Distributed Secure State Estimation and Control for CPSs Under Sensor Attacks

Wei Ao, Yongduan Song, *Senior Member, IEEE*, and Changyun Wen, *Fellow, IEEE*

***Abstract*—In this paper, we investigate the distributed secure state estimation and control problems for interconnected cyber-physical systems (CPSs) with some sensors being attacked. First, by exploring the distinct properties of the unidentifiable attacks to a CPS, an explicit sufficient condition that the secure state estimation problem can be solvable is established. Then distributed preselectors and observers are presented to solve the secure state estimation problems. Furthermore, with the obtained state estimation, fractional dynamic surface-based distributed secure controllers are also proposed for the secure control problem. Theoretical analysis shows that, with the proposed distributed secure observers and controllers, not only the state of the CPS under attacks can be obtained in a given finite time but also the dynamic surface can be achieved and maintained in a finite time. Finally, the results are applied to an islanded microgrid system as an illustration, which verifies the effectiveness of the proposed schemes.**

***Index Terms*—Cyber-physical system (CPS), distributed secure control, secure state estimation, sensor attacks.**

I. Introduction

CYBER-PHYSICAL systems (CPSs), whose most notable feature is tight integration and cooperation between cyber and physical components [1], have attracted attention from many researchers in the past decades. Typically, CPSs consist of processing units monitor, control physical processes by means of sensors and actuators networks, such as transportation networks, future power systems and smart grids, and high speed train systems. Thus, they are prone to failures especially cyber attacks on the data and communication channels, thus causing damages or breakdown, for example, the Stuxnet storm which damaged the Iran's nuclear program in [2], breakout accident in nuclear plant in [3], and power blackouts in Brazil in [4].

Many works devoting to the attack detection, secure estimation, and control of CPSs have recently appeared in the literature, which can be classified in three classes. The first class addresses attacks. Teixeira *et al.* [5] presented a novel attack space based on the adversary's model knowledge, disclosure, and disruption resources, and it illustrates the attack effects by implementing experiments on a wireless network control system, whereas the attack detection and secure control is not discussed. In second class, detection of attacks to CPSs is investigated. For example, [6] the detectability of an attack to CPSs is explored with structured system theory and a Luenberger like observer is proposed to detect the attack. Whereas, if only an upper bound on the cardinality of the attacked sensors is available, the number of needed monitors is combinatorial in the size of the attacked sensors. In [7], a sliding mode observer-based method is presented to estimate the attack to system dynamics and sensors separately, in addition to the state estimation. Nevertheless, the results are only applicable to the systems where the so called observer matched conditions are valid. In [8], a sufficient and necessary detectability condition of an attack is proposed in terms of the system dynamics eigenvectors by exploring the strong observability of the system. A sufficient and necessary condition of undetectable attacks in the presence of side initial state information is presented in [9], and a detector is proposed to detect attacks in a finite steps. It is noted that, secure state estimation is not involved in [9]. Even though the strong observability helps to describe the undetectable attacks, as many CPS are distributed, we feel that, a more explicit characterization is needed and distributed finite time attack detection is needed. The third class focuses on secure state estimation or secure control design in the presence of attacks. In [10], a specific computationally feasible decoding algorithm is proposed to estimate states of CPS when some sensors are corrupted and it also gives a characterization on the maximum number of attacked sensors allowed for this decoder to correctly estimate the states. By showing how to design a secure local control loop to improve the resilience of the system, and presenting L_1/L_r decoder for secure state estimation, these results are extended in [11]. In [12], by utilizing the sparse observability of a system, it shows that the state can be estimated securely under an s-sparse attack if and only if the system is $2s$-sparse observable, and an event triggered observer is proposed to estimate the state securely. Then [13] extends these results with

Manuscript received February 9, 2018; revised May 22, 2018 and August 5, 2018; accepted August 28, 2018. Date of publication December 18, 2018; date of current version October 22, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61773081 and Grant 61860206008, and in part by the Technology Transformation Program of Chongqing Higher Education University under Grant KJZH17102. This paper was recommended by Associate Editor Y. Shi. *(Corresponding author: Wei Ao.)*

W. Ao is with the School of Math and Physical, Chongqing University of Science and Technology, Chongqing 401331, China (e-mail: craneaow@cqu.edu.cn).

Y. Song is with the School of Automation, Chongqing University, Chongqing 400044, China, and also with the Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing University, Chongqing 400044, China (e-mail: ydsong@cqu.edu.cn).

C. Wen is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: ecywen@ntu.edu.sg).

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/TCYB.2018.2868781

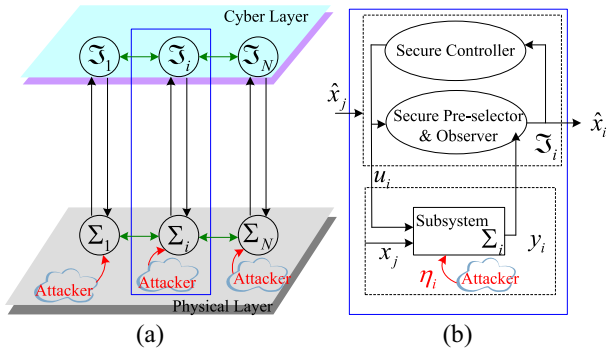


Fig. 1. Diagram of interconnected CPSs with attack and proposed schemes.

a novel multimodal Luenberger observer based on efficient satisfiability modulo theory to reduce the complexity of the estimation problem. Attack detection and secure estimation are also investigated in [14] for linear systems under sensor attacks in the presence of noise, which shows that detectable attacks can be detected in finite, yet sufficiently large number of steps. The complexity of the estimation problem can be efficiently reduced by satisfiability modulo theory. However, the estimation algorithms in [10]–[14] are in a centralized form. Mo *et al.* [15] investigated the resilient detection when there exist s attacks to p sensors. A minimax optimization method is proposed to minimize the worst-case probability of error against all possible manipulations by the attackers. These results are extended in [16]. Again, it only shows that, asymptotical convergence is obtained and when $s \geq p/2$, attackers can render the information provided by the manipulated measurement useless, thus an optimal worst-case detector is proposed by solely using the *a-priori* information, without utilizing all measurements. Also note that, the results in [10]–[16] are in centralized form and only admit exponential convergence of estimation errors or a finite, yet sufficiently large steps to obtain the secure state estimation, which implies that it may need quite long time. This calls for a prescribed finite time distributed secure estimation and secure control.

Therefore, motivated by these above discussions, we address distributed secure state estimation and control of the CPSs with some sensors being corrupted by malicious attackers, with the block diagram of the considered CPS and the proposed schemes given in Fig. 1. The presented schemes consist of distributed secure preselectors, distributed finite time observers, and a virtual fractional dynamic surface-based distributed secure controllers. Our contributions and methodologies can be outlined as follows.

1) By exploring the distinct properties of unidentifiable attacks for linear CPS, sufficient conditions that secure state estimation can be solvable is established.
2) Also based on the above conditions, we propose distributed observers with secure preselectors to solve the secure state estimation problem. It is shown that under the sufficient conditions, states can be exactly obtained in a given finite time.
3) Then with the obtained secure state estimation, distributed secure controllers based on a virtual fractional dynamic surface are designed, which guarantee that, the state of the CPS can be made track the desired trajectories with finite time containments, and all the signals are continuous and bounded. Also some guidelines on the choice of the design parameters are presented.

The remainder of this paper is organized as follows. In Section II, system models are given and some definitions are presented. Also our objectives are formulated as secure state estimation and secure control problems. In Section III, a sufficient condition ensuring that the secure state estimation can be solvable is proposed and established. Then finite time observers with secure preselectors are designed to solve the secure state estimation. Section IV proposes a fractional dynamic surface-based distributed secure controller to solve the secure control problem. Section V presents an numerical simulation of a islanded micro-grid (MG) system under sensor attacks to verify our theoretical findings. Finally, Section VI gives some concluding remarks.

Notation: Throughout this paper, $\mathbb{R}^n$ represents the n dimensional Euclidean space, $\mathbb{N}$ denotes the set of nature numbers. The Euclidean norm of a vector x and the corresponding induce norm of a matrix A are denoted by $\|x\|$ and $\|A\|$, respectively. For a vector x, Card(x) denotes the number of nonzero elements in x.

II. System Model and Problem Formulation

A. System Model and Attacks

Consider a CPS under sensor attacks similar to that in [17]–[19], consisting of N interconnected single-input-single–output linear subsystem. Its ith subsystem, $i = 1, \ldots, N$, can be expressed the observable canonical form as follows:

$$\Sigma_{a,i}: \begin{cases} \dot{x}_{i,1}(t) = a_{i,1}x_{i,1}(t) + x_{i,2}(t) \\ \dot{x}_{i,2}(t) = a_{i,2}x_{i,1}(t) + x_{i,3}(t) \\ \quad \vdots \\ \dot{x}_{i,n}(t) = a_{i,n}x_{i,1}(t) + b_i u_i(t) + \sum\limits_{j\in J_i} \Gamma_j^i x_{j,1}(t) \\ y_i(t) = C_i x_i(t) + \eta_i(t) + d_i(t) \end{cases} \tag{1}$$

where $x_i(t) = [x_{i,1}(t), \ldots, x_{i,n}(t)] \in \mathbb{R}^n$ is the unknown state, $u_i(t) \in \mathbb{R}$ is the input, $y_i(t) \in \mathbb{R}^{p_i}$ is the measured output vector which is potentially corrupted, $\eta_i(t) \in \mathbb{R}^{p_i}$ denotes the injected data by the adversarial attackers, $C_i = [C_{i,0}, \ldots, C_{i,0}]^T \in \mathbb{R}^{p_i \times n}$ is the output distribution matrix with $C_{i,0} = [1, 0, \ldots, 0] \in R^n$ $d_i(t)$ is the measurement white noise vector, J_i is the set of subsystems which affect the dynamics of the ith CPS, Γ_j^i and b_i are some known constants and t denotes the time.

