag{29}$$

while the elements of the set $\Theta^a(t)$ are listed from the maximum to minimum as follows:

$$\mathrm{d}_{\mu_1}(t) \geq \cdots \geq \mathrm{d}_{\mu_\kappa}(t) \geq \mathrm{d}_{\mu_{(\kappa+1)}}(t) \geq \cdots \geq \mathrm{d}_{\mu_L}(t). \tag{30}$$

Under this case, for the defender, a suboptimal solution to the problem (25) is given by:

$$\begin{cases} \gamma_{i\chi_1}(t) = \gamma_{i\chi_2}(t) = \cdots = \gamma_{i\chi_{r_i}}(t) = 1 \\ \gamma_{i\chi_{(r_i+1)}}(t) = \gamma_{i\chi_{(r_i+2)}}(t) = \cdots = \gamma_{i\chi_n}(t) = 0 \end{cases}, \tag{31}$$

where $i = 1, 2, \cdots, L$. For the attacker, a group of suboptimal decision variables in (26) are given by:

$$\begin{cases} \eta_{\mu_1}(t) = \cdots = \eta_{\mu_\kappa}(t) = 1 \\ \eta_{\mu_{(\kappa+1)}}(t) = \cdots = \eta_{\mu_L}(t) = 0 \end{cases}. \tag{32}$$

Proof: See A.2 in Appendix. ■

From Theorem 2, it can be concluded that: **i)** The χ_{ℓ_i}th ($\ell_i \in \{1, 2, \cdots, r_i\}$) component of $\hat{\mathrm{x}}_i(\mathrm{t})$ is allowed to be transmitted to the FC at time t, where χ_{ℓ_i} represents the subscript of $\mathrm{c}^i_{\chi_{\ell_i}}(t)$ in (29); **ii)** When the attacker launches a DoS attack at time t, the μ_ith ($i \in \{1, 2, \cdots, \kappa\}$) communication channel is jammed by the attacker at time t, where μ_i represents the subscript of $\mathrm{d}_{\mu_i}(t)$ in (30). On the other hand, it follows from (5) that $P_{ii}(t)$ can be separately calculated at the FC, and then the solution (31) can be obtained at the FC. Therefore, to determine $\hat{\mathrm{x}}_{s_i}(t)$, the order information of selected components for each local estimate is flagged in the FC, and then transmitted to the sink node through feedback channel. At the same time, it is known from (27) that the decision variables (32) are determined by the eavesdropped information (14), i.e., the attacker can execute an effective attack strategy based on the eavesdropped information.

According to Theorems 1–2, the computation procedures for the DKFE $\hat{\mathrm{x}}(t)$ can be summarized by Algorithm 1.

Algorithm 1 DKFE under dimensionality reduction and DoS attacks

```
1: Calculate each local estimate $\hat{x}_i(t)$ $(i \in \{1, \cdots, L\})$ and covariance matrix $P_{ij}(t)$ $(i \in \{i, \cdots, L\})$ by (4–6);
2: Dimensionality Reduction Strategy at time $t$:
3: for $i := 1$ to $L$ do
4:     Calculate $P_{ii}(t)$ and $\Sigma^{22}_{ii}(t)$ in the FC by (5) and (22);
5:     Sort the elements of the $\Theta^s_i(t)$ in the FC by (29);
6:     Determine $\eta_{ij}(t)$ in the FC by (31);
7:     The order information of selected components is transmitted to the sink node through feedback channel;
8:     Determine the selected ASC $\hat{x}_{s_i}(t)$ at the sink node.
9: end for
10: Attack Strategy at time $t$:
11: if $\eta(t) = 0$ then
12:     Go to Step 19;
13: end if
14: if $\eta(t) = 1$ then
15:     Calculate $\hat{x}_A(t-1)$ and $\hat{x}^i_{AC}(t-1)$ by the attacker using (27);
16:     Sort the elements of the $\Theta^a_i(t)$ by the attacker using (30);
17:     Determine $\eta_1(t), \cdots, \eta_L(t)$ by the attacker using (32);
18: end if
19: Calculate each CSE $\hat{x}^c_i(t)$ $(i \in \{1, \cdots, L\})$ by (10);
20: Calculate each covariance matrix $\Sigma_{ij}(t)$ by (22);
21: Calculate each weighting matrix $W_i(t)$ by (18);
22: Calculate the DKFE $\hat{x}(t)$ by (13).
```

Remark 2. For the defender, since the covariance matrix $\Sigma_{ii}(t-1)$ is calculated by a recursive form, the attack information $\eta(t_1)$ and $\eta_i(t_1)$ ($t_1 < t$) has been used to design each decision variable $\gamma_{ij}(t)$ at the FC. This means that the design of $H_i(t)$ resorting to the feedback channel utilizes more available information, and thus can reduce the influence of the attack to the maximum extent. In contrast, for the attacker, only when the adversary plans to launch an attack at time t, the attacker will eavesdrop on $z_x(t)$ and $z^i_c(t)$ to design $\tilde{\Sigma}_{ii}(t-1)$. According to Theorem 2, each attack decision variable $\eta_i(t)$ is dependent on the accuracy of $\tilde{\Sigma}_{ii}(t-1)$, which implies that the accurate defender's information is very important for the attacker to design an efficient attack schedule.

C. Stability Analysis

The problem **(P.III)** will be discussed in this subsection. When considering the fusion estimation performance of the DKFE, the statistical information of $\eta(t)$ is taken into account. Define $\Omega^\eta_{ii}(t) \triangleq \mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}^{\mathrm{c}}_i(t)]^{\mathrm{T}}|\eta(t)\}$ and $\Sigma^\eta_{ii}(t) \triangleq \mathrm{E}\{\tilde{\mathrm{x}}^{\mathrm{c}}_i(t)[\tilde{\mathrm{x}}^{\mathrm{c}}_i(t)]^{\mathrm{T}}|\eta(t)\}$. Then, it is derived from (22) that

$$\begin{aligned}\Omega^\eta_{ii}(t) = {} & (1-\eta\eta_i(t))[P_{ii}(t) - \mathrm{G}_{\mathrm{K}_i}(t)Q_w]H_i(t) \\ & +\mathrm{G}_{\mathrm{K}_i}(t)Q_w + \Phi_{\mathrm{K}_i}(t)\Omega^\eta_{ii}(t-1)A^{\mathrm{T}} \\ & \times[I_n - H_i(t) + \eta\eta_i(t)H_i(t)]\end{aligned} \tag{33}$$

$$\begin{aligned}\Sigma^\eta_{ii}(t) = {} & \mathrm{J}_{H_i}(t)\mathrm{diag}\{\Sigma^\eta_{ii}(t-1), \Sigma^\eta_{ii}(t-1)\}\mathrm{J}^{\mathrm{T}}_{H_i}(t) \\ & +(1-\eta\eta_i(t))\mathrm{V}_{ii}(t) \otimes [\Phi_{\mathrm{K}_i}(t)\Omega^\eta_{ii}(t-1)A^{\mathrm{T}} \\ & +\mathrm{G}_{\mathrm{K}_i}(t)Q_w] + (1-\eta\eta_i(t))\mathrm{V}^{\mathrm{T}}_{ii}(t) \\ & \otimes[A(\Omega^\eta_{ii}(t-1))^{\mathrm{T}}\Phi^{\mathrm{T}}_{\mathrm{K}_i}(t) + Q_w\mathrm{G}^{\mathrm{T}}_{\mathrm{K}_i}(t)]\end{aligned}, \tag{34}$$

where η is the rate of attack that has been defined in Section II, and

$$\mathrm{J}_{H_i}(t) \triangleq [\sqrt{1-\eta\eta_i(t)}(I_n - H_i(t))A \quad \sqrt{\eta\eta_i(t)}A]. \tag{35}$$

According to (33) and (34), the estimation performance of each CSE is dependent on the rate of attack η, decision variable $\eta_i(t)$ and compression matrix $H_i(t)$. Meanwhile, as mentioned in Section II, the ASC of $\hat{\mathrm{x}}_i(t)$ has Δ_i possible case, and thus $H_i(t)$ given by (11) only takes one value at arbitrary time from the following set:

$$S_{H_i} \triangleq \{H^i_1, \cdots, H^i_{s_i}, \cdots, H^i_{\Delta_i}\} \tag{36}$$

i.e., $H_i(t) \in S_{H_i}$, where Δ_i is determined by (7), and each $H^i_{s_i}(s_i \in \{1, 2, \cdots, \Delta_i\})$ denotes a diagonal matrix that contains r_i diagonal elements "1" and $n - r_i$ diagonal elements "0". Based on the above analysis, a stability condition for the DKFE will be given in Theorem 3.

