Residual-Based False Data Injection Attacks Against Multi-Sensor Estimation Systems

Haibin Guo, Jian Sun, *Senior Member, IEEE*, and Zhong-Hua Pang, *Senior Member, IEEE*

***Abstract*—This paper investigates the security issue of multi-sensor remote estimation systems. An optimal stealthy false data injection (FDI) attack scheme based on historical and current residuals, which only tampers with the measurement residuals of partial sensors due to limited attack resources, is proposed to maximally degrade system estimation performance. The attack stealthiness condition is given, and then the estimation error covariance in compromised state is derived to quantify the system performance under attack. The optimal attack strategy is obtained by solving several convex optimization problems which maximize the trace of the compromised estimation error covariance subject to the stealthiness condition. Moreover, due to the constraint of attack resources, the selection principle of the attacked sensor is provided to determine which sensor is attacked so as to hold the most impact on system performance. Finally, simulation results are presented to verify the theoretical analysis.**

***Index Terms*—Cyber-physical systems (CPSs), false data injection (FDI) attacks, remote state estimation, stealthy attacks.**

I. Introduction

CYBER-PHYSICAL systems (CPSs) combine various physical resources and complete the integrated design of the systems by computation, communication, sensing and control technologies [1]–[5], which have supported numerous applications such as power grid systems, unmanned systems, and multi-agent systems [6]–[9]. For these CPSs, the cyber security is a practical problem that has to be considered and solved due to the openness of communication networks [10].

It is well known that attack and defense have always been inseparable in CPSs, both of which promote the construction of their security framework. The former mainly focuses on how to design cyber attacks to vandalize a system [11]–[14]. This discloses the vulnerability of CPSs in advance, and further boosts the establishment of the corresponding defense measures including attack detection [15]–[20], secure state estimation [21]–[23], and secure control [24]–[29], etc. Hence, the design of attack strategies is of great importance in constructing secure CPSs, which has attracted more and more attention in recent years.

As one of typical cyber attacks, stealthy false data injection (FDI) attack aims at achieving the objective of damaging a target system, meanwhile being able to evade attack detection. Due to both the destructiveness and stealthiness, such an attack attracts many scholars and is also the research focus of this paper. In [30] and [31], Kullback-Leibler divergence (KLD) was adopted to quantify the attack stealthiness, based on which a notion of ϵ-stealthy FDI attack was proposed. In [32] and [33], stealthy FDI attacks were designed for the feedback and forward channels for the sake of destabilizing a closed-loop control system while bypassing a residual-based detector. In [34]–[36], an optimal stealthy FDI attack scheme, which tampers with measurement and control information, was developed to drive a system to attackers' desired state under the specific stealthiness constraint. In [37], for a remote estimation system with smart sensors, a residual-based FDI attack method was proposed to degrade its estimation performance to the greatest extent without triggering a χ^2 detector. Then, the effect of such an attack on the estimation performance was further explored in [38]–[40] by adopting the KLD-based attack stealthiness metric. Furthermore, the side information was considered and utilized in [41] to design residual-based attack signals. In order to further enhance the attack destructiveness, a novel residual-based attack scheme was studied in [42]–[44] to utilize both historical and current residuals to construct attack signals, and the corresponding results showed that this attack caused more loss of system estimation performance than that in [37].

All the aforementioned works address the vulnerability of single-sensor systems by designing the specific attacks. However, most of those attack schemes would lose stealthiness when attacking one of the transmission channels of a multi-sensor system, which has been investigated in [45]. That is to say, it becomes inappropriate to utilize the cyber attack strategies for single-sensor systems to analyze the vulnerability of multi-sensor systems. Hence, it is necessary to develop a novel stealthy FDI attack scheme against multi-sensor systems for the sake of exploring the possible existing vulnerability, which is the main motivation of this paper. Moreover, to the best of our knowledge, few works focus on designing stealthy FDI attacks against multi-sensor systems expect [46]

Manuscript received October 14, 2022; revised December 13, 2022; accepted January 11, 2023. This work was supported by the National Natural Science Foundation of China (61925303, 62173034, 62088101, U20B2073, 62173002), the National Key Research and Development Program of China (2021YFB1714800), and Beijing Natural Science Foundation (4222045). Recommended by Associate Editor Xiaohua Ge. *(Corresponding author: Zhong-Hua Pang.)*

Citation: H. B. Guo, J. Sun, and Z.-H. Pang, "Residual-based false data injection attacks against multi-sensor estimation systems," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1181–1191, May 2023.

H. B. Guo and J. Sun are with the National Key Laboratory of Autonomous Intelligent Unmanned Systems, School of Automation, Beijing Institute of Technology, Beijing 100081, China. J. Sun is also with the Beijing Institute of Technology Chongqing Innovation Center, Chongqing 401120, China (e-mail: haibin.guo@bit.edu.cn; sunjian@bit.edu.cn).

Z.-H. Pang is with the Key Laboratory of Fieldbus Technology and Automation of Beijing, North China University of Technology, Beijing 100144, China (e-mail: zhonghua.pang@ia.ac.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.123441

and [47]. However, in [46] and [47], only real-time residuals were used to design the attack signals to tamper with the measurement residuals of partial sensors. Inspired by [42]–[44], the historical residuals are additionally introduced in this paper to design the attack signals aiming at further improving the attack effect on the estimation performance of multi-sensor systems. Due to constrained attack resources, malicious attackers only can falsify the measurement residuals of partial sensors, and thus it is not a simple and easy extension from the single-sensor case in [42]–[44]. The main contributions of this paper are presented as follows.

1) A multi-sensor estimation system is considered, where each sensor sends its measurement residual to the remote estimator, and an optimal stealthy FDI attack scheme, which utilizes both the historical and current residuals, is proposed to tamper with the measurement residuals of the partial sensors under limited attack resources.

2) The stealthiness condition of the proposed attack scheme is derived, and then the compromised estimation error covariance is given to evaluate the system performance under attack. Several convex optimization problems, which aim at maximizing the estimation error under the stealthiness constraint, are formed to obtain the worst-case attack strategy at each attack interval.

3) With limited attack resources, the selection principle of the attacked sensor is derived to determine to tamper with the measurement residuals of which sensors such as to cause more degradation of the system performance. Also, all the theoretical results are verified by the offered numerical simulation.

The rest of this paper is organized as follows. Section II describes a multi-sensor remote state estimation system. Then, the proposed stealthy FDI attack scheme and its stealthiness condition are presented in Section III. Section IV derives the worst-case attack strategy and gives the selection principle of the attacked sensor. Section V provides several simulation results to verify all the theoretical analyses. Finally, this paper is concluded in Section VI.

Notations: Throughout this paper, $\mathbb{R}^n$ is the n-dimensional Euclidean space. The positive semi-definite and positive definite matrices are denoted by $X \geq 0$ and $X > 0$, respectively. $\mathrm{tr}(X)$ stands for the trace of the matrix X. $\mathcal{N}(a,b)$ denotes the Gaussian distribution with mean a and covariance b. $E[\cdot]$ is the mathematical expectation. I and 0 denote an identity matrix and a zero matrix with appropriate dimensions, respectively, and I_n is an $n\times n$-dimensional identity matrix. $\lceil\cdot\rceil$ denotes the value of a number rounded upwards to the nearest integer.

II. Problem Statement

A. System Model

A CPS with N sensors is modeled as

$$x_{k+1} = Ax_k + w_k \tag{1a}$$

$$y_{i,k} = H_i x_k + v_{i,k} \tag{1b}$$

where $x_k \in \mathbb{R}^n$ is the system state, $y_{i,k} \in \mathbb{R}^{q_i}$ is the measurement of sensor i ($i = 1,2,\ldots,N$), and the noises $w_k \in \mathbb{R}^n$ and $v_{1,k} \in \mathbb{R}^{q_1}$, $v_{2,k} \in \mathbb{R}^{q_2}, \ldots, v_{N,k} \in \mathbb{R}^{q_N}$ are independent of each other, which satisfy $w_k \sim \mathcal{N}(0,Q)$, $Q \geq 0$ and $v_{i,k} \sim \mathcal{N}(0,R_i)$, $R_i > 0$, $i = 1,2,\ldots,N$, respectively. It is assumed that $(A, \sqrt{Q})$ is stabilizable and (A, H_i) is detectable for $i = 1,2,\ldots,N$.

The following measurement residual of each sensor is calculated and sent to the remote estimator via its own channel:

$$z_{i,k} = y_{i,k} - H_i \hat{x}_{k|k-1} \tag{2}$$

where $\hat{x}_{k|k-1}$ is the priori estimate of the remote estimator, which is broadcasted back to each sensor [45]–[47].

B. Remote State Estimator

Define

$$H = \begin{bmatrix} H_1 \\ H_2 \\ \vdots \\ H_N \end{bmatrix},\ V_k = \begin{bmatrix} v_{1,k} \\ v_{2,k} \\ \vdots \\ v_{N,k} \end{bmatrix},\ R = \begin{bmatrix} R_1 & & & \\ & R_2 & & \\ & & \ddots & \\ & & & R_N \end{bmatrix}.$$

Then, the augmented form of all sensor measurements is described as

$$\begin{aligned} Y_k &= \begin{bmatrix} y_{1,k}^T & y_{2,k}^T & \cdots & y_{N,k}^T \end{bmatrix}^T \\ &= Hx_k + V_k \end{aligned} \tag{3}$$

where $Y_k \in \mathbb{R}^m$, $m = \sum_{i=1}^N q_i$, and $V_k \sim \mathcal{N}(0,R)$.

