Citation information: DOI10.1109/TSMC.2019.2960541

Recursive Filtering of Distributed Cyber-Physical Systems with Attack Detection

Derui Ding, *Member, IEEE*, Qing-Long Han, *Fellow, IEEE*, Zidong Wang, *Fellow, IEEE*, and Xiaohua Ge, *Member, IEEE*

***Abstract*—This paper is concerned with the distributed recursive filtering of cyber-physical systems consisting of a set of spatially distributed subsystems. Due to the vulnerability of communication networks, the transmitted data among subsystems could be subject to deception attacks. In this paper, attackers do not have enough knowledge of the full network topology and the system parameters and therefore cannot carry out stealth attacks. For this scenario, a defense strategy dependent on the received innovation is proposed to identify the occurring attacks as far as possible. In light of identified attacks, a novel distributed filter is constructed and its gain is designed via a set of recursive formulas on the upper bound of covariance of filtering errors. The utilization of upper bound is to avoid the calculational challenge of cross-covariance matrices and realize the requirement of distributed implementation, simultaneously. Furthermore, the developed scheme only depends on the neighboring information and the information from the subsystem itself, and thereby satisfying the requirement of the scalability. Finally, a standard IEEE 39-bus power system is utilized to verify the effectiveness of the proposed filtering scheme.**

***Index Terms*—Cyber-physical systems; distributed filtering; security defenses; deception attacks; power systems.**

I. Introduction

Cyber-physical systems (CPSs), one of the cornerstones in the era of Industry 4.0, are large-scale, geographically dispersed, networked systems, in which physical sensors/controllers and software components are deeply intertwined to implement real-time monitoring and control. The main merit of such systems is that integrate physical entities with cyber networks provides greater autonomy, efficiency, functionality and reliability, as well as adaptability [1]–[3]. As a new research frontier, they are being widely promoted by governments and industry around the world and representative systems include distributed energy resources, intelligent transportation networks, gas/water distribution networks, and unmanned factories [4], [5]. In order to describe the characteristic of complex coupling of subsystems, typical CPSs can be modeled as large-scale systems or discrete sequential systems when ignoring the function of cyber layers. It is worth noting that the inherent coupling among subsystems is difficult to be completely decoupled, which results in the critical challenge to guarantee the requirement of scalability, that is, the complexity of parameter design is almost no effect from the increased scale of CPSs. Generally speaking, the small gain condition, the game theory and the arithmetic mean-geometric mean inequality are some considerable approaches to realize the easy-to-implement design of expected gain parameters.

Distributed filtering plays a critical role in performing real-time monitoring and control in the area of CPSs, especially in power distribution grids and process control systems [6]–[8]. Some representative approaches, such as consensus/diffusion/distributed Kalman filtering as well as H_∞ filtering, have been developed in the literature. For instance, a consensus-based Kalman filtering has been proposed in [9] to carry out the dynamic state estimation for the purpose of real-time monitoring of power systems, and developed in [8] to estimate the slab temperature distribution in a hot rolling process monitoring system. Furthermore, a diffusion Kalman filtering has been designed in [10] for distributed hybrid power state estimation, where an auto-encoder technique has been employed to overcome the challenge from the data dimensionality in mixed measurements. Moreover, a distributed Kalman filtering relying on differences among neighbors' prediction has been designed to estimate the operating condition of renewable microgrids in [11] for the case of reliable channels and in [12] for the case subject to packet losses, and the corresponding convergence conditions have been analyzed simultaneously. It is worth mentioning that a distributed filter only using local data can effectively deal with the challenges from both communication latency and communication cost existing in a central paradigm. In other words, instead of all-to-all or all-to-one (i.e. centralized fusion) communication, the information only needs to be exchanged among neighbors, who are usually sparsely deployed in a predetermined region.

In comparison with the centralized system over sensor networks [13], the estimated states and/or covariance matrices from neighboring subsystems in distributed CPSs have to take part in the evolution of filter dynamics via interconnection [14]. This kind of structure leads to the sensibility to abnormal neighboring information even if some compensation schemes are employed. Unfortunately, data collection or transmission in practical systems could be incomplete or even unreliable due to the vulnerability of shared communication channels without enough capability or defense. That is to say, the resultant open network makes distributed CPSs vulnerable to the destruction coming from cyber-attacks [15]–[18]. This paper only focuses on deception attacks, under which adversaries have the capability of overhearing and modifying the information of data

This work was supported in part by the Australian Research Council Discovery Early Career Researcher Award under Grant DE200101128, and the Australian Research Council Discovery Project under Grant DP160103567. (*Corresponding author: Qing-Long Han.*)

D. Ding, Q.-L. Han, Z. Wang, and X. Ge are with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia. Z. Wang is also with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom.

packets in *cyber-layers* [19]. More specifically, we assume that attackers have no sufficient knowledge of full network topology and system parameters and therefore cannot implement undetectable attacks or stealth attacks [20]. Furthermore, the purpose of attacks is to give rise to either physical or economic impacts on CPSs by making filter's output unreliable values about the system operator. As a result, it is of great significance to design a suitable filter structure with a defense mechanism and develop a corresponding filtering algorithm that facilitates the implementation of target monitoring in a reliable manner.

In the framework of Kalman filtering, the implementation of filtering algorithms for distributed CPSs may depend on the estimate, the covariance (or its upper bound), or/and the innovation coming from neighboring subsystems. When cyber-attack is a concern, much progresses have been made on recursive filtering [21], [22], attack scheduling [23], [24] and attack detection [25]. In contrast with research on the delectability of attacks or the optimal attack allocation, we should take designed filters and attack detectors as a whole from the conception of system theory to ensure proper monitoring and operation of CPSs. It naturally leads to that the designed defense strategies should be realizable from the engineering point of view. That is, its parameter can be easily determined and the calculation burden is small such that the defense rule can be performed in time via general processors. It is noteworthy that residual-based detectors, such as the most prominent χ^2 detectors, are capable for the considered scenario. Surely, other model-based detectors, such as CUSUM detectors [26], likelihood ratio detectors [27] as well as graphic-based detectors [28], could be suitable especially for the scenario of stealth attacks if ignoring the limitation of the real-time and the communication burden.

Recalling the distributed filtering of CPSs modeled by large-scale systems,there is no appropriate compensation scheme to deal with the impact from the covariance subject to cyber-attacks so far. As such, a conservative strategy should be developed to enhance the reliability of designed filtering algorithm in the presence of deception attacks. Obviously, it is nontrivial to design the desired filter with attack detection to satisfy the requirement of scalability due mainly to the complex coupling among subsystems, which could not be decoupled into some independent subsystems. Summarizing the above discussions, in this paper, we focus on the distributed recursive filtering of CPSs with attack detection. The main contributions are highlighted as follows: *1) Via a designed attack detector, a distributed filter with a novel structure is designed in order to enhance the capability of dealing with unreliable information transmission due to deception attacks; 2) In light of the characteristic of χ^2 distribution, an upper bound of the filtering error covariance is recursively calculated by the solution of a Riccati-like difference equation; 3) A distributed design scheme in a scalable way is developed by resorting to a gradient-based method and the corresponding upper bound is suppressed via the designed gains; And 4) a standard IEEE 39-bus power system is utilized to verify the effectiveness of proposed filtering scheme.*

TABLE I
INDEX OF SYMBOLS

Notations	Descriptions
$x_{i,k}$	The state of subsystem i
$\hat{x}_{i,k}$	The estimation of state $x_{i,k}$
$z_{i,k}$	The innovation of subsystem i
$P_{i,k}$	The covariance of filtering errors of filter i
$\Pi_{i,k}$	An upper bound of $P_{i,k}$
$\hat{x}^r_{ij,k}$	Data on $\hat{x}_{j,k}$ received by neighboring filter i
$z^r_{ij,k}$	Data on $z_{j,k}$ received by neighboring filter i
$\Pi^r_{ij,k}$	Data on $\Pi_{j,k}$ received by neighboring filter i
$\theta\psi^z_{ij,k}$	The malicious data added in $z_{j,k}$
$\theta\psi^x_{ij,k}$	The malicious data added in $\hat{x}_{j,k}$
$\theta\psi^p_{ij,k}$	The malicious data added in $\Pi_{j,k}$
θ	The size of malicious data
Θ^x_{ij}, Θ^z_{ij}	The covariance of $\psi^x_{ij,k}$ and $\psi^z_{ij,k}$
Θ^{lp}_{ij}, Θ^{rp}_{ij}	The column and row covariance of $\psi^p_{ij,k}$
Q_i	The covariance of process noises $w_{i,k}$
R_i	The covariance of measurement noises $\nu_{i,k}$
$\mathcal{N}_i$	The set of neighbors of subsystem i
ς_i	The number of neighbors of subsystem i

The rest of this paper is organized as follows. Section II briefly introduces the problem under consideration. In Section III, a distributed design scheme with a scalable form is proposed in light of the minimized upper bound of filtering error covariance. Section IV provides a real application on power systems to validate the usefulness of obtained results. Finally, some conclusions are stated in Section V.