Remark 1: As shown in [6], [18], and [19], many practical CPSs, such as smart grids and the high speed train system, can be modeled as interconnected systems (1). In addition, with the improvement of information technology, more than one sensor is nowadays employed for measuring each signal to improve the security in many practical control systems [15], [16]. Then an output distribution matrix can be, for example C_i, described in the form of (1).

In this paper, we assume only s_i out of p_i sensors are manipulated arbitrarily by attackers. Except this, we do not need any

prior knowledge about the attackers. In addition, inspired by the works on compressed sensing in [20] and secure estimation in [10]–[12], we present the following definitions.

Definition 1 (s-Sparse Attack): The attack $\eta_i(t)$ is said s-sparse if there exists a set $\Lambda_i \subset \{1, \ldots, p_i\}$ satisfying that $\text{Card}(\Lambda_i) = p_i - s$ where $s \in \mathbb{N}$ and $\eta_{i,j}(t) = 0$ for all t where $\eta_{i,j}(t)$ is the jth element of $\eta_i(t)$ with $j \in \Lambda_i$, and the other s elements of $\eta_i(t)$ can be manipulated arbitrarily.

The secure state estimation problem is formulated as that, given a sequence of $y_i(t)$, design some estimators to obtain the state $x_i(t)$ and the attack $\eta_i(t)$. Clearly, if the secure state estimation problem is solvable, it is sufficient and necessary that a unique sequence of $y_i(t)$ is corresponding to a unique sequence of $x_i(t)$ and $\eta_i(t)$. Otherwise, if there exist two different attacks which are corresponding to the same $y_i(t)$, then the secure state estimation problem cannot be solved. Thus, the following definition, i.e., the unidentifiable attack, is needed.

Definition 2 (*Unidentifiable Attacks):* Two attacks $\eta_i(t)^1 \neq \eta_i(t)^2$ are said unidentifiable to the CPS in (1) in the absence of noise, if there exist two different initial state values $x_i(0)^1 \neq x_i(0)^2$, such that, the following equation is valid for all t:

$$y_i\Big(x_i(0)^1, u_i, \eta_i^1, t\Big) = y_i\Big(x_i(0)^2, u_i, \eta_i^2, t\Big). \tag{2}$$

Then we have the following result.

Lemma 1: Consider the CPS under attacks in (1), the absence of unidentifiable attacks is equivalent to the solvability of secure state estimation when $d_i(t) = 0$.

Proof: 1) Sufficiency is proved by a contraction. Assume there exists two unidentifiable attacks, i.e., $\eta_i(t)^1 \neq \eta_i(t)^2$, and the secure state estimation is achieved.

With Definition 2, there exist two different initial values $x_i(0)^1 \neq x_i(0)^2$, such that, (2) is valid when $d_i(t) = 0$. For convenience, the measurement y_i in the time interval $[0, t]$ is denoted as Y_i. Clearly, with Y_i, an estimator only gives one result, in other words, either $(x_i(0)^1, \eta_i^1)$ or $(x_i(0)^2, \eta_i^2)$ will be obtained by the estimator. Without loss of generality, suppose the initial state and attack is $(x_i(0)^1, \eta_i^1)$. Then it results in the measurements Y_i. However, in that case, $(x_i(0)^2, \eta_i^2)$ may be obtained by the estimator with Y_i. This is a contraction to that the secure estimation is achieved.

2) *Necessity:* We also resort to contraction. Assume there exists no unidentifiable attack, and the secure state estimation cannot be achieved when $d_i(t) = 0$. Then for a unique Y_i, two different estimations can be obtained, i.e., $(x_i(0)^1, \eta_i^1)$ and $(x_i(0)^2, \eta_i^2)$. In other words, both $(x_i(0)^1, \eta_i^1)$ and $(x_i(0)^2, \eta_i^2)$ are corresponding to the same measurements, i.e., (2) is valid. Thus, with Definition 2, $\eta_i^1(t)$ and $\eta_i^2(t)$ are unidentifiable attacks. This is also a contraction. ■

B. Problem Formulation

Our main objective is to solve the following three problems.

1) Sufficient Conditions for Secure State Estimation: Establish sufficient conditions that the secure state estimation problem of the CPS under sensor attacks in (1) can be solved in the absence of noise, i.e., $d_i(t) = 0$.

2) Distributed Finite Time Secure State Estimation: With the sufficient conditions, design a distributed estimator $\Gamma_i(\bar{y}, \bar{u}, t)$ such that its output $\hat{x}_i(t)$ can converge to the state $x_i(t)$ in a given finite time $T_{e,i}$ in the absence of noise, i.e., for $\forall t > T_{e,i}$

$$\hat{x}_i(t) = x_i(t) \tag{3}$$

where $i = 1, \ldots, N$.

3) Distributed Secure Control Design: Design distributed controller $u_i(x_i, \bar{y}t)$ such that the state $x_{i,1}(t)$ of the interconnected CPS in (1) can track a desired trajectory $x_{d,i}(t)$, i.e., $x_{i,1}(t) \to x_{d,i}(t)$ in the absence of noise, as $t \to \infty$, $i = 1, \ldots, N$.

III. Distributed Finite Time Secure State Estimation

In this section, we solve the first problem starting with the conditions that the secure state estimation can be achievable.

A. Secure State Estimation Conditions

To solve the secure state estimation problem of the CPSs in (1), a sufficient condition is presented as follows.

Condition 1: For the interconnected CPSs in (1) under s_i-sparse attacks, s_i satisfies that

$$s_i \leq \begin{cases} \frac{1}{2}(p_i - 1), & \text{if} \quad p_i \quad \text{odd} \\ \frac{1}{2}p_i - 1, & \text{if} \quad p_i \quad \text{even.} \end{cases} \tag{4}$$

Then, we have the following proposition.

Proposition 1: Consider the interconnected CPSs in (1). Then for any sparse attack $\eta(t)$, if Condition 1 holds, the secure state estimation problem is solvable when $d_i(t) = 0$.

Proof: For convenience, denote $\bar{\varpi}(t) = [\varpi_1^T(t), \ldots, \varpi_n^T(t)]^T$ with $\varpi_i(t) = [x_{1,i}(t), \ldots, x_{N,i}(t)]^T$, $\bar{y}(t) = [y_1^T(t), \ldots, y_N^T(t)]^T$, $\bar{u}(t) = [u_1(t), \ldots, u_N(t)]^T$, and $\bar{\eta}(t) = [\eta_1^T(t), \ldots, \eta_N^T(t)]^T$. Rewriting (1) gives that

$$\Sigma_a : \begin{cases} \dot{\bar{\varpi}}(t) = \bar{A}_{\varpi}\bar{\varpi}(t) + \bar{B}_{\varpi}\bar{u}(t) \\ \bar{y}(t) = \bar{C}_{\varpi}\bar{\varpi}(t) + \bar{\eta}(t) \end{cases} \tag{5}$$

where

$$\bar{A}_{\varpi} = \begin{bmatrix} \Delta_1 & I_N & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{n-1} & 0 & \cdots & I_N \\ \Gamma & 0 & \cdots & 0 \end{bmatrix}$$

Δ_i are some nonzero matrices, $\bar{B}_{\varpi} = \bar{T}\bar{B}$ with Γ is also a constant matrix and $\bar{C}_{\varpi} = \bar{C}\bar{T}^{-1}$ with $\bar{C} = \text{diag}\{C_1, \ldots, C_N\}$ and $\bar{T}$ being the transformation matrix such that $\bar{\varpi}(t) = \bar{T}\bar{x}(t)$.

With Lemma 1, the solvability of the secure state estimation problem is equivalent to the absence of unidentifiable sparse attacks. In other words, for any different attacks, i.e., $\bar{\eta}(t)^1 \neq \bar{\eta}(t)^2$, when Condition 1 is valid, then they are identifiable. To prove this, we resort to contradiction.

Assume Condition 1 is valid and $\bar{\eta}(t)^1 \neq \bar{\eta}(t)^2$ are two unidentifiable attacks. On one hand, from Definition 2, there exist two different initial state $\bar{x}(0)^1 \neq \bar{x}(0)^2$, such that $\bar{y}(\bar{x}(0)^1, \bar{u}, \bar{\eta}^1, t) = \bar{y}(\bar{x}(0)^2, \bar{u}, \bar{\eta}^2, t)$ for all $t > 0$. Furthermore, as the CPSs is linear, then it follows that:

$$0 = \bar{y}(\bar{e}_{\varpi}(0), 0, \bar{\eta}, t) \tag{6}$$

where $\bar{e}_{\varpi}(0) = \bar{T}\bar{e}(0)$ and $\bar{\eta}(t) = \bar{\eta}(t)^1 - \bar{\eta}(t)^2$ with $\bar{e}(0) = \bar{x}(0)^1 - \bar{x}(0)^2$.

