Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances

Dan Zhang, *IEEE Senior Member*, Gang Feng, *IEEE Fellow*, Yang Shi, *IEEE Fellow*, and Dipti Srinivasan, *IEEE Fellow*

***Abstract*—Multi-agent systems (MASs) are typically composed of multiple smart entities with independent sensing, communication, computing, and decision-making capabilities. Nowadays, MASs have a wide range of applications in smart grids, smart manufacturing, sensor networks, and intelligent transportation systems. Control of the MASs are often coordinated through information interaction among agents, which is one of the most important factors affecting coordination and cooperation performance. However, unexpected physical faults and cyber attacks on a single agent may spread to other agents via information interaction very quickly, and thus could lead to severe degradation of the whole system performance and even destruction of MASs. This paper is concerned with the safety/security analysis and synthesis of MASs arising from physical faults and cyber attacks, and our goal is to present a comprehensive survey on recent results on fault estimation, detection, diagnosis and fault-tolerant control of MASs, and cyber attack detection and secure control of MASs subject to two typical cyber attacks. Finally, the paper concludes with some potential future research topics on the security issues of MASs.**

***Index Terms*—Consensus, deception attack, deny-of-service (DoS) attack, fault detection, fault estimation, fault tolerant control, multi-agent systems.**

Manuscript received August 15, 2020; revised October 12, 2020; accepted October 23, 2020. This work was partially supported by the National Natural Science Foundation of China (61873237), the Fundamental Research Funds for the Central Universities, the Fundamental Research Funds for the Provincial Universities of Zhejiang (RF-A2019003), the Research Grants Council of the Hong Kong Special Administrative Region of China (CityU/11204315), and the Hong Kong Scholars Program (XJ2016030). Recommended by Associate Editor MengChu Zhou. *(Corresponding author: Dan Zhang.)*

Citation: D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021.

D. Zhang is with the Research Center of Automation and Artificial Intelligence, Zhejiang University of Technology, Hangzhou, 310023, and also with Key Laboratory of Advanced Control and Optimization for Chemical Processes (East China University of Science and Technology), Ministry of Education, Shanghai 200237, China (e-mail: danzhang@zjut.edu.cn).

G. Feng is with the Department of Biomedical Engineering, City University of Hong Kong, Hong Kong, China (e-mail: megfeng@cityu.edu.hk).

Y. Shi is with the Department of Mechanical Engineering, University of Victoria, Canada (e-mail: yshi@uvic.ca).

D. Srinivasan is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore (e-mail: dipti@nus.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/JAS.2021.1003820

I. Introduction

With rapid development of perception, communication, and computation technologies, distributed cooperative control of multi-agent systems (MASs) has received great attention from scholars in different disciplines due to their wide applications in large-scale process industries, multi-robot systems, intelligent transportation systems, sensor networks, smart grids, and internet systems [1]–[5]. In the field of intelligent transportation systems, as shown in Fig. 1, the distributed control framework of networked autonomous vehicles can provide new solutions for the safety and efficiency of transportation systems, and help solve practical problems such as traffic accidents, road congestion, energy conservation, and environmental protection [6]. Compared with traditional single-agent systems, multi-agent systems are more scalable and upgradeable while improving task execution efficiency and robustness due to its inherent ability to learn and make autonomous decisions cooperatively.

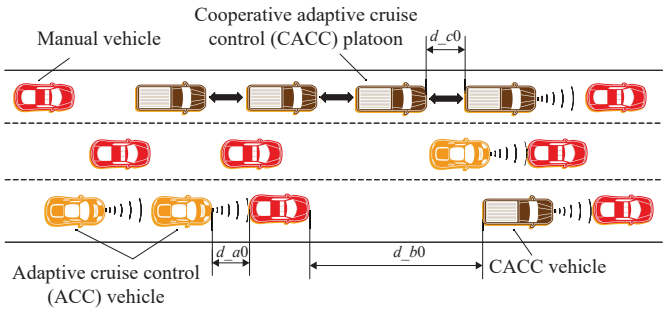

Fig. 1. The coordinated vehicles in transportation systems.

The analysis and synthesis of MASs have been extensively studied in a variety of disciplines including computer science, control engineering, electrical engineering, and civil engineering. Existing survey articles present discussions on communication mechanism of MASs [7], [8], consensus protocol of MASs [9], and communication constraints of MASs [10]. Survey works on MASs in the context of computer sciences are also found in [11]–[14]. However, none of these articles concentrate on the issue of securities of MASs though such a kind of networked systems are fragile to physical faults and cyber attacks [15]. It has been recently revealed in [16] that a small fault or cyber attack on an agent can degrade the performance and even paralyze the whole system. What shall we do when some agents are misbehaving,

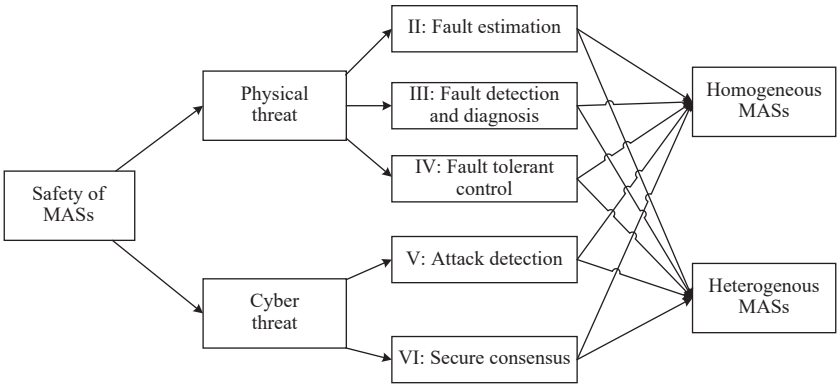

Fig. 2. The structure of paper.

wait, abandon, or adjust [17]? In [18], the issues of access control and trust/reputation of MASs were addressed for the security of MASs. In [19], fault-tolerant control methods of MASs were surveyed, and the attention was focused on topology reconfiguration methods. Nevertheless, there have been a large volume of works on physical safety and cyber security analysis and synthesis in literature recently, where the issues of fault estimation, detection and diagnosis, fault-tolerant control, attack detection, and secure consensus were investigated. These studies provide some systematic perspectives and methodologies for improving security of MASs effectively.

