Sparse Actuator and Sensor Attacks Reconstruction for Linear Cyber-physical Systems with Sliding Mode Observer

Hongyan Yang, Shen Yin, Honggui Han, and Haoyuan Sun

Abstract—**Driven by the rapid development of modern industrial processes, Cyber-Physical Systems (CPSs), which tightly conjoin computational and physical resources, have become ever more prevalent during recent years. However, due to the intrinsical vulnerability of the cyber layer, the system performances of CPSs are easily degraded by malicious false data injection (FDI) attacks which are launched by adversary. In this work, the issue of secure reconstruction is considered for linear CPSs with simultaneous sparse actuator and sensor attacks. First, an adaptive counteraction searching strategy is proposed to identify the potential combinational attack mode. In this way, malicious FDI attacks are excluded. Second, by constructing a descriptor switched sliding mode observer (SMO), the sparse FDI attacks and the system state are reconstructed effectively. Meanwhile, sufficient conditions of the error convergence can be derived. Finally, a numerical simulation is utilized to illustrate the applicability of the proposed theoretical derivation.**

Index Terms—**Sparse attack and state estimations, switched systems, descriptor sliding mode observer, cyber-physical systems.**

I Introduction

With the rapid development of modern industrial processes, increasing attention has been paid to Cyber-Physical Systems (CPSs) which can maintain the normal operation of many critical processes, such as intelligent vehicles [1], [2], healthcare systems [3], smart grids [4] those people rely on. From the perspective of interdiscipline, CPSs can deeply integrate control, computation, communication, cloud and cognition [5]. However, with the networked control technique embedded, CPSs become more vulnerable compared with traditional control systems, i.e., malicious cyber attacks can be launched by an adversary anywhere from sensor channels to actuator channels to degrade system performance. In other words, if an attack is successfully launched by an adversary at the network layer, it may induce serious failures or faults at the physical layer. Consequently, cyber attacks have become one of the main factors threatening the security of CPSs. Thought-provoking accidents related to cyber security such as RQ-170, Stuxnet and Jeep hack [6], [7] indicate that protecting security of CPSs is a critical issue in current.

Generally, cyber attacks can be roughly categorized into two classes: deception attacks and denial-of-service (DoS) attacks [8]. The purpose of DoS is compromising data exchangeability and availability by consuming computation or communication resources maliciously. Different from DoS, deception attacks aim to temper data trustworthiness by manipulating packets via communication networks [9]. Besides, model knowledge and/or disclosure resources are also necessary for deception attackers [10]. False data injection (FDI) attacks are considered as a class of typical deception attacks and fruitful results on the research of security issues of CPSs under FDI attacks have yielded recently, such as stealthy attack detection [11], [12], attack-resilient controller design [13]–[15], data integrity requirements relaxation [16], hybrid attack mitigation policy [17], distributed attack identification monitors [18], attack detection and identification [4], [19], [20] and so on.

Apart from the above significant results on security subjects of CPSs, considerable efforts have been paid to the issue of secure state estimation, the purpose of which is to reconstruct the system state from sporadic corruptions, i.e., sparse attacks. The construction of unobservable sparse attack vectors has been analyzed by data sparsity properties in [21]. Till now, there are two mainstream techniques, i.e., optimization relaxation (OR) and brute force search (BFS), to cope with the secure state estimation problem of CPSs. Several algorithms such as satisfiability modulo solvers [22], projected gradient-descent paradigms [23], optimal graph searching [24] and L_1/L_r decoders [25] belong to OR and the basic idea of which is to find the optimal solution in polynomial time. For BFS, a number of excellent results including observability Gramians [26], switched counteraction principle (SCP) [19] and identification filter [18] have been obtained.

In addition to the secure state estimation issue, several researchers have also noticed the significance of attack signal reconstruction [19], [27], [28]. A successful attack reconstruction scheme can monitor abnormal hijacking more reliably. How to achieve secure state estimation and attack reconstruction simultaneously in the context of BFS and ensure the convergence of the error system? Since any successful attack on CPSs may lead to catastrophic system failures and cause

Manuscript received ; revised ; accepted . This work was supported by National Natural Science Foundation of China under Grants 6210021576, 61890930-5, 61903010, 62021003 and 62125301, National Key Research and Development Project under Grant 2018YFC1900800-5, Beijing Outstanding Young Scientist Program under Grant BJJWZYJH01201910005020 and China Postdoctoral Science Foundation under Grant 2020M680275 and 2021T140032.

Hongyan Yang, Honggui Han and Haoyuan Sun are with Faculty of Information Technology, Beijing Key Laboratory of Computational Intelligence and Intelligent System, Engineering Research Center of Digital Community, Ministry of Education, Beijing Artificial Intelligence Institute and Beijing Laboratory for Intelligent environmental protection, Beijing University of Technology, Beijing, China. Shen Yin is with the Department of Mechanical and Industrial Engineering, Norwegien University of Science and Technology, Norway. (Email of Corresponding author Honggui Han: Rechardhan@sina.com.)

This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221

unbearable losses, in turn, this becomes a profit motive and means for opponents in reality. Therefore, it is of great significance to find the answer to this question for both academic and practical applications. The authors of [19] proposed a observer with a switching function matrix (SFM) to reconstruct the system state and sparse sensor attacks. Then, the designed SFM can turn off the attacked input channels automatically. In [29], a sliding mode observer (SMO)-based secure estimation scheme was developed for linear discrete-time CPSs with sparse sensor attacks and unknown input. Furthermore, the secure estimation issue was considered in the work [28] under the framework of sparse actuator and sensor attacks, and a defence strategy with a set cover approach was developed to relax the computation burden caused by combinational BFS. Recently, in [27], the authors designed two kinds of descriptor sliding mode observers to reconstruct the state and attack signals by augmenting the original system into a singular system. However, since the augmented system is singular, it inevitably increases the complexity of the design scheme, which motivates us for this further study. Besides, due to the utilization of the coordinate transformation technique in [27], there exists jumps in the system states after transformation, which may affect system performance. This is another reason that motivates us to carry out this research.

Based on the above observation, we investigate the secure state estimation and attack reconstruction issue for linear CPSs under sparse actuator and sensor attacks. Firstly, to identify the potential combinational attack mode, an adaptive counteraction searching strategy is proposed and then sparse FDI attacks are excluded. Secondly, to reconstruct the state and attack signals of CPSs, a descriptor switched SMO is developed. Meanwhile, sufficient conditions of the error convergence can be derived. Finally, a numerical example and a comparative simulation are utilized to demonstrate the applicability of the proposed theoretical derivation.

The main contributions of this work can be summarized in the following three aspects: (1) an effective attack reconstruction method which can simultaneously reconstruct the state, sparse actuator and sensor attacks of linear CPSs is developed; (2) the proposed SMO is constructed based on a regular augmented system approach (instead of a singular augmented system [27]), which decreases the complexity of the design scheme; (3) an adaptive switching algorithm (rather than OR technique) is employed and the sufficient conditions of the existence of the developed SMO can be obtained by only solving a set of linear matrix inequalities. Therefore, the computation burden is relaxed.

The structure of this paper is provided as follows. Section II gives the description of the notations, the system model and attack model and meanwhile describes the heuristic statements and formulates the main target. Section III gives main results of this work, including SMO construction, observer error derivation, dynamic analysis and a summary of the whole design procedures. Section IV presents a numerical simulation to illustrate the effectiveness of the developed observer and the conclusion is given in Section V.

II Problem Formulation

A. Notation Description

$\mathrm{Card}(\mathcal{G})$ represents the cardinality of a set $\mathcal{G}$. $\mathcal{D}(\mathcal{G}_1, \mathcal{G}_2)$ denotes the cartesian product of $\mathcal{G}_1$ and $\mathcal{G}_2$. For $a, b \in N^+$ with $a > b$, the binomial coefficient is C_a^b. $\{1, 2, \ldots, a\}$ is depicted by $[a]$.

For a vector $v \in \mathbb{R}^q$, the support of v is defined by $\mathrm{Supp}(v) = \{i \in [q] : v_i \neq 0\}$. If $\mathrm{Card}(\mathrm{Supp}(v)) = p$, the vector v is p-sparse. Besides, $\bar{0}$ and $\mathbf{0}$ represent the null vector and null matrix, respectively. For a matrix $\Xi \in \mathbb{R}^{m\times n}$, the superscripts "$T$, "† and "$-1$ (if $m \neq n$) denote the transposition, pseudo inversion and inversion, respectively. I denotes identity matrix with proper dimensions. I_Q denotes a matrix obtained from setting all diagonal entries indexed by Q of I as zeros.