Then, rewriting (5) gives that

$$\Sigma_a : \begin{cases} \dot{\bar{e}}_{\varpi}(t) = \bar{A}_{\varpi}\bar{e}_{\varpi}(t) \\ \begin{bmatrix} \bar{y}_a(t) \\ \bar{y}_0(t) \end{bmatrix} = \begin{bmatrix} \bar{C}_{\varpi,a} \\ \bar{C}_{\varpi,0} \end{bmatrix} \bar{e}_{\varpi}(t) + \begin{bmatrix} \bar{\eta}_a(t) \\ 0 \end{bmatrix} \end{cases} \tag{7}$$

where $\bar{e}_{\varpi}(t) = \bar{T}\bar{e}(t)$, a is the set that includes all corrupted sensors and 0 is its complementary, $\bar{C}_{\varpi,a}$ consists of all $\sum_i^N s_i$ rows of $\bar{C}_{\varpi}$ including the attacked sensors and $\bar{C}_{\varpi,0}$ has the rest rows without attacks, $\bar{\eta}_a(t)$ includes all potential nonzero elements of $\bar{\eta}(t)$. Clearly, it is easy to get that $s_i \leq (p_i - 1)/2$ is valid for both cases that p_i is odd and even. Thus, we only consider the case $s_i \leq (p_i - 1)/2$ in the following analysis.

With (7), (6) is valid if $\bar{\eta}_a(t)$ and $\bar{e}_{\varpi}(0)$ are given as follows:

$$\begin{cases} \bar{\eta}_a(t) = -\bar{C}_{\varpi,a}e^{\bar{A}_{\varpi}t}\bar{e}_{\varpi}(0) \\ 0 = \bar{C}_{\varpi,0}e^{\bar{A}_{\varpi}t}\bar{e}_{\varpi}(0). \end{cases} \tag{8}$$

With linear system theory, the existence of nonzero $\bar{e}_{\varpi}(0)$ that the second row of (8) is valid is equivalent to that there exist some $s \in \mathbb{C}$, such that the following condition is valid:

$$\operatorname{rank}\begin{bmatrix} sI_{nN} - \bar{A}_{\varpi} \\ \bar{C}_{\varpi,0} \end{bmatrix} < nN. \tag{9}$$

On the other hand, under Condition 1, two different attacks $\bar{\eta}(t)^1$ and $\bar{\eta}(t)^2$ only corrupt at most $(p_i - 1)/2$ sensors of the ith subsystem, respectively. Consider the worst case that $\bar{\eta}(t)^1$ and $\bar{\eta}(t)^2$ corrupt different $(p_i - 1)/2$ sensors, respectively, then $\bar{\eta}(t)$ can manipulates at most $p_i - 1$ sensors arbitrarily for the ith subsystem. Thus, there exists at least one out of p_i sensors in the ith subsystem that is free of attack, which means $\bar{C}_{\varpi,0} = [I_N, 0, \ldots, 0]$ in the worst case. Then with the definition of $\bar{A}_{\varpi}$ and $\bar{C}_{\varpi,0}$, it is easy to get that

$$\operatorname{rank}\begin{bmatrix} sI_{nN} - \bar{A}_{\varpi} \\ \bar{C}_{\varpi,0} \end{bmatrix} = nN \tag{10}$$

which contradicts to (9).

Thus, we can conclude that, when Condition 1 is valid, the secure state estimation problem of the CPS in (1) is solvable in the absence of noise. ■

B. Preselector Design

In this section, we will present a distributed scheme to obtain the sensor free attacks of the ith subsystem. Let us start with the median value operator Med$[\cdot]$ defined as follows.

Given a vector $y_i(t)$, rearranging it in increasing order of values results in a vector $v_i = [v_{i,1}, \ldots, v_{i,p_i}]^T$ satisfying that $v_{i,1} \leq \cdots \leq v_{i,p_i}$. Then the median value of $y_i(t)$ is

$$\operatorname{Med}\big[y_i(t)\big] = \begin{cases} v_{i,\text{in}}, & \text{in} = \frac{1}{2}(p_i + 1), \quad p_i \quad \text{odd} \\ \frac{1}{2}\big(v_{i,\text{in}} + v_{i,\text{in}+1}\big), & \text{in} = \frac{1}{2}p_i, \quad p_i \quad \text{even}. \end{cases} \tag{11}$$

Under Condition 1, we now present a distributed secure preselector of the ith subsystem as follows:

$$z_{p,i}(t) = \operatorname{Med}\big[y_i(t)\big]. \tag{12}$$

Then we have the following result.

Theorem 1: For the interconnected CPS (1) which is under sensor attacks, if Condition 1 is valid, then with the preselector in (12), we can obtain that, when $d_i(t) = 0$, for $\forall t > 0$

$$x_{i,1}(t) = z_{p,i}(t). \tag{13}$$

Proof: Suppose that for the ith subsystem in (1), s_i out of p_i sensors are attacked, and the rest $p_i - s_i$ sensors are free of attacks. Then the measurement can be written as follows:

$$y_i(t) = \big[x_{i,1}(t) + \eta_{i,1}(t), \ldots, x_{i,p_i}(t) + \eta_{i,p_i}(t)\big]^T \tag{14}$$

where only s_i elements of $\eta_i(t)$ is nonzero. Without loss of generality, suppose g_i out of s_i attacks are positive and the set of these sensors is G_i with $\text{Card}(G_i) = g_i$. The rest o_i are negative with set O_i and $\text{Card}(O_i) = o_i$. Also the set of sensors free of attack is R_i with $\text{Card}(R_i) = r_i$. Clearly, $g_i + o_i = s_i$ and $s_i + r_i = p_i$.

Denote the sets as $O_i = \{j_1, \ldots, j_{o_i}\}$ and $G_i = \{k_1, \ldots, k_{g_i}\}$. Then the nonzero attacks can be written as follows:

$$\eta_{i,j_1}(t) \leq \cdots \leq \eta_{i,j_{o_i}}(t) < 0 < \eta_{i,k_1}(t) \leq \cdots \leq \eta_{i,k_{g_i}}(t). \tag{15}$$

Rearranging the measurement $y_i(t)$ in increasing order of values gives that

$$\begin{aligned} \underbrace{y_{i,j_1}(t) \leq \cdots \leq y_{i,j_{o_i}}(t)}_{o_i} &< \underbrace{y_{i,r_1}(t) \cdots = y_{i,r_i}(t)}_{r_i} \\ &< \underbrace{y_{i,k_1}(t) \leq \cdots \leq y_{i,k_{g_i}}(t)}_{g_i}. \end{aligned} \tag{16}$$

Now we divide the proof into three parts, respectively, corresponding to three cases: 1) $g_i = 0, o_i = s_i$; 2) $g_i = s_i, o_i = 0$; and 3) $g_i \neq 0, o_i \neq 0$.

Case 1: This part also includes two subcases, i.e., p_i is odd and p_i is even. When p_i is odd, $s_i \leq (p_i - 1)/2$. So $r_i - s_i = p_i - 2s_i = q_i \geq 1$ and q_i is odd. Then rewriting (16) gives that

$$\begin{aligned} \underbrace{y_{i,j_1}(t) \leq \cdots \leq y_{i,j_{o_i}}(t)}_{s_i} &< \underbrace{y_{i,r_1}(t) \cdots = y_{i,r_{q_i}}(t)}_{q_i} \\ &= \underbrace{y_{i,r_{q_i+1}}(t) \cdots = y_{i,r_i}(t)}_{s_i}. \end{aligned} \tag{17}$$

Clearly, from (11), it follows that:

$$\operatorname{Med}\big[y_i(t)\big] = \operatorname{Med}\big[y_{q,i}(t)\big] \tag{18}$$

where $y_{q,i}(t) = [y_{i,r_1}(t), \ldots, y_{i,r_{q_i}}(t)]^T \in R^{q_i}$. Then, it is easy to get that, each element of $y_{q,i}(t)$ is free of attack, thus, (22) is also valid.

For the case that p_i is even, $s_i \leq p_i/2 - 1$, and thus $r_i - s_i = p_i - 2s_i = q_i \geq 2$ and q_i is even. By following similar approach from (17) and (18), (22) is also valid.

Case 2: When $g_i = s_i, o_i = 0$, the proof is similar to 1), and thus we omit it here.

Case 3: When $g_i \neq 0, o_i \neq 0$, without loss of generality, suppose $o_i \geq g_i$, then $o_i = q_i + g_i$ where $q_i \geq 0$. Note that,

$r_i - o_i = p_i - s_i - (s_i - g_i) = p_i - 2s_i + g_i \geq p_i - 2s_i$, clearly, $r_i > o_i$. Thus, rewriting (16) gives that

$$\begin{aligned} &\underbrace{y_{i,j_1}(t) \leq \cdots \leq y_{i,j_{o_i}}(t)}_{o_i} < \underbrace{y_{i,r_1}(t) = \cdots = y_{i,r_i-q_i}(t)}_{r_i-q_i} \\ &= \underbrace{y_{i,r_i-q_i+1}(t) \cdots = y_{i,r_i}(t)}_{q_i} < \underbrace{y_{i,k_1}(t) \leq \cdots \leq y_{i,k_{g_i}}(t)}_{g_i}. \end{aligned} \quad (19)$$

From (11), the median value of $y_i(t)$ is equal to that of the vector obtained after removing o_i items larger than the median value and o_i items less than the median value from $y_i(t)$, i.e.,

$$\text{Med}\big[y_i(t)\big] = \text{Med}\big[y_{rq,i}(t)\big] \quad (20)$$

where $y_{rq,i}(t) = [y_{i,r_1}(t), \ldots, y_{i,r_1-q_i}(t)]^T \in R^{r_i-q_i}$. Thus, it is easy to get that, each element of $y_{rq,i}(t)$ is free of attack, thus, (22) is also valid.