With (2) and (3), the measurement residuals received from all the sensors can be expressed as

$$\begin{aligned} Z_k &\triangleq \begin{bmatrix} z_{1,k}^T & z_{2,k}^T & \cdots & z_{N,k}^T \end{bmatrix}^T \\ &= Y_k - H\hat{x}_{k|k-1}. \end{aligned} \tag{4}$$

After receiving these measurement residuals, a Kalman filter is employed in the remote center to estimate the state of the physical system (1a), whose steady form is

$$\hat{x}_{k+1|k} = A\hat{x}_k \tag{5a}$$

$$\hat{x}_k = \hat{x}_{k|k-1} + KZ_k \tag{5b}$$

where $\hat{x}_{k|k-1}$ and $\hat{x}_k$ are the priori and posteriori estimates of the state x_k, respectively. The Kalman filter gain is given as

$$K = \Phi H^T (H\Phi H^T + R)^{-1} \tag{6}$$

where Φ is the priori estimation error covariance in the steady state, which is defined as

$$\Phi = \lim_{k\to+\infty} E[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})^T]$$

with

$$\Phi = A\Phi A^T + Q - A\Phi H^T (H\Phi H^T + R)^{-1} H\Phi A^T.$$

C. Anomaly Detector

With (4), the measurement residual Z_k in the steady state satisfies

$$Z_k \sim \mathcal{N}(0,\Xi) \tag{7}$$

where the covariance Ξ is

$$\Xi = H\Phi H^T + R = \begin{bmatrix} \Xi_1 & H_1\Phi H_2^T & \cdots & H_1\Phi H_N^T \\ H_2\Phi H_1^T & \Xi_2 & \cdots & H_2\Phi H_N^T \\ \vdots & \vdots & \ddots & \vdots \\ H_N\Phi H_1^T & H_N\Phi H_2^T & \cdots & \Xi_N \end{bmatrix} \tag{8}$$

with $\Xi_i = H_i\Phi H_i^T + R_i$.

Based on the statistical property of residual, a χ^2 detector is adopted at the side of the remote estimator to detect system anomaly. The corresponding detection index is defined as

$$g_k = \sum_{t=k-J+1}^{k} Z_t^T \Xi^{-1} Z_t \underset{H_1}{\overset{H_0}{\lessgtr}} \varepsilon \tag{9}$$

where J is the size of the detection window, ε is the detection threshold, and H_0 represents that the system operates normally, while H_1 means that the system is under attack. Once g_k is larger than ε, the detector will trigger an alarm.

Remark 1: It is clear from (8) that $E[z_{i,k}z_{j,k}^T] = H_i\Phi H_j^T \neq 0$ for $i \neq j$, i.e., the residual of each sensor is not independent. When existing single-sensor attack schemes are applied to multi-sensor systems, most of them only guarantee $E[z_{i,k}^a z_{i,k}^{aT}] = E[z_{i,k}z_{i,k}^T]$ in, e.g., [37] and [42], while not ensuring $E[z_{i,k}^a \tilde{z}_{i,k}^T] = E[z_{i,k}\tilde{z}_{i,k}^T]$, where $\tilde{z}_{i,k}$ is the residual of the normal sensors except attacked sensor i, which tends to cause the distribution of the residual in (7) to change and further induces detector (9) to trigger an alarm. This means that multi-sensor CPSs have some degree of disclosure capability to the existing single-sensor attack schemes, which has been analyzed in [45] and [47].

III. Stealthy FDI Attack Scheme

As shown in Fig. 1, the measurement residual $z_{i,k}$ of each sensor and the state estimate $\hat{x}_{k|k-1}^a$ are transmitted to specified destinations through communication networks, which are tampered as $z_{i,k}^a$ and $\hat{x}_{k|k-1}$ by a malicious attacker, respectively. It is assumed that the attacker can disclose the full knowledge of the target system (i.e., A, H, Q and R) and run a same Kalman filter as in (5).

A. Attack Model

Based on the historical and current measurement residuals, the stealthy FDI attack scheme is designed as

$$Z_k^a = F_k Z_{k-\tau} + L_k Z_k + b_k \tag{10}$$

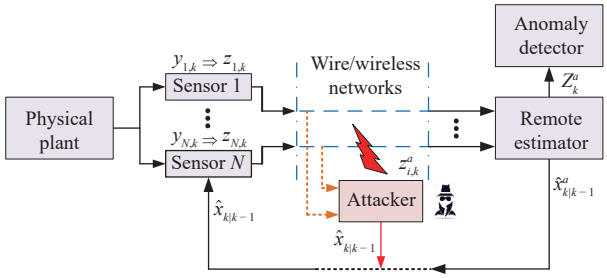

Fig. 1. A multi-sensor remote estimation system under attack.

where $Z_{k-\tau}$ is the historical residual stored by the attacker with the positive integer $\tau \leq k$, F_k and L_k are the attack matrices to be designed, and b_k is the injection Gaussian white noise which satisfies $b_k \sim \mathcal{N}(0, \Gamma_k)$ with $\Gamma_k \geq 0$. It is noted that the detection variable g_k obeys a χ^2 distribution, and in order to unchange its distribution, the parameter τ is restricted to $\tau \geq J$.

Due to resource constraint, for the convenience of analysis and without loss of the generality, it is assumed that the attacker only selects one sensor channel, denoted by sensor i, to launch the attack. Then, the attack matrices F_k and L_k in (10) are designed as

$$F_k = \begin{bmatrix} F_{i,k} & 0 \\ 0 & 0 \end{bmatrix}, \; L_k = \begin{bmatrix} L_{i,k} & N_{i,k} \\ 0 & I \end{bmatrix} \tag{11}$$

and the injection noise b_k and its covariance matrix are designed as

$$b_k = \begin{bmatrix} b_{i,k} \\ 0 \end{bmatrix}, \; \Gamma_k = \begin{bmatrix} \Gamma_{i,k} & 0 \\ 0 & 0 \end{bmatrix}. \tag{12}$$

Substituting (11) and (12) into (10) yields

$$\begin{aligned} Z_k^a &= F_k Z_{k-\tau} + L_k Z_k + b_k \\ &= \begin{bmatrix} F_{i,k} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} z_{i,k-\tau} \\ \tilde{z}_{i,k-\tau} \end{bmatrix} + \begin{bmatrix} L_{i,k} & N_{i,k} \\ 0 & I \end{bmatrix} \begin{bmatrix} z_{i,k} \\ \tilde{z}_{i,k} \end{bmatrix} + \begin{bmatrix} b_{i,k} \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} F_{i,k} z_{i,k-\tau} + L_{i,k} z_{i,k} + N_{i,k}\tilde{z}_{i,k} + b_{i,k} \\ \tilde{z}_{i,k} \end{bmatrix} \end{aligned} \tag{13}$$

where $\tilde{z}_{i,k}$ denotes the normal residual except for that of sensor i. It is clear from (13) that only the measurement residual of sensor i is tampered. Then, for the normal and compromised sensors, the corresponding system matrices are redescribed as

$$H = \begin{bmatrix} H_i \\ \tilde{H}_i \end{bmatrix}, \; R = \begin{bmatrix} R_i & \\ & \tilde{R}_i \end{bmatrix}, \; K = \begin{bmatrix} K_i & \tilde{K}_i \end{bmatrix}.$$

And, the normal residual covariance (8) is redivided as

$$\Xi = \begin{bmatrix} \Xi_i & M_i \\ M_i^T & \tilde{\Xi}_i \end{bmatrix} \tag{14}$$

where $M_i = H_i\Phi\tilde{H}_i^T$, and $\tilde{\Xi}_i = \tilde{H}_i\Phi\tilde{H}_i^T + \tilde{R}_i$.

B. Stealthiness Condition

It is well known that the attack stealthiness is an important precondition before successfully launching an attack. That is to say, once the attack is detected by an anomaly detector at the beginning, it is impossible to continue to attack the target system, not to mention to destroy the system. For the attack scheme (13), the stealthiness condition is given in the following theorem.

Theorem 1: In order to ensure that the attack scheme (13) is stealthy, the attack matrices (11) and the covariance matrix in (12) need to satisfy the following condition:

$$\begin{cases} F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}\Theta_i L_{i,k}^T + \Gamma_{i,k} = \Theta_i \\ N_{i,k} = (I - L_{i,k})M_i\tilde{\Xi}_i^{-1} \end{cases} \tag{15}$$

where $\Theta_i = \Xi_i - M_i\tilde{\Xi}_i^{-1}M_i^T$.