In this paper, we provide a comprehensive overview of recent advances in the physical safety and cyber security issues of MASs, where the actuator and sensor faults will be discussed in the physical safety analysis part, and the deny-of-service (DoS) attack and Deception attack will be addressed in the cyber security section. The paper is organized as follows. Section II introduces salient results on the fault estimation of MASs, along with some key analysis methods. Section III addresses fault detection and diagnosis of MASs. Section IV discusses fault-tolerant control of MASs. Section V is concerned with representative cyber attacks in MASs and corresponding attack detection schemes. Section VI presents some recent results on secure control of MASs. Finally, Section VII concludes the article with some potential future research topics. The structure of this paper is depicted in Fig. 2. The major differences between the relevant survey papers [18], [19] and our paper are summarized as follows:

1) Reference [18] is concerned with the access control and reputation of MASs. Instead we focus on the cyber security and physical safety of MASs and deal with the safety and security control problem.

2) In [19], the fault-tolerant control methods of MASs are surveyed with its attention focused on the topology reconfiguration methods. In contrary, we start with the physical threat and conduct a review on recent results on fault estimation, fault detection, and fault-tolerant control of MASs; Then, we pay attention to the cyber threat issue, and analyze recent advances on two typical attacks, DoS attack and Deception attack.

3) A more systematic and broader overview on the safety and security of MASs is given, aiming to provide a comprehensive survey on this emerging and challenging research direction.

II. Fault Estimation of Mass

In the past decades, there has been an increasing demand on safety and reliability of MASs, as a single fault on the sensor or actuator could lead to a significant performance degradation on the whole system and even the failure of the whole system. In [20], the performance of a group of unmmaned autonomous vehicles (UAVs) that are subject to different types of actuator faults was investigated, and it was shown that a consensus can still be achieved if a fault of the partial loss of effectiveness occurs in one actuator of an agent, but the transient performance could be degraded dramatically. The consensus would fail to be achieved when actuators are in complete loss of effectiveness. A good fault estimation scheme is capable of providing the timely and precise information of any faults within the system being monitored. Then the effective defense mechanism can be triggered to eliminate the effect of the fault to the system. In this section, we address the fault estimation problem, but only focus on the model-based fault estimation of MASs. The readers are referred to [21]–[23] for model-free ones. A detailed categorization of physical threats in the study of fault estimation of MASs is given in Table I.

TABLE I
Categorization of Physical Threats in the Study of Fault Estimation of MASs

Fault types	Reference
Actuator fault	[24]–[33]
Sensor fault	[34]
Actuator and sensor faults	[35], [36]

A. Homogeneous MASs

Online fault estimation of MASs is challenging due to the complex interactions among of MASs. Consider a homogeneous MAS with N agents, and each agent is modeled by the following linear system:

$$\begin{cases} \dot{x}_i(t) = Ax_i(t) + Bu_i(t) + Ef_i(t) + Dv_i(t) \\ y_i(t) = Cx_i(t), \quad i = 1,2,...,N \end{cases} \tag{1}$$

where $x_i(t) \in \mathbb{R}^n$, $u_i(t) \in \mathbb{R}^m$, and $y_i(t) \in \mathbb{R}^p$ are the state, input, and output of the i-th agent, respectively. $v_i(t) \in \mathbb{R}^d$ is the unknown disturbance, and $f_i(t) \in \mathbb{R}^r$ is the unknown fault, e.g., an actuator fault when $E = B$. A, B, C, D, and E are constant

matrices. In [24], the following system was introduced:

$$\begin{cases} \dot{\tilde{x}}_i(t) = A\tilde{x}_i(t) + B\tilde{u}_i(t) + E\tilde{f}_i(t) + D\tilde{v}_i(t) \\ \tilde{z}_i(t) = C\tilde{x}_i(t) \quad , i = 2, ..., N \end{cases} \tag{2}$$

where $\tilde{x}_i(t) = \bar{x}_i(t) \rightarrow T_i\bar{x}_i(t)$ is a new state after a change of coordinates with $\bar{x}_i(t) = x_i(t) - x_1$, and T_i is a transformation matrix. For the above agent system (2), the following sliding mode observer was designed [24]:

$$\begin{cases} \dot{\tilde{w}}_i(t) = A\tilde{w}_i(t) + B\tilde{u}_i(t) - G_1 e_{zi}(t) + G_2\varphi_i(t) \\ e_{zi}(t) = C\tilde{w}_i(t) - \tilde{z}_i(t) \\ \varphi_i(t) = -\alpha_i \|CE\| \dfrac{e_{zi}(t)}{\|e_{zi}(t)\|}, \quad \text{if } e_{zi}(t) \neq 0 \end{cases} \tag{3}$$

where $\alpha_i > 0$, and G_1 and G_2 were designed to ensure a stable sliding motion on the surface $\mathcal{S} = \{(e_2, e_3, \ldots, e_N) | Ce_i = 0\}$. It was shown that the fault can be estimated if the derivative of the fault is known a prior. However this condition appears to be restrictive. The similar sliding mode observer for a network of dynamical systems can also be found in [25]. To remove the assumption on the fault, some other methods were proposed. In [26], in order to estimate the system fault, an augmented system including the fault as an auxiliary state vector was constructed as follows:

$$\begin{cases} \dot{\bar{x}}_i(t) = \bar{A}\bar{x}_i(t) + \bar{B}u_i(t) + \bar{D}d_i(t) \\ y_i(t) = \bar{C}\bar{x}_i(t) \end{cases} \tag{4}$$

where $\bar{x}_i(t) = \begin{bmatrix} x_i(t) \\ f_i(t) \end{bmatrix}$. For the above augmented system (4), the following distributed fault estimator [26] was designed:

$$\begin{cases} \dot{\hat{x}}_i(t) = \bar{A}\hat{x}_i(t) + \bar{B}u_i(t) - \bar{H}\eta_i(t) - \alpha\bar{F}\dot{\eta}_i(t) \\ \hat{y}_i(t) = \bar{C}\hat{x}_i(t) \end{cases} \tag{5}$$

where $\hat{x}_i(t) \in \mathbb{R}^n$ and $\hat{y}_i(t) \in \mathbb{R}^p$ are the observer's state and output, respectively. $\eta_i(t) = \sum_{j\in N_i} a_{ij}((\hat{y}_i - y_i) - (\hat{y}_j - y_j)) + g_i \times ((\hat{y}_i - y_i))$ is the relative output variable with respect to its neighbors. $\bar{H}$ is the observer gain, α and $\bar{F}$ are adjustable parameters. With the help of the Lyapunov stability theory and via treating the derivative of the fault as an unknown disturbance, some sufficient conditions in terms of linear matrix inequalities (LMIs) were derived such that the estimation error system was ensured to be asymptotically stable and achieved a prescribed H_∞ performance level. Based on the similar augmented system method and with the average dwell time switching scheme, the process fault can be distributively estimated when the topology of MASs is slowly switching [27]. Meanwhile, the reduced-order fault estimation observer was reported in [28] based on a similar method. For the sensor fault estimation of a time-varying agent network, an augmentation system was also derived in [34] and then an unknown input observer (UIO) was designed to solve the sensor fault estimation problem.

In [35], the unknown input observer (UIO) was designed for linear MASs with actuator faults and sensor faults, respectively. The designed UIO was described as follows for the actuator fault estimation:

$$\begin{cases} \dot{\bar{z}}_i(t) = \bar{T}\bar{A}\left(\bar{z}_i(t) + \bar{H}y_i(t)\right) + \bar{T}\bar{B}u_i(t) - \bar{K}\eta_i(t) \\ \hat{f}_i(t) = \bar{I}_r\left(\bar{z}_i(t) + \bar{H}y_i(t)\right) \\ \hat{y}_i(t) = \bar{C}\left(\bar{z}_i(t) + \bar{H}y_i(t)\right) \end{cases} \tag{6}$$

where $\eta_i(t) = \sum_{j\in N_i} a_{ij}[(\hat{y}_i(t) - y_i(t)) - (\hat{y}_j(t) - y_j(t))] + g_i[(\hat{y}_i(t) - y_i(t)) - (\hat{y}_0(t) - y_0(t))]$ is the output estimation from itself and its neighbors. $\bar{I}_r = \begin{bmatrix} 0 \\ I \end{bmatrix}^T$. $\bar{T}, \bar{K}$, and H are the UIO gain matrices to be determined by solving two matrix inequalities. Recently, the fault estimation problem for a class of Lipschitz nonlinear MASs was also considered in the finite-frequency domain in [29] and [30], and the fault estimator gains which are determined by the generalized Kalman-Yakubovich-Popov (KYP) lemma. Although the fault can be estimated precisely in the above studies, the major issue is that an augmentation model including the fault as a new state must be established first, which may lead to some computation issue especially in the LMI-based design method. The main goal is to estimate the fault, thus one may only need to design a reduced-order estimator without estimating the whole state. By doing so, the computational burden may be reduced.

Different from the above state augmentation method, an intermediate variable $\tau_i(t) = f_i(t) - S x_i(t)$ was introduced in [31], where S is a design parameter. It is seen from this intermediate variable that it contains the information of the fault directly. Therefore, an estimator was designed for the estimation of $x_i(t)$ and $\tau_i(t)$ such that $\hat{f}_i(t) = \hat{\tau}_i(t) + S\hat{x}_i(t)$. The main limitation is that both the state observer and the intermediate variable observer were designed based on the interaction of the estimated states, which may require more communication than the above output-based results. Other works such as adaptive distributed fuzzy fault estimation can also be found in [36], where the fuzzy logic method was adopted to approximate the actuator and sensor faults in agents.

It is worth pointing out that the local fault in the i-th agent cannot be estimated by its neighbors in the aforementioned results as only the local state and fault were augmented for estimation. Recently, the distributed fault estimator design for a class of Lipschitz nonlinear MASs was investigated in [32], where a new augmented state vector including the local state fault and the neighboring state fault was constructed. The designed observer therein is capable of providing a good estimation of faults both in local agent and its neighbors. The common limitation is still the computational burden when the augmentation technique is used.