Therefore, we can conclude Theorem 1. ∎

Remark 2: The distributed preselector in (12) is inspired by the resilient detection in [15]. The proposed distributed preselectors ensure us to obtain the secure state estimation in a given finite time from the corrupted measurements.

In the presence of measurement white noise, i.e., $E[d_i(t)] = 0$ where $E[\cdot]$ denotes the expectation, by noting that $E[x_{i,j}(t)] = x_{i,j}(t)$ and $E[\eta_{i,j}(t)] = \eta_{i,j}(t)$, we have

$$E\big[y_i(t)\big] = \begin{bmatrix} x_{i,1}(t) + \eta_{i,1}(t) \\ \vdots \\ x_{i,p_i}(t) + \eta_{i,p_i}(t) \end{bmatrix}. \quad (21)$$

Corollary 1: For the interconnected CPS (1) which is under sensor attacks, if Condition 1 is valid, then with the preselector in (12), we can obtain that, for $\forall t > 0$

$$x_{i,1}(t) = E\big[z_{p,i}(t)\big]. \quad (22)$$

Proof: By replacing $y_i(t)$ and $z_{p,i}(t)$ with $E[y_i(t)]$ and $E[z_{p,i}(t)]$ and following a similar approach to the proof of Theorem 1, the results can be obtained. ∎

C. Design of Distributed Finite Time Secure State Estimator

In this section, we solve the distributed finite time secure state estimation problem.

With the preselector in (12) and inspired by the finite time observer in [21]–[23], we can design another observer for the ith subsystem as follows, to achieve finite time secure state estimation

$$\begin{cases} \dot{\hat{\bar{\zeta}}}_i(t) = \bar{F}_i \hat{\bar{\zeta}}_i(t) + \bar{H}_i \Lambda^i \bar{z}_p(t) + \bar{L}_i z_{p,i}(t) + \bar{H}_i B_i u_i(t) \\ \hat{x}_i(t) = \bar{M}_i \Big[\hat{\bar{\zeta}}_i(t) - e^{\bar{F}_i T_{e,i}} \hat{\bar{\zeta}}_i\big(t - T_{e,i}\big)\Big] \end{cases} \quad (23)$$

where $\hat{x}_i(t)$ is the estimation of $x_i(t)$, $\hat{\bar{\zeta}}_i(t) \in \mathbb{R}^{2n}$, $\bar{H}_i = [I_{n\times n}, I_{n\times n}]^T$, $\bar{F}_i = \text{diag}\{F_{i,1}, F_{i,2}\}$ and $\bar{L}_i = [L_{i,1}^T, L_{i,2}^T]^T$ with $L_{i,1}, L_{i,2} \in R^{n\times p}$ such that $F_{i,j} = A_{i,0} - L_{i,j}C_{i,0}$ is Hurwitz with $A_{i,0}$ being given in (1). The constant $T_{e,i}$ and matrix $\bar{M}_i$ are design parameters and their choices are given as follows.

Since the pair $(A_{i,0}, I_n)$ is observable, then the eigenvalues of $F_{i,1}$ and $F_{i,2}$ in (23) can be manipulated arbitrarily. Thus, the existence of the integer $T_{e,i}$ can be ensured by choosing such eigenvalues as follows:

$$0 < |\lambda^i_{1,\min}| < |\lambda^i_{1,\max}| < \tau_i < |\lambda^i_{2,\min}| < |\lambda^i_{2,\max}| \quad (24)$$

where $\lambda^i_{j,\min} = \min\{\lambda(F_{i,j})\}$ and $\lambda^i_{j,\max} = \max\{\lambda(F_{i,j})\}$ with $j = 1, 2$ and $i = 1, \ldots, N$.

Lemma 2 (Lemma 1 [21]): If the eigenvalues of $F_{i,1}$ and $F_{i,2}$ satisfy (24), there exists an integer $T_{e,i}$ such that

$$\det\Big[\bar{H}_i \; \bar{F}_i^{T_{e,i}} \bar{H}_i\Big] \neq 0. \quad (25)$$

Now the process to obtain the integer $T_{e,i}$ is given as follows.

Step 1: For the CPS under attack in (1), as the pair $(A_{i,0}, I_n)$ is known and observable, then two vectors $L_{i,1}, L_{i,2}$ can be chosen such that $F_{i,j} = A_{i,0} - L_{i,j}$ is Hurwitz and (24) is valid, $j = 1, 2$.

Step 2: From Lemma 2, the existence of $T_{e,i}$ is ensured, thus a constant $T_{e,i}$ can be chosen such that (25) is valid.

Then the matrix $\bar{M}_i$ is obtained

$$\bar{M}_i = \big[I_n \; 0_n\big]\Big[\bar{H}_i \; e^{\bar{F}_i}\bar{H}_i\Big]^{-1}. \quad (26)$$

For convenience, let $T_{e,i} = T_e$ for all $i = 1, \ldots, N$.

Thus, the following result on the finite time secure state estimation can be obtained.

Theorem 2: For the CPS under sparse attacks in (1), if Condition 1 is valid and $d_i(t) = 0$, then with the secure preselector in (12) and the distributed observer in (23), the state of (1) can be obtained in a finite time, i.e., for $\forall t \geq T_e$

$$x_i(t) = \hat{x}_i(t). \quad (27)$$

Proof: Let $\bar{e}_{\zeta,i}(t) = Hx_i(t) - \hat{\bar{\zeta}}(t)$, then

$$\dot{\bar{e}}_{\zeta,i}(t) = \bar{H}_i x_i(t) - \dot{\hat{\bar{\zeta}}}_i = F\bar{e}_{\zeta,i}(t). \quad (28)$$

Clearly, by denoting the initial estimation error as $\bar{e}_{\zeta,i}(0)$, we obtain from (28) that

$$\bar{e}_{\zeta,i}(t) = e^{\bar{F}_i t}\bar{e}_{\zeta,i}(0) = e^{\bar{F}_i T_e}\bar{e}_{\zeta,i}(t - T_e). \quad (29)$$

Then with $\bar{e}_{\zeta,i}(t) = \bar{H}_i x_i(t) - \hat{\bar{\zeta}}_i(t)$ and $\bar{e}_{\zeta,i}(t)(t - T_e) = Hx(t - T_e) - \hat{\bar{\zeta}}_i(t - T_e)$, (29) gives that

$$\bar{H}_i x_i(t) - e^{\bar{F}_i T_e}\bar{H}_i x_i(t - T_e) = \hat{\bar{\zeta}}_i(t) - e^{\bar{F}_i T_e}\hat{\bar{\zeta}}_i(t - T_e). \quad (30)$$

As F_1 and F_2 are chosen according to (24) and T_e is chosen according to (25), (26) yields that

$$\bar{M}_i\Big[\bar{H}_i \quad e^{\bar{F}_i T_e}\bar{H}_i\Big] = \big[I_{n\times n} \quad 0_{n\times n}\big]. \quad (31)$$

Clearly with (31), multiplying $\bar{M}_i$ on both sides of (30) results in that

$$x_i(t) = \bar{M}_i\Big[\hat{\bar{\zeta}}_i(t) - e^{\bar{F}_i T_e}\hat{\bar{\zeta}}_i(t - T_e)\Big]. \quad (32)$$

Comparing (32) with (23), we have $x_i(t) = \hat{x}_i(t)$ for all $t \geq T_e$. ∎

Remark 3: Note that the secure state estimation algorithms in [14] ensure the estimation error to converge to a given

small constant in N steps where N is not prespecified, whereas the exact secure state estimation in this paper is achieved in a pregiven finite time. Furthermore, the proposed scheme is in a distributed form, which is more convenient for practical implementation.

Corollary 2: For the CPS under sparse attacks in (1), if Condition 1 is valid, then with the secure preselector in (12) and the distributed observer in (23), then when $\forall t \geq T_e$

$$E[x_i(t)] = E\big[\hat{x}_i(t)\big]. \tag{33}$$

Proof: By replacing $x_i(t)$ and $\hat{x}_i(t)$ with $E[x_i(t)]$ and $E[\hat{x}_i(t)]$ and following a similar approach to the proof of Theorem 2, the results can be obtained. ■

Remark 4: Corollary 2 ensures the expectation of the state estimation converge to the real state exactly in a finite time, it is also needed to point out that, in the presence of the measurement noise, the exact secure estimation is impossible, thus the presented method is similar to that of the Kalman filter like method in [14].

IV. Distributed Finite Time Secure Control

In this section, we solve the secure control problem via virtual fraction dynamic surface.