B. Plant Model and Attack Description

Consider the following linear CPSs under FDI attacks:

$$\begin{cases} \dot{x}(t) &= Ax(t) + Bu(t) + F_a a_a(t), \\ y(t) &= Cx(t) + a_s(t) + F_d d(t), \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y(t) \in \mathbb{R}^p$ and $d(t) \in \mathbb{R}^d$ denote the plant state, input, output and the measurement noise, respectively. $a_a(t) = \left[a_{a1}(t), a_{a2}(t), \ldots, a_{ak}(t)\right]^T \in \mathbb{R}^k$ and $a_s(t) = \left[a_{s1}(t), a_{s2}(t), \ldots, a_{sp}(t)\right]^T \in \mathbb{R}^p$ represent the *r*-sparse actuator attack and the *s*-sparse sensor attack, respectively. *r*-sparse and *s*-sparse mean that the number of nonzero elements in $a_a(t)$ and $a_s(t)$ are no more than *r* and *s*, respectively. Besides, $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$, $F_a \in \mathbb{R}^{n\times a}$ and $F_d \in \mathbb{R}^{p\times d}$ are system matrices.

In this work, the sparse attacks considered belong to FDI attacks which are commonly existed in modern industry with the purpose of disrupting the system normal operation by misleading the system components [7]. Denote $\coprod_a = \{1, 2, \ldots, k\} = [k]$ as the index set of actuator, and $\coprod_s = \{1, 2, \ldots, p\}$ as the sensor index set, respectively. Then, for $i \in \coprod_a$,

$$a_{ai}(t) = \begin{cases} nonzero, & \text{if the } i\text{-th actuator is attacked;} \\ 0, & \text{otherwise.} \end{cases}$$

Similarly, for $j \in \coprod_s$,

$$a_{sj}(t) = \begin{cases} nonzero, & \text{if the } j\text{-th sensor is attacked;} \\ 0, & \text{otherwise.} \end{cases}$$

Due to the considered actuator and sensor attacks are *r*-sparse and *s*-sparse, the number of attacked actuators is no more than $r \in \mathbb{Z}^+$, $r \leq k$ and the number of attacked sensors is no more than $s \in \mathbb{Z}^+, s \leq p$. Define $\mathcal{M} = \{\Theta \subset \coprod_a | \mathrm{Card}(\Theta) = r\}$ and $\mathcal{N} = \{\Pi \subset \coprod_s | \mathrm{Card}(\Pi) = s\}$ as the combinational sets of actuator and sensor attacks, respectively. Obviously, we have $\mathrm{Card}(\mathcal{M}) = C_k^r$ and $\mathrm{Card}(\mathcal{N}) = C_p^s$.

To facilitate the subsequent analysis, the following assumptions are introduced.

(A1) The adversary can attack actuators and sensors synchronously. In addition, $\mathrm{Supp}(a_a(t))$ and $\mathrm{Supp}(a_s(t))$ are constant over time.

(A2) The considered sparse actuator attacks, sparse sensor attacks and measurement noises in this work satisfy:

$$||a_{ai}(t)|| \leq \alpha_{a1}, ||\dot{a}_{ai}(t)|| \leq \alpha_{a2},$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221, IEEE Transactions on Industrial Informatics

$$||a_{sj}(t)|| \leq \beta_{s1}, ||\dot{a}_{sj}(t)|| \leq \beta_{s2},$$
$$||d(t)|| \leq \bar{d}_1, ||\dot{d}(t)|| \leq \bar{d}_2$$

where $i = 1, \ldots, a$, $j = 1, \ldots, p$. α_{a1}, α_{a2}, β_{s1}, β_{s2}, $\bar{d}_1$ and $\bar{d}_2$ are prescribed positive constants.

(A3) The number of attacked sensors and actuators satisfying $s \leq p/2$ and $r \leq a$.

Remark 1: It is worthy noting that an actuator attack can be regarded as the bias corruptions on the actuators or on the channels of controller-to-actuator. Similarly, an sensor attack can be considered as the bias corruptions on the sensors or on the channels of sensor-to-device [25]. The above assumptions are reliable. Assumption (A1) indicates that the sensor and actuator attacks can be launched synchronously by an adversary and the attack signals $a_a(t)$ and $a_s(t)$ do not need to follow any particular models. Assumption (A2) gives rational limitations on the energy of the adversary since there always exist physical limitations in practical CPSs. Assumption (A3) is the sparse limitations which is borrowed from the works [19], [22], [23], [27]. The sparse constraint on attacked sensors and/or actuators are analysed by either contradiction proof [23] or rank criterion [19], [27].

Remark 2: There is one principle for attack signal description: the fewer mathematical constraints one rely on, the more effective secure estimation can be obtained. Therefore, in addition to the above assumptions, no further ones are employed to restrict the injected attacks.

Till now, all potential entry modes can be described by $\mathcal{C} = \mathcal{D}(\mathcal{M}, \mathcal{N})$, which further implies $\eta = \mathrm{J}(\mathcal{C}) \in [\bar{\eta}] \setminus \{1\}$, where $\bar{\eta} = C_k^r C_p^s + 1$ and J represents the cartesian product operator. Furthermore, $\eta = 1$ stands for the attack-free case. In addition, $\mathcal{C}_a^* = \mathcal{D}(\Theta^*, \Pi^*)$ is utilized to depict the desired mode, and correspondingly, $\eta* = \mathrm{J}(\mathcal{C}_a^*)$.

C. Heuristic Statements

In this work, the switched counteraction principle is employed to exclude the sparse corruptions with the help of an adaptive switching mechanism. The entry matrices are defined as $(I_a)_\Theta$ and $(I_s)_\Pi$, which implies that $(I_a)_{\Theta*} a_a(t) = \bar{0}$ and $(I_s)_{\Pi*} a_s(t) = \bar{0}$. Then, we hold $(\bar{I}_a)_{\Theta*} = I_a - (I_a)_{\Theta*}$ and $(\bar{I}_s)_{\Pi*} = I_s - (I_s)_{\Pi*}$ trivially. By now, the original CPSs (1) is tuned as follows:

$$\left\{ \begin{array}{rcl} \dot{x}(t) &=& Ax(t) + Bu(t) + F_{a\eta} a_a(t), \\ \bar{y}(t) &=& C_\eta x(t) + I_{p\eta} a_s(t) + F_{d\eta} d(t), \end{array} \right. \tag{2}$$

where $\bar{y} = (I_p)_\Pi y(t)$ is detectable. In the rest of this paper, for $\eta \in [\bar{\eta}]$, we represent $F_a(I_a)_\Theta$, $(I_p)_\Pi C$, $(I_p)_\Pi$ and $(I_p)_\Pi F_d$ by $F_{a\eta}$, C_η, $I_{p\eta}$ and $F_{d\eta}$ for notation simplicity, respectively.

In order to formulate the heuristic problems, the switching logic is better to be proposed in advance. Firstly, we define an auxiliary observed indicator in the following form:

$$\dot{\Psi}(t) = \left\{ \begin{array}{ll} \Phi(t)(||\tilde{e}_y(t)|| - \sigma)^2, & \text{if } ||\tilde{e}_y(t)|| > \sigma \\ 0, & \text{otherwise}, \end{array} \right. \tag{3}$$

where $\tilde{e}_y(t) = \bar{e}_y(t) + I_{p\eta} a_s(t)$. $\bar{e}_y(t)$ and σ will be determined later. $\Phi(t)$ is given by

$$\Phi(t) = \left\{ \begin{array}{ll} (\epsilon \Psi(t) + \varsigma)^{-1}, & \text{if } (\epsilon \Psi(t) + \varsigma)^{-1} > \bar{\Phi} \\ \bar{\Phi}, & \text{otherwise}, \end{array} \right. \tag{4}$$

where ϵ and ς are prescribed positive constants which satisfy $\varsigma^{-1} > \bar{\Phi}$. $\bar{\Phi}$ will be determined in the dynamic analysis part. Then, the switching logic can be proposed as

$$\eta(\Psi(t)) = \mathrm{Ceil}(\mathrm{Mod}(\Psi(\mathrm{t}), \bar{\eta})), \tag{5}$$

where $\mathrm{Ceil}(p)$ represents the ceiling function, i.e., the minimum integer is no less than p with $p \in \mathbb{R}^+$. $\mathrm{Mod(p, q)}$ represents the residual operator, i.e., the remainder after division of p by q.

Remark 3: It can be observed that the switching logic (5) is relied on the auxiliary indicator (3). In the work [19], $\Phi(t)$ is selected as a constant and this inevitably results in a slow increase of $\Psi(t)$ in (3). Consequently, the convergence of $\eta(t)$ in (5) is dull. While $\Phi(t)$ in the form of Eq. (4) will potentially speed up the convergence as $\Psi(t)$ increases and then assign $\Phi(t) = \bar{\Phi}$.

In the next, we conclude the problems of interest in the following three aspects.

(1) By considering the sparse FDI attacks on both actuator and sensor channels, how to construct a descriptor SMO combined with the switched counteraction principle to implement the attack and state reconstructions online?

(2) After design the developed SMO, how to derive the parameters of SMO and ensure the correctness of the attack and state reconstructions?