Proof: With (11) and (12), the covariance of the compro-

mised residual (13) is derived as

$$\begin{aligned}\Xi_k^a &= E[Z_k^a Z_k^{aT}]\\ &= F_k\Xi F_k^T + L_k\Xi L_k^T + \Gamma_k\\ &= \begin{bmatrix}F_{i,k} & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\begin{bmatrix}F_{i,k}^T & 0\\ 0 & 0\end{bmatrix}+\begin{bmatrix}\Gamma_{i,k} & 0\\ 0 & 0\end{bmatrix}\\ &\quad+\begin{bmatrix}L_{i,k} & N_{i,k}\\ 0 & I\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\begin{bmatrix}L_{i,k}^T & 0\\ N_{i,k}^T & I\end{bmatrix}\\ &= \begin{bmatrix}\Xi_{i,k}^a & L_{i,k}M_i + N_{i,k}\tilde{\Xi}_i\\ M_i^T L_{i,k}^T + \tilde{\Xi}_i N_{i,k}^T & \tilde{\Xi}_i\end{bmatrix}\end{aligned} \tag{16}$$

where

$$\begin{aligned}\Xi_{i,k}^a &= F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}\Xi_i L_{i,k}^T + N_{i,k}M_i^T L_{i,k}^T\\ &\quad + L_{i,k}M_i N_{i,k}^T + N_{i,k}\tilde{\Xi}_i N_{i,k}^T + \Gamma_{i,k}.\end{aligned} \tag{17}$$

In order to achieve strict stealthiness, compromised residual covariance (16) needs to keep the same as the normal one (14), i.e.,

$$\begin{bmatrix}\Xi_{i,k}^a & L_{i,k}M_i + N_{i,k}\tilde{\Xi}_i\\ M_i^T L_{i,k}^T + \tilde{\Xi}_i N_{i,k}^T & \tilde{\Xi}_i\end{bmatrix} = \begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}.$$

Then, we obtain

$$\begin{cases}\Xi_{i,k}^a = \Xi_i\\ L_{i,k}M_i + N_{i,k}\tilde{\Xi}_i = M_i.\end{cases} \tag{18}$$

It can be obtained from the second condition of (18) that

$$N_{i,k} = (I - L_{i,k})M_i\tilde{\Xi}_i^{-1}. \tag{19}$$

Substituting (19) into (17) yields

$$\begin{aligned}\Xi_{i,k}^a &= F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}\Xi_i L_{i,k}^T + \Gamma_{i,k}\\ &\quad + L_{i,k}M_i\tilde{\Xi}_i^{-1}M_i^T(I - L_{i,k}^T)\\ &\quad + (I - L_{i,k})M_i\tilde{\Xi}_i^{-1}M_i^T L_{i,k}^T\\ &\quad + (I - L_{i,k})M_i\tilde{\Xi}_i^{-1}M_i^T(I - L_{i,k}^T)\\ &= F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}(\Xi_i - M_i\tilde{\Xi}_i^{-1}M_i^T)L_{i,k}^T\\ &\quad + M_i\tilde{\Xi}_i^{-1}M_i^T + \Gamma_{i,k}.\end{aligned} \tag{20}$$

And then, with the first condition of (18), the following equation holds:

$$\begin{aligned}&F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}(\Xi_i - M_i\tilde{\Xi}_i^{-1}M_i^T)L_{i,k}^T + \Gamma_{i,k}\\ &\quad = \Xi_i - M_i\tilde{\Xi}_i^{-1}M_i^T\end{aligned}$$

which forms the stealthiness condition (15) with (19). ■

Remark 2: As shown in (13), when $N_{i,k} = 0$, the attack signal against sensor i becomes

$$z_{i,k}^a = F_{i,k}z_{i,k-\tau} + L_{i,k}z_{i,k} + b_{i,k} \tag{21}$$

which is the same as the single-sensor case in [42]. However, it is very difficult to guarantee stealthiness condition (15) due to the optimal attack matrix $L_{i,k} \neq I$ in [42]. That is to say, such an attack scheme is no longer stealthy for a multi-sensor system, which is consistent with the analysis in Remark 1. Therefore, in order to achieve both the destructiveness and stealthiness, the attack matrix $N_{i,k}$ is introduced into the attack scheme, which is the main difference with [42].

IV. Main Results

The attacker mainly aims at degrading the system estimation performance to the largest extent without being noticed by anomaly detector (9). Hence, under the stealthiness constraint (15), the objective of the attacker is formed as the following optimization problem:

$$\begin{aligned}&\max_{F_{i,k},L_{i,k},\Gamma_{i,k}} \operatorname{tr}(P_k^a)\\ &\text{s.t.}\quad F_{i,k}\Xi_i F_{i,k}^T + L_{i,k}\Theta_i L_{i,k}^T + \Gamma_{i,k} = \Theta_i\end{aligned} \tag{22}$$

where P_k^a is the posteriori estimation error covariance under attack, of which the evolution is derived in the following.

A. Estimation Performance of Compromised System

Under the attack (13), the Kalman filter (5) is rewritten as

$$\hat{x}_{k+1|k}^a = A\hat{x}_k^a \tag{23a}$$

$$\hat{x}_k^a = \hat{x}_{k|k-1}^a + KZ_k^a \tag{23b}$$

where $\hat{x}_{k|k-1}^a$ and $\hat{x}_k^a$ denote the priori and posteriori estimates under attack, respectively. The compromised estimation error covariance is given in the following theorem.

Theorem 2: The whole FDI attack duration $[k_a, k_a + \tilde{k})$ is split into the intervals $[k_a + f\tau, k_a + (f+1)\tau)$ with $f = 0, 1, \ldots, \lceil\tilde{k}/\tau\rceil - 1$, and for each attack interval, the estimation error covariance is given as follows.

1) $f = 0$: Sensor i is chosen to be attacked, and

$$\begin{aligned}P_k^a &= AP_{k-1}^a A^T + Q - K\Xi K^T\\ &\quad + K_i\Theta_i(I - L_{i,k}^T)K_i^T + K_i(I - L_{i,k})\Theta_i K_i^T.\end{aligned} \tag{24}$$

2) $f \geq 1$: Sensor j is chosen to be attacked including the following two cases:

i) $j = i$ (i.e., the attacked sensor in the current attack interval is the same as that in the previous interval)

$$\begin{aligned}P_k^a &= AP_{k-1}^a A^T + Q - K\Xi K^T\\ &\quad + K_i\Theta_i(I - L_{i,k}^T)K_i^T + K_i(I - L_{i,k})\Theta_i K_i^T\\ &\quad + A^\tau K_i(L_{i,k-\tau} - I)\Theta_i F_{i,k}^T K_i^T\\ &\quad + K_i F_{i,k}\Theta_i(L_{i,k-\tau}^T - I)K_i^T A^{\tau T}.\end{aligned} \tag{25}$$

ii) $j \neq i$ (i.e., the attacked sensor in the current attack interval is different from that in the previous interval)

$$\begin{aligned}P_k^a &= AP_{k-1}^a A^T + Q - K\Xi K^T\\ &\quad + K_j\Theta_j(I - L_{j,k}^T)K_j^T + K_j(I - L_{j,k})\Theta_j K_j^T.\end{aligned} \tag{26}$$

Proof: For the compromised filter (23), the priori and posteriori estimation errors are defined respectively as

$$e_{k|k-1}^a = x_k - \hat{x}_{k|k-1}^a$$

and

$$e_k^a = x_k - \hat{x}_k^a.$$

With (1a) and (23a), we have

$$e_{k|k-1}^a = Ae_{k-1}^a + w_{k-1}. \tag{27}$$

The priori estimation error covariance is derived as

$$\begin{aligned} P_{k|k-1}^a &= E[e_{k|k-1}^a e_{k|k-1}^{aT}] \\ &= AP_{k-1}^a A^T + Q \end{aligned} \tag{28}$$

where $P_k^a = E[e_k^a e_k^{aT}]$. And, subtracting (23b) from (1a) yields

$$e_k^a = e_{k|k-1}^a - KZ_k^a. \tag{29}$$

Thus, the posteriori estimation error covariance is obtained as

$$\begin{aligned} P_k^a = P_{k|k-1}^a &+ K\Xi K^T \\ &- E[e_{k|k-1}^a Z_k^{aT} K^T] - E[KZ_k^a e_{k|k-1}^{aT}]. \end{aligned} \tag{30}$$

Next, we only need to further derive the last two items of (30).

With (13), the next-to-last item of (30) is derived as

$$\begin{aligned} &E[e_{k|k-1}^a Z_k^{aT} K^T] \\ &= E[e_{k|k-1}^a (F_k Z_{k-\tau} + L_k Z_k + b_k)^T K^T] \\ &= E[e_{k|k-1}^a Z_{k-\tau}^T F_k^T K^T] + E[e_{k|k-1}^a Z_k^T L_k^T K^T]. \end{aligned} \tag{31}$$

Then, the last item of (31) is calculated as

$$\begin{aligned} &E[e_{k|k-1}^a Z_k^T L_k^T K^T] \\ &= E[(x_k - \hat{x}_{k|k-1}) Z_k^T L_k^T K^T] \\ &\quad + E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_k^T L_k^T K^T] \\ &= \Phi H^T L_k^T K^T + E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_k^T L_k^T K^T]. \end{aligned} \tag{32}$$

Combining (5) and (23) yields

$$\begin{aligned} &\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a \\ &= A(\hat{x}_{k-1|k-2} - \hat{x}_{k-1|k-2}^a) + AK(Z_{k-1} - Z_{k-1}^a) \\ &= A^{k-k_a}(\hat{x}_{k_a|k_a-1} - \hat{x}_{k_a|k_a-1}^a) + \sum_{t=k_a}^{k-1} A^{k-t} K(Z_t - Z_t^a) \\ &= \sum_{t=k_a}^{k-1} A^{k-t} K(Z_t - Z_t^a). \end{aligned} \tag{33}$$

Since Z_k is independent of Z_t and Z_t^a for $t < k$, the second item of (32) equals zero, i.e.,

$$E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_k^T L_k^T K^T] = 0.$$

Thus, (32) is obtained as

$$E[(x_k - \hat{x}_{k|k-1}^a) Z_k^T L_k^T K^T] = \Phi H^T L_k^T K^T. \tag{34}$$

For the first item of (31), we have

$$\begin{aligned} E[e_{k|k-1}^a Z_{k-\tau}^T F_k^T K^T] &= E[(x_k - \hat{x}_{k|k-1}) Z_{k-\tau}^T F_k^T K^T] \\ &\quad + E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_{k-\tau}^T F_k^T K^T]. \end{aligned} \tag{35}$$