Notation The notation used here is fairly standard except where otherwise stated. $\mathbb{R}^n$ denotes the n dimensional Euclidean space. $\mathbb{N}_m$ stands for the positive integer set $\{1, 2, \cdots, m\}$. The notation $A \geq B$ (respectively, $A > B$), where A and B are symmetric matrices, means that $A - B$ is positive semi-definite (respectively, positive definite). Finally, $\mathbb{E}\{\omega\}$ denotes the expectation of stochastic variable ω, and $\mathbb{P}\{\omega\}$ represents the occurrence probability of event ω.

II. Problem Formulation and Preliminaries

In this paper, the pair $\mathscr{G} = (\mathcal{V}, \mathcal{E})$ is employed to describe the topology of CPSs consisting of a set of interconnected subsystems, where $\mathcal{V} = \{1, 2, \cdots m\}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ stand for the sets of subsystems and interconnected edges. If there exists an edge (i, j), the subsystem j is called as a neighbor of the subsystem i. Furthermore, the general notations are provided in Table I.

A. The plant of interest

Let us investigate a class of CPSs consisting of m interconnected subsystems, whose dynamics is described by

$$x_{i,k+1} = A_{ii}x_{i,k} + \sum_{j\in\mathcal{N}_i} A_{ij}x_{j,k} + w_{i,k} \tag{1}$$

with measurements

$$y_{i,k} = C_i x_{i,k} + \nu_{i,k}, \quad i \in \mathbb{N}_m \tag{2}$$

where $x_{i,k} \in \mathbb{R}^{n_x}$ is the state of target subsystem i that cannot be observed directly, $y_{i,k} \in \mathbb{R}^{n_y}$ is the measurement output from sensor i, and $\{w_{i,k}\}_{k\geq 0}$, and $\{\nu_{i,k}\}_{k\geq 0}$ are independent and identically distributed (i.i.d) random sequences obeying

Gaussian distribution with zero mean and covariance Q_i and R_i. Additionally, we assume that all stochastic variables and the initial state $x_{i,0}$ are mutually independent. A_{ii}, A_{ij} and C_i are known matrices with compatible dimensions.

Considering the distributed characteristic, the following filter, called as filter i, is constructed:

$$\begin{aligned}\hat{x}_{i,k+1} = & A_{ii}\hat{x}_{i,k} + K_{ii,k}z_{i,k} \\ & + \sum_{j\in\mathcal{N}_i} A_{ij}\hat{x}_{j,k} + \sum_{j\in\mathcal{N}_i} K_{ij,k}z_{j,k}\end{aligned} \tag{3}$$

where $K_{ii,k}$ and $K_{ij,k}$ are the filter gains to be designed.

In what follows, we define the corresponding filtering error covariance:

$$P_{i,k} = \mathbb{E}\{(x_{i,k} - \hat{x}_{i,k})(x_{i,k} - \hat{x}_{i,k})^T\}. \tag{4}$$

Under the framework of distributed Kalman filtering, filter i usually needs to send its estimate $\hat{x}_{i,k}$, innovation $z_{i,k}$ and covariance $P_{i,k}$ (or its upper bound) to its neighbors at each time step for the purpose of implementation.

Remark 1: It is worth noting that the model (1) is a very general form and has been widely utilized to model various CPSs, such as power systems, automation processes, and series systems [29]–[32]. For example, in an array of masses, the elements of $x_{i,k}$ consist of the horizontal and vertical velocities and displacements of masses [29], where the displacements are with respect to a given equilibrium position in the plane. For multiple maneuvering targets, the elements of $x_{i,k}$ are the position coordinates and the corresponding velocities along X- and Y-axes [30]. Furthermore, the state vector $x_{i,k}$ is selected as $\begin{pmatrix} \Delta w_{i,k} & \Delta P_{ti,k} & \Delta P_{gi,k} & \Delta P^i_{tie,k} \end{pmatrix}^T$ in [14] in power systems, where $\Delta w_{i,k}$, $\Delta P_{ti,k}$, $\Delta P_{gi,k}$ and $\Delta P^i_{tie,k}$ describe, respectively, the deviation of frequency, generator mechanical power, turbine valve position and the net tie-line power flow, or selected as $\begin{pmatrix} V_{i,k} & I_{ti,k} & \Phi_{V,k} & \Phi_{I,k} & \Psi_{V,k} & \Psi_{I,k} \end{pmatrix}^T$ in [31], where $V_{i,k}$, $I_{ti,k}$, $\Phi_{V,k}$, $\Phi_{I,k}$, $\Psi_{V,k}$ and $\Psi_{I,k}$ denote, respectively, the load voltage at point of common coupling, the load current, the dynamics of primary control (the third and fourth elements), and the dynamics of secondary voltage controllers (the last two elements).

Remark 2: In the model (1), A_{ij} combining with the topology $\mathscr{G}$ reflects the physical connection of spatially distributed subsystems in CPSs. As such, in comparison with traditionally distributed filtering over sensor networks, the estimate $\hat{x}_{j,k}$ from neighbors of subsystem i is indispensable to guarantee the filter's implementation, which results in that the covariance matrix (or its upper bound) needs to be transmitted as well. On the other hand, different from the physical coupling of CPSs, the topology $\mathscr{G}$ in (3) describes the communication among filters and therefore the exchanged data could suffer from cyber-attacks. This kind of characteristic is clearly disclosed in Fig. 1 to be further discussed in the following subsection.

B. Cyber-attacks and a detection strategy

Due to the vulnerability of communication networks, the adversary may overhear and modify the information in the transmitted data packets in order to yield a larger estimation error in supervisory units, which will produce some negative impacts on the operation of systems [33]. In this paper, we only consider the case that attackers do not have knowledge of full network topology and system parameters. In other words, they cannot carry out stealth attack [20]. A schematic block diagram of CPSs under deception attacks is shown in Fig. 1. Specifically, we assume that attackers can overhear the information transmitted by unsecured channels and randomly modify them by adding malicious data $\theta\psi^x_{ij,k}$, $\theta\psi^z_{ij,k}$, and $\theta\psi^p_{ij,k}$ into three transmitted data $\hat{x}_{j,k}$, $z_{j,k}$ and $P_{j,k}$. Here, θ is a given constant quantifying the size of malicious data, and $\psi^x_{ij,k} \in \mathbb{R}^{n_x}$, $\psi^z_{ij,k} \in \mathbb{R}^{n_y}$ and $\psi^p_{ij,k} \in \mathbb{R}^{n_x\times n_x}$ are zero-mean white Gaussian variables with covariance Θ^x_{ij}, Θ^z_{ij}, Θ^{lp}_{ij}, and Θ^{rp}_{ij}. Furthermore, random variables $\psi^x_{ij,k}$, $\psi^z_{ij,k}$ and $\psi^p_{ij,k}$ are mutually independent at any instants.

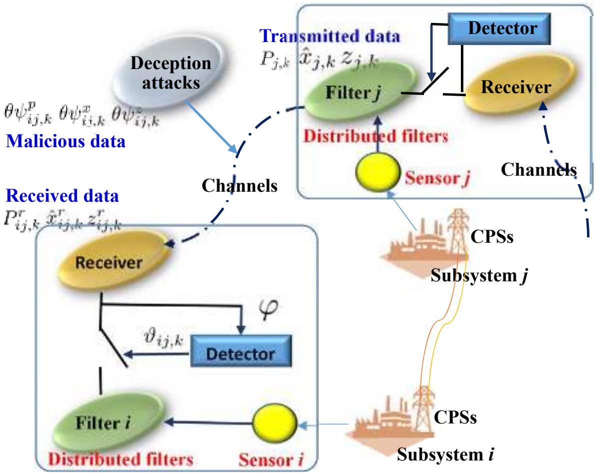


Fig. 1. A schematic block diagram of CPSs under deception attacks.

In what follows, for the purpose of description, we introduce a binary variable $\xi_{ij,k}$ $(j \in \mathcal{N}_i)$ to indicate whether the attackers launch the attack on data transmitted from filter j to filter i:

$$\xi_{ij,k} = \begin{cases} 1, & \text{Data from } j \text{ to } i \text{ subject to attacks;} \\ 0, & \text{Otherwise.} \end{cases} \tag{5}$$

and further assume that its statistical characteristic is $\mathbb{P}\{\xi_{ij,k} = 1\} = \bar{\xi}$.

With the help of the introduced binary stochastic variable, the received data by filter i from filter j are described by

$$\begin{cases} \hat{x}^r_{ij,k} = \hat{x}_{j,k} + \theta\xi_{ij,k}\psi^x_{ij,k}, \\ z^r_{ij,k} = z_{j,k} + \theta\xi_{ij,k}\psi^z_{ij,k}, \\ P^r_{ij,k} = P_{j,k} + \theta\xi_{ij,k}\psi^p_{ij,k}. \end{cases} \tag{6}$$

In this paper, a detection strategy dependent on both $z^r_{ij,k}$ and a predetermined threshold α is employed to improve the security of proposed distributed filter. To identify the attack, let us first introduce a value function $\varphi(\cdot)$:

$$\varphi(z^r_{ij,k}) = 1 - \exp\big(-(z^r_{ij,k})^T R_j^{-1} z^r_{ij,k}\big). \tag{7}$$

Then, the following indicator function

$$\vartheta_{ij,k} = \begin{cases} 0, & \alpha \le \varphi(z^r_{ij,k}), \\ 1, & \text{otherwise,} \end{cases} \tag{8}$$

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: DOI10.1109/TSMC.2019.2960541

is adopted to indicate whether attacks occur. Specifically, we claim that an attack to the communication between filter i and filter j occurs when $\vartheta_{ij,k} = 0$. Additionally, for the convenience of analysis, we denote $\vartheta_{ii,k} = 1$ for any instants. It is well known that $z_{j,k}^T R_j^{-1} z_{j,k}$ obeys the χ^2 distribution with degree of freedom n_y, and the corresponding distribution table can be easily obtained. Therefore, for any given probability p, we can easily obtain α_p such that $\mathbb{P}\{z_{j,k}^T R_j^{-1} z_{j,k} < \alpha_p\} > p$ and then calculate $\alpha = 1 - \exp(-\alpha_p)$.