Theorem 3: For a given rate of attack $\eta > 0$, if there exist a set S_{H_i} and a measurement matrix C_i such that

$$\begin{cases}\mathrm{rank}\{[\sqrt{Q_w}, A\sqrt{Q_w}, \cdots, A^{n-1}\sqrt{Q_w}]\} = n \\ \mathrm{rank}\{\mathrm{col}\{C_i, C_iA, \cdots, C_iA^{n-1}\}\} = n\end{cases} \tag{37}$$

$$\begin{aligned}(\mathrm{g}_{\eta_i} \triangleq {} & \max\{||\Phi_{\mathrm{K}_i}||_2||A^{\mathrm{T}}[I_n - H^i_{s_i} + \eta z_i H^i_{s_i}]||_2 \\ & |s_i = 1, 2, \cdots, \Delta_i; z_i = 0, 1\}) < 1\end{aligned} \tag{38}$$

$$\begin{aligned}(\mathrm{g}_{H_i} \triangleq {} & \max\{||[\sqrt{1-\eta z_i}(I_n - H^i_{s_i})A \quad \sqrt{\eta z_i}A]||_2 \\ & |s_i = 1, 2, \cdots, \Delta_i; z_i = 0, 1\}) < 1\end{aligned}, \tag{39}$$

where $H^i_{s_i}$ is determined by (36), and $\Phi_{\mathrm{K}_i} = \lim_{t\to\infty} \Phi_{\mathrm{K}_i}(t)$. Then, the MSE of the DKFE $\hat{\mathrm{x}}(t)$ will be bounded, i.e., there must exist a positive scalar $p > 0$ such that

$$\lim_{t\to\infty} \mathrm{Tr}\{P(t)\} \leq p \tag{40}$$

Proof: See A.3 in Appendix. ■

Remark 3. Since the stability condition in Theorem 3 is dependent on the adversary's rate of attack η and the defender's dimensionality reduction parameter $H^i_{s_i}$, the maximum rate of attack $\hat{\eta}$ can be obtained from this condition when the parameter r_i of dimensionality reduction is known a priori.

This can help to set the threshold of the rate of attack for the defender, i.e., once the defender finds $\eta > \hat{\eta}$, it will immediately adopt effective defense strategy to decrease the rate of attack to satisfy the stability condition in Theorem 3. On the other hand, the DKFE will be stable only if there exists a set S_{H_i} satisfying (38–39) (i.e., there exists a stable CSE). However, for the attacker, to completely destroy the stability of the DKFE, each CSE is required to become unstable at the same time under attacks. Thus, the adversary may pay a high price to completely destroy the DKFE. In this sense, the DKFE can effectively enhance reliability and robustness against attacks.

Remark 4. It should be pointed out that there are many other attacks that can affect the system in different ways, and how to design the dimensionality reduction strategy under other types of attacks is an interesting problem. Since different attack models have their own characteristic and the dimensionality reduction strategy is dependent on the characteristics of attacks, the proposed fusion estimation method against DoS attacks in this paper cannot be applicable to other types of attacks. At the moment, it is difficult to find a general fusion estimation algorithm based on a unified attack model. Our contribution in this paper takes a step further to handel DoS model. More research effort is needed to solve this problem.

IV. Simulation Examples

In this section, two illustrative examples will be given to show the effectiveness of the proposed methods.

A. Example 1

Consider the CPSs (1–2) with the following system parameters:

$$\begin{cases} A = \begin{bmatrix} 0.9 & 0.26 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0.2 & 0.3 & 0.2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.2 & 0.2 & 0.1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.3 & 0.9 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.8 & 0.3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.1 & 0.5 & 0.2 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0.3 & 0.3 & 0.6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.1 & 0.8 \end{bmatrix} \\ C_1 = \begin{bmatrix} 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&1&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}, C_2 = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&1 \end{bmatrix} \end{cases} \tag{41}$$

where the covariances of $w(t)$, $v_1(t)$ and $v_2(t)$ are taken as $Q_w = \text{diag}\{1.0, 0.8, 0.8, 0.7, 1.2, 0.9, 0.7, 1.0\}$, $Q_{v_1} = \text{diag}\{0.9, 0.5, 0.7, 1.0, 0.8, 0.5\}$ and $Q_{v_2} = \text{diag}\{0.5, 0.9, 0.3, 0.9, 1.2, 0.9\}$, respectively. It is known from (41) that the first and the eighth components of "x(t)" cannot be obtained by the first sink node, while the first, the fourth and the fifth components of "x(t)" cannot be obtained by the second sink node. Moreover, from (41), one has

$$\begin{cases} \text{rank}\{[\sqrt{Q_w}, A\sqrt{Q_w}, A^2\sqrt{Q_w}, A^3\sqrt{Q_w}, A^4\sqrt{Q_w}, \\ \quad A^5\sqrt{Q_w}, A^6\sqrt{Q_w}, A^7\sqrt{Q_w}]\} = 8 \\ \text{rank}\{\text{col}\{C_i, C_iA, C_iA^2, C_iA^3, C_iA^4, C_iA^5, \\ \quad C_iA^6, C_iA^7\}\} = 8 \ (i = 1, 2) \end{cases},$$

i.e., the condition (37) holds. Thus, one has $||\Phi_{\mathrm{K}_1}||_2 = 0.8341 < 1$ and $||\Phi_{\mathrm{K}_2}||_2 = 0.9103 < 1$.

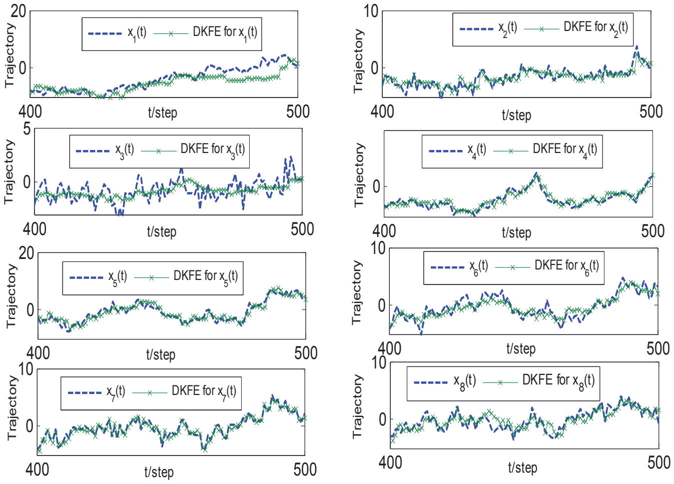


Fig. 3. Trajectories of the state x(t) and the DKFE $\hat{\mathrm{x}}(t)$.

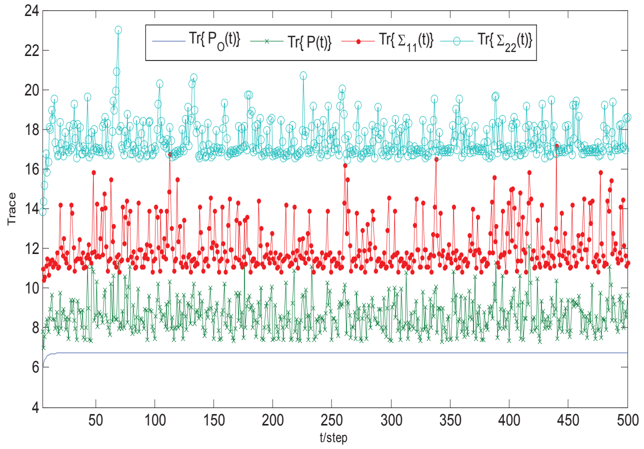


Fig. 4. Comparison of estimation performance for the ODKFE, DKFE and CSEs.