(3) Since the purpose is to construct an adaptive switching descriptor SMO, how to design suitable sliding motions is also an interesting problem.

III Attack Reconstruction via Switched SMO

A. SMO Construction

Before proceeding further, the following parameter, augmented vectors and matrices are defined:

$$\begin{array}{rcl} \bar{n} &=& n + k + p + d, \\ \bar{A}_\eta &=& \begin{bmatrix} A & F_{a\eta} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \alpha_\eta I_k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \alpha_\eta I_s & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \alpha_\eta I_d \end{bmatrix} \in \mathbb{R}^{\bar{n} \times \bar{n}}, \\ \bar{B} &=& \begin{bmatrix} B^T & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}^T \in \mathbb{R}^{\bar{n} \times p}, \\ \bar{D} &=& \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I_k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I_s & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_d \end{bmatrix} \in \mathbb{R}^{\bar{n} \times \bar{n}}, \\ \bar{C}_\eta &=& \begin{bmatrix} C_\eta & \mathbf{0} & I_{p\eta} & F_{d\eta} \end{bmatrix} \in \mathbb{R}^{p \times \bar{n}}, \\ \bar{x}(t) &=& \begin{bmatrix} x^T(t) & a_a^T(t) & a_s^T(t) & d^T(t) \end{bmatrix}^T \in \mathbb{R}^{\bar{n}}, \\ \bar{d}(t) &=& \begin{bmatrix} \bar{0} \\ -\alpha_\eta a_a(t) + \dot{a}_a(t) \\ -\alpha_\eta a_s(t) + \dot{a}_s(t) \\ -\alpha_\eta d(t) + \dot{d}(t) \end{bmatrix} \in \mathbb{R}^{\bar{n}}, \end{array}$$

where $\alpha_\eta \in \mathbb{R}^+$ denotes a prescribed parameter. Then, the augmented descriptor CPSs can be obtained as

$$\left\{ \begin{array}{rcl} \dot{\bar{x}}(t) &=& \bar{A}_\eta \bar{x}(t) + \bar{B}u(t) + \bar{D}\bar{d}(t), \\ \bar{y}(t) &=& \bar{C}_\eta \bar{x}(t). \end{array} \right. \tag{6}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221, IEEE Transactions on Industrial Informatics

Based upon the augmented CPSs (6), we construct the following descriptor SMO:

$$\begin{cases} \dot{\xi}(t) &= N_\eta \xi(t) + T_\eta \bar{B} u(t) + L_\eta \bar{y}(t) + L_{s\eta} u_s(t), \\ \hat{\bar{x}}(t) &= \xi(t) + Q_\eta \bar{y}(t), \\ \hat{\bar{y}}(t) &= \bar{C}_\eta \hat{\bar{x}}(t) - I_{p\eta}\hat{a}_s(t) - \hat{d}(t) = C_\eta \hat{x}(t), \end{cases} \tag{7}$$

where $\xi(t) \in \mathbb{R}^{\bar{n}}$ represents an immediate variable, $\hat{\bar{x}}(t) \in \mathbb{R}^{\bar{n}}$ is the estimated state of $\bar{x}(t)$, and $u_s(t)$ denotes the discontinuous input which will be designed later. $N_\eta \in \mathbb{R}^{\bar{n}\times\bar{n}}$, $T_\eta \in \mathbb{R}^{\bar{n}\times\bar{n}}$, $L_\eta \in \mathbb{R}^{\bar{n}\times p}$, $L_{s\eta} \in \mathbb{R}^{\bar{n}\times p}$ and $Q_\eta \in \mathbb{R}^{\bar{n}\times p}$ are observer gain matrices to be given later.

B. Derivation of Observation Error

By defining $\bar{e}(t) = \hat{\bar{x}}(t) - \bar{x}(t)$, one has

$$\bar{e}(t) = \hat{\bar{x}}(t) - \bar{x}(t) = \xi(t) + (Q_\eta \bar{C}_\eta - I_{\bar{n}})\bar{x}(t). \tag{8}$$

It is assumed that the gain matrices T_η and Q_η can satisfy

$$\begin{bmatrix} T_\eta & Q_\eta \end{bmatrix} \begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix} = I_{\bar{n}}. \tag{9}$$

Then, it can be easily obtained that $\bar{e}(t) = \xi(t) - T_\eta \bar{x}(t)$. By subtracting Eq. (6) from Eq. (7), the following result holds:

$$\begin{aligned} \dot{\bar{e}}(t) &= \dot{\xi}(t) - T_\eta \dot{\bar{x}}(t) \\ &= N_\eta \bar{e}(t) + (N_\eta T_\eta + L_\eta \bar{C}_\eta - T_\eta \bar{A}_\eta)\bar{x}(t) \\ &\quad + T_\eta \bar{D}\bar{d}(t) - L_{s\eta} u_s(t). \end{aligned} \tag{10}$$

Furthermore, if the observer gain matrices N_η, T_η and L_η can be selected in the following forms:

$$N_\eta = T_\eta \bar{A}_\eta - K_\eta \bar{C}_\eta, \tag{11}$$

$$K_\eta = L_\eta - N_\eta Q_\eta, \tag{12}$$

we have

$$N_\eta T_\eta + L_\eta \bar{C}_\eta - T_\eta \bar{A}_\eta = 0. \tag{13}$$

Then, by substituting (13) into (10), we have

$$\dot{\bar{e}}(t) = N_\eta \bar{e}(t) + T_\eta \bar{D}\bar{d}(t) - L_{s\eta} u_s(t). \tag{14}$$

Based upon $\text{rank}(\begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}) = \bar{n}$, $\text{rank}(\begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \\ I_{\bar{n}} \end{bmatrix}) = \text{rank}(\begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}) = \bar{n}$ can be obtained. Hence, the condition (9) is solvable. The general solutions can be given as follows:

$$T_\eta = T_{1\eta} - Z_\eta T_{2\eta}, Q_\eta = Q_{1\eta} - Z_\eta Q_{2\eta}, \tag{15}$$

where

$$\begin{aligned} T_{1\eta} &= \begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}^\dagger \begin{bmatrix} I_{\bar{n}} \\ 0_{p\times\bar{n}} \end{bmatrix}, Q_{1\eta} = \begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}^\dagger \begin{bmatrix} 0_{\bar{n}\times p} \\ I_p \end{bmatrix}, \\ T_{2\eta} &= (I_{\bar{n}+p} - \begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}\begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}^\dagger) \begin{bmatrix} I_{\bar{n}} \\ 0_{p\times\bar{n}} \end{bmatrix}, \\ Q_{2\eta} &= (I_{\bar{n}+p} - \begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}\begin{bmatrix} I_{\bar{n}} \\ \bar{C}_\eta \end{bmatrix}^\dagger) \begin{bmatrix} 0_{\bar{n}\times p} \\ I_p \end{bmatrix}, \end{aligned}$$

and Z_η is an arbitrary matrix.

At this step, substituting Eq.(9) into Eq.(13) yields that

$$\begin{aligned} & N_\eta T_\eta + L_\eta \bar{C}_\eta - T_\eta \bar{A}_\eta \\ &= N_\eta - N_\eta Q_\eta \bar{C}_\eta + L_\eta \bar{C}_\eta - T_\eta \bar{A}_\eta. \end{aligned} \tag{16}$$

For further analysis convenience, substituting Eq.(15) into Eq.(11) yields the following equation:

$$N_\eta = N_{1\eta} - Z_\eta N_{2\eta}, \tag{17}$$

where

$$N_{1\eta} = T_{1\eta}\bar{A}_\eta - K_\eta \bar{C}_\eta, \quad N_{2\eta} = T_{2\eta}\bar{A}_\eta. \tag{18}$$

Till now, the augmented error dynamic can be obtained in the form of

$$\begin{aligned} \dot{\bar{e}}(t) &= N_\eta \bar{e}(t) + T_\eta \bar{D}\bar{d}(t) - L_{s\eta} u_s(t), \\ \bar{e}_y(t) &= \bar{C}_\eta \bar{e}(t) - I_{p\eta}\hat{a}_s(t) - \hat{d}(t), \end{aligned} \tag{19}$$

where $\bar{e}_y(t) = \bar{y}(t) - \hat{\bar{y}}(t)$ denotes the captured output. Based upon the augmented error dynamic (19), the potential sliding mode surface can be designed as $S(t,\eta) = \bar{D}^T T_\eta^T P_\eta \bar{e}(t)$ with P_η being a positive matrix to be designed later and satisfying $\bar{D}^T T_\eta^T P_\eta = H_\eta \bar{C}_\eta$, then the discontinuous input term $u_s(t)$ can be constructed as

$$\begin{aligned} u_s(t) &= -(\alpha_\eta(\alpha_{a1} + \beta_{s1} + \bar{d}_1) + \alpha_{a2} + \beta_{s2} \\ &\quad + \bar{d}_2 + \epsilon) Sgn(s(t,\eta)), \end{aligned} \tag{20}$$

where the matrix $H_\eta \in \mathbb{R}^{\bar{n}\times p}$ and the parameter ϵ will be determined later.