According to above analysis, the adopted model is essentially the well-known χ^2-detector, which keeps the Gaussianity of filtering error dynamics [34] and hence possesses the irreplaceable superiority in performance analysis. Let us further disclose the reason of this kind of selection in comparison with existing detection approaches. First, detectors based on weighted least square are also χ^2-detectors essentially and can further generate cumulative-sum detectors [26] via detecting a change in the distribution, which could be the presence of a large detection delay; Second, detectors based on a Kullback-Leibler distance [35] are suitable for quasi-static systems and highly depend on the probability distribution of ideal measurements; Third, detectors based on Bayesian inference [36] have to calculate the filter gains in real-time and reveal the disadvantage in time complexity when the dynamical system is a concern. As such, for the case of no-stealth attacks, the employed detector should be the best one. Finally, more attack models can be found in [37] and corresponding detectors are not surveyed due to the limited space.

C. The object of this paper

With the help of this identification function, the distributed filter (3) is improved as follows:

$$\begin{aligned}\hat{x}_{i,k+1} = {} & A_{ii}\hat{x}_{i,k} + K_{ii,k}z_{i,k} \\ & + \sum_{j\in\mathcal{N}_i} A_{ij}\hat{x}_{ij,k}^r + \sum_{j\in\mathcal{N}_i} \vartheta_{ij,k}K_{ij,k}z_{ij,k}^r. \end{aligned} \tag{9}$$

According to the analysis in Subsection II-A and Subsection II-B, the objective of this paper is to design a Kalman-type distributed filter of the form (9) such that an upper bound of filtering error covariance is guaranteed over a given finite-horizon $\mathbb{N}_f$, that is, there exists a sequence of positive-definite matrices $\{\Pi_{i,k|k}\}_{k\in\mathbb{N}_f}$ satisfying

$$P_{i,k} \leq \Pi_{i,k}, \quad \forall k \in \mathbb{N}_f. \tag{10}$$

Furthermore, the sequence of upper bounds $\{\Pi_{i,k}\}_{k\in\mathbb{N}_f}$ is optimized via the designed filter parameters $K_{ij,k}$ for $j \in \mathcal{N}_i \cup \{i\}$. It is worth mentioning that such a bound $\Pi_{i,k}$ should own the computational advantage of Riccati-like difference equation and must reflect the attack detection $\vartheta_{ij,k}$ in real-time in order to guarantee its security.

Remark 3: Lots of results are essentially performed in a centralized way for recursive filtering issues of CPSs modeled by (1). Specifically, the desired gain is usually dependent on cross-variance matrices [30], or calculated via matrix parameters of augmented systems [38]. At the same time, various approaches have been proposed to overcome this disadvantage. For instance, 1) taking $\sum_{j\in\mathcal{N}_i} A_{ij}x_{j,k}$ as a whole input produces a new distributed Kalman filtering in [39], whose gain is related with the error cross correlation; 2) considering the utility function on prediction errors and measured local outputs leads to distributed moving horizon estimation [40], of which the developed approach is dependent on the Chebyshev approximation with the help of traditional lifting techniques; and 3) the technique of covariance's bounds is adopted in [7] to obtain partition-based distributed Kalman filtering, the idea of which is also employed in our paper. It is worth mentioning that, taking the addressed cyber-attacks into account, these approaches are commonly incapable due mainly to the high calculation burden of error cross correlation, the infeasibility of lifting techniques, and the covariance bounds subject to attacks.

III. Main results

This section is first concerned with the unbiasedness of designed distributed filter and then obtains an upper bound of filtering error covariance.

A. The design of filter gains

As mentioned in Subsection II-B, we need to propose a rule to replace the covariance matrix $P_{j,k}$ by the received one (i.e. $P_{ij,k}^r$) at instant k because the real covariance matrix could be unknown for filter i. For this purpose, we first find from (6) that

$$P_{j,k} = P_{ij,k}^r - \theta\xi_{ij,k}\psi_{ij,k}^p. \tag{11}$$

By resorting to the property of conditional expectation of random matrix [41], one has

$$\mathbb{E}\{P_{j,k} + P_{j,k}^T | P_{ij,k}^r\} = P_{ij,k}^r + (P_{ij,k}^r)^T \tag{12}$$

and

$$\begin{aligned} & \mathbb{E}\{(P_{j,k} - P_{ij,k}^r)(P_{j,k} - P_{ij,k}^r)^T | P_{ij,k}^r\} \\ & + \mathbb{E}\{(P_{j,k} - P_{ij,k}^r)^T (P_{j,k} - P_{ij,k}^r) | P_{ij,k}^r\} \\ = {} & \theta^2\bar{\xi}\big(\mathrm{trace}(\Theta_{ij}^{rp})\Theta_{ij}^{lp} + \mathrm{trace}(\Theta_{ij}^{lp})\Theta_{ij}^{rp}\big). \end{aligned} \tag{13}$$

For the analysis convenience, we denote

$$\Omega_{ij} = \theta^2\bar{\xi}\big(\mathrm{trace}(\Theta_{ij}^{rp})\Theta_{ij}^{lp} + \mathrm{trace}(\Theta_{ij}^{lp})\Theta_{ij}^{rp}\big), \tag{14}$$

and

$$\Upsilon_{ij,k} = \begin{cases} P_{i,k}, & i = j \\ \frac{1}{2}(P_{ij,k}^r + P_{ij,k}^{rT}) + \kappa_{\vartheta_{ij,k}}\Omega_{ij}, & \text{otherwise} \end{cases} \tag{15}$$

where the scalar $\kappa_{\vartheta_{ij,k}}$ (i.e. κ_0 and κ_1) predetermined by statistical experiments is utilized to adjust the probability of $\Upsilon_{ij,k} \geq P_{j,k}$.

In what follows, the upper bound of $P_{i,k}$ (denoted as $\Pi_{i,k}$) is employed to realize the distributed implementation of the filter (9) with attack detection. In this case, the corresponding matrix $\Upsilon_{ij,k}$ in (15) is replaced by

$$\bar{\Upsilon}_{ij,k} = \begin{cases} \Pi_{i,k}, & i = j \\ \frac{1}{2}(\Pi_{ij,k}^r + (\Pi_{ij,k}^r)^T) + \kappa_{\vartheta_{ij,k}}\Omega_{ij}, & \text{otherwise.} \end{cases} \tag{16}$$

Under this scheme, we have the same probability to guarantee

$$\bar{\Upsilon}_{ij,k} \geq \Pi_{j,k} \geq P_{j,k}.$$

Remark 4: A conservative bound $\bar{\Upsilon}_{ij,k}$ in (16) is adopted to improve the security of distributed filter. In this scheme, the parameter $\kappa_{\vartheta_{ij,k}}$, which takes the value κ_0 or κ_1, is utilized to adjust the effect from cyber-attacks. Obviously, κ_0 is greater than κ_1 because the probability of occurring cyber-attacks is higher when $\vartheta_{ij,k} = 0$.

Now, by means of above analysis, we have the following results.

Theorem 1: For CPSs described by(1), if $\hat{x}_{i,0} = \mathbb{E}\{x_{i,0}\}$ for any $i \in \mathbb{N}_m$, the proposed distributed filter with the form (9) is unbiased, that is, $\mathbb{E}\{x_{i,k} - \hat{x}_{i,k}\} = 0$.

Proof: The proof of the unbiasedness will be performed via mathematical induction. Under this conception, since $\hat{x}_{i,0} = \mathbb{E}\{x_{i,0}\}$ for any $i \in \mathbb{N}_m$, we first assume $\mathbb{E}\{x_{i,k} - \hat{x}_{i,k}\} = 0$ for any $i \in \mathbb{N}_m$ and then verify that this assumption is also true for the instant $k+1$.