According to the dimensionality reduction strategy, it is considered in this example that only *four components* of $\hat{\mathrm{x}}_i(t)$ are allowed to be transmitted to the FC at each time step, i.e., $r_1 = r_2 = 4$, and then $\hat{\mathrm{x}}_{s_i}(t)$ can be determined by (31). Moreover, from (7) and (36), one has $\Delta_1 = \Delta_2 = 70$. On the other hand, when each sink node sends the selected ASC $\hat{\mathrm{x}}_{s_i}(t)$ to the FC, the attacker may launch a DoS attack to degrade the fusion estimation performance. Due to the energy constraints the attacker can only intermittently execute DoS attacks. In fact, only one communication channel can be jammed in this example under a DoS attack launched at a particular time, and the optimal decision variables $\eta_i(t)$ $(i = 1, 2)$ can

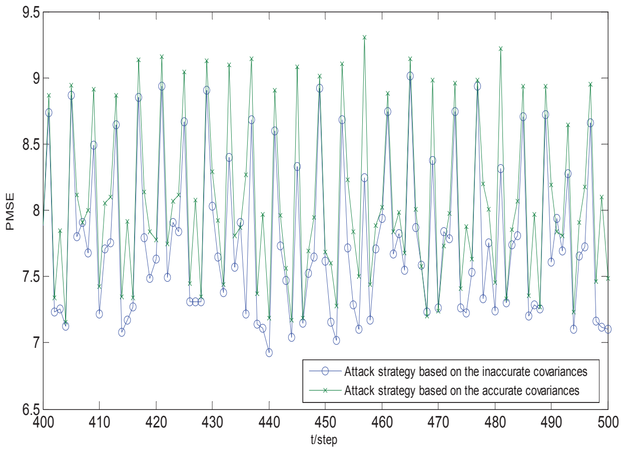


Fig. 5. Comparison of estimation performance under different attack strategies with accurate and inaccurate covariances.

be determined by (32). Then, the rate of attack η for the attacker is assumed to be $\eta = 0.3$, and it is calculated that $\mathrm{g}_{\eta_1} < 1, \mathrm{g}_{H_1} < 1$ and $\mathrm{g}_{\eta_2} < 1, \mathrm{g}_{H_2} < 1$. This means that the conditions (38) and (39) hold, and thus it is concluded from Theorem 3 that the MSE of the DKFE $\hat{\mathrm{x}}(t)$ for this example is bounded.

As pointed out in Section III, it is difficult for the attacker to obtain the accurate covariances $\Sigma_{ii}(t-1)(i=1,2)$, but the attacker can eavesdrop on $x(t)$ and $\hat{\mathrm{x}}_i^c(t)$ modeled by (14), where the observation matrices in (14) are given by:

$$\begin{cases} B_x(t) = B_{c_1}(t) = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,1\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1 \end{bmatrix} \\ B_{c_2}(t) = \begin{bmatrix} 1\,0\,1\,0\,0\,0\,0\,0 \\ 0\,1\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,1\,0\,1 \end{bmatrix} \end{cases} \tag{42}$$

and the disturbances $\varsigma(t)$, $\varepsilon_1(t)$, $\varepsilon_2(t)$ in (14) are Gaussian white noises with covariances $Q_\varsigma = 0.12I_4$, $Q_{\varepsilon_1} = 0.18I_4$ and $Q_{\varepsilon_2} = 0.19I_4$. Then, the least square estimates of $x(t)$ and $\hat{\mathrm{x}}_i^c(t)$ are obtained by (27) at the attacker. In this case, the inaccurate covariance $\tilde{\Sigma}_{ii}(t-1)$ is calculated by (28). By using Algorithm I, the trajectories of the DKFE "$\hat{\mathrm{x}}(t)$" and the state "x(t)" are plotted in Fig.3, which shows that the designed DKFE is able to estimate the state "x(t)" well. Let $P_O(t)$ denote the original DKFE (ODKFE) without dimensionality reduction and DoS attacks. Then, the estimation performance (assessed by the trace of estimation error covariance matrix) of the CSEs, DKFE and ODKFE are shown in Fig.4. It can be seen from this figure that the estimation performance of the DKFE is better than that of each CSE at each time step, which is in line with the result (24). However, the estimation precision of the DKFE is worse than that of ODKFE, which implies that the bandwidth constraints and DoS attacks can affect the fusion estimation performance. Moreover, it is known from this figure that the MSE of the DKFE is bounded, which accords with the result in Theorem 3. When the rate of attack is taken as $\eta = 0.3$, the practical MSEs (PMSEs) of the DKFE under different cases with the accurate covariances $\Sigma_{ii}(t-1)$ $(i=1,2)$ or the inaccurate covariances $\tilde{\Sigma}_{ii}(t-1)$ $(i=1,2)$, which are calculated by Monte Carlo method (ch.1, [11]) with an average of 5000 runs, are plotted in Fig.5. It can be seen from this figure that the attack effect with the accurate covariances $\Sigma_{ii}(t-1)$ $(i=1,2)$ is better than that with the inaccurate covariances $\tilde{\Sigma}_{ii}(t-1)$ $(i=1,2)$. This implies that the accuracy of the eavesdropped information is very important for the attacker to determine the attack strategy.

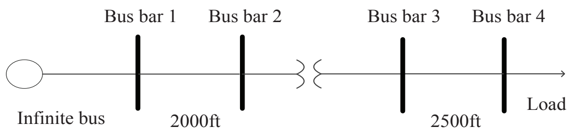


Fig. 6. An illustration of the IEEE 4-bus distribution system [21].

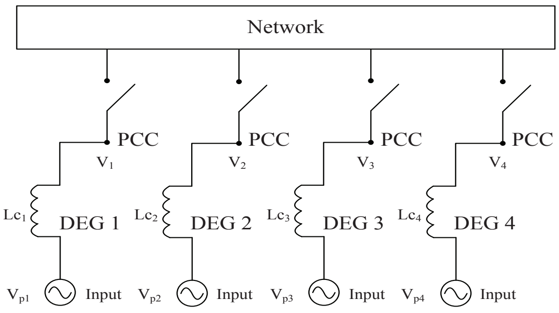


Fig. 7. An illustration of the model of four DEGs connecting to the power network [21].

B. Example 2

Consider the distributed fusion estimation problem for a power grid example with IEEE 4-bus distribution line as shown in Fig.6 (see [21]). We adopt the model of interconnected distributed energy generators (DEGs) from [21] as shown in Fig.7, and four DEGs are modeled as voltage sources whose input voltages are denoted by $\mathrm{v}_p \triangleq (v_{p1}, v_{p2}, v_{p3}, v_{p4})$, where v_{pi} is the ith DEG input voltage. The four DEGs are connected to the main power network at the corresponding Point of Common Coupling (PCC) whose voltages are denoted by $\mathrm{v}_s \triangleq (v_1, v_2, v_3, v_4)$, where v_i is the ith PCC voltages. In order to maintain the proper operation of DEGs, these PCC voltages need to be kept at their reference values. A coupling inductor exists between each DEG and the rest of the electricity network. Next, applying the Laplace transformation, the nodal voltage equation is given by [21]:

$$\mathrm{Y}(s)\mathrm{v}_s(s) = \frac{1}{s}\mathrm{L}_c^{-1}\mathrm{v}_p(s), \tag{44}$$

where $\mathrm{L}_c \triangleq \mathrm{diag}\{\mathrm{L}_{c1}, \mathrm{L}_{c2}, \mathrm{L}_{c3}, \mathrm{L}_{c4}\}$, and the admittance matrix $\mathrm{Y}(s)$ is defined by (43). The Laplace transform in (44) can be converted into the following linear state space dynamical model (see [21]):

$$\dot{\mathrm{x}}(t) = \mathrm{A}_c\mathrm{x}(t) + \mathrm{B}_c\mathrm{u}(t), \tag{45}$$

$$\mathrm{Y}(s)=\begin{bmatrix}\frac{1}{0.1750+0.0005s} & \frac{-1}{0.1750+0.0005s} & 0 & 0\\ \frac{-1}{0.1750+0.0005s} & \frac{1}{0.1750+0.0005s}+\frac{1}{0.1667+0.0004s} & \frac{-1}{0.1667+0.0004s} & 0\\ 0 & \frac{-1}{0.1667+0.0004s} & \frac{1}{0.1667+0.0004s}+\frac{1}{0.2178+0.0006s} & \frac{-1}{0.2178+0.0006s}\\ 0 & 0 & \frac{-1}{0.2178+0.0006s} & \frac{1}{0.2178+0.0006s}+\frac{1}{12.3413+0.0148s}\end{bmatrix} +(\mathrm{L}_c s)^{-1} \tag{43}$$

where $\mathrm{x}(t)\triangleq \mathrm{v}_s-\mathrm{v}_{ref}$ is the PCC state voltage deviation, v_{ref} is the PCC reference voltage, $\mathrm{u}(t)\triangleq \mathrm{v}_p-\mathrm{v}_{pref}$ is the DEG control input deviation, v_{pref} is the reference control effort. Meanwhile, the system matrices A_c, B_c are given by:

$$\begin{aligned}\mathrm{A}_c&=\begin{bmatrix}175.9 & 176.8 & 511 & 103.6\\ -350 & 0 & 0 & 0\\ -544.2 & -474.8 & -408.8 & -828.8\\ -119.7 & -554.6 & -968.8 & -1077.5\end{bmatrix}\\ \mathrm{B}_c&=\begin{bmatrix}0.8 & 334.2 & 525.1 & -1036\\ -350 & 0 & 0 & 0\\ -69.3 & -66.1 & -420.1 & -828.8\\ -434.9 & -414.2 & -108.7 & 1077.5\end{bmatrix}\end{aligned}. \tag{46}$$