B. Heterogenous MASs

It is worth pointing out that all the above studies [24]–[32], [34]–[36] focused on homogeneous MASs. In reality, most of multi-agent systems have different agent dynamics, see, trucks, buses and cars in transportation systems. Therefore, distributed fault estimation of heterogeneous MASs has received increasing attention. For a class of linear discrete-time heterogeneous linear MASs, a distributed l_1-norm-based optimization method was introduced to estimate the state and

fault simultaneously in [33]. It was shown that if and only if the number of faulty agents is smaller than the half of number of agents and the following optimization problem:

$$\hat{x}(k+1) = \arg\min \|x - A\hat{x}(k) + Bu(k)\|_1$$
$$\text{s.t.} \quad y(k) = Cx(k) \tag{7}$$

has a solution, then the fault $f(k)$ can be estimated. It was further shown that if the state estimation at time k is bounded, and the fault estimation error at time $k+1$ would also be bounded, i.e., when $\|\hat{x}(k) - x(k)\|_1 \le \alpha_{\max}$, the fault estimation error is bounded as $\left\|\hat{f}(k+1) - f(k+1)\right\|_1 \le 2(M-N)/(M-2N) \times \eta\alpha_{\max}$, where M and N are the number of agents and faulty agents, respectively. $\eta = \sum_{i=1}^{nM}\sum_{j=1}^{nM}\left|A^{(i,j)}\right|$, n is the dimension of the fault. By the fact that the above optimization problem is solved in a centralized manner, which results in large computation cost especially when the system size is large. In order to reduce the computational burden, a distributed framework inspired by the distributed basis pursuit (DBP) algorithm [37] was introduced:

$$\min \frac{1}{M}\sum_{i=1}^{M}\left\|\lambda_i - A\hat{\lambda}_i(k) - B\kappa\left(\hat{\lambda}_i(k)\right)\right\|_1$$
$$\text{s.t.} \begin{cases} y_1(k) = C_{1q}\lambda_1 \\ y_i(k) = C_i\lambda_i \quad \forall i \in \{2,3,\ldots,M\} \end{cases} \tag{8}$$

where $\hat{\lambda}_i$ is the estimation of $x(k)$ and $\kappa\left(\hat{\lambda}_i(k)\right) = \rho\sum_{j\in N_i}\left(\hat{\lambda}_i(k) - \hat{\lambda}_j(k)\right)$. The fault estimation can be determined by $\hat{f}_i(k+1) = \hat{\lambda}_i(k+1) - A\hat{\lambda}_i(k) - B\kappa\left(\hat{\lambda}_i(k)\right)$. However, the proposed distributed algorithm is working only when the leader can collect the local measurement and relative measurement simultaneously at the initial time, and there is no fault at the initial time instant. In addition, the global system state matrix A and B are still required to be known to all agents. Design of a fully distributed fault estimator for heterogeneous MASs is still a challenging task, and deserves further investigation.

III. Fault Detection and Diagnosis

Compared with fault estimation, traditional fault detection and diagnosis is less demanding as it only seeks to trigger an alarm signal when a fault is detected in the system (and then isolate the fault). It has been extensively adopted in many real systems such as power systems [38], mechatronic systems [39], chemical systems [40], etc. We now address the fault detection and diagnosis issue of MASs, and present some recent results in this area. A detailed categorization of physical threats in the study of fault detection and diagnosis of MASs is given in Table II.

TABLE II
Categorization of Physical Threats in the Study of Fault Detection and Diagnosis of MASs

Fault types	Reference
Actuator fault	[41]−[44]
Sensor fault	[45]
Actuator and sensor faults	[46]−[51]

A. Homogenous MASs

Distributed fault detection for a network of second-order linear MASs was studied in [41], where a bank of unknown input observers (UIOs) were designed to detect the fault by regarding the fault as an unknown input. The faulty agent was removed from the network when it was detected by comparing the residual evaluation function with a threshold. The approach presented in [41] was feasible only if a single additive fault was present. Based on the analysis results in [41], distributed fault detection of a networked dynamical system with multiple faults was investigated in [46], where the minimum amount of information required by an agent to detect the faults was revealed. The distributed unknown input observer was also designed in [42] for a class of discrete-time high-order systems. The reduced-order unknown input observer was also applied to the high-order MASs as in [43]. It must be pointed out that the matching condition is a direct restriction of those observers, e.g., $rank(CE) = rank(E)$, where C is the output matrix, and E is the weighting matrix of the unknown disturbance.

In [47], distributed fault detection for general high-order linear MASs was discussed, where the relative output information was used to construct the observer. In [44], the interval observer was proposed for a class of discrete-time MASs such that the lower and upper bounds of state observation were obtained, see the following interval observer designed for the i-th agent:

$$\begin{cases} x_L^i(k+1) = \left(A - F_L^i W_i C\right)x_L^i(k) + F_L^i W_i y(k) \\ \qquad\qquad -H_L^i\left(x_U^i(k) - x_L^i(k)\right) + D^+ v_L(k) - D^- v_U(k) \\ x_U^i(k+1) = \left(A - F_U^i W_i C\right)x_L^i(k) + F_U^i W_i y(k) \\ \qquad\qquad -H_U^i\left(x_U^i(k) - x_L^i(k)\right) + D^+ v_U(k) - D^- v_L(k) \\ Y_L^i(k) = (W_iC)^+ x_L^i(k) - (W_iC)^- x_U^i(k) \\ Y_U^i(k) = (W_iC)^+ x_U^i(k) - (W_iC)^- x_L^i(k) \end{cases} \tag{9}$$

where $x_L^i(k)$ and $x_U^i(k)$ are the lower and upper estimation of the lumped state $x(k)$, respectively; $Y_L^i(k)$ and $Y_U^i(k)$ are the lower and upper estimation of $Y_i(k)$, respectively, with $Y_i(k) = W_i y(k)$, $v_L(k)$ and $v_U(k)$ are the lower and upper bounds on the unknown disturbance $v(k)$, respectively; and F_L^i, F_U^i, H_L^i, and H_U^i are the observer gains that were determined by some dilated LMIs. $(W_iC)^+ = \max\{0, W_iC\}$, $(W_iC)^- = (W_iC)^+ - W_iC$. The lower and upper residual signals were also constructed. Then a mixed l_1 and H_∞ performance index was proposed to compute the observer gains, which can maximize the robustness of the lower and upper residuals against disturbances and increase the sensitivity of the lower and upper residuals to faults simultaneously. The proposed design scheme directly compared the residual signal with the fault signal, which may simplify the detection process.