A. Finite Time Secure Control Design

Denote the tracking error of the ith subsystem of the interconnected CPS as $e_{i,1}(t) = x_{i,1}(t) - x_{d,i}(t)$ and $e_{i,j}(t) = \dot{e}_{i,j-1}(t)$ where $j = 2, \ldots, n$. Clearly, we have

$$\begin{cases} \dot{e}_{i,k}(t) = \sum\limits_{j=1}^{k+1} \vartheta_{i,k,j} x_{i,j}(t) - x_{i,d}^{(k)}(t) \\ \dot{e}_{i,n}(t) = \sum\limits_{j=1}^{n} \vartheta_{i,n,j} x_{i,j}(t) + b_i u(t) + \sum\limits_{j \in J_i} \Gamma_j^i x_{j,1}(t) - x_{i,d}^{(n)}(t) \end{cases} \tag{34}$$

where $x_{d,i}^{(k)}(t)$ is the (k)th order derivative of $x_{d,i}(t)$, $j = 2, \ldots, n$ and $\vartheta_{i,n,j}$ is given as follows:

$$\vartheta_{i,k,j} = \begin{cases} \sum\limits_{l=1}^{k} a_{i,l} \vartheta_{i,k-1,l} & j = 1 \\ \vartheta_{i,k-1,j-1} & j \geq 2 \end{cases} \tag{35}$$

where $\vartheta_{i,1,1} = a_{i,1}$, $\vartheta_{i,1,2} = 1$ and $1 \leq k \leq i-1$ with $1 \leq i \leq n$.

Let $\varsigma_i(t) = \sum_{j=0}^{n-1} k_{i,n-j} e_{i,j+1}(t)$ and the virtual fractional dynamic surface be $\varsigma_i^{\alpha_i}(t)$ where $0 < \alpha_i < 1$, $k_{i,n} = 1$ and $k_{i,j}$ is chosen such that $k_{i,1} + k_{i,2} s + \cdots + s^{n-1}$ is a Hurwitz polynomial. For convenience, by denoting $K_i = [k_{i,1}, \ldots, 1]$, it gives that $\varsigma_i(t) = K_i e_i(t)$ where $e_i(t) = [e_{i,1}(t), \ldots, e_{i,n}(t)]^T$, and the error dynamics is as follows:

$$\dot{\varsigma}_i(t) = K_i \dot{e}_i(t) = K_i A_i x_i(t) + K_i \Gamma_i z_p(t) + K_i B_i u_i(t) - K_i \bar{x}_{d,i}(t) \tag{36}$$

where $\bar{x}_{d,i}(t) = [x_{d,i}(t), \ldots, x_{d,i}^{(n-1)}(t)]^T$, $B_i = [0, \ldots, 0, b_i]$, $\Gamma_i = [\Gamma_i^1, \ldots, \Gamma_i^N]$ and

$$A_i = \begin{bmatrix} \varsigma_{i,1,1} & \varsigma_{i,1,2} & \cdots & 0 \\ \varsigma_{i,2,1} & \varsigma_{i,2,2} & \ddots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ \varsigma_{i,n,1} & \varsigma_{i,n,2} & \cdots & \varsigma_{i,n,n} \end{bmatrix}$$

with $\varsigma_{i,j,k}$ being given in (35).

As the exact state can be obtained with the secure estimator in (23) in a finite time. Based on this, a distributed finite time secure control of the ith subsystem is designed as follows:

$$u_i(t) = \begin{cases} 0 & 0 < t < T_e \\ \frac{1}{b_i} \gamma_i(t) & T \geq T_e \end{cases} \tag{37}$$

where $\gamma_i(t)$ is given as

$$\begin{aligned} \gamma_i(t) = -\big[& c_{i,1} \hat{\varsigma}_i(t) + c_{i,2} \hat{\varsigma}_i^{\alpha_i}(t) + K_i A_i \hat{x}_i(t) \\ & + K_i \Gamma_i \bar{z}_p(t) - K_i \bar{x}_{d,i}(t) \big] \end{aligned} \tag{38}$$

where $\hat{\varsigma}_i(t) = \sum_{j=0}^{n-1} k_{i,n-j} \hat{e}_{i,j}(t)$ with $\hat{e}_{i,j}(t) = \hat{x}_{i,j}(t) - x_{d,i}^{(j-1)}(t)$, $c_{i,1}, c_{i,2} > 0$ and $\alpha_i = h_{i,1}/h_{i,2}$ are design parameters with $1 \leq h_{i,1} < h_{i,2}$ being two designed odd integers.

Remark 5: The fractional dynamic surface $\varsigma_i^{\alpha_i}(t)$ is inspired by the work in [24], which plays an important role in the presented distributed control in (37). It not only ensures the dynamic surface $\varsigma_i(t)$ to be achieved and maintained in a finite time, but also guarantees that the control law $u_i(t)$ is bounded and continuous for $\forall t$. Also the secure controllers are in distributed form and simple for practical implementation.

B. Stability Analysis

We are at the position to present our result on finite time secure control.

Theorem 3: For the interconnected CPS in (1), suppose Condition 1 is valid and $d_i(t) = 0$. Then with the secure preselector in (12), the distributed finite time observer in (23), and the distributed secure control law in (37), the following statements are hold.

1) The dynamic surface $\varsigma_i(t)$ can be reached in a finite time no more than $T_s = T_e + T_c$, where T_e to meet (25) and T_c is as follows:
$$T_c = 2^{-\beta_i} V_i^{1-\beta_i}(T_e)/c_{i,2} \tag{39}$$
where $\beta_i = ([3\alpha_i - 1]/2\alpha_i)$.
2) Furthermore, $x_{i,1}(t)$ can track the desired trajectory $x_{d,i}(t)$ exponentially, and the designed control law $u_i(t)$ is also bounded and continuous.

Proof: 1) First, we would show that $\varsigma_i(t)$ can be reached in a finite time no more than $T_s = T_e + T_c$, and this proof can be divided into two parts, i.e., $0 < t \leq T_e$ and $T_e < t \leq T_e + T_c$.

a) With Theorem 2, the exact state of (1) can be obtained by the distributed finite time observer in (23) with the secure preselector in (12), i.e., $\hat{x}_i(t) = x_i(t)$ for $\forall t \geq T_e$, $i = 1, \ldots, N$.

Second, as $u_i(t) = 0$ when $0 < t \leq T_e$, then the CPS in (1) can be treated as an autonomous system which is expressed as $\bar{x}(t) = \bar{T}^{-1}\bar{\varpi}(t)$ where $\bar{\varpi}(t) = e^{\bar{A}_{\varpi} t}\bar{\varpi}(0)$, $\bar{T}$ is a transformation matrix such that $\bar{\varpi}(t) = \bar{T}\bar{x}(t)$ and $\bar{A}_{\varpi}$ is given in (5). Clearly, at the time $t = T_e$, the state in (1) can be given as follows:

$$\bar{x}(T_e) = \bar{T}^{-1} e^{\bar{A}_{\varpi} T_e} \bar{T}\bar{x}(0) \tag{40}$$

where $\bar{x}(0)$ is the initial value of $\bar{x}(t)$. As $\bar{x}(0)$ and T_e are finite, thus $\bar{x}(T_e)$ is finite, which implies that $x_i(T_e)$ is also so.

b) When $T_e < t \leq T_e + T_c$, we will show that $\varsigma_i(t)$ converges to zero when $t = T_e + T_c$ and remains 0 afterward. Define a Lyapunov function $V_i(t) = (1/2)\varsigma_i^{2\alpha_i}(t)$. By noting that $x_i(t) = \hat{x}_i(t)$ for $t \geq T_e$, then $e_{i,j}(t) = \hat{e}_{i,j}(t)$ and $\varsigma_i(t) = \hat{\varsigma}_i(t)$ for all $t \geq T_e$.

The derivative of $V_i(t)$ along the dynamics in (36) satisfies

$$\begin{aligned}\dot{V}_i(t) = \varsigma_i^{2\alpha_i - 1}(t)\big[&K_i A_i x_i(t) + K_i \Gamma_i z_p(t) \\ &+ K_i B_i u_i(t) - K_i \bar{x}_{d,i}(t)\big].\end{aligned} \tag{41}$$

Substituting the control law in (37) to (41) gives that

$$\begin{aligned}\dot{V}_i(t) &= -c_{i,1}\varsigma_i^{2\alpha_i}(t) - c_{i,2}\varsigma_i^{3\alpha_i - 1}(t) \\ &= -c_{i,1}\varsigma_i^{2\alpha_i}(t) - c_{i,2}\varsigma_i^{2\alpha_i \beta_i}(t)\end{aligned} \tag{42}$$

where $\beta_i = ([3\alpha_i - 1]/2\alpha_i)$. As $h_{i,1}, h_{i,2}$ are odd, it gives that $3h_{i,1} - h_{i,2}$ is even, thus $\varsigma_i^{2\alpha_i\beta_i}(t) > 0$ for $\forall \varsigma_i(t) \neq 0$.

By noting the definition of $V_i(t)$, (42) gives that

$$\dot{V}_i(t) = -c_{i,1}V_i(t) - c_{i,2}V_i^{\beta_i}(t) \leq -c_{i,2}V_i^{\beta_i}(t). \tag{43}$$

Clearly, as $0.5 < \alpha_i < 1$, then we have that $0 < \beta_i < 1$.

Then integrating (42) in the time interval (T_e, t), we obtain

$$V_i^{1-\beta_i}(t) \ \leq -c_{i,2}2^{\beta_i}(t - T_e) + V_i^{1-\beta_i}(T_e). \tag{44}$$

As $V_i(t) \geq 0$ for $\forall \varsigma_i(t)$, for $t \geq T_s = T_e + T_c$ with T_c being given in (39), we can have $V_i^{1-\beta_i}(t) \leq 0$. Then with the definition of $V_i(t)$, it gives $\varsigma_i(t) = 0$, for $t \geq T_s$. This implies that the dynamic surface $\varsigma_i(t) = 0$ can be reached at $t = T_s$ and maintained afterward.