By means of the statistical properties of cyber-attacks, it follows from (20) that

$$\begin{aligned}\mathbb{E}\{x_{i,k} - \hat{x}_{i,k}\} &= \mathbb{E}\{e_{i,k+1}\}\\ &= \sum_{j\in\mathcal{N}_i\cup\{i\}} \mathbb{E}\Big\{\big(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j\big)e_{j,k}\Big\}\\ &= 0\end{aligned}$$

which implies that the proposed filter is unbiased. The proof is now complete. ■

Theorem 2: For any i, let $\Pi_{i,0} \geq P_{i,0}$ be given. For the distributed filter (9) with gains

$$K_{ij,k} = A_{ij}\bar{\Upsilon}_{ij,k}C_j^T\big(C_j\bar{\Upsilon}_{ij,k}C_j^T + \hat{\mathcal{V}}_{ij}\big)^{-1}, \tag{17}$$

a feasible upper bound $\Pi_{i,k+1}$ of the covariance matrix $P_{i,k+1}$ is calculated by

$$\begin{aligned}\Pi_{i,k+1} = {}&(1+\varsigma_i\zeta_{i,k})A_{ii}S_{ii,k}A_{ii}^T + Q_i\\ &+ \sum\nolimits_{j\in\mathcal{N}_i}(\varsigma_i + \zeta_{i,k}^{-1})A_{ij}S_{ij,k}A_{ij}^T\end{aligned} \tag{18}$$

where $\zeta_{i,k}$ is any positive scalar and

$$\begin{aligned}\hat{\mathcal{W}}_{ij} &= \theta^2\bar{\xi}\Theta_{ij}^x,\\ \hat{\mathcal{V}}_{ij} &= \begin{cases} R_i, & i = j,\\ R_j + \theta^2\bar{\xi}\Theta_{ij}^z, & i \neq j,\end{cases}\\ \bar{\Upsilon}_{ij,k} &= \begin{cases} \Pi_{i,k}, & i = j,\\ \frac{1}{2}(\Pi_{ij,k}^r + (\Pi_{ij,k}^r)^T) + \kappa_{\vartheta_{ij,k}}\Omega_{ij}, & i \neq j,\end{cases}\\ S_{ij,k} &= \bar{\Upsilon}_{ij,k} - \vartheta_{ij,k}\bar{\Upsilon}_{ij,k}C_j^T\\ &\quad\times\big(C_j\bar{\Upsilon}_{ij,k}C_j^T + \hat{\mathcal{V}}_{ij}\big)^{-1}C_j\bar{\Upsilon}_{ij,k} + \hat{\mathcal{W}}_{ij}.\end{aligned}$$

Proof: Recalling (4) and (10), we can find that the evaluation of filtering performance is based on the filtering errors describing the deviation between the real state $x_{i,k}$ and the estimated state $\hat{x}_{i,k}$. In what follows, let us denote $x_{i,k} - \hat{x}_{i,k}$ as $e_{i,k}$ for the convenience of analysis. Subtracting (9) from (1) leads to the following filtering error dynamics

$$\begin{aligned}&e_{i,k+1}\\ &= (A_{ii} - K_{ii,k}C_i)e_{i,k} + w_{i,k} - K_{ii,k}\nu_{i,k}\\ &\quad+ \sum_{j\in\mathcal{N}_i}\Big(\big(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j\big)e_{j,k} - \theta\xi_{ij,k}A_{ij}\psi_{ij,k}^x\\ &\quad- \vartheta_{ij,k}K_{ij,k}(\nu_{j,k} + \theta\xi_{ij,k}\psi_{ij,k}^z)\Big)\end{aligned} \tag{19}$$

which is further written as

$$\begin{aligned}e_{i,k+1} = \sum_{j\in\mathcal{N}_i\cup\{i\}}&\Big(\big(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j\big)e_{j,k}\\ &- \vartheta_{ij,k}K_{ij,k}\tilde{\nu}_{ij,k} - \theta\xi_{ij,k}A_{ij}\psi_{ij,k}^x\Big) + w_{i,k}\end{aligned} \tag{20}$$

where

$$\tilde{\nu}_{ij,k} = \begin{cases} \nu_{i,k}, & i = j\\ \nu_{j,k} + \theta\xi_{ij,k}\psi_{ij,k}^z & i \neq j\end{cases}$$

It is not difficult to see from (20) that the accurate covariance $P_{i,k+1}$ depends on

$$\begin{aligned}\sum_{j\in\mathcal{N}_i\cup\{i\}}\ \sum_{s\in\mathcal{N}_i\cup\{i\}}&\big(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j\big)\\ &\times\mathbb{E}\{e_{j,k}e_{s,k}^T\}\big(A_{is} - \vartheta_{is,k}K_{is,k}C_s\big)^T\end{aligned}$$

that is, depends on all cross-variance matrices $P_{js,k}$ (i.e. $\mathbb{E}\{e_{j,k}e_{s,k}^T\}$, $j,s \in \mathcal{N}_i$). Considering the connectivity of topology, the optimal filtering is only realized in a centralized way, which results in the serious burden in both calculation and communication as increasing the scale of subsystems. As such, in order to overcome this shortage, its upper bound of $P_{i,k}$ (denoted as $\Pi_{i,k}$) is employed to realize the distributed implementation of the filter (9) with attack detection.

In what follows, in order to develop a distributed design method on desired filter gains $K_{ij,k}$, we introduce the following auxiliary dynamics

$$\begin{aligned}\eta_{j,k+1} = {}&\big(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j\big)e_{j,k}\\ &- \vartheta_{ij,k}K_{ij,k}\tilde{\nu}_{ij,k} - \theta\xi_{ij,k}A_{ij}\psi_{ij,k}^x.\end{aligned} \tag{21}$$

For this dynamics, one has

$$\begin{aligned}&\Phi_{j,k+1}^{\eta}\\ &= \mathbb{E}\{\eta_{j,k+1}\eta_{j,k+1}^T\}\\ &= (A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j)P_{j,k}(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j)^T\\ &\quad+ \vartheta_{ij,k}K_{ij,k}\mathbb{E}\{\tilde{\nu}_{ij,k}\tilde{\nu}_{ij,k}^T\}K_{ij,k}^T\\ &\quad+ A_{ij}\mathbb{E}\{\theta^2\xi_{ij,k}^2\psi_{ij,k}^x(\psi_{ij,k}^x)^T\}A_{ij}^T.\end{aligned} \tag{22}$$

Then, the expectation in the above equation is calculated as follows

$$\mathbb{E}\{\tilde{\nu}_{ij,k}\tilde{\nu}_{ij,k}^T\} = \hat{\mathcal{V}}_{ij}, \quad \mathbb{E}\{\xi_{ij,k}^2\psi_{ij,k}^x(\psi_{ij,k}^x)^T\} = \hat{\mathcal{W}}_{ij}.$$

Therefore, it is easy to obtain that

$$\begin{aligned}&\Phi_{j,k+1}^{\eta}\\ &= (A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j)P_{j,k}(A_{ij} - \vartheta_{ij,k}K_{ij,k}C_j)^T\\ &\quad+ \vartheta_{ij,k}K_{ij,k}\hat{\mathcal{V}}_{ij}K_{ij,k}^T + A_{ij}\hat{\mathcal{W}}_{ij}A_{ij}^T.\end{aligned} \tag{23}$$

In what follows, replacing $P_{j,k}$ by $\bar{\Upsilon}_{ij,k}$, one has an upper bound

$$\begin{aligned}&\Phi^{\eta}_{j,k+1}\\&\le \big(A_{ij}-\vartheta_{ij,k}K_{ij,k}C_j\big)\bar{\Upsilon}_{ij,k}\big(A_{ij}-\vartheta_{ij,k}K_{ij,k}C_j\big)^T\\&\quad+\vartheta_{ij,k}K_{ij,k}\hat{\mathcal{V}}_{ij}K^T_{ij,k}+A_{ij}\hat{\mathcal{W}}_{ij}A^T_{ij}\end{aligned}\tag{24}$$

and its trace is suppressed by selecting

$$K_{ij,k}=A_{ij}\bar{\Upsilon}_{ij,k}C^T_j\big(C_j\bar{\Upsilon}_{ij,k}C^T_j+\hat{\mathcal{V}}_{ij}\big)^{-1},\tag{25}$$

which means that

$$\begin{aligned}\Phi^{\eta}_{j,k+1}&\le A_{ij}(\bar{\Upsilon}_{ij,k}+\hat{\mathcal{W}}_{ij})A^T_{ij}-\vartheta_{ij,k}A_{ij}\bar{\Upsilon}_{ij,k}\\&\quad\times C^T_j\big(C_j\bar{\Upsilon}_{ij,k}C^T_j+\hat{\mathcal{V}}_{ij}\big)^{-1}C_j\bar{\Upsilon}_{ij,k}A^T_{ij}\\&=A_{ij}S_{ij,k}A^T_{ij}.\end{aligned}\tag{26}$$

Finally, according to the relationship between (19) and (20), one has

$$\begin{aligned}P_{i,k+1}&=\mathbb{E}\Big\{\Big(\sum_{j\in\mathcal{N}_i\cup\{i\}}\eta_{j,k+1}\Big)\Big(\sum_{j\in\mathcal{N}_i\cup\{i\}}\eta^T_{j,k+1}\Big)\Big\}\\&=\mathbb{E}\Big\{\eta_{i,k+1}\eta^T_{i,k+1}\Big\}\\&\quad+\sum_{j\in\mathcal{N}_i}\mathbb{E}\Big\{\eta_{i,k+1}\eta^T_{j,k+1}+\eta_{j,k+1}\eta^T_{i,k+1}\Big\}\\&\quad+\sum_{j\in\mathcal{N}_i}\sum_{s\in\mathcal{N}_i}\mathbb{E}\Big\{\eta_{j,k+1}\eta^T_{s,k+1}\Big\}+Q_i\\&\le(1+\varsigma_i\zeta_{i,k})\Phi^{\eta}_{i,k+1}\\&\quad+(\varsigma_i+\zeta^{-1}_{i,k})\sum_{j\in\mathcal{N}_i}\Phi^{\eta}_{j,k+1}+Q_i\\&\le\Pi_{i,k+1}\end{aligned}\tag{27}$$

which completes the proof. ■

So far, we have realized the mentioned objective in Subsection II-C, that is, obtaining the upper bound and the desired filter parameters via formulas in Theorem 2. In what follows, we will further discuss the developed result in comparison with existing ones to systematically expose the main contribution.