In [48], the fault detection problem for discrete-time linear MASs with sensor and actuator faults was considered. In order to cooperatively perform the fault detection task, a

cooperative detecting network was proposed as follows:

$$\begin{cases} x_i^j(k+1) = Ax_i^j(k) + B_1u_i(k) + B_2d_i^j(k) + B_3f_i(k) \\ y_i^j(k) = Cx_i^j(k) + D_1d_i^j(k) + D_2f_i(k) \end{cases} \tag{10}$$

where $x_i^j(k), y_i^j(k)$ are the reference state and output of the i-th agent obtained by agent j, respectively, and $d_i^j(k) = d_i(k) + d_j(k)$. Then, a set of distributed Luenberger observers were designed. With the consideration of designing a fault detection observer that is sensitive to faults while robust to disturbances, the mixed H_∞/H_2 optimization method was presented to obtain the optimal detector. Note that the unknown faults may be detected successfully in the above-mentioned work, but those faults cannot be located as they do not have such a mechanism. It is also worth pointing out that most of the above-mentioned results only focused on fault detection of MASs without consideration of consensus protocol design.

Very recently, the fault detection and consensus control protocol design problem was addressed simultaneously for a network of linear MASs in [49], and the fault detection filter and controller were given by

$$\begin{cases} \dot{\hat{x}}_i(t) = A\hat{x}_i(t) + B_1u_i(t) + Fr_i(t) \\ u_i(t) = K\hat{x}_i(t) \\ r_i(t) = \eta_i(t) - \hat{\eta}_i(t) \end{cases} \tag{11}$$

where $r_i(t)$ is the residual signal constructed for the fault detection purpose, K is the controller, and F is the filter gains to be determined. $\eta_i(t) = \sum_{j\in N_i}\left(y_i - y_j\right)$ and $\hat{\eta}_i(t) = \sum_{j\in N_i} C(\hat{x}_i - \hat{x}_j)$. Equation (11) is a common observer to detect the fault in control systems. With the help of neighboring measurement, it is able to detect the fault in MASs. In order to attenuate the disturbance effects on the residuals and the system outputs, and guarantee the sensitivity of the residuals to the faults, the mixed H_∞ and $H\_$ indices were introduced. With the multi-objective optimization technique, all agents can reach a state consensus and meanwhile collaboratively detect the occurrence of any additive fault. However, since the weights of different performance indices were selected by trial and error, it is hard to determine their appropriate values. Therefore, some better approaches should be developed. Further investigation on simultaneous fault detection and consensus control of MASs in the finite-time frequency domain case was reported in [50], where the impact of disturbances on the residual signals was attenuated by using the finite frequency H_∞ performance index.

B. Heterogeneous MASs

In [51], the fault detection problem for a class of general high-order linear MASs was investigated. Due to the heterogeneity of agent dynamics, it is impossible to adopt the above observer design methods. For the purpose of fault detection, the following virtual model for the i-th agent was introduced:

$$\begin{cases} \dot{x}_{Ni}(t) = \tilde{A}_ix_{Ni}(t) + \tilde{B}_{1i}u_{Ni}(t) + \tilde{B}_{2i}d_{Ni}(t) + \tilde{B}_{3i}f_{Ni}(t) \\ z_i(t) = \bar{C}_ix_{Ni}(t) + \bar{D}_{1i}d_{Ni}(t) + \bar{D}_{2i}f_{Ni}(t) \end{cases} \tag{12}$$

where $x_{Ni} = [x_i^T, x_{i_1}^T, \ldots, x_{i_{|N_i|}}^T]^T$, $d_{Ni} = [d_i^T, di_1{}^T, \ldots, d_{i_{|N_i|}}^T]^T$, $u_{Ni} = [u_i^T, ui_1{}^T, \ldots, u_{i_{|N_i|}}^T]^T$, $f_{Ni} = [f_i^T, fi_1{}^T, \cdots, f_{i_{|N_i|}}^T]^T$, $z_{ij} = y_i - y_j$, $z_i = [y_i^T, z_{i,i_1}^T, \ldots, z_{i,i_{|N_i|}}^T]^T$. Based on the virtual system (12), the following observer was proposed:

$$\begin{cases} \dot{\hat{x}}_i(t) = A_{Ci}\hat{x}_i(t) + B_{C_i}z_i(t) \\ z_i(t) = \bar{C}_i\hat{x}_i(t) \\ r_i(t) = H_i(z_i(t) - \hat{z}_i(t)) \end{cases} \tag{13}$$

where $\bar{C}_i = \begin{bmatrix} C_i & 0 & \cdots & 0 \\ C_i & -C_{i_1} & \cdots & 0 \\ C_i & 0 & \ddots & \vdots \\ C_i & 0 & \cdots & -C_{i_{|N_i|}} \end{bmatrix}$, and A_{Ci}, B_{Ci}, and H_i are the observer gains to be determined. An optimization problem was presented to design the optimal fault detection observer such that the impact of disturbance and control input on the residual is minimized, the impact of the fault on the residual is maximized and the sensitivity of the residual to the fault is maximized simultaneously. For the fault detection of heterogeneous MASs, a virtual system model is usually designed as the standard observer like (11) fails to work due to heterogeneous dynamics of MASs. In [45], the distributed sensor fault diagnosis was discussed for a network of heterogeneous MASs, where a two-level diagnosis method was proposed. In the first level, an observer was designed to generate the residual signal and then an adaptive threshold was introduced to help detect the occurrence of sensor fault. In the second level, a decision logic based sensor fault isolation technique was presented. The fault detection of heterogeneous MASs is a challenging task, and the common method is to establish a virtual model with all the information of its neighbors, but it would lead to computation issue when the agent number becomes large.