2) Furthermore, we would show that, $x_{i,1}(t)$ converges to $x_{i,d}(t)$ exponentially, $i = 1, \ldots, N$.

First, let us begin with the performance of $\varsigma_i(t)$. Clearly, with (44), it gives that, $\varsigma_i(t) \leq \varsigma_i(T_e)$, for $\forall t \geq T_e$. In addition, with the definition of $\varsigma_i(t)$, we have

$$|\varsigma_i(t)| \leq |\varsigma_i(T_e)| \leq \sum_{j=0}^{n-1} k_{i,n-j}|e_{i,j}(T_e)| \tag{45}$$

where $k_{i,n-j} > 0$, $i = 1, \ldots, N$.

Also, we have

$$\dot{\bar{e}}_i(t) = \Theta_i \bar{e}_i(t) + \bar{\varsigma}_i(t) \tag{46}$$

where $\bar{e}_i(t) = [e_{i,1}(t), \ldots, e_{i,n-1}(t)]^T$, $\bar{\varsigma}_i(t) = [0, \ldots, \varsigma_i(t)]^T$ and

$$\Theta_i = \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ -k_{i,1} & -k_{i,2} & \cdots & -k_{i,n-1} \end{bmatrix}$$

being a Hurwitz matrix as $k_{i,1} + k_{i,2}s + \cdots + s^{n-1}$ is a Hurwitz polynomial.

Multiplying $e^{-\Theta_i t}$ on both sides of (46) and then integrating it in the time interval (T_e, t) result in

$$e^{-\Theta_i t}\bar{e}_i(t) - e^{-\Theta_i T_e}\bar{e}_i(T_e) = \int_{T_e}^{t} e^{-\Theta_i \tau}\bar{\varsigma}_i(\tau)d\tau. \tag{47}$$

Clearly, multiplying $e^{\Theta_i t}$ on both sides of (47) yields

$$\bar{e}_i(t) = e^{\Theta_i(t - T_e)}\bar{e}_i(T_e) + \int_{T_e}^{t} e^{\Theta_i(t-\tau)}\bar{\varsigma}_i(\tau)d\tau. \tag{48}$$

As Θ_i is Hurwitz, then there exist constants γ_i and $\kappa_i > 0$, such that $\|e^{\Theta_i t}\| \leq \gamma_i e^{-\kappa_i t}$ for $\forall t \geq 0$. From (47), we have

$$\|\bar{e}_i(t)\| \leq \gamma_i e^{-\kappa_i(t - T_e)}\|\bar{e}_i(T_e)\| + \gamma_i e^{-\kappa_i t}\int_{T_e}^{T_s} e^{\kappa_i \tau}\|\bar{\varsigma}_i(\tau)\|d\tau. \tag{49}$$

Noting that $\varsigma_i(t) \leq \varsigma_i(T_e)$ as $t \in (T_e, T_s]$ and $\varsigma_i(t) = 0$ as $t \geq T_s$ with $T_s = T_e + T_c$, then substituting (45) into (49) gives

$$\begin{aligned}\|\bar{e}_i(t)\| \leq{}& \gamma_i e^{-\kappa_i(t - T_e)}\|\bar{e}_i(T_e)\| \\ &+ \frac{\gamma_i}{\kappa_i}e^{-\kappa_i t}e^{\kappa_i T_e}\big(e^{\kappa_i T_c} - 1\big)|\varsigma_i(T_e)|.\end{aligned} \tag{50}$$

From (39) and the definition of $V_i(t)$, we have

$$T_c \leq \frac{1}{2^{1+\beta_i}c_{i,2}}\varsigma_i^{\varrho_i}(T_e) \leq \frac{1}{2^{1+\beta_i}c_{i,2}}\left(\sum_{j=0}^{n-1} k_{i,n-j}|e_{i,j}(T_e)|\right)^{1+\varrho_i} \tag{51}$$

where $\varrho_i = 2\alpha_i(1 - \beta_i)$. Note that $\beta_i = ([3\alpha_i - 1]/2\alpha_i)$, then we have $\varrho_i = 1 - \alpha_i$.

Clearly, from the definition of $\bar{e}_i(t)$ and (50), $|e_{i,j}(t)| \leq \gamma_i e^{-\kappa_i(t-T_e)}\|\bar{e}_i(T_e)\| + \frac{\gamma_i}{\kappa_i}e^{-\kappa_i t}e^{\kappa_i T_e}(e^{\kappa_i T_c} - 1)|\varsigma_i(T_e)|$ where $j = 1, \ldots, n-1$. Also with the definition of $\varsigma_i(t)$, $|e_{i,n}(t)| \leq |\varsigma_i(t)| + \sum_{j=0}^{n-2} k_{i,n-j}e_{i,j+1}(t)$. As $\varsigma_i(t)$ converges to zero in a finite time with and (49), thus $e_{i,n}(t)$ also converges to zero exponentially.

In addition, as $x_{i,j}(t)$ is bounded and continuous, then $\hat{\varsigma}_i(t)$ and $\bar{z}_p(t)$ are also bounded and continuous, and since $0 < \alpha_i < 1$, then $\hat{\varsigma}_i(t)_i^{\alpha}$ is also so, thus the proposed distributed control $u_i(t)$ is bounded and continuous, where $j = 1, \ldots, n$. ■

Remark 6: The introduction of the virtual fractional dynamic surface not only ensures that the dynamic surface can be achieved and maintained in a finite time but also the problem of explosion of complexity inherent in backstepping design of pure-feedback systems can be avoided, which makes

the proposed distributed schemes elegant and easy for practical implementation. In addition, as $0 < \alpha_i < 1$, the proposed distributed control $u_i(t)$ is also bounded and continuous, thus it avoids the discontinuous control problem of the traditional sliding mode control.

C. Discussion on the Choice of Design Parameters

In this section, we present some discussions the choice of design parameters. Substituting (45) and (51) into (50) gives

$$\|\bar{e}_i(t)\| \le \gamma_i e^{-\kappa_i(t-T_e)}\|\bar{e}_i(T_e)\| + \frac{\gamma_i}{\kappa_i}e^{-\kappa_i t}e^{\kappa_i T_e}\left(e^{\kappa_i T_c}-1\right)\left(\sum_{j=0}^{n-1}k_{i,n-j}|e_{i,j}(T_e)|\right). \tag{52}$$

Thus, with the definition of $\bar{e}_i(t)$ and noting that $\|\bar{e}_i(T_e)\| \le (\sum_{j=0}^{n-1}|e_{i,j}(T_e)|)^{1/2}$, then for the first $n-1$ state of the ith subsystem, we have

$$|e_{i,j}(t)| \le \|\bar{e}_i(t)\| \le \gamma_i e^{-\kappa_i(t-T_e)}\left(\sum_{j=0}^{n-1}|e_{i,j}(T_e)|\right)^{1/2} + \frac{\gamma_i}{\kappa_i}e^{-\kappa_i t}e^{\kappa_i T_e}\left(e^{\kappa_i T_c}-1\right)\left(\sum_{j=0}^{n-1}k_{i,n-j}|e_{i,j}(T_e)|\right) \tag{53}$$

where $j = 1, \ldots, n-1$.

Therefore, we have the following guidelines on the choice of the design parameter.

1) From (53), smaller $k_{i,j}$ and larger κ_i may result in smaller bound for $|e_{i,j}(t)|$ for $t \in (0, \infty)$, where $j = 1, \ldots, n-1$.
2) In addition, with (51), we can conclude that, smaller $c_{i,2}$ gives larger T_C.
3) Noting that $e_{i,j+1}(t) = \dot{e}_{i,j}(t)$ can be treated as a surge, as $e_{i,j}(t)$ converges to zero exponentially, thus we can get that, larger T_C and smaller $|e_{i,j}(t)|$ give smaller $|e_{i,j+1}(t)|$, where $j = 1, \ldots, n-1$.

Remark 7: It is noted that, certain tradeoff is needed just as any other control schemes in practice. In particular, $k_{i,j}$ needs to be smaller and κ_i be larger to make $\max(|e_{i,j}(t)|)$ smaller, but this may require larger control efforts as shown in the simulation example. In addition, $c_{i,2}$ should be larger to make the convergence time T_C shorter, but possibly resulting larger magnitude of the higher order state such as $e_{i,j}(t)$, where $j = 2, \ldots, n$. Thus, an appropriate acceptable combination of the parameters needs to be considered to meet given specifications.