B. Two modified versions

It is worth noting that the obtained upper bound $\Pi_{i,k+1}$ is dependent on the scalar $\zeta_{i,k}$, and therefore such a bound can be further optimized, which leads to the following corollary.

Corollary 1: For any i, let $\Pi_{i,0}\ge P_{i,0}$ be given. For the distributed filter (9) with gain (17), a feasible upper bound $\Pi_{i,k+1}$ of the covariance matrix $P_{i,k+1}$ is optimized by

$$\begin{aligned}\Pi_{i,k+1}=\min_{\zeta_{i,k}>0}\Big(&(1+\varsigma_i\zeta_{i,k})A_{ii}S_{ii,k}A_{ii}+Q_i\\&+\textstyle\sum_{j\in\mathcal{N}_i}(\varsigma_i+\zeta^{-1}_{i,k})A_{ij}S_{ij,k}A_{ij}\Big).\end{aligned}$$

In some practical engineering, the innovation from neighbors may not be employed to perform the state estimation. An improved version of distributed filter design is easily accessed, and provided in the following corollary.

Corollary 2: For any i, let $\Pi_{i,0}\ge P_{i,0}$ be given. For the distributed filter

$$\hat{x}_{i,k+1}=A_{ii}\hat{x}_{i,k}+\sum_{j\in\mathcal{N}_i}A_{ij}\hat{x}^r_{ij,k}+K_{ii,k}z_{i,k}\tag{28}$$

with the gain

$$K_{ii,k}=A_{ii}\Pi_{i,k}C^T_i\big(C_i\Pi_{i,k}C^T_i+0.5R_i\big)^{-1},\tag{29}$$

a feasible upper bound $\Pi_{i,k+1}$ of the covariance matrix $P_{i,k+1}$ is calculated by

$$\begin{aligned}\Pi_{i,k+1}=&\,2A_{ii}S_{ii,k}A_{ii}+Q_i\\&+\sum_{j\in\mathcal{N}_i}\varsigma_iA_{ij}(2\bar{\Upsilon}_{ij,k}+\hat{\mathcal{W}}_{ij})A^T_{ij}\end{aligned}\tag{30}$$

where

$$\begin{aligned}\bar{\Upsilon}_{ij,k}&=\frac{1}{2}(\Pi^r_{ij,k}+(\Pi^r_{ij,k})^T)+\kappa_{\vartheta_{ij,k}}\Omega_{ij},\\S_{ii,k}&=\Pi_{i,k}-\Pi_{i,k}C^T_i\big(C_i\Pi_{i,k}C^T_i+0.5R_i\big)^{-1}C_i\Pi_{i,k}.\end{aligned}$$

Proof: For the adopted filter (28), one has

$$\begin{aligned}&e_{i,k+1}\\&=\big(A_{ii}-K_{ii,k}C_i\big)e_{i,k}-K_{ii,k}\nu_{i,k}\\&\quad+\sum_{j\in\mathcal{N}_i}\big(A_{ij}e_{j,k}-\theta\xi_{ij,k}A_{ij}\psi^x_{ij,k}\big)+w_{i,k}\\&=\sqrt{2}\varsigma^{-1}_i\sum_{j\in\mathcal{N}_i}\Big(\frac{1}{\sqrt{2}}\big(A_{ii}-K_{ii,k}C_i\big)e_{i,k}+\frac{\varsigma_i}{\sqrt{2}}A_{ij}e_{j,k}\\&\quad-\frac{1}{\sqrt{2}}K_{ii,k}\nu_{i,k}-\frac{\varsigma_i\theta\xi_{ij,k}}{\sqrt{2}}A_{ij}\psi^x_{ij,k}\Big)+w_{i,k}.\end{aligned}\tag{31}$$

Then, along the similar line of the proof of Theorem 2, one selects the following auxiliary dynamics

$$\begin{aligned}\eta^i_{j,k+1}=&\,\frac{1}{\sqrt{2}}\big(A_{ii}-K_{ii,k}C_i\big)e_{i,k}+\frac{\varsigma_i}{\sqrt{2}}A_{ij}e_{j,k}\\&-\frac{1}{\sqrt{2}}K_{ii,k}\nu_{i,k}-\frac{\varsigma_i\theta\xi_{ij,k}}{\sqrt{2}}A_{ij}\psi^x_{ij,k}.\end{aligned}\tag{32}$$

For above dynamics, one has

$$\begin{aligned}\Phi^{i,\eta}_{j,k+1}&=\mathbb{E}\{\eta^i_{j,k+1}\eta^{iT}_{j,k+1}\}\\&\le\big(A_{ii}-K_{ii,k}C_i\big)P_{i,k}\big(A_{ii}-K_{ii,k}C_i\big)^T\\&\quad+\varsigma^2_iA_{ij}P_{j,k}A^T_{ij}+\frac{1}{2}K_{ii,k}R_iK^T_{ii,k}\\&\quad+\frac{\varsigma^2_i}{2}A_{ij}\hat{\mathcal{W}}_{ij}A^T_{ij}.\end{aligned}\tag{33}$$

In what follows, replacing $P_{j,k}$ by $\bar{\Upsilon}_{ij,k}$ results in

$$\begin{aligned}\Phi^{i,\eta}_{j,k+1}\le&\,\big(A_{ii}-K_{ii,k}C_i\big)\Pi_{i,k}\big(A_{ii}-K_{ii,k}C_i\big)^T\\&+\varsigma^2_iA_{ij}\bar{\Upsilon}_{ij,k}A^T_{ij}+\frac{1}{2}K_{ii,k}R_iK^T_{ii,k}\\&+\frac{\varsigma^2_i}{2}A_{ij}\hat{\mathcal{W}}_{ij}A^T_{ij}.\end{aligned}\tag{34}$$

Then, selecting the filtering gain (29), one has an upper bound of $\Phi^{i,\eta}_{i,k+1}$

$$\Phi^{i,\eta}_{j,k+1}\le A_{ii}\bar{S}_{i,k}A^T_{ii}+\frac{\varsigma^2_i}{2}A_{ij}(2\bar{\Upsilon}_{ij,k}+\hat{\mathcal{W}}_{ij})A^T_{ij}.\tag{35}$$

Finally, according to the relationship between (31) and (32), one has

$$P_{i,k+1}$$

$$
\begin{aligned}
&= \mathbb{E}\Big\{\Big(\sqrt{2}\varsigma_i^{-1}\sum_{j\in\mathcal{N}_i}\eta^i_{j,k+1}\Big)\Big(\sqrt{2}\varsigma_i^{-1}\sum_{j\in\mathcal{N}_i}\eta^i_{j,k+1}\Big)^T\Big\}\\
&= 2\varsigma_i^{-2}\mathbb{E}\Big\{\Big(\sum_{j\in\mathcal{N}_i}\eta^i_{j,k+1}\Big)\Big(\sum_{j\in\mathcal{N}_i}\eta^i_{j,k+1}\Big)^T\Big\}\\
&= 2\varsigma_i^{-2}\sum_{j\in\mathcal{N}_i}\sum_{s\in\mathcal{N}_i}\mathbb{E}\Big\{\eta^i_{j,k+1}(\eta^i_{s,k+1})^T\Big\}+Q_i\\
&\le 2\varsigma_i^{-1}\sum_{j\in\mathcal{N}_i}\Phi^{i,\eta}_{j,k+1}+Q_i\\
&\le 2\varsigma_i^{-1}\sum_{j\in\mathcal{N}_i}\Big(A_{ii}\bar{S}_{i,k}A_{ii}^T\\
&\quad+\frac{\varsigma_i^2}{2}A_{ij}(2\bar{\Upsilon}_{ij,k}+\hat{\mathcal{W}}_{ij})A_{ij}^T\Big)+Q_i\\
&= \Pi_{i,k+1},
\end{aligned}
$$

which completes the proof. ■

In summary, this paper made a successful attempt to develop a novel distributed filtering algorithm with attack detection. The developed result is nontrivial and processes the following identified characteristics: 1) the adopted detector is simplistic and can be carried out in usual processors. There is no doubt that the utilization of detectors can effectively identify abnormal data and therefore increases the security of distributed filtering when occurring a deception attack. 2) the filtering algorithm developed in Theorem 2 is only dependent on the subsystem information itself and the received data from neighboring subsystem, that is, the implementation of algorithm is mutually independent among subsystems. In other words, such an algorithm is carried out in a distributed way and is not affected by increasing the scale of subsystems (i.e. the requirement of scalability).

IV. Simulation Results

In this section, the developed recursive algorithm with attack detection is verified by resorting to the standard IEEE 39-bus power system, which includes 10 generators, 29 loads, and 40 transmission lines. The objective is to design a set of desired filter gains $K_{ii,k}$ and $K_{ij,k}$ via Theorem 2 to realize secure filtering. Similar to the application in [42], the system is partitioned into 10 areas, with one generator in each area, as shown in Fig. 2 for clear description. The dynamics of each power generation area is modeled by the following linear continuous-time model:

$$\dot{x}_i(t) = A^c_{ii}x_i(t) + \sum_{j\in\mathcal{N}_i} A^c_{ij}x_j(t) + B^c_i u_i$$

where x_i and u_i are, respectively, the system state and the control input of area i. More specifically, the system state consists of

$$x_i = [\ \Delta w_i \quad \Delta P_{ij} \quad \Delta P_{m_i} \quad \Delta P_{v_i}\ ]^T$$

where the definitions of elements (i.e. system variables of power systems) are shown in Table II.