With (1a) and (5), we obtain

$$\begin{aligned} x_k - \hat{x}_{k|k-1} &= A(x_{k-1} - \hat{x}_{k-1|k-2}) + w_{k-1} - AKZ_{k-1} \\ &= A^\tau (x_{k-\tau} - \hat{x}_{k-\tau|k-\tau-1}) + \sum_{t=0}^{\tau-1} A^t w_{k-t-1} \\ &\quad - \sum_{t=0}^{\tau-1} A^{t+1} KZ_{k-t-1}. \end{aligned}$$

Then, since $Z_{k-\tau}$ is independent of w_{k-t-1} and Z_{k-t} for $t < \tau$, the first item of (35) is

$$\begin{aligned} &E[(x_k - \hat{x}_{k|k-1}) Z_{k-\tau}^T F_k^T K^T] \\ &= A^\tau E[(x_{k-\tau} - \hat{x}_{k-\tau|k-\tau-1}) Z_{k-\tau}^T] F_k^T K^T \\ &\quad - A^\tau E[KZ_{k-\tau} Z_{k-\tau}^T] F_k^T K^T \\ &= A^\tau (\Phi H^T - K\Xi) F_k^T K^T \\ &= 0. \end{aligned} \tag{36}$$

With (33), the second item of (35) is

$$\begin{aligned} &E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_{k-\tau}^T F_k^T K^T] \\ &= E\left[\sum_{t=k_a}^{k-1} A^{k-t} K(Z_t - Z_t^a) Z_{k-\tau}^T F_k^T K^T\right] \\ &= E\left[\sum_{t=k_a}^{k-1} A^{k-t} K(Z_t - F_t Z_{t-\tau} - L_t Z_t - b_t) Z_{k-\tau}^T F_k^T K^T\right] \\ &= E\left[\sum_{t=k_a}^{k-1} A^{k-t} K(Z_t - L_t Z_t) Z_{k-\tau}^T F_k^T K^T\right]. \end{aligned} \tag{37}$$

When $f = 0$, i.e., $k \in [k_a, k_a + \tau)$, we have $k - \tau \in [k_a - \tau, k_a)$, which means that $E[Z_t Z_{k-\tau}^T] = 0$ for $t = k_a, k_a + 1, \ldots, k - 1$. Thus, during this attack interval, (37) becomes

$$E[(\hat{x}_{k|k-1} - \hat{x}_{k|k-1}^a) Z_{k-\tau}^T F_k^T K^T] = 0. \tag{38}$$

With (36) and (38), (35) becomes

$$E[e_{k|k-1}^a Z_{k-\tau}^T F_k^T K^T] = 0. \tag{39}$$

And, with (34) and (39), (31), i.e., the next-to-last item of (30), is obtained as

$$E[e_{k|k-1}^a Z_k^{aT} K^T] = \Phi H^T L_k^T K^T.$$

Then, the last item of (30) is derived as

$$E[KZ_k^a e_{k|k-1}^{a\,T}] = KL_k H\Phi.$$

Hence, for $k \in [k_a, k_a + \tau)$, the compromised estimation error covariance is derived as

$$P_k^a = AP_{k-1}^a A^T + Q + K\Xi K^T - \Phi H^T L_k^T K^T - KL_k H\Phi. \tag{40}$$

Furthermore, since only sensor i is attacked in $[k_a, k_a + \tau)$, substituting (11) into (40) yields

$$\begin{aligned} P_k^a &= AP_{k-1}^a A^T + Q - K\Xi K^T \\ &\quad + K\Xi(I - L_k^T) K^T + K(I - L_k)\Xi K^T \\ &= AP_{k-1}^a A^T + Q - K\Xi K^T \end{aligned}$$

$$
\begin{aligned}
&+\begin{bmatrix}K_i & \tilde{K}_i\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\begin{bmatrix}I-L_{i,k}^T & 0\\ -N_{i,k}^T & 0\end{bmatrix}\begin{bmatrix}K_i^T\\ \tilde{K}_i^T\end{bmatrix}\\
&+\begin{bmatrix}K_i & \tilde{K}_i\end{bmatrix}\begin{bmatrix}I-L_{i,k} & -N_{i,k}\\ 0 & 0\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\begin{bmatrix}K_i^T\\ \tilde{K}_i^T\end{bmatrix}\\
&=AP_{k-1}^aA^T+Q-K\Xi K^T\\
&\quad+K_i\Theta_i(I-L_{i,k}^T)K_i^T+K_i(I-L_{i,k})\Theta_iK_i^T.
\end{aligned}
$$

When $f\geq 1$, i.e., $k\in[k_a+f\tau,k_a+(f+1)\tau)$, we get $k-\tau\in[k_a+(f-1)\tau,k_a+f\tau)\in[k_a,k-1]$. Thus, (37) becomes

$$
\begin{aligned}
&E[(\hat{x}_{k|k-1}-\hat{x}_{k|k-1}^a)Z_{k-\tau}^TF_k^TK^T]\\
&\quad=E[\sum_{t=k_a}^{k-1}A^{k-t}K(Z_t-L_tZ_t)Z_{k-\tau}^TF_k^TK^T]\\
&\quad=A^\tau\Phi H^TF_k^TK^T-A^\tau KL_{k-\tau}\Xi F_k^TK^T.
\end{aligned}
$$

Thus, in this case, the compromised estimation error covariance is derived as

$$
\begin{aligned}
P_k^a=&AP_{k-1}^aA^T+Q+K\Xi K^T\\
&-\Phi H^TL_k^TK^T-A^\tau\Phi H^TF_k^TK^T+A^\tau KL_{k-\tau}\Xi F_k^TK^T\\
&-KL_kH\Phi-KF_kH\Phi A^{\tau T}+KF_k\Xi L_{k-\tau}^TK^TA^{\tau T}. \qquad (41)
\end{aligned}
$$

Then, there exist two cases: 1) The attacked sensor j is the same as sensor i in the previous attack interval (i.e., $j=i$); 2) The attacked sensor j is different from sensor i in the previous attack interval (i.e., $j\neq i$).

1) $j=i$: The compromised estimation error covariance is obtained as

$$
\begin{aligned}
P_k^a=&AP_{k-1}^aA^T+Q-K\Xi K^T\\
&+K\Xi(I-L_k^T)K^T+A^\tau K(L_{k-\tau}-I)\Xi F_k^TK^T\\
&+K(I-L_k)\Xi K^T+KF_k\Xi(L_{k-\tau}^T-I)K^TA^{\tau T}\\
=&AP_{k-1}^aA^T+Q-K\Xi K^T\\
&+K_i\Theta_i(I-L_{i,k}^T)K_i^T+K_i(I-L_{i,k})\Theta_iK_i^T\\
&+A^\tau\begin{bmatrix}K_i & \tilde{K}_i\end{bmatrix}\begin{bmatrix}L_{i,k-\tau}-I & N_{i,k-\tau}\\ 0 & 0\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\\
&\times\begin{bmatrix}F_{i,k}^T & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}K_i^T\\ \tilde{K}_i^T\end{bmatrix}\\
&+\begin{bmatrix}K_i & \tilde{K}_i\end{bmatrix}\begin{bmatrix}F_{i,k} & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\\
&\times\begin{bmatrix}L_{i,k-\tau}^T-I & 0\\ N_{i,k-\tau}^T & 0\end{bmatrix}\begin{bmatrix}K_i^T\\ \tilde{K}_i^T\end{bmatrix}A^{\tau T}\\
=&AP_{k-1}^aA^T+Q-K\Xi K^T\\
&+K_i\Theta_i(I-L_{i,k}^T)K_i^T+K_i(I-L_{i,k})\Theta_iK_i^T\\
&+A^\tau K_i(L_{i,k-\tau}-I)\Theta_iF_{i,k}^TK_i^T\\
&+K_iF_{i,k}\Theta_i(L_{i,k-\tau}^T-I)K_i^TA^{\tau T}.
\end{aligned}
$$

2) $j\neq i$: The estimation error covariance under attack is derived as

$$
\begin{aligned}
P_k^a=&AP_{k-1}^aA^T+Q-K\Xi K^T\\
&+K_j\Theta_j(I-L_{j,k}^T)K_j^T+K_j(I-L_{j,k})\Theta_jK_j^T\\
&+A^\tau K(L_{k-\tau}-I)\Xi F_k^TK^T\\
&+KF_k\Xi(L_{k-\tau}^T-I)K^TA^{\tau T}. \qquad (42)
\end{aligned}
$$

Since in the previous attack interval, only sensor i is attacked, the following equation holds:

$$
\begin{aligned}
(L_{k-\tau}-I)\Xi&=\begin{bmatrix}L_{i,k-\tau}-I & N_{i,k-\tau}\\ 0 & 0\end{bmatrix}\begin{bmatrix}\Xi_i & M_i\\ M_i^T & \tilde{\Xi}_i\end{bmatrix}\\
&=\begin{bmatrix}(L_{i,k-\tau}-I)\Xi_i+N_{i,k-\tau}M_i^T & 0\\ 0 & 0\end{bmatrix}.
\end{aligned}
$$

And further, we obtain

$$
\begin{aligned}
&(L_{k-\tau}-I)\Xi F_k^T\\
&\quad=\begin{bmatrix}(L_{i,k-\tau}-I)\Xi_i+N_{i,k-\tau}M_i^T & 0 & 0\\ 0 & 0^j & 0\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}0^i & 0 & 0\\ 0 & F_{j,k}^T & 0\\ 0 & 0 & 0\end{bmatrix}\\
&\quad=0.
\end{aligned}
$$