Note that most of the above works only address the fault diagnosis including fault estimation, detection, and isolation of physical faults in MASs, the design of control protocols is yet to be further investigated. In the following section, the issue of fault-tolerant control is discussed.

IV. Fault-Tolerant Control

The main role of fault-tolerant control is to trigger an adjustment control mechanism to deal with the faults when they are detected. Sometimes, the fault-tolerant controller is designed on the basis of the precise fault estimation information. Recent studies on this topic are summarized in this section. A detailed categorization of physical threats in the study of fault-tolerant control of MASs is given in Table III.

TABLE III
CATEGORIZATION OF PHYSICAL THREATS IN THE STUDY OF FAULT-TOLERANT CONTROL OF MASS

Fault types	Reference
Actuator fault	[52]–[66]
Sensor fault	[67]
Actuator and sensor faults	[68]

A. Homogeneous MASs

In [52], an adaptive fault-tolerant controller synthesis problem for linear and Lipschitz nonlinear MASs was studied. A fault-tolerant control protocol was designed based on real-time fault estimation and feedback gain update. For the agent modeled as $\dot{x}_i = Ax_i + B(I_m - \rho_i)u_i$, $i = 1, \ldots, N$, where ρ_i is the failure matrix of the actuator, and the controller was designed as follows:

$$u_i = \sum_{j\in N_i} a_{ij} K(\hat{\rho}_i)\left(x_i - x_j\right) + cg\left(\sum_{j\in N_i} -a_{ij} B^T P^{-1}\left(x_i - x_j\right)\right) \tag{14}$$

where $g(\lambda) = \begin{cases} (1 + 1/\|\lambda\|)\lambda, & \|\lambda\| \neq 0 \\ 0, & \|\lambda\| = 0. \end{cases}$ The controller gains depending on the real-time estimate of ρ_i are separated into three parts: $K(\hat{\rho}_i) = K_0 + K_a(\hat{\rho}_i) + K_b(\hat{\rho}_i)$, where K_0 is the normal gain, and $K_a(\hat{\rho}_i)$ and $K_b(\hat{\rho}_i)$ are two additional gains that were introduced to compensate for the effect of fault, and have the form $K_a(\hat{\rho}_i) = \sum_{h=1}^{m} K_{ah}\hat{\rho}_{ih}$ and $K_b(\hat{\rho}_i) = \sum_{h=1}^{m} K_{bh}\hat{\rho}_{ih}$, respectively. The fault estimation in the h-th actuator of the i-th agent was designed based on the following projection operator:

$$\dot{\hat{\rho}}_{ih} = \text{Porj}_{\left[\min\limits_l\{^l_{ih}\},\ \max\limits_l\{\bar{\rho}^l_{ih}\}\right]}\{T_{ih}\} = \begin{cases} 0, & \hat{\rho}_{ih} = \min\limits_l\{^l_{ih}\} \quad \text{and} \quad T_{ih} \leq 0 \\ & \text{or } \hat{\rho}_{ih} = \max\limits_l\{^l_{ih}\} \quad \text{and} \quad T_{ih} > 0 \\ T_{ih}, & \text{otherwise} \end{cases} \tag{15}$$

where

$$T_{ih} = -\theta_{ih}\left[\sum_{j\in N_i} a_{ij}\left(x_i - x_j\right)\right]^T \times \left[P^{-1}B^h K_b(\hat{\rho}_i) + P^{-1}B^h K_{ah}\right]\left[\sum_{j\in N_i} a_{ij}\left(x_i - x_j\right)\right].$$

By estimating the actuator fault on-line, the controller gain matrices $K(\hat{\rho}_i)$ are updated adaptively to compensate for the failure effect on the consensus performance of MASs.

In [53], the adaptive fault-tolerant control problem for a class of non-Lipschitz nonlinear MASs was addressed, where the actuator fault was assumed to be multiplicative, i.e., $u_i^F(t) = \theta_i u_i(t)$, with θ_i being the failure factor of the actuator. The control protocol consists of two parts: $u_i = u_{0i} + u_{ai}$, where u_{0i} is the normal control input and u_{ai} is the compensation term, which is related to the estimation of the fault factor. Finally, a robust adaptive control scheme [54] was adopted to on-line update the fault factor estimation $\hat{\theta}_i$ as in [53]. Note that most of the existing methods require the continuous communication among agents, which may lead to communication congestions. In fact, if the state of an agent does not change much, it may not be necessary to keep continuous transmission of information between neighbors.