Remark 4: It should be noted that the sparse constraints on attacked sensors and actuators have been given in Assumption (A3). According to the work [30], we analysis the reliability of Assumption (A3) by rank criterion. Since the sparse constraints described in Assumption (A3) can be used as the prior knowledge for the dynamic analysis. It is obvious that, when $u_s(t) = \bar{0}$ and $\bar{d}(t) = \bar{0}$, the augmented error dynamic (19) is

$$\begin{aligned} \dot{\bar{e}}(t) &= N_\eta \bar{e}(t), \\ \bar{e}_y(t) &= \bar{C}_\eta \bar{e}(t) + I_{p\eta}\bar{I}_{p\eta^*}\hat{a}_s(t). \end{aligned} \tag{21}$$

Then, the (r,s)-sparse $strong^*$ detectability of the error dynamic (19) is equivalent to those of the error dynamic (21). In light of [30], the error dynamic (21) is said to be (r,s)-sparse $strong^*$ detectable if and only if the following two rank conditions satisfied:

$$\text{rank}\begin{bmatrix} sI - N_\eta & \mathbf{0} \\ \bar{C}_\eta & I_{p\eta}\bar{I}_{p\eta^*} \end{bmatrix} = \bar{n} + \text{rank}\begin{bmatrix} \mathbf{0} \\ I_{p\eta}\bar{I}_{p\eta^*} \end{bmatrix}, \tag{22}$$

$$\begin{aligned} & \text{rank}\begin{bmatrix} \bar{C}_\eta \times \mathbf{0} & I_{p\eta}\bar{I}_{p\eta^*} \\ I_{p\eta}\bar{I}_{p\eta^*} & \mathbf{0} \end{bmatrix} \\ &= \text{rank}[I_{p\eta}\bar{I}_{p\eta^*}] + \text{rank}\begin{bmatrix} \mathbf{0} \\ I_{p\eta}\bar{I}_{p\eta^*} \end{bmatrix}. \end{aligned} \tag{23}$$

The rank condition (22) can be further calculated as

$$\begin{aligned} & \text{rank}\begin{bmatrix} sI - N_\eta & \mathbf{0} \\ \bar{C}_\eta & I_{p\eta}\bar{I}_{p\eta^*} \end{bmatrix} \\ &= \text{rank}\begin{bmatrix} sI - T_\eta \bar{A} - K_\eta \bar{C}_\eta \\ \bar{C}_\eta \end{bmatrix} + \text{rank}[I_{p\eta}\bar{I}_{p\eta^*}]. \end{aligned} \tag{24}$$

After the elementary transformation, we have

$$\text{rank}\begin{bmatrix} sI - T_\eta \bar{A} - K_\eta \bar{C}_\eta \\ \bar{C}_\eta \end{bmatrix} = \bar{n}. \tag{25}$$

Similarly, by the elementary transformation techniques, it is obvious that the rank condition (23) is satisfied. Till now, the reliability of Assumption (A3) is verified.

C. Dynamic Analysis

In order to illustrate the feasibility of the proposed attack reconstruction method, the Lyapunov function is selected in the form of $V(t) = \bar{e}^T(t)P_\eta\bar{e}(t)$, where $P_\eta > 0$ is in proper dimensions. Then, the following derivation can be obtained:

$$\dot{V}(t) = 2\bar{e}^T(t)P_\eta[N_\eta\bar{e}(t) + T_\eta\bar{D}\bar{d}(t) - L_{s\eta}u_s(t)]. \quad (26)$$

Recalling Eq.(17), we can further derive that

$$\begin{aligned} \dot{V}(t) &= \bar{e}^T(t)[(P_\eta T_{1\eta}\bar{A}_\eta - P_\eta K_\eta\bar{C}_\eta - P_\eta Z_\eta T_{2\eta}\bar{A}_\eta)^T \\ &\quad +P_\eta T_{1\eta}\bar{A}_\eta - P_\eta K_\eta\bar{C}_\eta - P_\eta Z_\eta T_{2\eta}\bar{A}_\eta]\bar{e}(t) \\ &\quad +2\bar{e}^T(t)P_\eta T_\eta\bar{D}\bar{d}(t) - 2\bar{e}^T(t)P_\eta L_{s\eta}u_s(t). \quad (27) \end{aligned}$$

By letting $L_{s\eta} = T_\eta\bar{D} = P_\eta^{-1}\bar{C}_\eta^T H_\eta^T$, based upon Eq. (20), the last two terms of Eq. (27) can be further calculated as:

$$2\bar{e}^T(t)P_\eta[T_\eta\bar{D}\bar{d}(t) - L_{s\eta}u_s(t)] \leq -2\epsilon||S(t,\eta)||. \quad (28)$$

In view of the above detailed analysis, the first result related to the existence condition for the observer and the stability of the error dynamics (21) is given in the following theorem.

***Theorem** 1:* Consider the CPSs (19) with the descriptor SMO (7) and the switch logic (5). For the entry mode $\eta \in 1 \cup \mathrm{J}(\mathcal{C})$, under Assumptions (A1)-(A3), if there exist parameters γ, δ, ζ and $\bar{h} \in \mathbb{R}^+$ and matrices $P_\eta \in \mathbb{R}^{\bar{n}\times\bar{n}}$, $X_\eta \in \mathbb{R}^{\bar{n}\times\bar{n}+p}$, $Y_\eta \in \mathbb{R}^{\bar{n}\times p}$ and $H_\eta \in \mathbb{R}^{\bar{n}\times\bar{n}}$, such that

$$\Gamma = \begin{bmatrix}\Gamma_1 & \mathbf{0} \\ \mathbf{0} & -\delta^2 I_d\end{bmatrix} < 0, \begin{bmatrix}\zeta I_{\bar{n}} & \star \\ \Gamma_2 & -I_{a+p+d}\end{bmatrix} < 0, \quad (29)$$

where

$$\begin{aligned} \Gamma_1 &= \bar{A}_\eta^T T_{1\eta}^T P_\eta - \bar{C}_\eta^T Y_\eta^T - \bar{A}_\eta^T T_{2\eta}^T X_\eta^T \\ &\quad +P_\eta T_{1\eta}\bar{A}_\eta - Y_\eta\bar{C}_\eta - X_\eta T_{2\eta}\bar{A}_\eta, \\ \Gamma_2 &= \bar{D}^T T_\eta^T P_\eta - H_\eta\bar{C}_\eta, \end{aligned}$$

with $\star$ being the transpose of matrix Γ_2, then, we have $K_\eta = P_\eta^{-1}Y_\eta$ and $Z_\eta = P_\eta^{-1}X_\eta$. In addition, the boundary of the estimation error $\bar{e}(t)$ is $(\lambda_1\gamma)^{-1/2}\delta\bar{d}_1$ with $\lambda_1 = \min_\eta\{\lambda_{min}(P_\eta)\}$. The ultimate boundary of $\tilde{e}_y(t)$ is $\sigma = ||\bar{C}||(\lambda_1\gamma)^{-1/2}\delta\bar{d}_1 + \bar{d}_1$. Besides, $\bar{\Phi}$ in (4) is decided by $\bar{\Phi} = \gamma^2\lambda_1/(||\bar{C}||^2(\bar{h}+\delta^2\bar{d}_1))$ with $\bar{C} = \begin{bmatrix}C & \mathbf{0}_{p\times a} & I_p & F_d\end{bmatrix}$.

Proof: Resort to Schur complement, we can formulate (29) into the following form:

$$\dot{V}(t) \leq -\gamma V(t) + \delta^2 d^T(t)d(t), \quad (30)$$

which can further earn $\varphi^T(t)\Gamma\varphi(t) \leq 0$ with $\varphi(t) = (\bar{e}^T(t), d^T(t))^T$. Subsequently, we proceed the proof in two specific cases.