Hence, the compromised estimation error covariance (42) is

$$
\begin{aligned}
P_k^a=&AP_{k-1}^aA^T+Q-K\Xi K^T\\
&+K_j\Theta_j(I-L_{j,k}^T)K_j^T+K_j(I-L_{j,k})\Theta_jK_j^T.
\end{aligned}
$$

■

Remark 3: From (25), it is clear that the parameter τ directly affects the estimation error covariance when the attacked sensor is unchanged. Two cases need to be considered: 1) When A is stable, as τ increases, the last two items of (25) tend to zero, which implies that the destruction effect declines. 2) When A is unstable, it is easy to make us instinctively believe that the larger τ causes more system performance loss, but it is wrong. For a simple example ($\tau_1=1$ and $\tau_2=2$), the absolute value of the largest eigenvalue of A^{τ_2} is larger than that of A^{τ_1} with unstable A. Therefore, the trace of the last two items of (25) with $\tau_2=2$ is larger than that with $\tau_1=1$. Nevertheless, since $\tau_2>\tau_1$, the attack with τ_1 enters into the next stage earlier than that with τ_2. That is to say, for the first attack interval $[k_a,\ k_a+\tau_2)$, the compromised estimation error covariance with τ_2 becomes

$$
\begin{aligned}
P_k^{a\tau_2}=&AP_{k-1}^{a\tau_2}A^T+Q-K\Xi K^T\\
&+K_i\Theta_i(I-L_{i,k}^T)K_i^T+K_i(I-L_{i,k})\Theta_iK_i^T.
\end{aligned}
$$

Since $\tau_2>\tau_1$, the compromised estimation error covariance with τ_1 in the attack interval $[k_a,\ k_a+\tau_2)$ includes two stages: $[k_a,\ k_a+\tau_1)$ and $[k_a+\tau_1,\ k_a+\tau_2)$. For $k\in[k_a,\ k_a+\tau_1)$

$$
\begin{aligned}
P_k^{a\tau_1}=&AP_{k-1}^{a\tau_1}A^T+Q-K\Xi K^T\\
&+K_i\Theta_i(I-L_{i,k}^T)K_i^T+K_i(I-L_{i,k})\Theta_iK_i^T
\end{aligned}
$$

and for $k\in[k_a+\tau_1,\ k_a+\tau_2)$

$$
\begin{aligned}
P_k^{a\tau_1} &= AP_{k-1}^{a\tau_1}A^T + Q - K\Xi K^T \\
&\quad + K_i\Theta_i(I - L_{i,k}^T)K_i^T + K_i(I - L_{i,k})\Theta_i K_i^T \\
&\quad + A^{\tau_1}K_i(L_{i,k-\tau_1} - I)\Theta_i F_{i,k}^T K_i^T \\
&\quad + K_i F_{i,k}\Theta_i(L_{i,k-\tau_1}^T - I)K_i^T A^{\tau_1 T}.
\end{aligned}
$$

Since the trace of the last four terms of (25) is greater or equal to the trace of the last two terms of (24) under the optimal attack strategy (see (57)), with unstable A, $\mathrm{tr}(P_k^{a\tau_1}) \geq \mathrm{tr}(P_k^{a\tau_2})$ holds in the same attack duration. That is to say, when A is unstable, the result is the same as that for stable A. Hence, when the attacked sensor is unchanged, in order to degrade the estimation performance to the best extent, the parameter τ is chosen as $\tau = J$.

B. Worst-Case Attack Strategy

The main focus of this part is to search the worst-case attack strategy by solving the optimization problem (22).

Theorem 3: The optimal attack matrices $F_{i,k}^*$ and $L_{i,k}^*$ are obtained by solving the following convex optimization problems.

1) For $k \in [k_a,\ k_a + \tau)$, Sensor i Is Attacked:

$$
\begin{aligned}
&\min_{S_{i,k}} \mathrm{tr}(S_{i,k}\Psi_i) \\
&\text{s.t.} \begin{bmatrix} \Theta_i & S_{i,k} \\ S_{i,k}^T & \Lambda_i^{-1} \end{bmatrix} \geq 0
\end{aligned} \tag{43}
$$

where

$$
S_{i,k} = [F_{i,k} \quad L_{i,k}],\ \Psi_i = \begin{bmatrix} 0 \\ \Theta_i K_i^T K_i \end{bmatrix},\ \Lambda_i = \begin{bmatrix} \Xi_i & \\ & \Theta_i \end{bmatrix}.
$$

2) For $k \in [k_a + f\tau,\ k_a + (f+1)\tau)$, $f \geq 1$:

i) Sensor $j = i$ is attacked:

$$
\begin{aligned}
&\min_{S_{i,k}} \mathrm{tr}(S_{i,k}\Upsilon_{i,k}) \\
&\text{s.t.} \begin{bmatrix} \Theta_i & S_{i,k} \\ S_{i,k}^T & \Lambda_i^{-1} \end{bmatrix} \geq 0
\end{aligned} \tag{44}
$$

where

$$
\Upsilon_{i,k} = \begin{bmatrix} \Theta_i(I - L_{i,k-\tau}^T)K_i^T A^{\tau T} K_i \\ \Theta_i K_i^T K_i \end{bmatrix}.
$$

ii) Sensor $j \neq i$ is attacked:

$$
\begin{aligned}
&\min_{S_{j,k}} \mathrm{tr}(S_{j,k}\Psi_j) \\
&\text{s.t.} \begin{bmatrix} \Theta_j & S_{j,k} \\ S_{j,k}^T & \Lambda_j^{-1} \end{bmatrix} \geq 0.
\end{aligned} \tag{45}
$$

Moreover, the attack matrices $N_{i,k}^*$ and $\Gamma_{i,k}^*$ are as follows:

$$
\begin{aligned}
N_{i,k}^* &= (I - L_{i,k}^*)M_i\tilde{\Xi}_i^{-1} \\
\Gamma_{i,k}^* &= \Theta_i - S_{i,k}^*\Lambda_i S_{i,k}^{*T}.
\end{aligned}
$$

Proof: For $k \in [k_a,\ k_a + \tau)$, the trace of the compromised estimation error covariance (24) is

$$
\begin{aligned}
\mathrm{tr}(P_k^a) &= \mathrm{tr}(AP_{k-1}^a A^T + Q - K\Xi K^T) \\
&\quad + 2\mathrm{tr}(K_i\Theta_i K_i^T) - 2\mathrm{tr}(L_{i,k}\Theta_i K_i^T K_i)
\end{aligned} \tag{46}
$$

which shows that only the last term is related to the attack matrix. Hence, the optimization problem (22) is equivalent to the following problem:

$$
\begin{aligned}
&\max_{F_{i,k},L_{i,k}} -\mathrm{tr}(L_{i,k}\Theta_i K_i^T K_i) \\
&\text{s.t. } \Theta_i - F_{i,k}\Xi_i F_{i,k}^T - L_{i,k}\Theta_i L_{i,k}^T \geq 0.
\end{aligned} \tag{47}
$$

Let $S_{i,k} = [F_{i,k} \quad L_{i,k}]$, and the above stealthiness constraint is transformed into

$$
\Theta_i - S_{i,k}\Lambda_i S_{i,k}^T \geq 0
$$

which can be further converted into

$$
\begin{bmatrix} \Theta_i & S_{i,k} \\ S_{i,k}^T & \Lambda_i^{-1} \end{bmatrix} \geq 0 \tag{48}
$$

by using the Schur complement lemma. Then, the constraint optimization problem (47) is transformed into a convex optimization problem as shown in (43).

For $k \in [k_a + f\tau,\ k_a + (f+1)\tau)$, $f \geq 1$, the trace of the estimation error covariance (25) for attacked sensor $j = i$ is

$$
\begin{aligned}
\mathrm{tr}(P_k^a) &= \mathrm{tr}(AP_{k-1}^a A^T + Q - K\Xi K^T) + 2\mathrm{tr}(K_i\Theta_i K_i^T) \\
&\quad + 2\mathrm{tr}(F_{i,k}\Theta_i(L_{i,k-\tau}^T - I)K_i^T A^{\tau T} K_i) \\
&\quad - 2\mathrm{tr}(L_{i,k}\Theta_i K_i^T K_i).
\end{aligned} \tag{49}
$$

Then, the optimization problem (22) is equivalent to

$$
\begin{aligned}
&\max_{F_{i,k},L_{i,k}} \mathrm{tr}(F_{i,k}\Theta_i(L_{i,k-\tau}^T - I)K_i^T A^{\tau T} K_i - L_{i,k}\Theta_i K_i^T K_i) \\
&\text{s.t. } \Theta_i - F_{i,k}\Xi_i F_{i,k}^T - L_{i,k}\Theta_i L_{i,k}^T \geq 0
\end{aligned} \tag{50}
$$

which is converted into (44) by combining with (48).

Furthermore, for the attacked sensor case $j \neq i$, the optimization problem is formed as shown in (44) by using the same way in $[k_a,\ k_a + \tau)$.