Notice that not all eigenvalues of A_c are negative, and thus the system (45) is unstable when there is no feedback control. In this case, we design the controller $\mathrm{u}(t)\triangleq \mathrm{K}_c\mathrm{x}(t)$ such that this system is stable, i.e., all eigenvalues of $\mathrm{A}_s\triangleq \mathrm{A}_c+\mathrm{B}_c\mathrm{K}_c$ are negative. Here, we choose the controller gain K_c as follows:

$$\mathrm{K}_c=\begin{bmatrix}-1.0057 & 0 & 0 & 0\\ 1.2883 & -0.2003 & -1.4687 & -1.4687\\ -1.1696 & -0.2936 & -0.1024 & -1.1021\\ -0.0824 & -0.4081 & -0.3242 & -0.3242\end{bmatrix}.$$

Under this condition, the system (45) can be rewritten as:

$$\dot{\mathrm{x}}(t)=\mathrm{A}_s\mathrm{x}(t). \tag{47}$$

To monitor the work status of this power grid example (i.e., (47)), there are two sink nodes collecting their sensor measurements, and the local estimates computed by the sink node are sent to the FC. However, when the local estimation signals with dimensionality reduction are transmitted to the FC through the bandwidth-constrained communication channels, they will encounter with DoS attacks. Meanwhile, the system noises are not considered when designing the controller for the system (45), however, these noises may be unavoidable due to the imperfect external environment. Therefore, setting the sampling period $T_0=5s$, the discretized form of (47) can be transformed to the same form of (1), where

$$A=\begin{bmatrix}-0.837 & 0.5427 & 0 & 0\\ -0.5427 & -0.837 & 0 & 0\\ 0 & 0 & 0.9851 & 0\\ 0 & 0 & 0 & 0.9556\end{bmatrix}, \tag{48}$$

and the covariance matrix of the system noise $w(t)$ is taken as $Q_w=\mathrm{diag}\{0.1,0.2,0.2,0.1\}$. Then, the measurement matrices C_1 and C_2 in (2) are taken as:

$$C_1=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&1&0&1\\0&0&0&1\end{bmatrix}, C_2=\begin{bmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&1&1&0\end{bmatrix}, \tag{49}$$

and the covariance matrices of the measurement noises are taken as $Q_{v_1}=\mathrm{diag}\{0.5,0.6,0.3,0.2\}$ and $Q_{v_2}=\mathrm{diag}\{0.8,0.3,0.5,0.9\}$. Due to the bandwidth constraints, only two components of $\hat{\mathrm{x}}_i(t)$ are allowed to be transmitted to the FC at each time step, while the attacker can only intermittently execute DoS attacks. Particularly, only one communication channel can be jammed under a DoS attack. When the rate of attack is taken as $\eta=0.3$, it can be easily verified that $\mathrm{rank}\{[\sqrt{Q_w},A\sqrt{Q_w},A^2\sqrt{Q_w},A^3\sqrt{Q_w}]\}=4$, $\mathrm{rank}\{\mathrm{col}\{C_i,C_iA,C_iA^2,C_iA^3\}\}=4$, $\mathrm{g}_{\eta_i}<1$ and $g_{H_i}<1$ $(i=1,2)$, i.e., the conditions (37–39) hold. Then, it is concluded from Theorem 3 that the MSE of the DKFE $\hat{\mathrm{x}}(t)$ for this example is bounded.

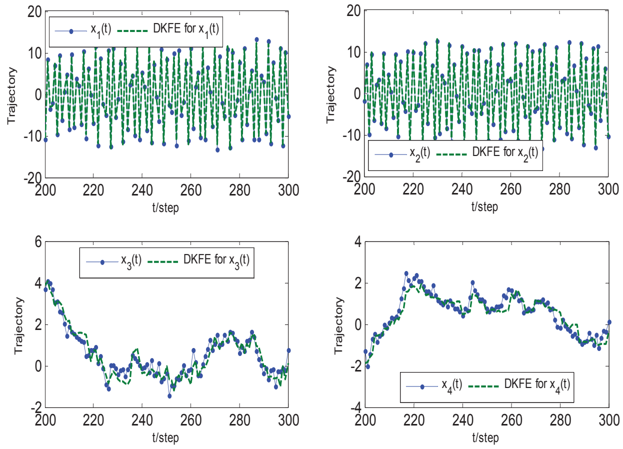


Fig. 8. Trajectories of the state x(t) and the DKFE $\hat{\mathrm{x}}(t)$.

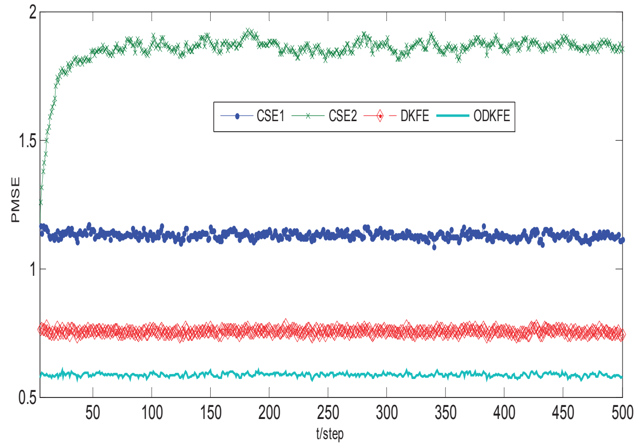


Fig. 9. Comparison of estimation precision for the DKFE, ODKFE and CSEs.

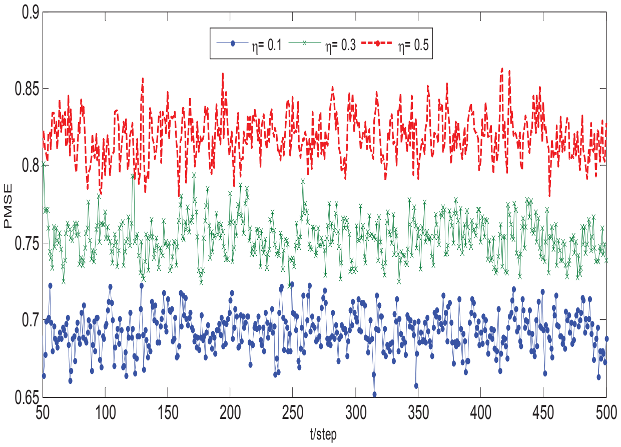


Fig. 10. Comparison of estimation performance under different attack strategies with accurate and inaccurate covariances.

For the adversary, the accurate covariances $\Sigma_{ii}(t-1)(i=1,2)$ cannot be obtained. Thus, similar to Example 1, $\Sigma_{ii}(t-1)$ is replaced by $\tilde{\Sigma}_{ii}(t-1)$ to design the attack strategy, where the observation matrices $B_x(t)$ and $B_{c_i}(t)(i=1,2)$ in (14) are given by

$$B_x(t)=B_{c_1}(t)=\begin{bmatrix}1\,1\,0\,0\\0\,0\,1\,1\end{bmatrix},B_{c_2}(t)=\begin{bmatrix}1\,0\,1\,0\\0\,1\,0\,1\end{bmatrix}, \quad (50)$$

and the disturbances $\varsigma(t)$, $\varepsilon_1(t)$, $\varepsilon_2(t)$ in (14) are Gaussian white noises with covariances $Q_\varsigma=0.52I_2$, $Q_{\varepsilon_1}=0.68I_2$ and $Q_{\varepsilon_2}=0.15I_2$. By using Algorithm I, Fig.8 shows that the DKFE "$\hat{\mathrm{x}}(t)$" can track the state "x(t)" well in the presence of bandwidth constraints and DoS attacks. Different from the Fig.4, the PMSE of the ODKFE, DKFE and CSEs, which are calculated by Monte Carlo method with an average of 5000 runs, are plotted in Fig.9. It can be seen from this figure that the fusion estimation precision of the DKFE is higher than that of each CSE, which is as expected for the fusion estimation systems. It also shows that the fusion estimation precision of the DKFE is lower than that of the ODKFE, because the dimensionality reduction and DoS attacks degrade the estimation performance. Moreover, the relationship between the different rates of attack and fusion estimation performance is shown in Fig.10, where the PMSE for the DKFE is calculated by Monte Carlo method with an average of 10000 runs. It is observed from this figure that the larger rate of attack η is, the lower the fusion estimation precision is. In this sense, the DoS attack existing in CPSs is an important factor causing the deterioration of the fusion estimation performance.