In [54], adaptive event-triggered fault-tolerant control for linear MASs with multiplicative faults was investigated, where the fault model was the same as that in [52]. Different from the work in [69], the controller gain K in [54] is independent of the fault and it was designed to be $K = B^T P$, where P is the solution of the standard algebraic Riccati equation (ARE): $A^T P + PA - PBB^T P + Q = 0$. The main contribution is to introduce a new event-triggered mechanism with mixed state-dependent and time-dependent threshold to reduce the communication load, shown as follows:

$$t_{k+1}^i = \inf\left\{t > t_k^i : g_i\left(e_{\xi_i}(t), \xi_i(t_k^i)\right) > 0\right\} \tag{16}$$

where $g_i\left(e_{\xi_i}(t), \xi_i(t_k^i)\right)$ is a triggering function defined as $g_i\left(e_{\xi_i}(t), \xi_i(t_k^i)\right) = \delta_i e_{\xi_i}^T(t) PBB^T P e_{\xi_i}(t) - \alpha_1 \exp[-r(t - t_0)] - \hat{\theta}_i(t_k^i)\hat{c}_i(t_k^i)\xi_i^T(t_k^i) PBB^T P\xi_i(t_k^i)$, and $e_{\xi_i}(t) = \xi_i(t_k^i) - \xi_i(t)$, $\xi_i(t) = \sum_{j\in N_i} a_{ij}(x_i - x_j)$. δ_i is an adjustable scalar, $\alpha_1 \in (0, 1)$ and $0 < r \leq \|A\|$. An adaptive algorithm was also proposed to estimate the unknown fault factor θ_i that is involved in the event triggering function. Based on such an event-triggering mechanism, the communication burden can be alleviated. However, a major challenge lies in the determination of an optimal event-triggering mechanism, which is yet to be reported in literature.

Note that besides the multiplicative faults studied in the aforementioned works, the *bias* fault issue was also considered in literature. For example, the actuator's bias fault model was considered as $u_i^f = u_i + s(t - T_0)\varphi_i(t, y_i)$ in [55], where $s(t - T_0)$ is the time profile of the fault and $\varphi_i(t, y_i)$ is an bounded time-varying function characterizing the unknown fault. To compensate for the bias fault in the actuator, an additional control input $u_{ai} = -\hat{\rho}_{1i}\tanh\left(B^T F(y_i - o_i)/\varepsilon_2\right)$ was introduced, where $\hat{\rho}_{1i}$ is the estimation of the uncertainty induced by the bias fault signal, $\varepsilon_2 > 0$ is a scalar, and o_i is the average output consensus value.

Recently in [56], the distributed intermediate estimator proposed in [34] (see Section II) was adopted to design the fault-tolerant control protocol, where the general process fault, and sensor fault can be handled in a unified framework. The designed controller was dependent on the estimation of the state, fault and intermediate variable, and computation complexity can be reduced as it does not need the adaptive mechanism.

Some other topics such as output regulation, time-varying formation and containment were also studied in literature for the fault-tolerant control of MASs with various faults, see [57]–[59], [67] for more details. Different agent systems such as nonlinear affine dynamics [60], fuzzy dynamics [61], and descriptor dynamics [62] were also addressed. Other topics such as complex-weighted topology was also investigated in [63], but the main results can only be applied to double-integrator dynamics.

B. Heterogeneous MASs

In addition to those works on homogeneous MASs, fault-tolerant control of heterogeneous MASs also attracted tremendous attention recently. For example, robust adaptive fault-tolerant control for MASs with uncertain heterogeneous dynamics and actuator faults was studied in [64], where the

agent dynamics was modeled by a nonlinear double-integrator system. The control input was described by $u_{oi} = \rho_i u_i + \gamma_i(t)$, where ρ_i is a faulty factor with $0 \le \rho_i \le 1$, and $\gamma_i(t)$ is the uncertainty injected into the control input. Due to the fact that when a fault of partial loss of effectiveness occurs, the system became time-varying. Furthermore, the controller gain is unknown due to the existence of uncertain system dynamics. An adaptive fault-tolerant controller consisting of a normal controller and a compensation controller was proposed. The compensation controller was given as $u_{di} = \hat{c}_i \varphi_i^2 s_i/(\varphi_i |s_i| + \delta) - \hat{\varepsilon}_i s_i/(|s_i| + \delta)$, where $\hat{c}_i$ is determined by an adaptive mechanism, which together with $\hat{\varepsilon}_i$ are two estimates of virtual parameters of c_i and ε_i, respectively. s_i is the filtered consensus error signal, and $\delta > 0$ is a constant.

The distributed adaptive fault-tolerant control for a class of uncertain MASs with process and actuator faults was investigated in [65], where each agent was modeled by $\dot{x}_i = \phi_i(x_i) + u_i + \eta_i(x_i, t) + \alpha_i(t - T_{iu})\theta_i u_i + \alpha_i(t - T_{if}) f_i(x_i)$, with nonlinear smooth vectors $\phi_i(x_i), \eta_i(x_i, t)$, and $g_i(x_i)$, and $\alpha_i(t - T_{if}) f_i(x_i)$ denotes the dynamic changes induced by the fault. First of all, a neural network was introduced to estimate the unknown process fault function $\alpha_i f_i$, then it was fed into the control algorithm to compensate for the effect of the process fault. For the actuator fault factor θ_i, a projection operation method was proposed to adaptively update the estimate of θ_i in the control algorithm.

In [66], the distributed adaptive fault-tolerant control problem for heterogeneous MASs with actuator faults was investigated, where a distributed finite-time observer was first proposed to estimate the state of exosystem and then a fault-tolerant controller was designed to compensate for the influence of the matched system uncertainties and unknown actuator faults. In addition, the fault that affects the connection topology was also considered as in [70]. It was shown that the target point can also be achieved if the active agents are not influenced by the faulty agents. In [65], the link failure, sensor and actuator failure were simultaneously considered for formation control of discrete-time heterogeneous MASs, where a robust fault estimator was designed to compensate for the effects of the sensor and actuator faults without any adaptive mechanism, which may lead to some reduced computational burden.

According to those papers on fault tolerant control of MASs, a common strategy is to estimate the unknown fault and reconfigure the controller to compensate for the effect of unknown fault, and the adaptive control method seems to be dominant in this area. Another observation is that some studies focus on the event-triggering communication mechanism design together with the fault tolerant control design as in [54]. More effort is needed on optimal event-triggering function design that can not only reduce the communication load but also improve the control performance.