TABLE II
System variables of the IEEE 39-bus systems

Δw_i	Deviation of the the angular velocity of the rotor
ΔP_{m_i}	Deviation of the mechanical power
ΔP_{v_i}	Deviation of the electrical power
ΔP_{ij}	Deviation of the power flow on the tie-line from area i to area j
H_i	Inertia constant defined as $H_i = \frac{\text{Kinetic energy at rated speed}}{\text{Machine rating}}$
R_i	Speed regulation
D_i	The load damping constant
T_{ch_i}	The time delay of non-reheat turbine
T_{g_i}	The time constant of the governor
T_{ij}	The synchronizing torque coefficient

TABLE III
Parameters for the IEEE 39-bus systems

	D_i	T_{ch_i}	T_{g_i}	R_i	H_i
Area 1	5	0.2	0.25	0.5	12
Area 2	4	0.2	0.25	0.5	8
Area 3	4	0.2	0.25	0.5	8
Area 4	6	0.2	0.25	0.5	10
Area 5	3.5	0.2	0.25	0.5	7
Area 6	3	0.2	0.25	0.5	7
Area 7	7.5	0.2	0.25	0.5	10
Area 8	4	0.2	0.25	0.5	4
Area 9	6.5	0.2	0.25	0.5	6
Area 10	5	0.2	0.25	0.5	5

Introducing stochastic noises, all system matrices in this application are

$$
A^c_{ii} = \begin{bmatrix} -\frac{D_i}{2H_i} & -\frac{1}{2H_i} & \frac{1}{2H_i} & 0\\ \sum_{j\in\mathcal{N}_i} T_{ij} & 0 & 0 & 0\\ 0 & -\frac{1}{T_{ch_i}} & 0 & \frac{1}{T_{ch_i}}\\ -\frac{1}{R_iT_{g_i}} & 0 & 0 & -\frac{1}{T_{g_i}} \end{bmatrix},
$$

$$
A^c_{ij} = \begin{bmatrix} 0 & 0 & 0 & 0\\ -T_{ij} & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 \end{bmatrix},\quad B^c_i = \begin{bmatrix} 0\\ 0\\ 0\\ \frac{1}{T_{g_i}} \end{bmatrix},
$$

and the covariance of process noises is $Q_i = 0.5I$. Furthermore, the model parameters in above matrices are given in Table III, where T_{ij} is the same with that in [42], and omitted here due to the limited space. In what follows, the measurement matrix is

$$
C^c_i = \begin{bmatrix} 0 & 1 & 0 & 0.1\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix}
$$

and the covariance of measurement noises is $R_i = 0.1I$. We can find that the information Δw_i cannot be involved in measurements. For the purpose of gain design and system simulation, the sampling period is selected as $0.02s$ and the corresponding discrete-time model is not difficult to be obtained approximatively.

For checking the effectiveness of proposed algorithm, malicious data in deception attacks (6) are randomly produced via Matlab software. Specifically, the Matlab command used

Citation information: DOI10.1109/TSMC.2019.2960541

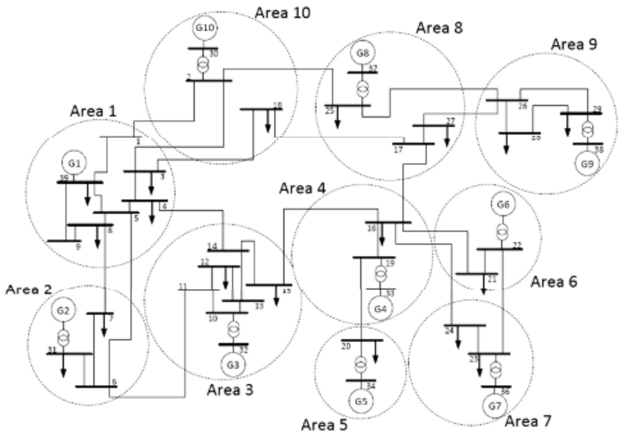


Fig. 2. IEEE 39-bus power system decomposed into ten control areas [42].

in this paper is "normrnd(0, Σ)", where "Σ" stands for Θ^{x}_{ij}, Θ^{x}_{ij} or Θ^{lp}_{ij}. Moreover, the attack instants are from $k = 55$ to $k = 74$, the size of malicious data is assumed to be $\theta = 0.55$, the statistical characteristic is $\bar{\xi} = 0.95$, and the covariance of malicious data are

$$\Theta^{x}_{ij} = I,\ \Theta^{z}_{ij} = I,$$
$$\Theta^{lp}_{ij} = \Theta^{rp}_{ij} = 0.45 \times [\begin{array}{cccc} 1 & 1 & 1 & 1 \end{array}][\begin{array}{cccc} 1 & 1 & 1 & 1 \end{array}]^{T}.$$

This simulation is concerned with distributed filtering, and the controller u_i is designed directly via the corresponding augmented system in the framework of linear quadratic regulators. The adopted Matlab code is "lqr($[A^{c}_{ij}]_{10\times10}$, $\mathrm{diag}_{10}\{B^{c}_{i}\}$, $0.1I_{40}$, $1.1I_{10}$)". For the proposed algorithm, we select the parameters $\alpha = 0.85$, $\kappa_0 = 3$ and $\kappa_1 = 1$. The simulation is run by the PC deployed an Intel Core CPU i7-5500U at 2.40Hz and 8GB RAM, and MATLAB (R2014a). The initial conditions of IEEE 39-bus power systems are chosen as

$$\begin{aligned} x_{9,0} &= x_{5,0} = x_{1,0} = [1.4,\ 1.5,\ 1.3,\ 1.4]^{T}, \\ x_{6,0} &= x_{2,0} = [1.1,\ 1.2,\ 1.8,\ 1.3]^{T}, \\ x_{7,0} &= x_{3,0} = [1.1,\ 2.8,\ 2.8,\ 1.6]^{T}, \\ x_{10,0} &= x_{8,0} = x_{4,0} = [1.3,\ 1.3,\ 1.1,\ 1.4]^{T}, \\ \Pi_{i,0} &= 0.5I,\ \hat{x}_{i,0} = 0.5x_{i,0},\ i \in \mathbb{N}_{10}. \end{aligned}$$

Without loss of generality, we only analyze the test results on Areas 1, 3, 6, and 8. First, the trajectories of true states Δw_i, ΔP_{ij}, ΔP_{m_i}, ΔP_{v_i} (solid lines) and their estimation (dotted lines) are depicted in Figs. 3-6, where Fig. 3 and Fig. 4 occur some fluctuations from instant $k = 55$ to instant $k = 74$. Comparing the estimated trajectories with true ones, we can see that errors are small even though deception attacks happen. Then, the successful detection rate of designed detector is obtained in Table IV, and the values are over 95% based on Monte Carlo simulations with 400 runs, which verifies the effectiveness of adopted attack detector.

In what follows, keeping the same deception attacks, noises and initial conditions, performing traditional filtering (i.e. without any defense) results in the corresponding estimation of Δw_i, ΔP_{v_i}, which are plotted in Figs. 7-8. We can find from these two figures that the filtering errors are obviously larger than that in Fig. 3 and Fig. 6 over the time range $[55,\ 74)$, and such errors further lead to the degradation of filtering performance after attacks vanish. These verify that the developed filter is performed very well while showing good defense capacity.

TABLE IV
SUCCESSFUL DETECTION RATE

Areas	1	2	3	4	5
Rate (%)	96.40	96.87	97.38	95.47	97.23
Areas	6	7	8	9	10
Rate (%)	96.09	96.22	95.18	97.50	97.45

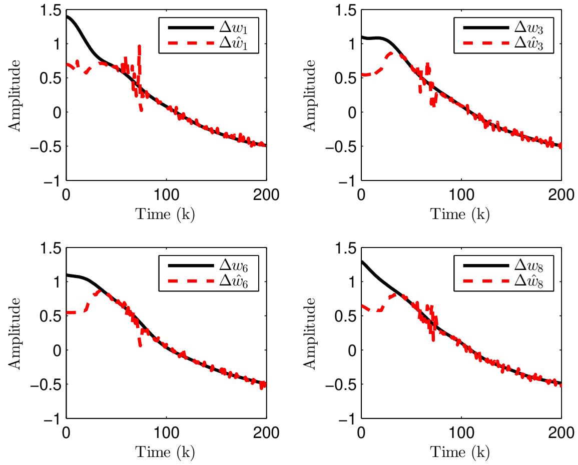


Fig. 3. The true value Δw_i and its estimation $\Delta\hat{w}_i$ $(i = 1, 3, 6, 8)$.