V. Conclusions and Discussion

In this paper, the distributed dimensionality reduction fusion estimation problem has been investigated for a class of CPSs under DoS attacks. The dimensionality reduction and DoS attacks were characterized by a unified mathematical model with compensation strategy, and the optimal DKFE was designed in the linear minimum variance sense. By simultaneously considering decision processes of the defender and attacker, an effective dimensionality reduction and information compensation strategy for the defender has been obtained according to a simple judgement criterion, and a suboptimal attack strategy to maximize the MSE of the DKFE has been designed for the attacker based on the eavesdropped information. Then, the attack-dependent condition was derived such that the MSE of the DKFE was bounded. Finally, two illustrative examples were given to show the effectiveness of the proposed methods.

On the other hand, when considering the time-delay attack at time t, the compressed signal $\hat{\mathrm{x}}_{s_i}(t)$ has two different handling methods: the first method is that the signal $\hat{\mathrm{x}}_{s_i}(t)$ is directly discarded, and thus the dimensionality reduction fusion estimation method in this paper can be directly applicable to this case; The second method is that the signal $\hat{\mathrm{x}}_{s_i}(t)$ is modeled as a time-delay signal at the FC, and then the corresponding dimensionality reduction fusion estimation algorithm shall be designed. Notice that the second method is difficult to be obtained along the line of this paper, and will be our future work.

Since multi-sensor fusion (i.e., data fusion) technique can enhance the reliability by using redundant information between sensors, it can provide an attractive alternative to study the problem of attack detection. For example, the anomaly detection of cyber-attacks has been studied in [32], [45] by using the data fusion methods. Notice that the attack detection strategy is not discussed in this paper when considering DoS attacks in this paper. This is because a DoS attack can be easily judged by the FC, i.e., according to the function of DoS attacks, if the FC does not receive information from the sensors at time t, the FC will know that a DoS attack is launched at time t; Otherwise, if the FC receives information, the FC will know that there is no attack at time t. However, when considering other types of attacks such as false data injection attacks and collusion attacks, the design of attack detection is a very important problem in CPSs. In this case, how to cooperatively design fusion-based detector of attacks and distributed fusion estimator will be one of our future works.

Appendix

A.1: It follows from (1), (4) and (10) that

$$\begin{aligned}\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)=&(1-\eta_i(t)\eta(t))\{(I_n-H_i(t))A\tilde{\mathrm{x}}_i^{\mathrm{c}}(t-1)\\&+(I_n-H_i(t))w(t-1)+H_i(t)\tilde{\mathrm{x}}_i(t)\}\\&+\eta_i(t)\eta(t)[A\tilde{\mathrm{x}}_i^{\mathrm{c}}(t-1)+w(t-1)]\end{aligned}\quad(51)$$

$$\tilde{\mathrm{x}}_i(t)=\Phi_{\mathrm{K}_i}(t)\tilde{\mathrm{x}}_i(t-1)+\mathrm{G}_{\mathrm{K}_i}(t)w(t-1)-\mathrm{K}_i(t)v_i(t)(52)$$

From the geometric meaning of $\tilde{\mathrm{x}}_i(t)$, one has by (51–52) that

$$\begin{cases}\tilde{\mathrm{x}}_i(t)\perp w(t_1)(t_1\geq t),w(t)\perp v_i(t_1)(\forall t,t_1)\\\tilde{\mathrm{x}}_i(t)\perp v_i(t_1)(t_1>t),\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)\perp w(t_1)(t_1\geq t)\\\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)\perp v_j(t_1)(i=j,t_1>t\text{ or }i\neq j,\forall t,t_1)\end{cases}\quad(53)$$

Then combining (51–53) yields that

$$\begin{cases}\mathrm{E}\{\tilde{x}_i(t)(\tilde{\mathrm{x}}_j^{\mathrm{c}}(t-1))^{\mathrm{T}}\}=\Phi_{\mathrm{K}_i}(t)\Omega_{ij}(t-1)\\\mathrm{E}\{\tilde{x}_i(t)w^{\mathrm{T}}(t-1)\}=\mathrm{G}_{\mathrm{K}_i}(t)Q_w\end{cases}\quad(54)$$

Meanwhile, it is derived from (51) and (52) that

$$\begin{aligned}\Omega_{ij}(t)=&(1-\eta_j(t)\eta(t))\mathrm{E}\{\tilde{\mathrm{x}}_i(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\}H_j(t)\\&+\mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}_j^{\mathrm{c}}(t-1)]^{\mathrm{T}}\}A^{\mathrm{T}}+\mathrm{E}\{\tilde{\mathrm{x}}_i(t)w^{\mathrm{T}}(t-1)\}\\&-(1-\eta_j(t)\eta(t))\mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}_j^{\mathrm{c}}(t-1)]^{\mathrm{T}}\}A^{\mathrm{T}}H_j(t)\\&-(1-\eta_j(t)\eta(t))\mathrm{E}\{\tilde{\mathrm{x}}_i(t)w^{\mathrm{T}}(t-1)\}H_j(t)\end{aligned}\quad(55)$$

Then, (23) can be obtained by substituting (54) into (55).

Define $\tilde{\mathrm{x}}_i^{\mathrm{A}}(t) \triangleq A\tilde{\mathrm{x}}_i^{\mathrm{c}}(t-1) + w(t-1)$. Then, (51) can be rewritten as:

$$\begin{aligned}\tilde{\mathrm{x}}_i^{\mathrm{c}}(t) = (1-\eta_i(t)\eta(t))\{(I_n - H_i(t))\tilde{\mathrm{x}}_i^{\mathrm{A}}(t) \\ +H_i(t)\tilde{\mathrm{x}}_i(t)]\} + \eta_i(t)\eta(t)\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)\end{aligned} \quad (56)$$

From (56), one has

$$\begin{aligned}&\Sigma_{ij}(t) = (1-\eta_i(t)\eta(t))(1-\eta_j(t)\eta(t)) \\ &\times\{[I_n - H_i(t)]\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\}(I_n - H_j(t)) \\ &+[I_n - H_i(t)]\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\}H_j(t) + H_i(t) \\ &\times\mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\}(I_n - H_j(t)) + H_i(t) \\ &\times\mathrm{E}\{\tilde{\mathrm{x}}_i(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\}H_j(t)\} + (1-\eta_i(t)\eta(t))\eta_j(t)\eta(t) \\ &\times\{[I_n - H_i(t)]\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\} + H_i(t) \\ &\times\mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\} + \eta_i(t)\eta(t)((1-\eta_j(t)\eta(t))) \\ &\times\{\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\}(I_n - H_j(t)) + \mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\} \\ &\times H_j(t)\} + \eta(t)\eta_i(t)\eta_j(t)\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)[\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)]^{\mathrm{T}}\}\end{aligned} \quad (57)$$

Moreover, it follows from (53) and (54) that

$$\begin{cases}\mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{A}}(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\} = A\Sigma_{ij}(t-1)A^{\mathrm{T}} + Q_w \\ \mathrm{E}\{\tilde{\mathrm{x}}_i(t)[\tilde{\mathrm{x}}_j^{\mathrm{A}}(t)]^{\mathrm{T}}\} = \Phi_{\mathrm{K}_i}(t)\Omega_{ij}(t-1) + \mathrm{G}_{\mathrm{K}_i}(t)Q_w\end{cases}, \quad (58)$$

where $\Omega_{ij}(t-1)$ is calculated by (23). Meanwhile, it is concluded from Lemma 1 and the definitions of $\mathrm{V}_{ij}(t)$ and $\Omega_{ij}(t)$ that

$$\begin{cases}H_i(t)\mathrm{X}H_j(t) = [H_i(t)\odot H_j(t)]\otimes \mathrm{X} \\ (I_n - H_i(t))\odot H_j(t) = \mathrm{V}_{ji}^{\mathrm{T}}(t) \\ \mathrm{E}\{\tilde{\mathrm{x}}_i^{\mathrm{c}}(t)\tilde{\mathrm{x}}_j^{\mathrm{T}}(t)\} = \Omega_{ji}^{\mathrm{T}}(t)\end{cases}, \quad (59)$$

where $\mathrm{X} \in \mathrm{R}^{n\times n}$ is a given matrix. Therefore, (22) is derived by substituting (58–59) into (57). On the other hand, at each time step, the optimal fusion estimation error covariance matrix for the DKFE $\hat{\mathrm{x}}(t)$ is calculated by (20), while the estimation error covariance matrix for each CSE is given by $\Sigma_{ii}(t) = (1-\eta(t)\eta_i(t))\Sigma_{ii}^{11}(t) + \eta(t)\eta_i(t)\Sigma_{ii}^{22}(t)$, where $\Sigma_{ii}^{11}(t)$ and $\Sigma_{ii}^{22}(t)$ are determined by (22). Hence, (24) is obtained from the result of [12]. This completes the proof.