In addition, with the solution of $F_{i,k}^*$ and $L_{i,k}^*$, the attack matrices $N_{i,k}^*$ and $\Gamma_{i,k}^*$ can also be obtained according to the stealthiness condition (15). ■

Remark 4: As shown in (43) and (45), the objective function only includes the attack matrix $L_{i,k}$ or $L_{j,k}$, which is consistent with our previous work [47]. Hence, the analytical solutions of optimization problems (43) and (45) are given as follows:

1) For $k \in [k_a,\ k_a + \tau)$:

$$
F_{i,k}^* = 0,\ L_{i,k}^* = -I,\ N_{i,k}^* = 2M_i\tilde{\Xi}_i^{-1},\ \Gamma_{i,k}^* = 0. \tag{51}
$$

2) For $k \in [k_a + f\tau,\ k_a + (f+1)\tau)$, $f \geq 1$, $j \neq i$:

$$
F_{j,k}^* = 0,\ L_{j,k}^* = -I,\ N_{j,k}^* = 2M_j\tilde{\Xi}_j^{-1},\ \Gamma_{j,k}^* = 0. \tag{52}
$$

It is clear that the optimal solutions of (43) and (45) are time-invariant matrices, as shown in (51) and (52). Reconsidering the optimization problem (44), for $k \in [k_a + \tau,\ k_a + 2\tau)$, the coefficient matrix $\Upsilon_{i,k}$ is given as

$$
\Upsilon_{i,k} = \begin{bmatrix} 2\Theta_i K_i^T A^{\tau T} K_i \\ \Theta_i K_i^T K_i \end{bmatrix}
$$

which is time-invariant. Therefore, the optimal solution of (44) is also time-invariant for $k \in [k_a+\tau,\ k_a+2\tau)$. Then, it can be concluded that in whole attack intervals, the optimal attack strategy is piecewise time-invariant.

C. Selection of Attacked Sensor

In the above subsections, the optimal attack strategy in each attack interval is derived for one arbitrarily attacked sensor i. However, different attacked sensors may cause different impacts on the system performance (see (24)–(26)). This part focuses on deriving the selection principle of the attacked sensor for the sake of maximizing the degradation of the system estimation performance under limited attack resources.

Theorem 4: In the whole attack interval, under the optimal attack strategy, the selection principle of the attacked sensor is

$$i^\star = \arg\max_i \ \mathrm{tr}(K_i\Theta_i K_i^T). \tag{53}$$

Proof: For $k \in [k_a,\ k_a+\tau)$, with the optimal attack strategy (51), the trace of the compromised estimation error covariance in (46) is

$$\mathrm{tr}(P_k^a) = \mathrm{tr}(AP_{k-1}^a A^T + Q - K\Xi K^T) + 4\mathrm{tr}(K_i\Theta_i K_i^T) \tag{54}$$

which implies that the largest last item corresponds to the sensor to be attacked, and further forms (53).

For $k \in [k_a+f\tau,\ k_a+(f+1)\tau)$, $f \geq 1$, when the attacked sensor is different from that in the previous attack interval, with the optimal attack strategy (52), the trace of the compromised estimation error covariance (26) is the same as (54). Hence, like (53), the sensor $j \neq i$ is determined by

$$j^{\star'} = \arg\max_{j\neq i} \ \mathrm{tr}(K_j\Theta_j K_j^T). \tag{55}$$

When the attacked sensor in the f-th attack interval ($f \geq 1$) is the same as that in the previous one, i.e., $j = i$, under the optimal attack strategy, the last three terms of (49) satisfy

$$\begin{aligned} &2\mathrm{tr}(K_i F_{i,k}^* \Theta_i (L_{i,k-\tau}^{*T} - I)K_i^T A^{\tau T}) \\ &\quad + 2\mathrm{tr}(K_i(I - L_{i,k}^*)\Theta_i K_i^T) \\ &\geq 2\mathrm{tr}(K_i(I - L_{i,k})\Theta_i K_i^T). \end{aligned} \tag{56}$$

If (56) is not satisfied, we have $F_{i,k}^* = 0$, and then, the optimization problem (50) is transformed into (47). Therefore, under the optimal attack strategy, considering (55), (56) becomes

$$\begin{aligned} &2\mathrm{tr}(K_i F_{i,k}^* \Theta_i (L_{i,k-\tau}^{*T} - I)K_i^T A^{\tau T}) \\ &\quad + 2\mathrm{tr}(K_i(I - L_{i,k}^*)\Theta_i K_i^T) \\ &\geq 4\mathrm{tr}(K_i\Theta_i K_i^T) \\ &\geq 4\mathrm{tr}(K_j\Theta_j K_j^T),\ j \neq i. \end{aligned} \tag{57}$$

Hence, the attacked sensor is selected according to (53), which shows that the attacked sensor is fixed in the whole attack interval. ■

V. Simulation Results

In this section, a stable system and an unstable system are provided as the target systems, and 5000 Monte Carlo simulations are run to verify the above theoretical analyses.

A. Stable System

The stable system matrix and process noise covariance matrix are randomly chosen as

$$A = \begin{bmatrix} 0.7698 & 0.5094 & 0.2197 \\ 0.0156 & 0.9127 & 0.0251 \\ 0.0073 & 0.0260 & 0.8526 \end{bmatrix},\ Q = 0.1I_3.$$

Three sensors are employed to measure the system output, and the corresponding parameters are randomly set as

$$H_1 = \begin{bmatrix} 0.6190 & 0.0597 & 0.5853 \\ 0.1034 & 0.2404 & 0.1238 \end{bmatrix},\ R_1 = 0.5I_2$$

$$H_2 = \begin{bmatrix} 0.7513 & 0.1060 & 0.6010 \\ 0.0051 & 0.8091 & 0.0593 \end{bmatrix},\ R_2 = 0.1I_2$$

$$H_3 = \begin{bmatrix} 0.5472 & 0.0493 & 0.4407 \\ 0.2386 & 0.3575 & 0.6543 \end{bmatrix},\ R_3 = 0.7I_2.$$

With (6), the Kalman filter gain is given as

$$K = [K_1 \quad K_2 \quad K_3]$$

where

$$K_1 = \begin{bmatrix} 0.0535 & 0.0112 \\ -0.0005 & 0.0346 \\ 0.0804 & 0.0109 \end{bmatrix},\ K_2 = \begin{bmatrix} 0.4159 & 0.0718 \\ 0.0485 & 0.6168 \\ 0.3112 & -0.0990 \end{bmatrix}$$

$$K_3 = \begin{bmatrix} 0.0424 & -0.0270 \\ 0.0018 & 0.0229 \\ 0.0340 & 0.1058 \end{bmatrix}.$$

The system operates in the time interval $[0, 200]$. The detection window length is set as $J = 5$. And the attacker injects attack signals in $[101, 200]$.

Define

$$\rho_f = \begin{cases} 4\mathrm{tr}(K_i\Theta_i K_i^T), & f = 0 \\ 2\mathrm{tr}(K_i F_{i,k}^* \Theta_i (L_{i,k-\tau}^{*T} - I)K_i^T A^{\tau T}) & \\ \quad + 2\mathrm{tr}(K_i(I - L_{i,k}^*)\Theta_i K_i^T), & f \geq 1. \end{cases}$$

For $\tau = 5$, the values of ρ_f for each sensor under different attack intervals are shown in Fig. 2. It is clear that, when sensor 2 is attacked, the values of ρ_f are larger than those of the other two sensors. Furthermore, ρ_f with $f \geq 1$ is always larger than ρ_0. Therefore, the selection principle of the attacked sensor applies to the whole attack interval. And then, for $\tau = 5$, the estimation performance of the system with different attacked sensors is shown in Fig. 3, which is consistent with the result in Fig. 2. Furthermore, the randomly attacked sensor scheme, which selects the attacked sensor with a same probability for each attack interval, is adopted (see green line in Fig. 3), which further illustrates the effectiveness of the selection principle of the attacked sensor.

Next, for the attacked sensor 2, three experiments under different τ: $\tau = 5$, $\tau = 15$ and $\tau = 25$, are conducted. Furthermore, an attack scheme without considering historical residuals investigated in [47] is adopted for comparison. The corresponding simulation results are shown in Fig. 4, which clearly shows that, as the value of τ increases, the corresponding esti-

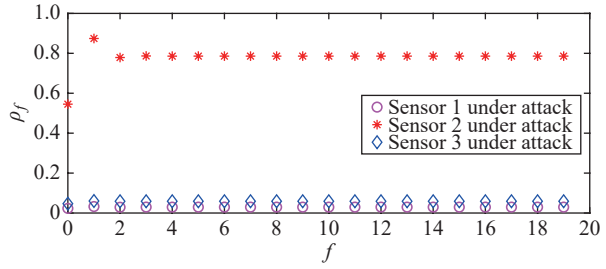

Fig. 2. The values of ρ_f for the stable system under $\tau = 5$.

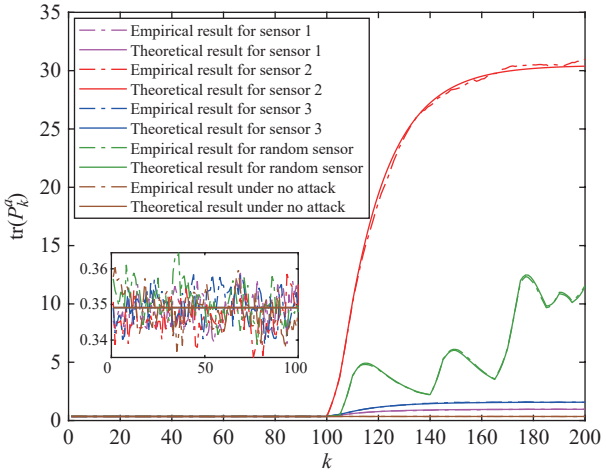

Fig. 3. The estimation errors of the stable system with different attacked sensors under $\tau = 5$.