Case 1: It is assumed that the desired η^* is properly selected at the time instant $\check{t}$, i.e., the attacked signals are successfully excluded. Then, the error dynamics (19) can be rewritten as

$$\begin{aligned} \dot{\bar{e}}(t) &= N_\eta\bar{e}(t) + T_\eta\bar{D}\bar{d}(t) - L_{s\eta}u_s(t), \\ \bar{e}_y(t) &= \bar{C}_\eta\bar{e}(t) + \hat{d}(t). \quad (31) \end{aligned}$$

It is obvious that the modified captured output $\tilde{e}_y(t) = \bar{e}_y(t) = \bar{C}_\eta\bar{e}(t) + \hat{d}(t)$. Since we have got (30), then the following can be derived:

$$\begin{aligned} V(t) &\leq e^{-\gamma(t-\check{t})}V(t_0) + \int_{\check{t}}^{t} e^{-\gamma(t-\tau)}\delta^2 d^T(\tau)d(\tau)d\tau \\ &\leq e^{-\gamma(t-\check{t})}V(\check{t}) + \gamma^{-1}\delta^2\bar{d}_1^2, \quad (32) \end{aligned}$$

which further implies the following formula can be obtained:

$$\bar{e}^T(t)P_\eta\bar{e}(t) \leq e^{-\gamma(t-\check{t})}V(\check{t}) + \gamma^{-1}\delta^2\bar{d}_1^2. \quad (33)$$

Then, it is easy to derive $||\bar{e}(t)|| \leq \lambda_1^{1/2}e^{-\gamma(t-\check{t})/2}V^{1/2}(\check{t}) + (\lambda_1\gamma)^{-1/2}\delta\bar{d}_1$ and further leads to $||\tilde{e}_y(t)|| \leq \Omega^* + \sigma$ with $\Omega^* = ||\bar{C}||\lambda_1^{-1/2}e^{-\gamma(t-\check{t})/2}V^{1/2}(\check{t})$ and $\sigma = ||\bar{C}||(\lambda_1\gamma)^{-1/2}\delta\bar{d}_1 + \bar{d}_1$.

In addition, for $||\tilde{e}_y(t)|| > \sigma$, recalling (3), we can derive $\dot{\Psi}(t) \leq \bar{\Phi}(\Omega^*)^2$ which indicates $\Psi(t)$ will converge to a desired constant.

Case 2: It is assumed that a wrong enter mode is selected at time $\hat{t}$. In this case, there are two possibilities.

♦ The first possibility is $\int_{\hat{t}}^{+\infty}\dot{\Psi}(s)ds \leq 1$. In this situation, the switch logic $\eta(\Psi(t))$ will not jump to another integer, thus leading to a failure in excluding the FDI attacks.

♦ The second possibility is $\int_{\hat{t}}^{+\infty}\dot{\Psi}(s)ds > 1$. This situation is still promising since under the switch logic $\eta(\Psi(t))$, the current mode will switch to the next one. In this situation, we hope that there exists a time t^* at which the right mode can be located.

According to Case 1, for $[0, t^*)$, the result $\dot{\Psi}(t) \leq \Phi(t)||\bar{C}||\lambda_1^{-1}e^{-\gamma(t-t^*)}V(t^*)$ can be obtained easily. Then, considering $[t^*, +\infty)$, the result of $\int_{t^*}^{+\infty}\dot{\Psi}(s)ds$ can be derived as follows:

$$\begin{aligned} \int_{t^*}^{+\infty}\dot{\Psi}(s)ds &\leq \int_{t^*}^{+\infty}\bar{\Phi}||\bar{C}||^2\lambda_1^{-1}e^{-\gamma(s-t^*)}V(t^*)ds \\ &\leq \bar{\Phi}[||\bar{C}||^2(e^{-\gamma t^*}V(0) + \delta^2\bar{d}_1^2/\gamma)/(\lambda_1\gamma)] \\ &= \Xi \quad (34) \end{aligned}$$

By letting $\bar{\Phi} = \gamma^2\lambda_1/(||\bar{C}||^2(\upsilon+\delta^2\bar{d}_1^2))$ and $e^{-\gamma t^*}V(0)\gamma \leq \upsilon$, the result $\Xi \leq 1$ can be reached. Therefore, as $t \to +\infty$, we have $||\tilde{e}_y(t)|| \leq \sigma$.

Particularly, when the considered CPS is without noise which means $d(t) = 0$, the value of σ is zero. At this time, $\tilde{e}_y(t) \to \bar{0}$ as $t \to +\infty$. Then, we can derive $V(t) \leq \delta^2\bar{d}_1^2\gamma^{-1}$, and $||\bar{e}(t)|| \leq (\lambda_1\gamma)^{-1/2}\delta\bar{d}_1$ can be further obtained. Till now, the proof of Theorem 1 is finished. ■

By accomplishing the above analysis, we further conduct the issue of the reachability analysis of sliding motion surface and give the following theorem.

***Theorem** 2:* If the sufficient condition in Theorem 1 holds, then the discontinuous input term $u_s(t)$ guarantees that the sliding motion will be driven to the sliding surface $S(t,\eta) = \bar{D}^T T_\eta^T P_\eta\bar{e}(t) = 0$.

Proof: Firstly, we select the Lyapunov function as

$$V_s(t) = S^T(t,\eta)(W_\eta P_\eta W_\eta^T)^{-1}S(t,\eta), \quad (35)$$

where $W_\eta = \bar{D}^T T_\eta^T$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221, IEEE Transactions on Industrial Informatics

Secondly, by recalling $\bar{D}^T T_\eta^T P_\eta = H_\eta \bar{C}_\eta$, we can derive

$$\begin{aligned} \dot{V}_s(t) \quad &= \quad S^T(t,\eta)(W_\eta P_\eta W_\eta^T)^{-1} W_\eta P_\eta (N_\eta \bar{e}(t) \\ &\quad + T_\eta \bar{D}\bar{d}(t) - L_{s\eta} u_s(t)). \end{aligned} \tag{36}$$

From (28), it can be easily obtained that $S^T(t,\eta)(\bar{d}(t) - u_s(t)) \le -\epsilon||S(t,\eta)||$.

Thirdly, by defining $\varrho_\eta = W_\eta P_\eta W_\eta^T)^{-1} W_\eta P_\eta N_\eta$, $V_s(t) < -||S(t,\eta)||(\epsilon - \varrho_\eta ||\bar{e}(t)||)$ can be concluded.

Then, for each $\eta \in 1 \cup \mathrm{J}(\mathcal{C})$, we define a region as

$$\digamma = \cap_{\eta=1}^{\eta=\bar{\eta}} \digamma_\eta(\varrho_\eta), \tag{37}$$

where $\digamma_\eta(\varrho_\eta) = \{\epsilon - \varrho_\eta ||\bar{e}(t)|| > 0\}$. Till now, we can conclude that the trajectories of $\bar{e}(t)$ will enter into the region $\digamma$ and then sustain there. The proof of Theorem 2 is completed. ■

D. The whole design scheme

The whole design scheme is demonstrated in Fig. 1, which mainly includes four modules: depicting FDI attacks in red, physical system in purple, switching logic unit in orange, and descriptor SMO in blue, respectively.

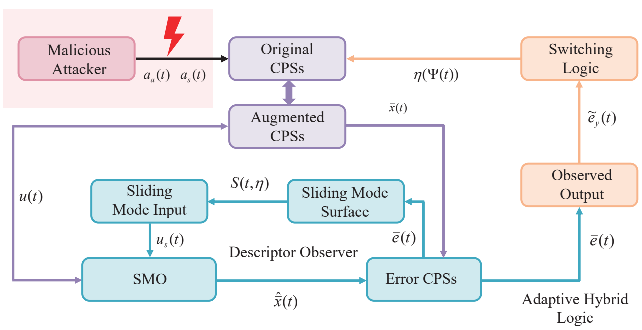

Fig. 1. The block diagram.

In terms of the above detailed analysis, the whole design procedures are summarized in the following form:

Design procedure.

Step 1. Construct descriptor CPS (6).
a. Prescribe the parameters of CPS (1);
b. Identify the potential entry modes $\eta \in [\bar{\eta}]$;
c. Define augmented vector and matrices to obtain the standard descriptor augmented CPS (6).
Step 2. Calculate the SMO gains (7).
a. Solve Eq. (9) and Eq. (15) to get matrices $T_{1\eta}$, $T_{2\eta}$, $Q_{1\eta}$ and $Q_{2\eta}$;
b. Select suitable parameters γ and δ and solve linear matrix equalities Eq. (29) to get ζ, K_η and Z_η;
c. Find matrix N_η according to Eq. (17);
d. Get matrix T_η, Q_η, L_η and $L_{s\eta}$ according to Eqs. (15)-(12).
Step 3. Design the adaptive switching logic depicted in (3)-(4).
Step 4. Obtain the SMO (7).

IV Simulation Results

In this section, a practical simulation is carried out to demonstrate the effectiveness of the proposed attack and state reconstruction method.