A.2: It is concluded from (24) that $\mathrm{Tr}\{P(t)\} \leq P_\Sigma(t)$, where $P_\Sigma(t) \triangleq \min\{\mathrm{Tr}\{\Sigma_{11}(t)\}, \cdots, \mathrm{Tr}\{\Sigma_{LL}(t)\}\}$. Under this relaxation condition, the optimization object in (25) reduces to:

$$\min_{\{H_1(t),\cdots,H_L(t),\forall\eta_i(t)\}} P_\Sigma(t) \ \text{ s.t : (12).} \quad (60)$$

According to the (***F1***), when designing dimensionality reduction strategy at time t, it is not necessary to consider the attack parameters. In this case, $\mathrm{Tr}\{\Sigma_{ii}(t)\}(i\in\{1,\cdots,L\})$ in the optimization object of (60) should be replaced by "$\mathrm{Tr}\{\Sigma_{ii}^{11}(t)\}$". Moreover, it is known from (22) that the computation procedure for $\Sigma_{ii}^{11}(t)$ only depends on the variables $H_i(t)$ and $\Sigma_{ii}(t-1)$. From the above analysis, the optimization problem (60) can be divided into L subproblems with the following form:

$$\begin{cases}\min\limits_{H_i(t)} \ \mathrm{Tr}\{\Sigma_{ii}^{11}(t)\} \\ \text{s.t. : } \sum_{j=1}^n \gamma_{ij}(t) = r_i \text{ and } \gamma_{ij}\in\{0,1\}\end{cases}, \quad (61)$$

where $\Sigma_{ii}^{11}(t)$ is calculated by (22). According to the property of "$\odot$", all the diagonal elements of $\mathrm{V}_{ii}(t)$ are the "0". Then, it follows from the properties of "$\otimes$" and "$\mathrm{Tr}\{\bullet\}$" that

$$\begin{aligned}\mathrm{Tr}\{\mathrm{V}_{ii}(t)\otimes[\Phi_{\mathrm{K}_i}(t)\Omega_{ii}(t-1)A^{\mathrm{T}} + \mathrm{G}_{\mathrm{K}_i}(t)Q_w]\} = 0 \\ \mathrm{Tr}\{\mathrm{V}_{ii}^{\mathrm{T}}(t)\otimes[A\Omega_{ii}^{\mathrm{T}}(t-1)\Phi_{\mathrm{K}_i}^{\mathrm{T}}(t) + Q_w\mathrm{G}_{\mathrm{K}_i}^{\mathrm{T}}(t)]\} = 0\end{aligned} \quad (62)$$

It is derived from (22) and (62) that

$$\begin{aligned}\mathrm{Tr}\{\Sigma_{ii}^{11}(t)\} = \mathrm{Tr}\{\Lambda_{ii}(t)\otimes P_{ii}(t) + \mathrm{M}_{ii}(t)\otimes\Sigma_{ii}^{22}(t)\} \\ = \sum\nolimits_{j=1}^n \{[P_{ii}(t)(j,j) - \Sigma_{ii}^{22}(t)(j,j)]\gamma_{ij}(t)\} \\ +\mathrm{Tr}\{\Sigma_{ii}^{22}(t)\}\end{aligned} \quad (63)$$

Notice that each $\gamma_{ij}(t)$ is a binary variable taking "1" or "0", and thus when minimizing the objective function $\mathrm{Tr}\{\Sigma_{ii}^{11}(t)\}$ in (61) subject to (12), (31) is the optimal solution to (61) from (63). Then, it is concluded from (60) that (31) is the suboptimal solution of (25).

On the other hand, it is concluded from (40-41) in [23] that, the optimization problem (26) can reduce to:

$$\max_{\{\eta_1(t),\cdots,\eta_L(t),\forall H_i(t)\}} \mathrm{Tr}\{\Sigma(t)\} = \sum_{i=1}^{L}\mathrm{Tr}\{\Sigma_{ii}(t)\} \ \text{ s.t. :(8)} \quad (64)$$

According to the (***F2***), when the attacker launches a DoS attack at time t, the attack strategy will be designed based on the estimation information at time $t-1$, and is independent of each compression matrix $H_i(t)$. In this case, $\mathrm{Tr}\{\Sigma_{ii}(t)\}(i\in\{1,\cdots,L\})$ in the optimization object of (64) should be replaced by "$\eta_i(t)\mathrm{Tr}\{\Sigma_{ii}^{22}(t)\}$". Since $\sum_{i=1}^L \eta_i(t)\mathrm{Tr}\{\Sigma_{ii}^{22}(t)\} = \sum_{i=1}^L \eta_i(t)\mathrm{Tr}\{A\Sigma_{ii}(t-1)A^{\mathrm{T}}\} + \kappa Q_w$, the optimization problem (64) is equivalent to:

$$\max_{\{\eta_1(t),\cdots,\eta_L(t)\}} \sum\nolimits_{i=1}^L \eta_i(t)\mathrm{Tr}\{A\Sigma_{ii}(t-1)A^{\mathrm{T}}\} \ \text{ s.t. :(8),} \quad (65)$$

where $\Sigma_{ii}(t-1)$ is the estimation error covariance of the ith CSE at time $t-1$. Though it is difficult for the attacker to obtain the accurate information $\Sigma_{ii}(t-1)$ at time t, the attacker can eavesdrop on inaccurate $x(t-1)$ and $\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)$ by the monitoring device (see (14)). Then, the optimal estimates $\hat{\mathrm{x}}_{\mathrm{A}}(t-1)$ and $\hat{\mathrm{x}}_{\mathrm{AC}}^i(t-1)$ (see (27)) can be obtained by using the least square estimation method. Notice that $\mathrm{E}\{\hat{\mathrm{x}}_{\mathrm{A}}(t-1)\} = \mathrm{E}\{x(t-1)\}$ and $\mathrm{E}\{\hat{\mathrm{x}}_{\mathrm{AC}}^i(t-1)\} = \mathrm{E}\{\hat{\mathrm{x}}_i^{\mathrm{c}}(t-1)\}$. Under this condition, $\Sigma_{ii}(t-1)$ is proposed to be replaced by $\tilde{\Sigma}_{ii}(t-1)$, where

$$\begin{aligned}\tilde{\Sigma}_{ii}(t-1) = [\hat{\mathrm{x}}_{\mathrm{A}}(t-1) - \hat{\mathrm{x}}_{\mathrm{AC}}^i(t-1)] \\ \times[\hat{\mathrm{x}}_{\mathrm{A}}(t-1) - \hat{\mathrm{x}}_{\mathrm{AC}}^i(t-1)]^{\mathrm{T}}\end{aligned}. \quad (66)$$

Then, the optimization problem (65) is modified as:

$$\begin{cases}\max\limits_{\{\eta_1(t),\cdots,\eta_L(t)\}} \sum_{i=1}^L \eta_i(t)\mathrm{Tr}\{A\tilde{\Sigma}_{ii}(t-1)A^{\mathrm{T}}\} \\ \text{s.t. : } \sum_{i=1}^L \eta_i(t) = \kappa, \eta_i(t)\in\{0,1\}\end{cases}. \quad (67)$$

Since $\eta_i(t)$ is a binary variable satisfying the constraint (8), (32) is the solution to (67). Then, it is concluded from (64) and (67) that a group of suboptimal decision variables in (26) can be given by (32). This completes the proof.

A.3: It is concluded from [44] that when the condition (37) holds, one has

$$\begin{cases}\lim\limits_{t\to\infty}\mathrm{G}_{\mathrm{K}_i}(t) = \mathrm{G}_{\mathrm{K}_i}, \lim\limits_{t\to\infty}\Phi_{\mathrm{K}_i}(t) = \Phi_{\mathrm{K}_i} \\ \lim\limits_{t\to\infty}P_{ii}(t) = P_{ii}\end{cases}, \quad (68)$$

where Φ_{K_i} is a stable matrix. Therefore, it follows from (33) and (68) that there exists an integer $N_{\eta_i} > 0$ such that

$$\begin{aligned}\Omega_{ii}^{\eta}(t) = \Phi_{\mathrm{K}_i}\Omega_{ii}^{\eta}(t-1)A^{\mathrm{T}}[I_n - H_i(t)\\ +\eta\eta_i(t)H_i(t)] + \Delta\Omega_{ii}^{\eta}(t)\end{aligned} \tag{69}$$

for $t \geq N_{\eta_i}$, where $\Delta\Omega_{ii}^{\eta}(t) \triangleq (1-\eta\eta_i(t))[P_{ii} - \mathrm{G}_{\mathrm{K}_i}Q_w]H_i(t) + \mathrm{G}_{\mathrm{K}_i}Q_w$ and $\eta_i(t) \in \{0,1\}$. From the matrix structure of $H_i(t)$, there must exist a positive scalar ϕ_{η_i} such that

$$||\Delta\Omega_{ii}^{\eta}(t)||_2 \leq \phi_{\eta_i}\ (t \geq N_{\eta_i}) \tag{70}$$