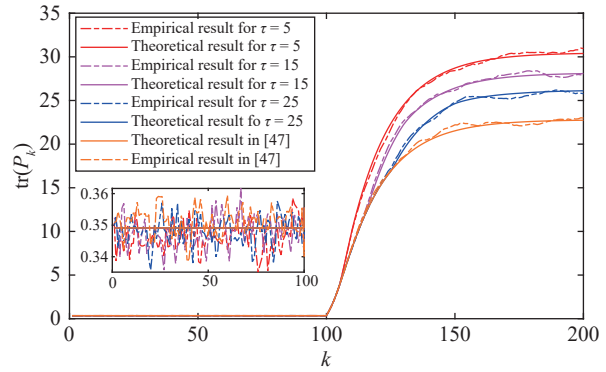

Fig. 4. The estimation errors of the stable system with attacked sensor 2 under different τ.

mation error decreases, which is consistent with Remark 3. And, compared with the effect of the attack scheme [47] (see orange line in Fig. 4), the proposed attack scheme based on the historical and current residuals causes more loss of system estimation performance. In addition, from all the above experiments (Figs. 3 and 4), it is easy to see that the empirical results are extremely close to the theoretical results, which directly verifies the theoretical analysis.

In order to show the stealthiness of the proposed attack scheme, the detection index under $\tau = 5$ is shown in Fig. 5. It shows that the distribution of the detection index has no change in the normal and compromised situations, which means that the proposed attack scheme can successfully evade

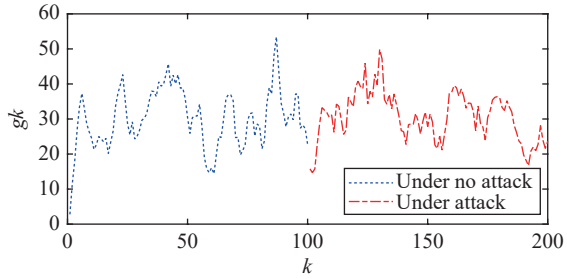

Fig. 5. The detection index of the stable system with attacked sensor 2 under $\tau = 5$.

the anomaly detector.

B. Unstable System

An unstable system is considered with

$$A = \begin{bmatrix} 1.0063 & 0.3023 & 0.2459 \\ 0.0035 & 0.7514 & 0.4268 \\ 0.0012 & 0.0025 & 0.6105 \end{bmatrix}.$$

Other parameters are the same as those in the stable system case. And, the Kalman filter gain is

$$K = [K_1 \quad K_2 \quad K_3]$$

where

$$K_1 = \begin{bmatrix} 0.0727 & 0.0054 \\ 0.0022 & 0.0354 \\ 0.0543 & 0.0159 \end{bmatrix}, \; K_2 = \begin{bmatrix} 0.5033 & -0.0929 \\ 0.0359 & 0.6136 \\ 0.2113 & 0.0814 \end{bmatrix}$$

$$K_3 = \begin{bmatrix} 0.0524 & -0.0201 \\ 0.0007 & 0.0383 \\ 0.0224 & 0.0829 \end{bmatrix}.$$

The simulation results are displayed in Figs. 6−9, which are similar to those in the aforementioned stable system simulation case. In addition, it is worth noting that the estimation errors of the unstable system under attack diverge, which means that the unstable system is very weak when facing the attack.

VI. Conclusion

This paper has explored how to design the stealthy attack strategy to maximally degrade the estimation performance of a multi-sensor system under limited attack resources. A stealthy FDI attack scheme based on historical and current residuals has been proposed against partial sensors. The attack stealthiness condition has been derived for the sake of bypassing the residual-based detector. Then, the compromised estimation

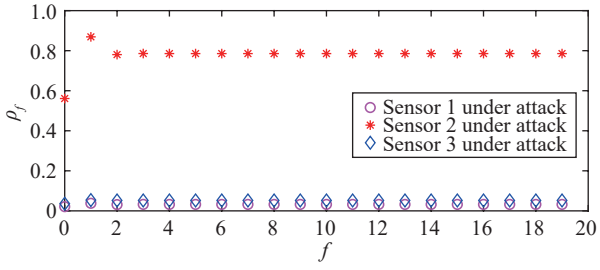

Fig. 6. The values of ρ_f for the unstable system under $\tau = 5$.

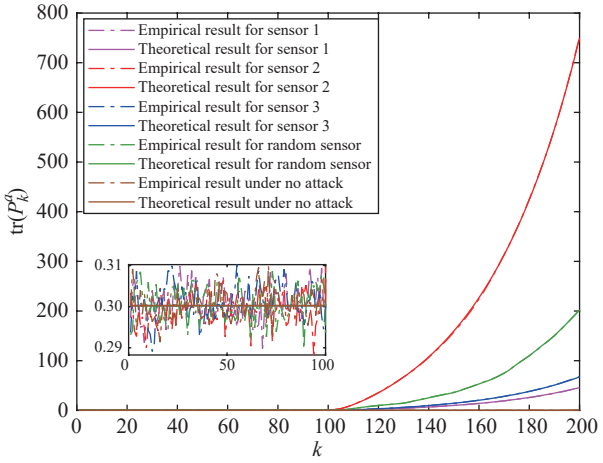

Fig. 7. The estimation errors of the unstable system with different attacked sensors under $\tau = 5$.

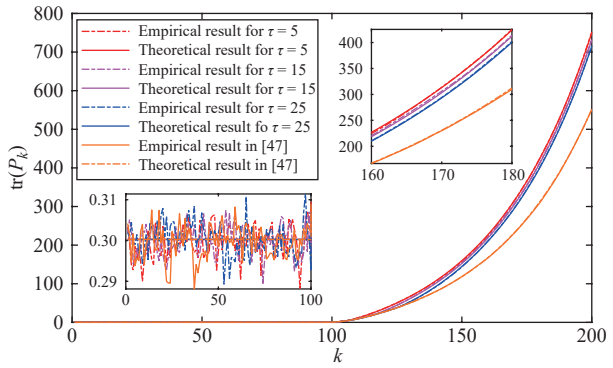

Fig. 8. The estimation errors of the unstable system with attacked sensor 2 under different τ.

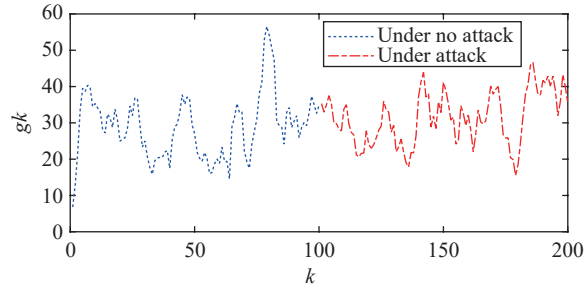

Fig. 9. The detection index of the unstable system with attacked sensor 2 under $\tau = 5$.

error covariance has been given and used to quantify the system performance under attack. And, it has been analyzed and determined to utilize which time instants of historical data to design the attack signals to cause more attack effect. Several convex optimization problems have been formed to obtain the optimal attack strategy for each attack interval. Moreover, the selection principle of the attacked sensor has been derived by analyzing which sensor is attacked to cause the worst effect on the system. Finally, some simulation results have been provided to verify the theoretical analyses and demonstrate the superiority of the proposed attack scheme.

It is noted that the design of the stealthy attack scheme has been studied for the security of multi-sensor remote estimation systems. However, our ultimate goal is to construct effective attack detection methods and secure estimation methods against such an attack [48], [49], which are much more challenging and will be further explored in our future work.

REFERENCES

[1] X. M. Zhang, Q.-L. Han, X. H. Ge, D. R. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.

[2] C. Song, L. Liu, G. Feng, Y. Fan, and S. Y. Xu, "Coverage control for heterogeneous mobile sensor networks with bounded position measurement errors," *Automatica*, vol. 120, p. 109118, Oct. 2020.

[3] D. R. Ding, Q.-L. Han, X. H. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 51, no. 1, pp. 176–190, Jan. 2021.

[4] Z. H. Pang, C. D. Bai, G. P. Liu, Q.-L. Han, and X. M. Zhang, "A novel networked predictive control method for systems with random communication constraints," *J. Syst. Sci. Complex.*, vol. 34, no. 4, pp. 1364–1378, Feb. 2021.

[5] J. Hu, C. Q. Jia, H. Yu, and H. J. Liu, "Dynamic event-triggered state estimation for nonlinear coupled output complex networks subject to innovation constraints," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 941–944, May 2022.

[6] G. Y. Wu, G. Wang, J. Sun, and J. Chen, "Optimal partial feedback attacks in cyber-physical power systems," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3919–3926, Sept. 2020.

[7] Z. H. Pang, W. C. Luo, G. P. Liu, and Q.-L. Han, "Observer-based incremental predictive control of networked multi-agent systems with random delays and packet dropouts," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 68, no. 1, pp. 426–430, Jan. 2021.

[8] C. B. Zheng, Z. H. Pang, J. X. Wang, J. Sun, G. P. Liu, and Q.-L. Han, "Null-space-based time-varying formation control of uncertain nonlinear second-order multi-agent systems with collision avoidance," *IEEE Trans. Ind. Electron.*, to be published

[9] J. Chen, J. Sun, and G. Wang, "From unmanned systems to autonomous intelligent systems," *Engineering*, vol. 12, pp. 16–19, May 2022.

[10] W. L. Duo, M. C. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 784–800, May 2022.

[11] Z. H. Pang, L. Z. Fan, Z. Dong, Q.-L. Han, and G. P. Liu, "False data injection attacks against partial sensor measurements of networked control systems," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 69, no. 1, pp. 149–153, Jan. 2022.