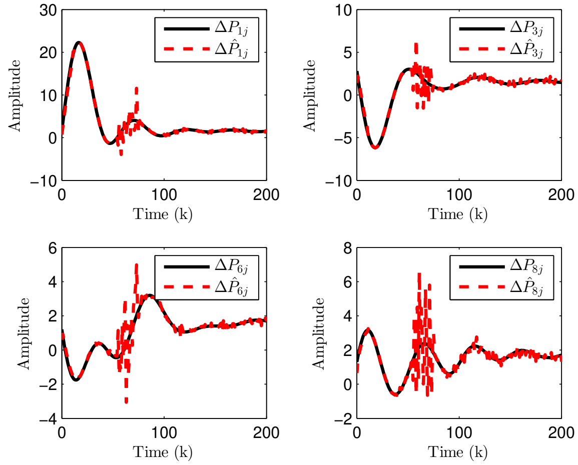


Fig. 4. The true value ΔP_{ij} and its estimation $\Delta\hat{P}_{ij}$ $(i = 1, 3, 6, 8)$.

V. Conclusions

In this paper, the distributed recursive filtering issue with attack detection has been investigated for a class of CPSs

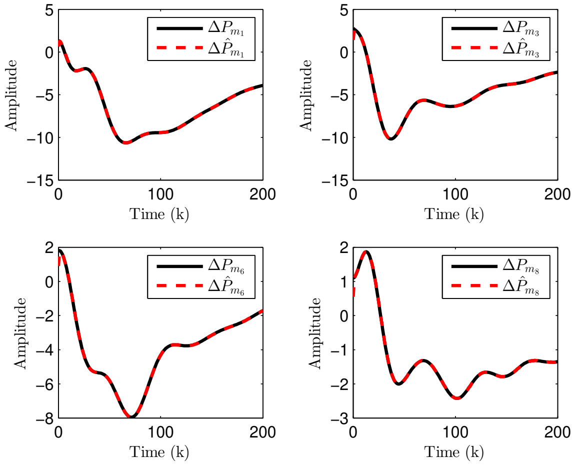


Fig. 5. The true value ΔP_{m_i} and its estimation $\Delta \hat{P}_{m_i}$ $(i = 1, 3, 6, 8)$.

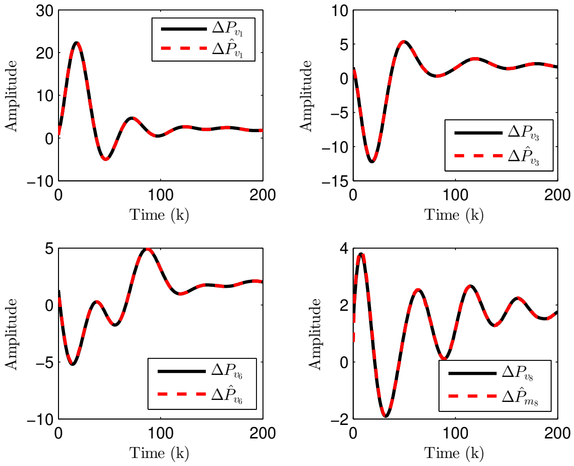


Fig. 6. The true value ΔP_{v_i} and its estimation $\Delta \hat{P}_{v_i}$ $(i = 1, 3, 6, 8)$.

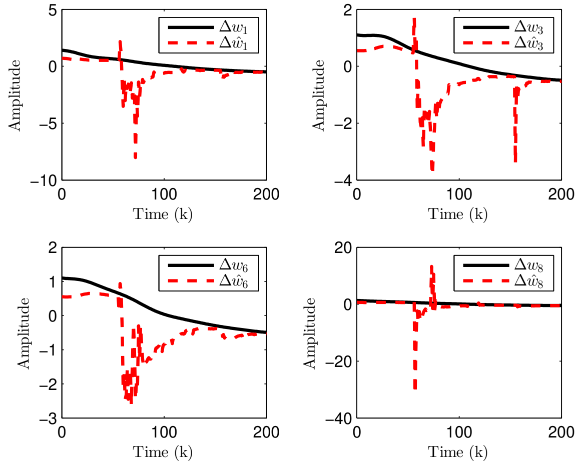


Fig. 7. The true value Δw_i and its estimation $\Delta \hat{w}_i$ $(i = 1, 3, 6, 8)$.

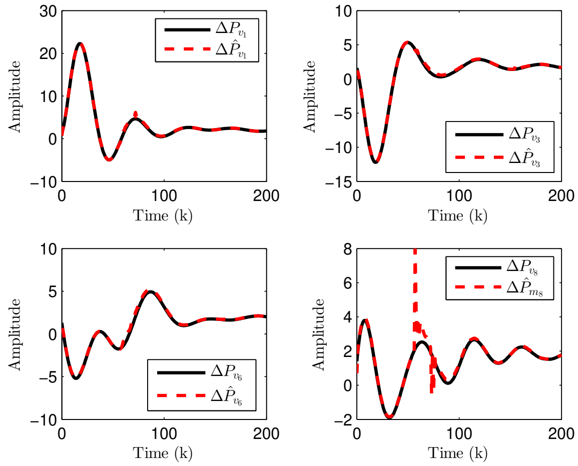


Fig. 8. The true value ΔP_{v_i} and its estimation $\Delta \hat{P}_{v_i}$ $(i = 1, 3, 6, 8)$.

consisting of a set of spatially distributed subsystems. According to deception attacks coming from inherent security vulnerability of communication networks, a detector, dependent on both the received innovation and a predetermined threshold α, has been proposed to identify the occurring attacks as far as possible. In light of identified attacks, a novel distributed filter has been constructed and its gains have been designed via a set of recursive formulas. These formulas have been derived by resorting to a set of auxiliary error dynamics and have also been utilized to calculate the upper bound of covariance of filtering errors. It has been further found that the upper bound only depends on the neighboring information and the information from the subsystem itself. As such, the calculation burden almost remains unchanged when the scale of addressed CPSs increases and thereby satisfying the requirement of the scalability. Moreover, noting the rule of attack detectors, the proposed filter is applicable for the case that attackers cannot carry out stealth attack. Finally, a standard IEEE 39-bus power systems has been utilized to verify the effectiveness of proposed filtering scheme. The test results shown that the designed filter has the good capability to reduce the impact from deception attacks. Further research topics include extending our results to more complex scenarios as well as various engineering applications: 1) CPSs with varying or switching topologies, 2) communication scheduling with various protocols, 3) communications subject to different attacks or network-induced phenomena, and 4) more effective detection schemes for cyber-attacks [43]–[45].

References

[1] L. Ding, L. Wang, G. Yin, W. Zheng, and Q.-L. Han, “Distributed energy management for smart grids with an event-triggered communication scheme,” *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 5, pp. 1950-1961, Sep. 2019.

[2] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 2483-2499, May 2019.

[3] G. Wen, Y. Wan, J. Cao, T. Huang, and W. Yu, “Master-slave synchronization of heterogeneous systems under scheduling communication,”

IEEE Trans. Syst., Man, Cybern., Syst., vol. 48, no. 3, pp. 473-484, Mar. 2018.

[4] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang, "Distributed event-triggered estimation over sensor networks: A survey," *IEEE Trans. Cybern.*, to be published, doi:10.1109/TCYB.2019.2917179.

[5] L. Ding, Q.-L. Han, and X.-M. Zhang, "Distributed secondary control for active power sharing and frequency regulation in islanded microgrids using an event-triggered communication mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 3910-3922, Jul. 2019.

[6] B. Shen, Z. Wang, D. Wang, J. Luo, H. Pu, Y. Peng, "Finite-horizon filtering for a class of nonlinear time-delayed systems with an energy harvesting sensor," *Automatica*, Vol. 100, no. 2, pp. 144-152, Feb. 2019.

[7] M. Farina, and R. Carli, "Partition-based distributed Kalman filter with plug and play features," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 560-570, Mar. 2018.

[8] C. Chen, J. Yan, N. Lu, Y. Wang, X. Yang, and X. Guan, "Ubiquitous monitoring for industrial cyber-physical systems over relay-assisted wireless sensor networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 3, pp. 352-362, Jul. 2015.

[9] M. Rostami and S. Lotfifard, "Distributed dynamic state estimation of power systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3395-3404, Aug. 2018.

[10] J. Du, S. Ma, Y.-C. Wu, and H. V. Poor, "Distributed hybrid power state estimation under PMU sampling phase errors," *IEEE Trans. Signal Process.*, vol. 62, no. 16, pp. 4052-4063, Aug. 2014.

[11] M. Rana, L. Li, S. W. Su, and W. Xiang, "Microgrid state estimation: A distributed approach," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3368-3375, Aug. 2018.

[12] M. Rana, L. Li, and S. W. Su, "Distributed state estimation over unreliable communication networks with an application to smart grids," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 1, pp. 89-96, Mar. 2017.

[13] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1148-1159, Apr. 2019.

[14] W. Chen, D. Ding, H. Dong, and G. Wei, "Distributed resilient filtering for power systems subject to denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 8, pp. 1688-1697, Aug. 2019.

[15] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for a class of discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 5, pp. 779-789, May 2018.

[16] B. Shen, Z. Wang, D. Wang, and Q. Li, "State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published, doi: 10.1109/TNNLS.2019.2946290.

[17] J. Liu, Z.-G. Wu, D. Yue, and J. H. Park, "Stabilization of networked control systems with hybrid-driven mechanism and probabilistic cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2018.2888633.

[18] S. Hu, D. Yue, X. Chen, Z. Cheng, and X. Xie, "Resilient H_∞ filtering for event-triggered networked systems under nonperiodic DoS jamming attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2019.2896249.