V. Numerical Simulation

To illustrate the effectiveness of our proposed scheme, we apply it to the secondary frequency restoration of a islanded MG under sensor attack shown in Fig. 2. This MG consists of four distributed generators (DGs), four local loads, and three transmission lines. Following the methods in [25], with the lossless transmission lines of the MG network, the phase angle droop of the ith DG is

$$\begin{cases}\dot{\delta}_i(t) = \omega_i(t) \\ \tau_{Pi}\dot{\omega}_i(t) + \omega_i(t) + k_{Pi}\left(P_i(t) - P_i^d(t)\right) + u_i(t) = 0\end{cases} \tag{54}$$

where $\delta_i(t)$ and $\omega_i(t)$ are the relative phase angle and frequency, $u_i(t)$ is the controlled mechanical power input of the ith generator, τ_{Pi} is the time constant of a filter to measure the real power, k_{Pi} is the frequency droop gain, $P_i^d(t)$ is the desired real power, $P_i(t)$ is the real and reactive power output

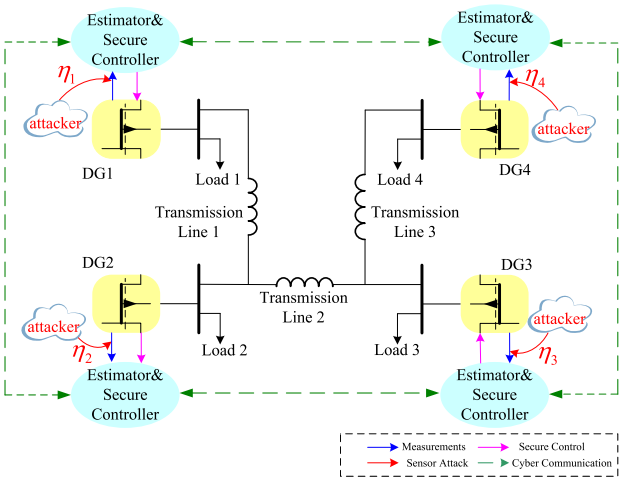


Fig. 2. MG with four interconnected generators under sensor attacks.

TABLE I
PARAMETERS OF MG SYSTEMS

		DG1	DG2	DG3	DG4
Model	τ_{Pi}	0.016	0.016	0.016	0.016
	k_{Pi}	6e-5	3e-5	2e-5	1.5e-5
Load	P_{1i}	0.01	0.01	0.01	0.01
	P_{2i}	1	2	3	4
	P_{3i}	1e4	1e4	1e4	1e4
Line	$B_{12} = 10\Omega^{-1}$, $B_{23} = 10.67\Omega^{-1}$, $B_{34} = 9.82\Omega^{-1}$				
Reference	δ_i^d=1 (rad)				

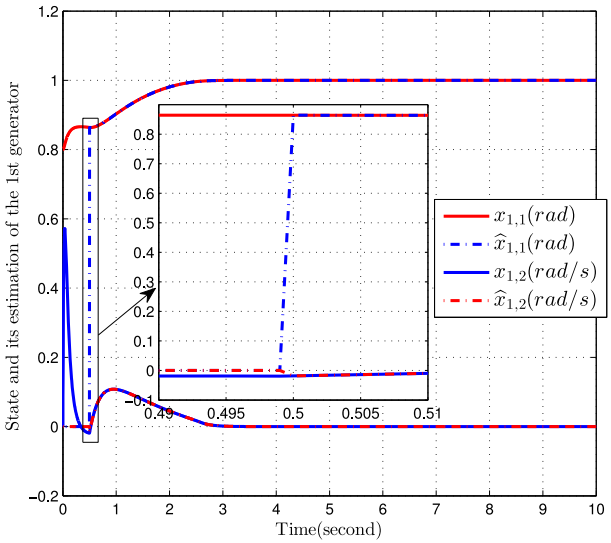


Fig. 3. State and its estimation of the first generator under attack with the second group of parameters.

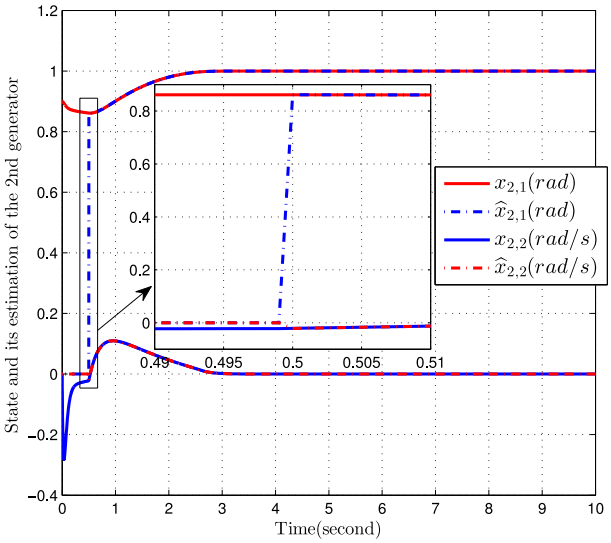


Fig. 4. State and its estimation of the second generator under attack with the second group of parameters.

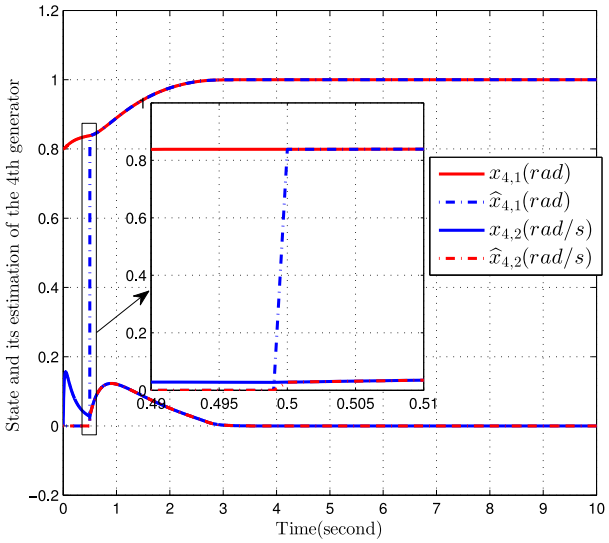


Fig. 6. State and its estimation of the fourth generator under attack with the second group of parameters.

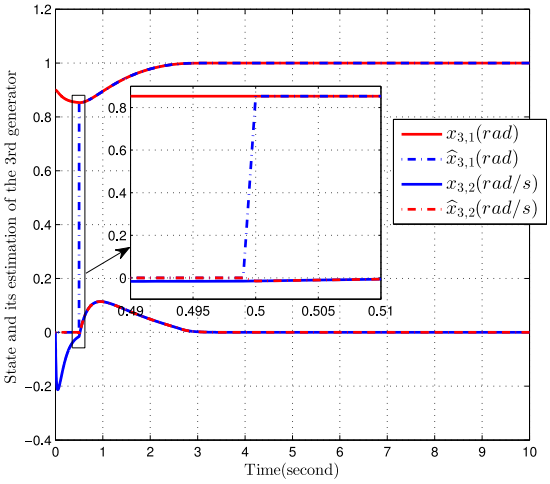


Fig. 5. State and its estimation of the third generator under attack with the second group of parameters.

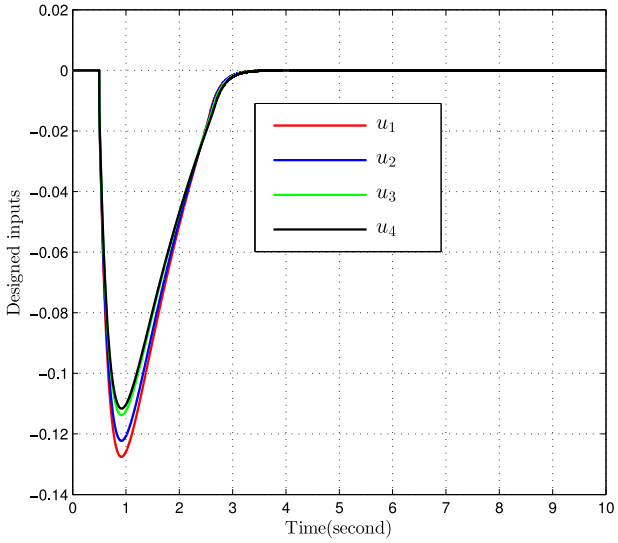


Fig. 7. Designed distributed secure control for the MG under attacks with the second group of parameters.

of the ith DG, which is

$$P_i(t) = P_{1i}V_i^2(t) + P_{2i}V_i(t) + P_{3i} + \sum_{j\in N_i} V_i(t)V_j(t)\left|B_{ij}\right|\sin\left(\delta_i - \delta_j\right) \tag{55}$$

where B_{ij} is the ith row and jth column element of nodal susceptance matrix at the internal nodes after eliminating all physical buses, $i, j = 1, \ldots, N$ with $N = 4$, $V_i(t)$ is the voltage of the ith DG, P_{1i}, P_{2i}, and P_{3i} are nominal constant impedance, constant current, and constant power load, respectively. The parameters of the MG is given in Table I.

Note that, with some finite time voltage restoration methods in [25] and [26], the voltage of the ith can be maintained, thus, for convenience, $V_i(t) = V_i^{\text{ref}} = 110$ V in the simulation. Furthermore, following the Kron-reduced form of the power system based on the classic small signal method in [6], i.e., the difference between $\delta_i(t)$ and $\delta_j(t)$ is small, then the fourth term of the output power in (55) can be approximated as $\sin(\delta_i(t) - \delta_j(t)) \approx \delta_i(t) - \delta_j(t)$, thus the phase droop model of the ith DG with sensor attacks is given as follows:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) + B_i f_i(t) + \Gamma^i \bar{z}(t) \\ y_i(t) = C_i x_i(t) + \eta_i(t) \end{cases} \tag{56}$$

where $x_i(t) = [\delta_i(t), \omega_i(t)]^T$, $y_i(t) = [y_{i,1}(t), \ldots, y_{i,p_i}(t)]^T$, and $\bar{z}(t) = [x_{1,1}(t), \ldots, x_{N,1}(t)]^T$. The parameters of A_i, B_i, and Γ^i can be obtained from Table I, and $C_i = [1, 0; 1, 0; 1, 0]$, $i = 1, \ldots, N$ with $N = 4$. $f_i(t) = P_{1i}V_i^2(t) + P_{2i}V_i(t) + P_{3i} - P_i^d$ is a known function. The attack signals $\eta_{1,3}(t) = [1, 0]e^{A_1 t}$, $\eta_{2,1}(t) = [1, 0]e^{A_2 t}$, $\eta_{3,2}(t) = [1, 0]e^{A_3 t}$, and $\eta_{4,1}(t) = [1, 0]e^{A_4 t}$ and others are zero. Clearly, Condition 1 is valid, thus the secure state estimation and secure control can be obtained.