[12] H. B. Guo, J. Sun, Z. H. Pang, and G. P. Liu, "Event-based optimal stealthy false data-injection attacks against remote state estimation systems," *IEEE Trans. Cybern.*, 2023. DOI: 10.1109/TCYB.2023.3255583.

[13] W. Y. Xu, Z. D. Wang, L. Hu, and J. Kurths, "State estimation under joint false data injection attacks: Dealing with constraints and insecurity," *IEEE Trans. Autom. Control*, vol. 67, no. 12, pp. 6745–6753, Dec. 2022.

[14] F. Y. Hou, J. Sun, Q. L. Yang, and Z. H. Pang, "Deep reinforcement learning for optimal denial-of-service attacks scheduling," *Sci. China Inf. Sci.*, vol. 65, no. 6, p. 162201, Jun. 2022.

[15] X. H. Ge, Q.-L. Han, M. Y. Zhong, and X. M. Zhang, "Distributed Krein space-based attack detection over sensor networks under deception attacks," *Automatica*, vol. 109, p. 108557, Nov. 2019.

[16] D. Ye and T. Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, Jun. 2020.

[17] Z. H. Pang, L. Z. Fan, J. Sun, K. Liu, and G. P. Liu, "Detection of stealthy false data injection attacks against networked control systems via active data modification," *Inf. Sci.*, vol. 546, pp. 192–205, Feb. 2021.

[18] H. B. Guo, Z. H. Pang, J. Sun, and J. Li, "An output-coding-based detection scheme against replay attacks in cyber-physical systems," *IEEE Trans. Circuits Syst. II: Express Briefs*, vol. 68, no. 10, pp. 3306–3310, Oct. 2021.

[19] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: A survey," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 3, pp. 377–391, Mar.

2022.

[20] H. B. Guo, Z. H. Pang, J. Sun, and J. Li, "Detection of stealthy false data injection attacks against cyber-physical systems: A stochastic coding scheme," *J. Syst. Sci. Complex.*, vol. 35, no. 5, pp. 1668–1684, Aug. 2022.

[21] Y. L. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[22] W. Ao, Y. D. Song, and C. Y. Wen, "Distributed secure state estimation and control for CPSs under sensor attacks," *IEEE Trans. Cybern.*, vol. 50, no. 1, pp. 259–269, Jan. 2020.

[23] H. C. Xiao, D. R. Ding, H. L. Dong, and G. L. Wei, "Adaptive event-triggered state estimation for large-scale systems subject to deception attacks," *Sci. China Inf. Sci.*, vol. 65, no. 2, p. 122207, Feb. 2022.

[24] D. Zhang, C. Deng, and G. Feng, "Resilient cooperative output regulation for nonlinear multi-agent systems under DoS attacks," *IEEE Trans. Autom. Control*, vol. 68, no. 4, pp. 2521–2528, Apr. 2023.

[25] Z. H. Pang and G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sept. 2012.

[26] S. Feng, A. Cetinkaya, H. Ishii, P. Tesi, and C. De Persis, "Networked control under DoS attacks: Tradeoffs between resilience and data rate," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 460–467, Jan. 2021.

[27] B. Chen, Y. W. Tan, Z. Sun, and L. Yu, "Attack-resilient control against FDI attacks in cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 6, pp. 1099–1102, Jun. 2022.

[28] W. J. Liu, J. Sun, G. Wang, F. Bullo, and J. Chen, "Resilient control under quantization and denial-of-service: Codesigning a deadbeat controller and transmission protocol," *IEEE Trans. Autom. Control*, vol. 67, no. 8, pp. 3879–3891, Jun. 2022.

[29] X. H. Ge, Q.-L. Han, Q. Wu, and X. M. Zhang, "Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks," *IEEE/CAA J. Autom. Sinica*, 2022. DOI: 10.1109/JAS.2022.105845.

[30] E. Kung, S. Dey, and L. Shi, "The performance and limitations of ϵ-stealthy attacks on higher order systems," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 941–947, Feb. 2017.

[31] C. Z. Bai, V. Gupta, and F. Pasqualetti, "On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds," *IEEE Trans. Autom. Control*, vol. 62, no. 12, pp. 6641–6648, Dec. 2017.

[32] Z. H. Pang, G. P. Liu, D. H. Zhou, F. Y. Hou, and D. H. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, May 2016.

[33] Z. Pang, Y. Fu, H. Guo, and J. Sun, "Analysis of stealthy false data injection attacks against networked control systems: Three case studies," *J. Syst. Sci. Complex*, 2023. DOI: 10.1007/s11424-022-2120-6.

[34] Y. Chen, S. Kar, and J. M. F. Moura, "Cyber-physical attacks with control objectives," *IEEE Trans. Autom. Control*, vol. 63, no. 5, pp. 1418–1425, May 2018.

[35] Y. Chen, S. Kar, and J. M. F. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 1157–1168, Sept. 2018.

[36] Q. R. Zhang, K. Liu, Y. Q. Xia, and A. Y. Ma, "Optimal stealthy deception attack against cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 9, pp. 3963–3972, Sept. 2020.

[37] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.

[38] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, Mar. 2018.

[39] Y. G. Li and G. H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Inf. Sci.*, vol. 481, pp. 474–490, May 2019.

[40] J. Shang, H. Yu, and T. W. Chen, "Worst-case stealthy innovation-based linear attacks on remote state estimation under Kullback-Leibler divergence," *IEEE Trans. Autom. Control*, vol. 67, no. 11, pp. 6082–6089, Nov. 2022.

[41] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Worst-case innovation-Based integrity attacks with side information on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 6, no. 1, pp. 48–59, Mar. 2019.

[42] Y. G. Li and G. H. Yang, "Optimal stealthy innovation-based attacks with historical data in cyber-physical systems," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 51, no. 6, pp. 3401–3411, Jun. 2021.

[43] J. Shang and T. W. Chen, "Optimal stealthy integrity attacks on remote state estimation: The maximum utilization of historical data," *Automatica*, vol. 128, p. 109555, Jun. 2021.

[44] H. X. Liu, Y. Q. Ni, L. H. Xie, and K. H. Johansson, "How vulnerable is innovation-based remote state estimation: Fundamental limits under linear attacks," *Automatica*, vol. 136, p. 110079, Feb. 2022.

[45] Y. Z. Li, L. Shi, and T. W. Chen, "Detection against linear deception attacks on multi-sensor remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 3, pp. 846–856, Sept. 2018.

[46] Z. Y. Guo, D. W. Shi, K. H. Johansson, and L. Shi, "Worst-case analysis of innovation-based linear attack on remote state estimation with resource constraint," in *Proc. IEEE 55th Conf. Decision and Control*, Las Vegas, USA, 2016, pp. 6303–6308.

[47] H. B. Guo, J. Sun, and Z. H. Pang, "Stealthy false data injection attacks with resource constraints against multi-sensor estimation systems," *ISA Trans.*, vol. 127, pp. 32–40, Aug. 2022.

[48] Z. H. Pang, L. Z. Fan, H. B. Guo, Y. T. Shi, R. Q. Chai, J. Sun, and G. P. Liu, "Security of networked control systems subject to deception attacks: A survey," *Int. J. Syst. Sci.*, vol. 53, no. 16, pp. 3577–3598, Nov. 2022.

[49] C. Trapiello and V. Puig, "A zonotopic-based watermarking design to detect replay attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 11, pp. 1924–1938, Nov. 2022.

Haibin Guo received the B.Sc. degree in applied physics from the Shandong University of Science and Technology in 2017. He is currently pursuing the Ph.D. degree in control science and engineering at the National Key Laboratory of Autonomous Intelligent Unmanned Systems, School of Automation, Beijing Institute of Technology. His research interests include networked control systems, attack modeling and detection, and security of cyber-physical systems.

Jian Sun (Senior Member, IEEE) received the B.Eng. degree in electrical engineering from the Jilin Institute of Technology in 2001, the M.Eng. degree in mechatronical engineering from the Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences (CAS) in 2004, and the Ph.D. degree in control theory and control engineering from the Institute of Automation, CAS, in 2007. From 2008 to 2009, he was a Research Fellow with the University of Glamorgan, UK. From 2007 to 2010, he was a Postdoctoral Research Fellow with the Beijing Institute of Technology. In 2010, he joined the School of Automation, Beijing Institute of Technology, where he has been a Professor since 2013. His research interests include networked control systems, time-delay systems, and security of cyber-physical systems. He is an Editorial Board Member of the *IEEE Transactions on Systems*, *Man and Cybernetics*: *Systems*, and *the Journal of Systems Science and Complexity*.

Zhong-Hua Pang (Senior Member, IEEE) received the B.Eng. degree in automation and M.Eng. degree in control theory and control engineering from the Qingdao University of Science and Technology, in 2002 and 2005, respectively, and the Ph.D. degree in control theory and control engineering from the Institute of Automation, Chinese Academy of Sciences in 2011. He was a Postdoctoral Research Fellow with the Tsinghua University, from September 2011 to February 2014, a Visiting Scholar at the University of South Wales, UK from Nov. 2016 to Oct. 2017, and a Visiting Scholar at the Swinburne University of Technology, Australia from July 2019 to August 2019 and from January 2020 to March 2020, respectively. Since 2014, he has been with the North China University of Technology, first as an Associate Professor and since 2017 as a Professor. His research interests include networked control systems, multi-agent systems, security of cyber-physical systems, and data-driven control systems.