A. Simulation setup

Consider an F-404 aircraft engine system [31] modeled by three-order CPS and the system parameters are given as follows:

$$\begin{aligned} A \quad &= \quad \begin{bmatrix} -1.4600 & 0.0000 & 2.4280 \\ -0.8357 & -2.400 & -0.3788 \\ 0.3107 & 0.0000 & -2.2300 \end{bmatrix}, \\ B^T \quad &= \quad \begin{bmatrix} -12.5068 & -9.4796 & -7.4111 \end{bmatrix}, \\ C \quad &= \quad \begin{bmatrix} -0.0700 & 0.5000 & 1.0000 \\ 0.5000 & -0.5000 & -0.1000 \\ 0.1000 & 0.2000 & 0.4000 \end{bmatrix}, \\ F_a^T \quad &= \quad \begin{bmatrix} 0.2747 & -0.6727 & 0.5742 \end{bmatrix}, \\ F_d^T \quad &= \quad \begin{bmatrix} -0.7023 & 0.2513 & 0.3524 \end{bmatrix}. \end{aligned}$$

The system state $x(t)$ contains three components, i.e., the sideslip angle $x_{(1)}(t)$, roll rate $x_{(2)}(t)$ and yaw rate $x_{(3)}(t)$. The actuator attack signal $a_a(t)$, sensor attack signal $a_s(t)$ and external disturbance $d(t)$ are given by

$$a_a(t) = \begin{cases} 0, & 0 \le t \le 3, \\ 2 + 0.5\cos(t), & 3 < t \le 20, \end{cases} \tag{38}$$

$$a_s(t) = \begin{cases} 0, & 0 \le t \le 3, \\ 1 + 0.8\sin(t), & 3 < t < 20, \end{cases} \tag{39}$$

and $d(t) = 0.01\cos(t)$, which are upper-bounded by $\alpha_{a1} = 2.7$, $\alpha_{a2} = 0.7$, $\beta_{s1} = 2$, $\beta_{s2} = 1$ and $\bar{d}_1 = \bar{d}_2 = 0.01$.

B. Results illustration and discussion

We set $r = 1$ and $s = 1$, then all the potential entry modes can be concluded as follows: $\mathcal{C}_{(1)} = \mathcal{D}(\{0\},\{0\})$, $\mathcal{C}_{(2)} = \mathcal{D}(\{1\},\{1\})$, $\mathcal{C}_{(3)} = \mathcal{D}(\{1\},\{2\})$, $\mathcal{C}_{(4)} = \mathcal{D}(\{1\},\{3\})$. It is obvious that $\eta \in [4]$ and the desired mode is set as $\eta^* = 2$. Then, the Step 1 in the summarized design procedure of section III-D is almost finished.

Based upon Step 2-a, we can obtain: $T_{1\eta}$, $T_{2\eta}$ (at the bottom of this page), $Q_{1\eta}$ and $Q_{2\eta}$.

$$Q_{1\eta} = \begin{bmatrix} 0.0000 & 0.1943 & 0.0430 \\ 0.0000 & -0.1943 & 0.0856 \\ 0.0000 & -0.0388 & 0.1713 \\ 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.3886 & 0.0002 \\ 0.0000 & 0.0002 & 0.4284 \end{bmatrix},$$

$$Q_{2\eta} = \begin{bmatrix} 0.0000 & -0.1943 & -0.0430 \\ 0.0000 & 0.1943 & -0.0856 \\ 0.0000 & 0.0388 & -0.1713 \\ 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & -0.3886 & -0.0002 \\ 0.0000 & -0.0002 & -0.4284 \\ 0.0000 & -0.0977 & -0.1510 \\ 1.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.3886 & 0.0002 \\ 0.0000 & 0.0002 & 0.4284 \end{bmatrix}.$$

Next, according to Step 2-b, the parameters are selected as $\gamma = 0.5$ and $\delta = 0.7$. Then, by solving linear matrix

© 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221, IEEE Transactions on Industrial Informatics
This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221

inequalities, we can obtain $\zeta = 8.495 \times 10^{-1}$ and matrices K_η and Z_η (at the bottom of the next page):

$$K_\eta = \begin{bmatrix} 0 & -2.2712 & -1.3478 \\ 0 & -0.6929 & -3.7473 \\ 0 & -0.5048 & 0.0834 \\ 0 & -0.6356 & 0.1159 \\ 0 & 1.2456 & -4.2559 \\ 0 & 2.4228 & 1.2495 \\ 0 & 1.2178 & 3.1401 \\ 0 & 0.7883 & 15.5586 \end{bmatrix}.$$

Based on Step 2-c and Step 2-d, the observer gain matrices N_η (at the bottom of the next page), T_η, Q_η, L_η and $L_{s\eta}$ can be obtained:

$$T_\eta = \begin{bmatrix} 0 & -2.2712 & -1.3478 \\ 0 & -0.6929 & -3.7473 \\ 0 & -0.5048 & 0.0834 \\ 0 & -0.6356 & 0.1159 \\ 0 & 1.2456 & -4.2559 \\ 0 & 2.4228 & 1.2495 \\ 0 & 1.2178 & 3.1401 \\ 0 & 0.7883 & 15.5586 \end{bmatrix}, Q_\eta = \begin{bmatrix} 0 & -2.2712 & -1.3478 \\ 0 & -0.6929 & -3.7473 \\ 0 & -0.5048 & 0.0834 \\ 0 & -0.6356 & 0.1159 \\ 0 & 1.2456 & -4.2559 \\ 0 & 2.4228 & 1.2495 \\ 0 & 1.2178 & 3.1401 \\ 0 & 0.7883 & 15.5586 \end{bmatrix},$$

$$L_\eta = \begin{bmatrix} 0 & -2.2712 & -1.3478 \\ 0 & -0.6929 & -3.7473 \\ 0 & -0.5048 & 0.0834 \\ 0 & -0.6356 & 0.1159 \\ 0 & 1.2456 & -4.2559 \\ 0 & 2.4228 & 1.2495 \\ 0 & 1.2178 & 3.1401 \\ 0 & 0.7883 & 15.5586 \end{bmatrix}, L_{s\eta} = \begin{bmatrix} 0 & -2.2712 & -1.3478 \\ 0 & -0.6929 & -3.7473 \\ 0 & -0.5048 & 0.0834 \\ 0 & -0.6356 & 0.1159 \\ 0 & 1.2456 & -4.2559 \\ 0 & 2.4228 & 1.2495 \\ 0 & 1.2178 & 3.1401 \\ 0 & 0.7883 & 15.5586 \end{bmatrix}.$$

By setting $\alpha_\eta = 1$ and selecting $\epsilon = 0.1$, we can earn $u_s(t) = \mathrm{Sgn}(S(t, \eta))$.

In addition, the switching parameters ϵ and ς are set as 0.1 and 0.5, respectively. The initial conditions of the original system states and augmented error system s-tates are set as $x(0) = \begin{bmatrix} -2 & 1 & 1 \end{bmatrix}^T$ and $\bar{e}(0) = \begin{bmatrix} 15 & -10 & -15 & 0 & -10 & -15 & 10 & 0 \end{bmatrix}^T$. Based on the above setting and derivation, the simulation results are displayed in Figs. 2-6. Fig. 2 displays the states of the augmented error system, in which the error trajectories of the system states ($\bar{e}_1(t) - \bar{e}_3(t)$), actuator attacks ($\bar{e}_4(t)$), sensor attacks ($\bar{e}_5(t) - \bar{e}_7(t)$) and disturbances ($\bar{e}_8(t)$) are all convergent. The reconstruction results of attacks and disturbances are shown in Figs.3-5, in which the blue lines are the attack and disturbance signals and the red lines are the reconstruction signals. It can be seen that the performance of reconstruction is satisfied. In Fig. 6, the switching logic $\eta(t)$ and the indicator Ψ are given, in which it can be seen that both two trajectories are convergent. Therefore, the reliability of our method has been verified by this simulation.

To further verify the correctness and effectiveness of the proposed algorithm, we set different attack forms and attack duration to test. At this time, the desired attack mode is set as $\eta^* = 3$. The attack signals are changed in the constant form ($a_a = 2, a_s = 1.5$) and the state-dependant form ($a_a(t) = 0.5\cos(x_1(t))$ and $a_s(t) = 0.8\sin(x_2(t))$). The simulation results can be seen in Figs. 7-11. From Fig. 7, it can be seen that the switch logic can locate the desired mode 3 accurately (Due to the page limitation, only the switch logic result of attacks in the constant form is given). In Figs. 8-11, the reconstruction results of both constant and state-dependant attacked signals are satisfied.

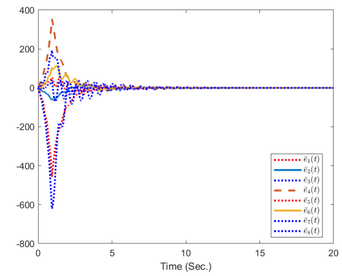

Fig. 2. State variables of error system $\bar{e}(t)$.

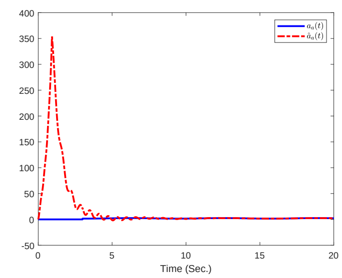

Fig. 3. Attack signal $a_a(t)$ and its estimation $\hat{a}_a(t)$.