We implement the simulation tests with the following parameters: $T_e = 0.5$ s, $\bar{F}_i = [-17.5, 1.0, 0.0, 0.0; -2106.3, -62.5, 0.0, 0.0; 0.0, 0.0, 42.5.34, 1.0; 0.0,$

$0.0, -2856.3, -62.5]$, $\bar{L}_i = [17.5, 2106.3, -42.5, 2856.3]^T$, $\bar{M}_i = [1.0, 0, 0, 0; 0, 1.0, 0.0, 0.0]$, $c_{i,1} = 0.5$, $c_{i,2} = 0.5$, $K_i = [5, 1]$, $h_{i,1} = 3$, and $h_{i,2} = 7$, where $i = 1, \ldots, 4$. The simulation results are observed in Figs. 3–6. As shown in Fig. 3, with the proposed secure control, the relative angle of the first DG is ensured to track the desired one exponentially, the converge time T_c is about 2.9 s, the track error converges to a very small vicinity of zero in about $T_s = T_e + T_c \approx 3.4$ s, the relative speed peaks at about 0.12 rad/s when $t = 0.9$ s, and the estimation error converges to zero in no more than $T_e = 0.5$ s, where T_e is given in Theorem 2, and T_c and T_s in Theorem 3. This is also consistent with our theoretical findings. Also similar results observations are made for the second, third, and fourth generators from Figs. 4–6, respectively. The presented distributed secure control is given in Fig. 7, which is continuous and bounded. It is shown that, each control input peaks at about -0.125 when $t = 0.9$ s. All the simulation results are satisfactory, which illustrate the effectiveness of the proposed schemes.

VI. Conclusion

In this paper, we investigate the distributed secure state estimation and control problem for linear interconnected CPSs under sensor attacks. First, by exploring the equivalence between the solvability of the secure state estimation and the existence of unidentifiable attacks, a sufficient condition that the secure state estimation can be obtained is established. Then distributed secure preselector and observers are proposed to solve the secure state estimation problem, which ensure that the exact state of the CPS can be obtained in a given finite time. With the obtained secure estimation, a fractional dynamic surface-based distributed secure control is designed to make the CPS track desired trajectories exponentially. In the future works, we would focus more attention on nonlinear and/or distributed CPSs under attack in the presence of uncertainties and noises.

References

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Comput. Commun.*, vol. 36, no. 1, pp. 1–7, 2012.

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

[3] C.-H. Lee, B.-K. Chen, N.-M. Chen, and C.-W. Liu, "Lessons learned from the blackout accident at a nuclear power plant in Taiwan," *IEEE Trans. Power Del.*, vol. 25, no. 4, pp. 2726–2733, Oct. 2010.

[4] J. P. Conti, "The day the samba stopped," *Eng. Technol.*, vol. 5, no. 4, pp. 46–47, Mar. 2010.

[5] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, no. 1, pp. 135–148, 2015.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[7] W. Ao, Y. Song, and C. Wen, "Adaptive cyber-physical system attack detection and reconstruction with application to power systems," *IET Control Theory Appl.*, vol. 10, no. 12, pp. 1458–1468, Aug. 2016.

[8] Y. Chen, S. Kar, and J. M. F. Moura, "Cyber-physical systems: Dynamic sensor attacks and strong observability," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, 2015, pp. 1752–1756.

[9] Y. Chen, S. Kar, and J. M. F. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4618–4624, Sep. 2017.

[10] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure state-estimation for dynamical systems under active adversaries," in *Proc. 49th Annu. Allerton Conf.*, Monticello, IL, USA, 2011, pp. 337–344.

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

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

[13] Y. Shoukry *et al.*, "SMT-based observer design for cyber-physical systems under sensor attacks," in *Proc. 7th ACM/IEEE Int. Conf. Cyber Phys. Syst.*, Vienna, Austria, 2016, pp. 1–10.

[14] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 49–59, Mar. 2017.

[15] Y. Mo, J. P. Hespanha, and B. Sinopoli, "Resilient detection in the presence of integrity attacks," *IEEE Trans. Signal Process.*, vol. 62, no. 1, pp. 31–43, Jan. 2014.

[16] Y. 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.

[17] F. Pasqualetti, A. Bicchi, and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities," in *Proc. Amer. Control Conf.*, San Francisco, CA, USA, 2011, pp. 3918–3923.

[18] V. Reppa, M. M. Polycarpou, and C. G. Panayiotou, "Distributed sensor fault diagnosis for a network of interconnected cyberphysical systems," *IEEE Trans. Control Netw. Syst.*, vol. 2, no. 1, pp. 11–23, Mar. 2015.

[19] Y. Wang, Y. Song, H. Gao, and F. L. Lewis, "Distributed fault-tolerant control of virtually and physically interconnected systems with application to high-speed trains under traction/braking failures," *IEEE Trans. Intell. Transport. Syst.*, vol. 17, no. 2, pp. 535–545, Feb. 2016.

[20] M. F. Duarte and Y. C. Eldar, "Structured compressed sensing: From theory to applications," *IEEE Trans. Signal Process.*, vol. 59, no. 9, pp. 4053–4085, Sep. 2011.

[21] R. Engel and G. Kreisselmeier, "A continuous-time observer which converges in finite time," *IEEE Trans. Autom. Control*, vol. 47, no. 7, pp. 1202–1204, Jul. 2002.

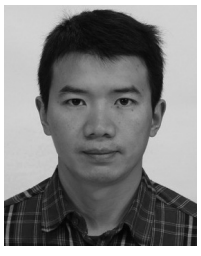
[22] G. Kreisselmeier and R. Engel, "Nonlinear observers for autonomous Lipschitz continuous systems," *IEEE Trans. Autom. Control*, vol. 48, no. 3, pp. 451–464, Mar. 2003.

[23] T. Raff and F. Allgower, "An impulsive observer that estimates the exact state of a linear continuous-time system in predetermined finite time," in *Proc. Mediterranean. Conf. Control Autom.*, Athens, Greece, 2007, pp. 1–3.

[24] Y. Wang and Y. Song, "Fraction dynamic-surface-based neuroadaptive finite-time containment control of multiagent systems in nonaffine pure-feedback form," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 3, pp. 678–689, Mar. 2017.

[25] F. Guo, C. Wen, J. Mao, and Y.-D. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Trans. Ind. Electron.*, vol. 62, no. 7, pp. 4355–4364, Jul. 2015.

[26] N. M. Dehkordi, N. Sadati, and M. Hamzeh, "Distributed robust finite-time secondary voltage and frequency control of islanded microgrids," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3648–3659, Sep. 2017.



Wei Ao received the B.S. degree in automation from the National University of Defense Technology in Automation, Changsha, China, in 2003 and the Ph.D. degree in control science and control theory from Chongqing University, Chongqing, China, in 2017.

He was with the School of Automation, Chongqing University. His current research interests include adaptive control, fault tolerant control and attack detection, and secure control of cyber-physical systems.

Yongduan Song (SM'02) received the Ph.D. degree in electrical and computer engineering from Tennessee Technological University, Cookeville, TN, USA, in 1992.

He is currently the Dean with the School of Automation, Chongqing University, Chongqing, China. His current research interests include intelligent systems, guidance navigation and control, bioinspired adaptive control, and system cooperation and reliability.

Dr. Song is the Standing Director of the Automation Association of China and the Chair of the Committee on Reliable Control Systems under the Automation Association of China. He is also the Founding Chair of the Chongqing Chapter of IEEE Computational Intelligence Society. He is currently serving as an Associate Editor for six international scientific journals, including the IEEE TRANSACTIONS ON AUTOMATIC CONTROL.

Changyun Wen (F'10) received the B.Eng. degree in automation from Xi'an Jiaotong University, Xi'an, China, in 1983 and the Ph.D. degree in electrical and electronic engineering from the University of Newcastle, Callaghan, NSW, Australia, in 1990.

From 1989 to 1991, he was a Postdoctoral Fellow with the University of Adelaide, Adelaide, SA, Australia. He is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, where he has been a tenured Full Professor since 2008. His current research interests include adaptive control, autonomous robotic systems, intelligent power management systems, and complex systems and networks.

Dr. Wen was a recipient of the IES Prestigious Engineering Achievement Award by the Institution of Engineers, Singapore, in 2005 and the Best Paper Award of the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS in 2017. He was a member of the IEEE Fellow Committee from 2011 to 2013 and a Distinguished Lecturer of the IEEE Control Systems Society from 2010 to 2013. He was an Associate Editor of a number of journals, including the IEEE TRANSACTIONS ON AUTOMATIC CONTROL from 2000 to 2002 and has been an Associate Editor of *Automatica* since 2006, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS since 2013, and the *IEEE Control Systems Magazine* since 2009.