Combining (69) and (70) yields that

$$\begin{aligned}||\Omega_{ii}^{\eta}(t)||_2 \leq \phi_{\eta_i} + \mathrm{g}_{\eta_i}||\Omega_{ii}^{\eta}(t-1)||_2\\ \leq \mathrm{g}_{\eta_i}^{t-N_{\eta_i}}||\Omega_{ii}^{\eta}(N_{\eta_i})||_2 + \textstyle\sum_{\ell=0}^{t-N_{\eta_i}+1}\mathrm{g}_{\eta_i}^{\ell}\phi_{\eta_i}\end{aligned}, \tag{71}$$

where g_{η_i} is defined in (38). Notice that

$$\lim_{t\to\infty}\mathrm{g}_{\eta_i}^{t-N_{\eta_i}} = 0, \lim_{t\to\infty}\sum\nolimits_{\ell=0}^{t-N_{\eta_i}+1}\mathrm{g}_{\eta_i}^{\ell}\phi_{\eta_i} = \frac{\phi_{\eta_i}}{1-g_{\eta_i}} \tag{72}$$

Then, when the condition (38) holds, one has by (71-72) that

$$\lim_{t\to\infty}||\Omega_{ii}^{\eta}(t)||_2 \leq \frac{\phi_{\eta_i}}{1-g_{\eta_i}} \tag{73}$$

In this case, it can be concluded from (34), (68) and (73) that there exists an integer $N_{H_i} > N_{\eta_i}$ such that

$$\begin{aligned}\Sigma_{ii}^{\eta}(t) = \Xi_{ii}(t) + \mathrm{J}_{H_i}(t)\\ \times\mathrm{diag}\{\Sigma_{ii}^{\eta}(t-1), \Sigma_{ii}^{\eta}(t-1)\}\mathrm{J}_{H_i}^{\mathrm{T}}(t)\end{aligned} \tag{74}$$

for $t \geq N_{H_i}$, where $\Xi_{ii}(t) \triangleq (1-\eta\eta_i(t))\{\mathrm{V}_{ii}(t)\otimes[\Phi_{\mathrm{K}_i}\Omega_{ii}^{\eta}(t-1)A^{\mathrm{T}} + \mathrm{G}_{\mathrm{K}_i}Q_w] + \mathrm{V}_{ii}^{\mathrm{T}}(t)\otimes[A(\Omega_{ii}^{\eta}(t-1))^{\mathrm{T}}\Phi_{\mathrm{K}_i}^{\mathrm{T}} + Q_w\mathrm{G}_{\mathrm{K}_i}^{\mathrm{T}}]\}$. Then, similar to (73), there must exist a positive scalar ϕ_{H_i} such that

$$||\Delta\Sigma_{ii}^{\eta}(t)||_2 \leq \phi_{H_i}(t \geq N_{H_i}) \tag{75}$$

From the property of "$||\bullet||_2$" and the matrix structure of "$H_i(t)$", one has

$$\begin{cases}||\mathrm{diag}\{\Sigma_{ii}^{\eta}(t-1), \Sigma_{ii}^{\eta}(t-1)\}||_2 = ||\Sigma_{ii}^{\eta}(t-1)||_2\\ ||\mathrm{J}_{H_i}(t)||_2 < \mathrm{g}_{H_i}\end{cases}, \tag{76}$$

where $\mathrm{J}_{H_i}(t)$ is defined by (35), and g_{H_i} is defined in (39). Subsequently, it is derived from (74–76) that

$$\begin{aligned}||\Sigma_{ii}^{\eta}(t)||_2 \leq \phi_{H_i} + \mathrm{g}_{H_i}||\Sigma_{ii}^{\eta}(t-1)||_2\\ \leq \mathrm{g}_{H_i}^{t-N_{H_i}}||\Sigma_{ii}^{\eta}(N_{H_i})||_2 + \textstyle\sum_{\ell=0}^{t-N_{H_i}+1}\mathrm{g}_{H_i}^{\ell}\phi_{H_i}\end{aligned} \tag{77}$$

According to (77), when the condition (39) holds, it follows from the similar derivation of (73) that there must exist a positive scalar φ_{η_i} such that $\lim\limits_{t\to\infty}||\Sigma_{ii}^{\eta_i}||_2 \leq \varphi_{\eta_i}$. This implies that $\lim\limits_{t\to\infty}\mathrm{Tr}\{\Sigma_{ii}^{\eta}(t)\}$ is bounded when the conditions (37–39) hold. Moreover, it follows from (24) that $\lim\limits_{t\to\infty}\mathrm{Tr}\{P(t)\} \leq \lim\limits_{t\to\infty}\mathrm{Tr}\{\Sigma_{ii}^{\eta}(t)\}(i \in \{1, 2, \cdots, L\})$, and thus the result (40) holds. This completes the proof.

REFERENCES

[1] S. Peisert, J. Margulies, D.M. Nicol, H. Khurana, C. Sawall, Designed-in security for cyber-physical systems, *IEEE Security and Privacy*, vol. 12, no. 5, 2014, pp. 9-12.

[2] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, Y. Jin, Cyber-physical systems: A security perspective, *Proceedings of the 20th IEEE European Test Symposium (ETS)*, Cluj-Napoca, Romania, 2015, pp. 1-8.

[3] A Di Pietro, S Panzieri, A Gasparri, Situational Awareness Using Distributed Data Fusion with Evidence Discounting, *Critical Infrastructure Protecton IX*, Volume 466 of the series IFIP Advances in Information and Communication Technology, pp. 281-296, 2015.

[4] B. Genge, P. Haller, I. Kiss, Cyber-security-aware network design of industrial control systems, *IEEE System Journal*, 2015, Article in press, Doi:10.1109/JSYST.2015.2462715.

[5] Y.F. Huang, S. Werner, J. Huang, N. Kashyap, V. Gupta, State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid, *IEEE Signal Processing Magazine*, vol. 29, no. 5, 2012, pp. 33-43.

[6] X. Cao, P. Cheng, J. Chen, S.S. Ge, Y. Cheng, Y. Sun, Cognitive radio based state estimation in cyber-physical systems, *IEEE Journal on Selected Areas in Communicaiton,* vol. 32, no. 3, 2014, pp. 489-502.

[7] S. Deshmukh, B. Natarajan, A. Pahwa, State estimation over a lossy network in spatially distributed cyber-physical systems, *IEEE Transactions on Signal Processing,* vol. 62, no. 15, 2014, pp. 3911-3923.

[8] B. Chen, G. Hu, D.W.C. Ho, L. Yu, Distributed covariance intersection fusion estimation for cyber-physical systems with communication constraints. *IEEE Transactions on Automatic Control*, vol. 61, no. 12, 2016, pp. 4020–4026.

[9] D. Zhang, H. Song, L. Yu, Robust fuzzy-model-based filtering for nonlinear cyber-physical systems with multiple stochastic incomplete measurements. *IEEE Transactions on Systems, Man, and Cybernetics: Systmes*, Article in Press, Doi: 10.1109/TSMC.2016.2551200.

[10] X.R. Li, Y.M. Zhu, J. Wang, C.Z. Han, Optimal linear estimation fusion-part I: unified fusion rules, *IEEE Transactions on Information Theory*, vol. 49, no.9, 2003, pp. 2192-2208.

[11] Y. Bar-Shalom, X.R. Li, T. Kirubarajan, *Estimation with applications to tracking and navigation*, John Wilely and Sons, Inc., 2001.

[12] S. Sun, Z. Deng, Muti-sensor optimal information fusion Kalman filter, *Automatica*, vol. 40, 2004, pp. 1017-1023.

[13] L. Zhang, Z. Ning, Z. Wang, Distributed filtering for fuzzy time-delay systems with packet dropouts and redundant channels, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 4, 2016, pp. 559-572.

[14] Y. Gao, X.R. Li, E. Song, Robust linear estimation fusion with allowable unknown cross-covariance, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 9, 2016, pp. 1314-1325.

[15] B. Chen, G. Hu, D.W.C. Ho, W. Zhang, L. Yu. Distributed robust fusion estimation with application to state monitoring systems, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2016, Article in Press, Doi: 10.1109/TSMC.2016.2558103.

[16] H. Lin, S. Sun. Distributed fusion estimator for multisensor multirate systems with correlated noises, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2017, Article in Press, Doi: 10.1109/TSMC.2016.2645599.