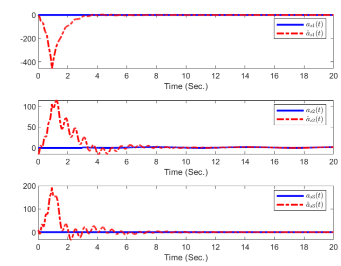

Fig. 4. Attack signals $a_s(t)$ and the estimation $\hat{a}_s(t)$.

$$T_{1\eta} = \begin{bmatrix} 0.8985 & 0.0886 & 0.0022 & 0.0000 & 0.0000 & -0.1943 & -0.0430 & -0.0640 \\ 0.0886 & 0.8858 & -0.0537 & 0.0000 & 0.0000 & 0.1943 & -0.0856 & 0.0187 \\ 0.0022 & 0.0537 & 0.9276 & 0.0000 & 0.0000 & 0.0388 & -0.1713 & -0.0506 \\ -0.0000 & 0.0000 & 0.0000 & 1.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ -0.0000 & 0.0000 & -0.0000 & 0.0000 & 1.0000 & 0.0000 & 0.0000 & 0.0000 \\ -0.1943 & 0.1943 & 0.0388 & 0.0000 & 0.0000 & 0.6114 & -0.0002 & -0.0977 \\ -0.0430 & -0.0856 & -0.1713 & 0.0000 & 0.0000 & -0.0002 & 0.5716 & -0.1510 \\ -0.0640 & 0.0187 & -0.0506 & 0.0000 & 0.0000 & -0.0977 & -0.1510 & 0.9222 \end{bmatrix}.$$

$$T_{2\eta} = \begin{bmatrix} 0.1015 & -0.0886 & -0.0022 & 0.0000 & 0.0000 & 0.1943 & 0.0430 & 0.0640 \\ -0.0886 & 0.1142 & 0.0537 & 0.0000 & 0.0000 & -0.1943 & 0.0856 & -0.0187 \\ -0.0022 & 0.0537 & 0.0724 & 0.0000 & 0.0000 & -0.0388 & 0.1713 & 0.0506 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.1943 & -0.1943 & -0.0388 & 0.0000 & 0.0000 & 0.3886 & 0.0002 & 0.0977 \\ 0.0430 & 0.0856 & 0.1713 & 0.0000 & 0.0000 & 0.0002 & 0.4284 & 0.1510 \\ 0.0640 & -0.0187 & 0.0506 & 0.0000 & 0.0000 & 0.0977 & 0.1510 & 0.0778 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 \\ -0.1943 & 0.1943 & 0.0388 & 0.0000 & 0.0000 & -0.3886 & -0.0002 & -0.0977 \\ -0.0430 & -0.0856 & -0.1713 & 0.0000 & 0.0000 & -0.0002 & -0.4284 & -0.1510 \end{bmatrix}.$$

This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221

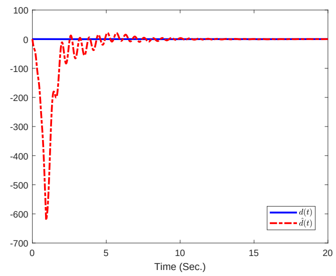

Fig. 5. Disturbance signal $d(t)$ and its estimation $\hat{d}(t)$.

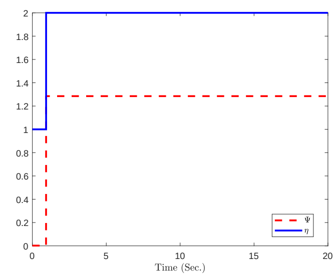

Fig. 6. Response of η and Ψ ($\eta^\star = 2$).

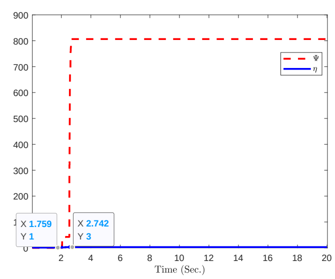

Fig. 7. Response of η and Ψ ($\eta^\star = 3$).

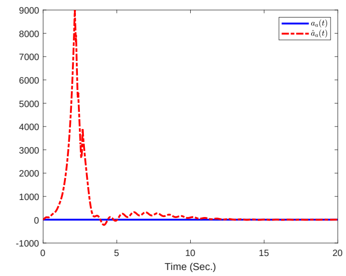

Fig. 8. Constant attack signal $a_a(t)$ and its estimation $\hat{a}_a(t)$.

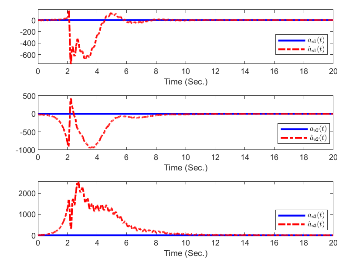

Fig. 9. Constant attack signals $a_s(t)$ and the estimation $\hat{a}_s(t)$.

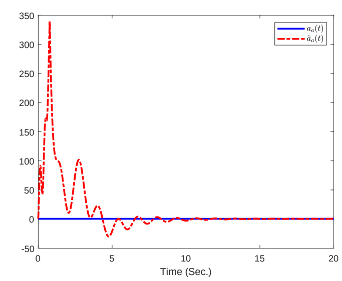

Fig. 10. State-dependant attack $a_a(t)$ and its estimation $\hat{a}_a(t)$.

Reconsidering the attack form in (38) and (39), it can be seen that the duration time is 17s. By adjusting the duration time to 27s and 32s, the results can be found in Figs.12-15. It can be found that, the longer the attack duration time is, the more attack reconstruction time will take.

Besides, a comparative simulation is also carried out to demonstrate the superiority of the proposed method. We revisit the first SMO method in [27] with same system parameters and initial conditions. The simulation results of [27] can been seen in Figs. 16-17. Fig. 16 shows the states of the augmented error system. The reconstruction results of actuator and sensor attacks are displayed in Fig. 17. Compared with Figs. 2-4, it can be seen that the convergence time of [27] is longer than that of the proposed method in this paper.

V Conclusions

In this paper, a SMO-based attack and state reconstruction strategy, based on system augmentation technique and linear matrix inequality technique is developed for a class of CPSs in which FDI attacks happen in simultaneous actuator and

$$Z_\eta = \begin{bmatrix} 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0.0000 & 0 & 0.0000 & 0.0000 \\ -0.0018 & -1.2443 & -2.2236 & -3.5728 & -0.7241 & -0.2845 & 1.8155 & -1.2386 & 0 & 0.2478 & 0.2405 \\ 0.0066 & 2.7313 & 2.0433 & 4.2116 & -4.4848 & 1.4585 & -0.3897 & -2.1232 & 0 & 0.6417 & 0.2263 \\ -0.0090 & 0.1655 & 0.1469 & -0.0077 & 0.0120 & -0.0215 & 0.2434 & 0.1131 & 0 & 0.0951 & 0.3742 \\ -0.0126 & 0.2321 & 0.2059 & -0.0108 & 0.0168 & -0.0302 & 0.3414 & 0.1586 & 0 & -0.1333 & 0.5248 \\ 0.0359 & -0.6587 & -0.5844 & 0.0307 & -0.0476 & 0.0857 & -0.9687 & -0.4501 & 0 & 0.3783 & -1.4892 \end{bmatrix}.$$

$$N_\eta = \begin{bmatrix} -0.5145 & -1.6477 & 1.5555 & -0.0000 & -0.0000 & 2.2926 & 3.0296 & 1.6438 \\ 0.7741 & -1.9642 & 1.3002 & -0.0000 & -0.0000 & -0.3810 & 0.9941 & 0.2546 \\ -1.0672 & 0.7957 & -1.1712 & 0.0000 & 0.0000 & 3.0080 & 3.9560 & 2.1500 \\ 0.2329 & -1.0389 & 1.6684 & -0.9045 & -0.0305 & -0.2991 & -0.5847 & -0.3343 \\ -0.6841 & -2.0497 & 0.7544 & -0.0290 & -0.8517 & -0.3123 & 0.4434 & 0.1047 \\ -2.5042 & -2.6209 & -0.5387 & -0.0012 & 0.0024 & -1.0748 & -1.4998 & -0.5688 \\ -3.0398 & -4.6450 & -1.1025 & -0.0017 & 0.0034 & 0.0706 & -1.3811 & -0.1418 \\ -2.1200 & 9.0344 & -9.6045 & 0.0049 & -0.0096 & 2.4719 & 2.4154 & 0.5538 \end{bmatrix}.$$

This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221

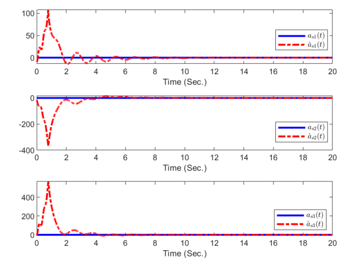

Fig. 11. State-dependant attacks $a_s(t)$ and the estimation $\hat{a}_s(t)$.

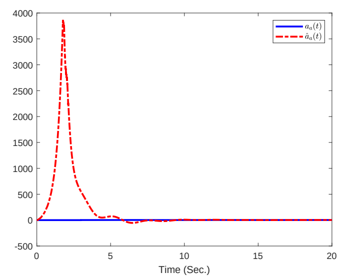

Fig. 12. Attack signal $a_a(t)$ and its estimation $\hat{a}_a(t)$(27s).