[19] Q. Wang, W. Tai, Y. Tang, M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 2, pp. 101-107, Jun. 2019.

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

[21] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Contr. Syst. Mag.*, vol. 37, no. 2 pp. 66-81, Apr. 2017.

[22] B. Chen, D. W. C. Ho, W.-A. Zhang, and L. Yu, "Distributed dimensionality reduction fusion estimation for cyber-physical systems under DoS attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 2, pp. 455-468, Feb. 2019.

[23] L. Peng, L. Shi, X. Cao, and C. Sun, "Optimal attack energy allocation against remote state estimation," *IEEE Trans. Autom. Control*, vol. 63, no. 7, pp. 2199-2205, Jul. 2018.

[24] Y. Wu and J. Dong, "Cyber-physical attacks against state estimators based on a finite frequency approach," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2018.2882852.

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

[26] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532-543, Jun. 2016.

[27] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[28] S. Bi, and Y. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216-1227, May 2014.

[29] S. Riverso, M. Farina, and G. Ferrari-Trecate, "Plug-and-play state estimation and application to distributed output feedback model predictive control," *Eur. J. Control*, vol. 25, pp. 17-26, 2015.

[30] B. Chen, G. Hu, D. W. C. Ho, and L. Yu, "Distributed Kalman filtering for time-varying discrete sequential systems," *Automatica*, vol. 99, pp. 228-236, Jan. 2019.

[31] S. Sahoo and S. Mishra, "An adaptive event-triggered communication based distributed secondary control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674-6683, Nov. 2018.

[32] L. Ding, Q.-L. Han, L. Wang, and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 3924-3935, Sep. 2018.

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

[34] W. Yang, Y. Zhang, G. Chen, C. Yang, and L. Shi, "Distributed filtering under false data injection attacks," *Automatica*, vol. 102, pp. 34-44, 2019.

[35] C. Gu, J. Panida, and M. Mehul, "Detecting false data injection attacks in AC state estimation," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2476-483, Sep. 2015.

[36] H. M. Khalid, and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026-2037, Jul. 2016.

[37] G. Bernieri, E. Miciolino, F. Pascucci, R. Setol, "Monitoring system reaction in cyber-physical testbed under cyber-attacks," *Comput. Electr. Eng.*, vol. 59, pp. 86-98, Apr. 2017.

[38] L. Hu, Z. Wang, I. Rahman, and X. Liu, "A constrained optimization approach to dynamic state estimation for power systems including PMU and missing measurements," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 2, pp. 703-710, Mar. 2016.

[39] U. A. Khan and J. M. F.Moura, "Distributing the Kalman Filters for large-scale systems," *IEEE Trans. Signal Process.*, vol. 56, no. 10, pp. 4919-4935, Oct. 2008.

[40] A. Haber and M. Verhaegen, "Moving horizon estimation for large-scale interconnected systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2834-2847, Nov. 2013.

[41] Z. Chen, B. Wang, and A. N. Gorban, "Multivariate Gaussian and student-t process regression for multi-output prediction," arXiv preprint, arXiv: 1703.04455, Mar. 2017.

[42] I. E. Atawi, An advance distributed control design for wide-area power system stability. *PhD Diss.*, University of Pittsburgh, 2013.

[43] D. Ding, Z. Wang, and Q.-L. Han, "A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks," *IEEE Trans. Autom. Control*, to be published, doi: 10.1109/TAC.2019.2934389.

[44] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: a survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, to be published, doi: 10.1109/JAS.2019.1911651.

[45] W. Chen, D. Ding, X. Ge, Q.-L. Han, and G. Wei, "$\mathcal{H}_\infty$ containment control of multi-agent systems under event-triggered communication scheduling: The finite-horizon case," *IEEE Trans. Cybern.*, to be published, doi:10.1109/TCYB.2018.2885567.

Derui Ding (M'16) received both the B.Sc. degree in Industry Engineering in 2004 and the M.Sc. degree in Detection Technology and Automation Equipment in 2007 from Anhui Polytechnic University, Wuhu, China, and the Ph.D. degree in Control Theory and Control Engineering in 2014 from Donghua University, Shanghai, China. From July 2007 to December 2014, he was a teaching assistant and then a lecturer in the Department of Mathematics, Anhui Polytechnic University, Wuhu, China.

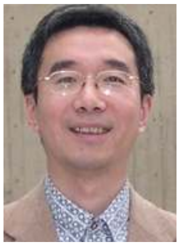
He is currently a senior research fellow with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, Australia. From June 2012 to September 2012, he was a research assistant in the Department of Mechanical Engineering, the University of Hong Kong, Hong Kong. From March 2013 to March 2014, he was a visiting scholar in the Department of Information Systems and Computing, Brunel University London, UK. His research interests include nonlinear stochastic control and filtering, as well as multi-agent systems and sensor networks. He has published around 40 papers in refereed international journals.

Dr. Ding is serving as an Associate Editor for *Neurocomputing* and *IET Control Theory* & *Applications*. He is also a very active reviewer for many international journals.

Qing-Long Han (M'09-SM'13-F'19) received the B.Sc. degree in Mathematics from Shandong Normal University, Jinan, China, in 1983, and the M.Sc. and Ph.D. degrees in Control Engineering and Electrical Engineering from East China University of Science and Technology, Shanghai, China, in 1992 and 1997, respectively.

From September 1997 to December 1998, he was a Post-doctoral Researcher Fellow with the Laboratoire d'Automatique et d'Informatique Industielle (currently, Laboratoire d'Informatique et d'Automatique pour les Systémes), École Supérieure d'Ingénieurs de Poitiers (currently, École Nationale Supérieure d'Ingénieurs de Poitiers), Université de Poitiers, France. From January 1999 to August 2001, he was a Research Assistant Professor with the Department of Mechanical and Industrial Engineering at Southern Illinois University at Edwardsville, USA. From September 2001 to December 2014, he was Laureate Professor, an Associate Dean (Research and Innovation) with the Higher Education Division, and the Founding Director of the Centre for Intelligent and Networked Systems at Central Queensland University, Australia. From December 2014 to May 2016, he was Deputy Dean (Research), with the Griffith Sciences, and a Professor with the Griffith School of Engineering, Griffith University, Australia. In May 2016, he joined Swinburne University of Technology, Australia, where he is currently Pro Vice-Chancellor (Research Quality) and a Distinguished Professor. His research interests include networked control systems, multi-agent systems, time-delay systems, complex dynamical systems and neural networks.

Professor Han is a Highly Cited Researcher according to Clarivate Analytics (formerly Thomson Reuters). He is a Fellow of The Institution of Engineers Australia. He is an Associate Editor of several international journals, including the IEEE TRANSACTIONS ON CYBERNETICS, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE INDUSTRIAL ELECTRONICS MAGAZINE, the IEEE/CAA JOURNAL OF AUTOMATICA SINICA, Control Engineering Practice, and Information Sciences.



Zidong Wang (SM'03-F'14) was born in Jiangsu, China, in 1966. He received the B.Sc. degree in mathematics in 1986 from Suzhou University, Suzhou, China, and the M.Sc. degree in applied mathematics in 1990 and the Ph.D. degree in electrical engineering in 1994, both from Nanjing University of Science and Technology, Nanjing, China.

He is currently Professor of Dynamical Systems and Computing in the Department of Computer Science, Brunel University London, U.K. From 1990 to 2002, he held teaching and research appointments in universities in China, Germany and the UK. Prof. Wang's research interests include dynamical systems, signal processing, bioinformatics, control theory and applications. He has published more than 300 papers in refereed international journals. He is a holder of the Alexander von Humboldt Research Fellowship of Germany, the JSPS Research Fellowship of Japan, William Mong Visiting Research Fellowship of Hong Kong.

Prof. Wang serves (or has served) as the Editor-in-Chief for Neurocomputing, Deputy Editor-in-Chief for International Journal of Systems Science, and an Associate Editor for 12 international journals including IEEE TRANSACTIONS ON AUTOMATIC CONTROL, IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, IEEE TRANSACTIONS ON NEURAL NETWORKS, IEEE TRANSACTIONS ON SIGNAL PROCESSING, and IEEE TRANSACTIONS ON SYSTEMS, MAN, and CYBERNETICS - Part C. He is a Fellow of the IEEE, a Fellow of the Royal Statistical Society and a member of program committee for many international conferences.

Xiaohua Ge (M'18) received the B.Eng. degree in electronic and information engineering from Nanchang Hangkong University, Nanchang, China, in 2008, the M.Eng. degree in control theory and control engineering from Hangzhou Dianzi University, Hangzhou, China, in 2011, and the Ph.D. degree in computer engineering from Central Queensland University, Rockhampton, Australia, in 2014.

From 2011 to 2013, he was a Research Assistant with the Centre for Intelligent and Networked Systems (CINS, now known as Centre for Intelligent Systems), Central Queensland University. In 2014, he was a Research Fellow with the CINS, Central Queensland University, Rockhampton, Australia. From 2015 to 2017, he was a Research Fellow with the Griffith School of Engineering, Griffith University, Gold Coast, Australia. He is currently a Lecturer with the School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, Australia.

His research interests include distributed estimation and control of sensor networks, multi-agent systems, and cyber-physical systems and their applications.