[17] J.A. Roecker, C.D. McGillen, Comparison of two-sensor tracking methods based on state vector fusion and measurement fusion, *IEEE Transactions on Aerospace and Electronic Systems*, vol. 24, no. 4, 1988, pp. 447-449.

[18] S. Amin, A. Cárdenas, S. Sastry, Safe and secure networked control systems under denial-of-serivce attacks, *Hybrid Systems: Computation and Control*, 2009, pp. 31-45.

[19] G. Carl, G. Kesidis, R.R. Brooks, S. Rai, Denial-of-service attack-detection techniques, *IEEE Internet Computing Magazine*, vol. 10, no. 1, 2006, pp. 82-89.

[20] Y. Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, H. Jee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure, *Proceedings of the IEEE*, vol. 100, no. 1, 2012, pp. 195–209.

[21] H. Li, L. Lai, V. Poor, Multicast routing for decentralized control of cyber physical systems with an application in smart grid, *IEEE Journal of on Selected Areas in Communicaiton*, vol. 30, 2012, pp. 1097–1107.

[22] B. Chen, W.A. Zhang, L. Yu, Distributed finite-horizon fusion Kalman filtering for bandwidth and energy constrained wireless sensor networks, *IEEE Transactions on Signal Processing*, vol.62, no.4, 2014, pp.797-812.

[23] B. Chen, W.A. Zhang, L. Yu, G. Hu, H. Song, Distributed fusion estimation with communication bandwidth constraints, *IEEE Transactions on Automatic Control*, vol. 60, no. 5, 2015, pp. 1398-1403.

[24] B. Chen, D.W.C. Ho, W.A. Zhang, L. Yu, Networked fusion estimation with bounded noises, *IEEE Transactions on Automatic Control*, 2017, Article in Press, Doi: 10.1109/TAC.2017.2696746.

[25] J. Fang, H. Li, Hyperplane-based vector quantization for distributed estimation in wireless sensor networks, *IEEE Transactions on Information Theory*, vol. 55, 2009, pp. 5682-5699.

[26] B. Chen, L. Yu, W.A. Zhang, H. Wang, Distributed H_∞ fusion filtering with communication bandwidth constraints, *Signal Processing*, vol. 96, 2014, pp. 284-289.

[27] A. N.Bishop, A. V.Savkin, On false-data attacks in robust multi-sensor-based estimation, *The 9th IEEE International Conference on Control and Automation*, Santiago, Chile, 2011, pp. 10-17.

[28] H. Fawzi, P. Tabuada, S. Diggavi, Secure estimation and control for cyber-physical systems under adversarial attacks, *IEEE Transactions on Automatic Control*, vol. 59, no. 6, 2014, pp. 1454-1467.

[29] Y. Mo, B. Sinopoli, Secure estimation in the presence of integrity attacks, *IEEE Transactions on Automatic Control*, vol. 60, 2015, pp. 1145-1151.

[30] D. Ding, Y. Shen, Y. Song, Y. Wang, Recursive state estimation for discrete time-varying stochastic nonlinear systems with randomly occuring deception attacks, *International Journal of General Systems*, vol. 45, no. 5, 2015, pp. 548-560.

[31] D. Wang, X. Guan, T. Liu, Y. Gu, C. Shen, Z. Xu, Extended distributed state estimation: a detection method against tolerable false data injection in smart grids, *Energies*, vol. 7, 2014, pp. 1517-1538.

[32] T. Liu, Y. Sun, Y. Liu, Y. Gui, Y. Zhao, D. Wang, C. Shen, Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection, *Future Generation Computer Systems*, vol. 49, 2015, pp. 94-103.

[33] J. Zhang, R.S. Blum, X. Lu, D. Conus, Asymptotically optimum distributed estimation in the presence of attacks, *IEEE Transactions on Signal Processing*, vol. 63, no. 5, 2015, pp. 1086-1101.

[34] J. Kim, L. Tong, R. J.Thomas, Subspace methods for data attack on state estimator: A data driven approach, *IEEE Transactions on Signal Processing,* vol. 63, no. 5, 2015, pp. 1102-1114.

[35] Y. Law, M. Palaniswami, L. Hoesel, J. Doumen, P. Hartel, P. Havinga, Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols, *ACM Transactions on Sensor Networks*, vol. 5, no. 1, 2009, pp. 1139-1141.

[36] T. Kavitha, D. Sirdharan, Security vulnerabilities in wireless sensor networks: A survey, *Journal of Information Assurance and Security*, vol. 5, no. 1, 2010, pp. 31-44.

[37] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-serivce attack scheduling with energy constraints, *IEEE Transactions on Automatic Control*, vol. 60, no. 11, 2015, pp. 3023-3028.

[38] Y. Li, L. Shi, P. Cheng, J. Chen, D. E.Quevedo, Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach, *IEEE Transactions on Automatic Control*, vol. 60, no. 10, 2015, pp. 2831-2836.

[39] Y. Yuan, F. Sun, H. Liu, Resilient control of cyber-physical systems against intelligent attacker: a hierarchal stackelberg game approach, *International Journal of Systems Science*, vol. 47, 2016, pp. 2067-2077.

[40] Y. Yuan, H. Yuan, L. Guo, H. Yang, S. Sun, Resilient control of networked control systems under DoS attacks: a unified game approach, *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, 2016, pp. 1786–1794.

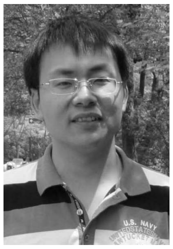
[41] D. Ding, Z. Wang, G. Wei, F. E.Alsaadi, Event-based security control for discrete-time stochastic systems, *IET Control Theory and Applications*, 2016, vol. 10, no. 15, pp. 1808-1815.

[42] D. Ding, Z. Wang, G. Wei, Security control for discrete-time stochastic nonlinear systems subject to deception attacks, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2016, Article in Press, Doi: 10.1109/TSMC.2016.2616544.

[43] Z. Feng, G. Wen, G. Hu, Distributed secure coordinated control for multi-agent systems under strategic attacks, *IEEE Transactions on Cybernetics*, Article in press, Doi: 10.1109/TCYB.2016.2544062.

[44] A.H. Jazwioski, *Stochastic Processes and Filtering Theory*, New York: Academic, 1970.

[45] B. Genge, C. Siaterlis, G. Karopoulos, Data fusion-based anomaly detection in networked critical infrastructures, *43th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)*, Workshop on Reliability and Security Data Analysis (RSDA 2013), Budapest, Hungary, pp. 1-8, 2013.



Bo Chen (M'17) 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 is currently a research fellow at school of electrical and electronic engineering, Nanyang Technology University, Singapore. He was a postdoctoral research fellow (Hong Kong Scholar) at college of science and engineering, City University of Hong Kong, 2015–2017. He was also a research fellow at school of electrical and electronic engineering, Nanyang Technology University, 2014–2015. His current research interests include information fusion estimation, networked fusion systems and secure estimation of cyber-physical systems.

Daniel W.C. Ho (M'90–SM'05–F'17) received the B.S., M.S., and Ph.D. degrees in mathematics from the University of Salford, Greater Manchester, U.K., in 1980, 1982, and 1986, respectively.

From 1985 to 1988, he was a Research Fellow with the Industrial Control Unit, University of Strathclyde, Glasgow, U.K. He is currently a Chair Professor in applied mathematics with the Department of Mathematics, and the Assistant Dean (Teaching Innovations) with the College of Science and Engineering, City University of Hong Kong, Hong Kong which he joined in 1989. His current research interests include control and estimation theory, complex dynamical distributed networks, multi-agent networks, and stochastic systems. He has over 200 publications in scientific journals.

Prof. Ho is a Fellow of the IEEE. He was honored to be the Chang Jiang Chair Professor awarded by the Ministry of Education, China, in 2012. He has been on the editorial board of a number of journals including IEEE Transactions on Neural Networks and Learning Systems, IET Control Theory and its Applications, Journal of the Franklin Institute and Asian Journal of Control. He is named as ISI Highly Cited Researchers (2014-2016) in Engineering by Thomson Reuters.

Wen-An Zhang (M'13) received the B.Eng. degree in Automation and the Ph.D. degree in Control Theory and Control Engineering from Zhejiang University of Technology, China, in 2004 and 2010, respectively.

He has been with Zhejiang University of Technology since 2010 where he is now a professor at Department of Automation. He was a senior research associate at Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong, 2010-2011. He was awarded an Alexander von Humboldt Fellowship in 2011-2012. His current research interests include networked control systems, wireless sensor networks and intelligent mobile robots.

Li Yu (M'09) 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. He has authored or co-authored three books and over 200 journal or conference papers. His current research interests include wireless sensor networks, networked control systems and motion control.