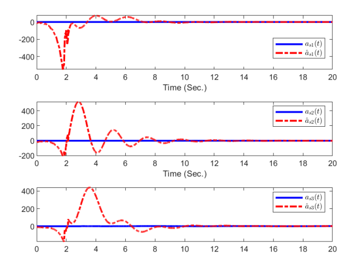

Fig. 13. Attack signals $a_s(t)$ and the estimation $\hat{a}_s(t)$(27s).

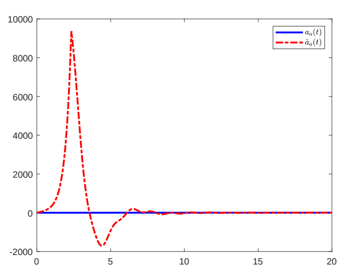

Fig. 14. Attack signal $a_a(t)$ and its estimation $\hat{a}_a(t)$(32s).

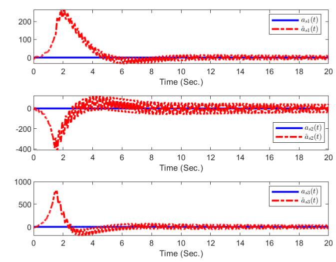

Fig. 15. Attack signals $a_s(t)$ and the estimation $\hat{a}_s(t)$(32s).

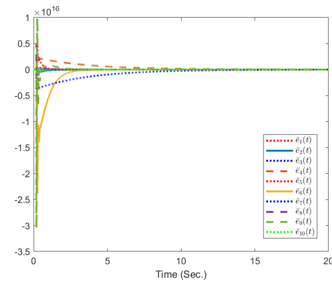

Fig. 16. State variables of error system $\bar{e}(t)$ in [27].

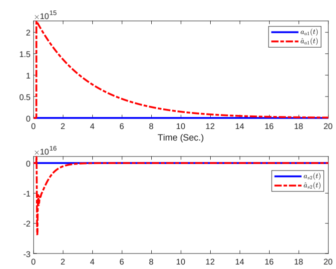

Fig. 17. Attack signals and the reconstruction signals in [27].

sensor channels. The advantages of the proposed attack and state reconstruction strategy lie in the following three aspects: 1) The auxiliary observed indicator used in this work can boost the convergence of the switching logic which is superior to some existing excellent works [19]. 2) The developed SMO can handle the case that the simultaneous occurrence of sparse actuator attacks and sensor attacks which extends its ability in application. 3) The proposed SMO is constructed based on a regular augmented system approach rather a singular augmented system [27], which decreases the complexity of the design scheme. Finally, the applicability and reliability of our method have been verified by a simulation. The CPS considered in this work is linear, while non-linearity is always existed in actual systems. Hence, we will further pay attention to the issue of attack and state reconstruction for nonlinear CPSs.

References

[1] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[2] Y. Jiang and S. Yin, "Recursive total principle component regression based fault detection and its application to vehicular cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1415–1423, 2018.

[3] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyber physical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2015.

[4] E. Hammad, A. Farraj, and D. Kundur, "On cyber-physical coupling and distributed control in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 8, pp. 4418–4429, 2019.

[5] S. Yin, J. J. Rodriguez-Andina, and Y. Jiang, "Real-time monitoring and control of industrial cyberphysical systems: With integrated plant-wide monitoring and control framework," *IEEE Industrial Electronics Magazine*, vol. 13, no. 4, pp. 38–47, 2019.

This article has been accepted for publication in IEEE Transactions on Industrial Informatics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2021.3111221, IEEE Transactions on Industrial Informatics

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[7] S. M. Dibaji, M. Pirani, D. Flamholz, A. M. Annaswamy, and K. H. Johansson, "A systems and control perspective of cps security," *Annual Reviews in Control*, vol. 47, pp. 394–411, 2019.

[8] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyberphysical systems under dos attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4920–4927, 2020.

[9] W. Fu, J. Qin, Y. Shi, W. X. Zheng, and Y. Kang, "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4868–4877, 2020.

[10] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[11] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 106–117, 2017.

[12] C. Kwon and I. Hwang, "Reachability analysis for safety assurance of cyber-physical systems against cyber attacks," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2272–2279, 2018.

[13] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 6058–6064, 2017.

[14] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3432–3439, 2018.

[15] H. Song, P. Shi, W. Zhang, C. Lim, and L. Yu, "Distributed h_∞ estimation in sensor networks with two-channel stochastic attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 2, pp. 465–475, 2020.

[16] I. Jovanov and M. Pajic, "Relaxing integrity requirements for attack-resilient cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4843–4858, 2019.

[17] C. Kwon and I. Hwang, "Cyber attack mitigation for cyberphysical systems: hybrid system approach to controller design," *IET Control Theory Applications*, vol. 10, no. 7, pp. 731–741, 2016.

[18] F. Pasqualetti, F. Drfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[19] L. An and G. Yang, "Secure state estimation against sparse sensor attacks with adaptive switching mechanism," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2596–2603, 2018.

[20] ——, "Lq secure control for cyber-physical systems against sparse sensor and actuator attacks," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 833–841, 2019.

[21] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, 2011.

[22] M. Showkatbakhsh, Y. Shoukry, S. N. Diggavi, and P. Tabuada, "Securing state reconstruction under sensor and actuator attacks: Theory and design," *Automatica*, vol. 116, p. 108920, 2020.

[23] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2016.

[24] X. Luo, M. Pajic, and M. M. Zavlanos, "A scalable and optimal graph-search method for secure state estimation," arXiv: 1903.10620v2, 2019.

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

[26] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," *Proceedings of the American Control Conference*, vol. 2015, pp. 2439–2444, 2015.

[27] R. Ma, P. Shi, and L. Wu, "Sparse false injection attacks reconstruction via descriptor sliding mode observers," *IEEE Transactions on Automatic Control*, pp. 1–1, 2020.

[28] R. Ma and P. Shi, "Secure state estimation for cyber-physical systems under sparse data injection attacks: a switched counteraction approach," *International Journal of Control*, no. 5, pp. 1–12, 2020.

[29] C. Wu, Z. Hu, J. Liu, and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.

[30] M. L. J. Hautus, "Strong detectability and observers," *Linear Algebra & Its Applications*, vol. 50, pp. 353–368, 1983.

[31] M. Liu, L. Zhang, Zheng, and W. Xing, "Fault reconstruction for stochastic hybrid systems with adaptive discontinuous observer and non-homogeneous differentiator," *Automatica*, vol. 85, pp. 339–348, 2017.

Hongyan Yang (S'16) received the B.S. degree in Mathematics and Applied Mathematics and the M.S. degree in Optimization and Automatic Control Theory in College of Mathematics and Physic from Bohai University, JinZhou, P.R. China, in 2013 and 2016, respectively; and the Ph.D degree in control theory and control engineering from Harbin Institute of Technology, Harbin, P.R. China, in 2020.

She is currently a lecturer with Beijing University of Technology. Her research interests include fault diagnosis and fault tolerant control of nonlinear systems, Markovian jump systems and cyber-physical systems.

Shen Yin (M'12-SM'15) received the B.E. degree in automation from Harbin Institute of Technology, Harbin, China, in 2004, the M.Sc. degree in control and information system and the Ph.D. degree in electrical engineering and information technology from University of Duisburg-Essen, Germany, in 2007 and 2012.

He is currently DNV-GL Professor with the Department of Mechanical and Industrial Engineering, Norwegien University of Science and Technology. His research interests include safety, reliability of complicated systems, system and control theory, data-driven and machine learning approaches, applications in large-scale systems and industrial cyber-physical systems.

Honggui Han (M'10-SM'15) received the B.S. degree in automatic from Civil Aviation University of China, Tianjin, China, in 2005, the M.E. and Ph.D. degrees in control theory and control engineering from the Beijing University of Technology, Beijing, China, in 2007 and 2011, respectively.

He has been with Beijing University of Technology since 2011, where he is currently a Professor. His current research interests include neural networks, fuzzy systems, intelligent systems, modeling and control in process systems, and civil and environmental engineering. Prof. Han is currently an associate editor of IEEE Transactions on Cybernetics and International Journal of Fuzzy Systems. Moreover, Prof. Han is currently a reviewer of IEEE Transactions on Fuzzy Systems, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Control Systems Technology, etc.

Haoyuan Sun received the bachelors degree in measurement and control technology and instrument from Jilin University, Changchun, China, in 2013, the master's degree in pattern recognition and intelligent systems from the Beijing Institute of Technology, Beijing, China, in 2016, and the Ph.D. degree in pattern recognition and intelligent systems from the Beijing Institute of Technology, Beijing, China, in 2020.

In 2020, he joined the Beijing Key Laboratory of Computational Intelligence and Intelligent Systems, Beijing University of Technology. His current research interests include stochastic sampled-data control system, consensus control, predictive control and networked control systems.

1551-3203 (c) 2021 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.