V. Cyber Attack Detection of MASs

We have made a comprehensive survey on physical fault estimation, detection, isolation, and fault-tolerant control of MASs in the previous sections. All those results deal with the physical threats in MASs. With recent development of information technology, the communication networks of MASs are exposed to the general public, with a great risk of being attacked by adversaries. In this article, we only focus on two typical attacks: the deny-of-service (DoS) attack and the Deception attack. A DoS attacker can exhaust the network or system resources of the target agent, causing the service of MASs to be temporarily interrupted, stopped, or crashed. On the other hand, wrong decision may be made when some false data are injected into sensors or actuators. In this case, the man-made fault could occur. The attack detection for networked systems has received increasing attention in past few years as in [71]–[73]. In this section, we focus our attention on the attack detection problem of MASs. A detailed categorization of cyber threats in the study of cyber attack detection of MASs is given in Table IV.

TABLE IV
Categorization of Cyber Threats in the Study of Cyber Attack Detection of MASs

Attack types	Reference
DoS attack	[73]
Deception attack	[71]–[76]
Reply attack	[77]

A. Homogeneous MASs

In [78], the DoS attack detection problem was considered for a network of vehicle systems, and an augmented system including the vehicle state (position, velocity) and controller state was proposed as follows:

$$\begin{cases} \dot{d}_i(t) = v_{i-1}(t) - v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = \dfrac{k_p}{l} d_i(t) - \left(k_p + \dfrac{k_d}{l}\right) v_i(t) - \left(k_p + \dfrac{1}{l}\right) a_i(t) \\ \qquad + \dfrac{k_p}{l} v_{i-1}(t) + \dfrac{1}{l}\left(a_i(t) - \dot{a}_{i-1}(t)\tau\right) \end{cases} \tag{17}$$

where $d_i(t)$ is the relative distance between vehicles, $v_i(t)$ is the velocity of the i-th vehicle, and $a_i(t)$ is the acceleration signal of the i-th vehicle. τ is the unknown delay introduced to describe the duration time that the communication network was occupied by an illegal user. In order to estimate τ, the following sliding mode observer was designed:

$$\begin{cases} \dot{\tilde{v}}_i(t) = H_1 \operatorname{sgn}(v_i(t) - \tilde{v}_i(t)) \\ \dot{\tilde{a}}_i(t) = \dfrac{k_p}{l} d_i(t) - \left(k_p + \dfrac{k_d}{l}\right) \tilde{v}_i(t) - \left(k_p + \dfrac{1}{l}\right) f(t) \\ \qquad + \dfrac{k_p}{l} v_{i-1}(t) + \dfrac{1}{l}\left(a_i(t) - \dot{a}_{i-1}(t)\tilde{\tau}\right) \\ \qquad + H_3\left(f(t) - \tilde{a}_i(t)\right) \\ \dot{\tilde{\tau}}(t) = -\dfrac{H_2}{l} \dot{a}_{i-1}(t)\left(f(t) - \tilde{a}_i(t)\right) \end{cases} \tag{18}$$

where $\tilde{v}_i(t)$ is the estimation of the relative velocity, and $\tilde{a}_i(t)$ is the estimation of the acceleration. $f(t)$ is the filtered signal of $H_1 \operatorname{sgn}(v_i(t) - \tilde{v}_i(t))$. $\tilde{\tau}(t)$ is the estimation of time delay τ induced by the DoS attack. $H_s, (s = 1, 2, 3)$ are observer gains

that are selected to satisfy $H_2, H_3 > 0$, and $H_1 > |a_i(t)| > 0$. However, the local observer was designed in a decentralized way, and thus has no interaction with its neighbors. This may lead to a poor estimation performance.

The Deception attack detection problem for a linear consensus network consisting of first-order agent dynamics was studied in [74], where an unknown input signal was injected into the system:

$$x(k+1) = \mathcal{A}x(k) + d(k) \tag{19}$$

where $\mathcal{A}$ is the consensus matrix and the (i, j) entry of $\mathcal{A}$ is nonzero if the i-th agent and the j-th agent are neighbors. $d(k)$ is the unknown signal injected into the system, of which u_i is nonzero if the i-th agent is attacked, and $u_i = 0$, otherwise. It was shown that the network connectivity should be at least $2k+1$ if there are k malicious agents. Furthermore, the misbehaving agents $K_1 \in \mathcal{K}$ can be detected from the j-th agent if and only if the consensus system $(\mathcal{A}, [\ B_{K_1}\ \ B_{K_2}\ ], C_j)$ has no zero dynamics from every $K_2 \in \mathcal{K}$, where $B_{K_s} = [e_{i_1}\ e_{i_1}\ \cdots]$, $s = 1, 2$ with e_i being the i-th vector of the canonical basis. C_j denotes the output matrix of the j-th agent. The major drawback is that the global model information is required to perform monitoring and detection.

Some other attack detection problems such as the Replay attack can also be found in [77], which will not be discussed in detail as it is beyond the scope of this paper.

B. Heterogeneous MASs

The distributed attack detection problem for a class of heterogeneous MASs was studied in [79], where the agent dynamics were modeled as follows:

$$\begin{cases} x_i(k+1) = A_{ii}x_i(k) + \displaystyle\sum_{j\in N_i} A_{ij}x_j(k) + B_i u_i(k) \\ \qquad\qquad + M_i d_i(k) + G_i v_i(k) + \varpi_i(k) \\ y_i(k) = x_i(k) + \rho_i(k) \end{cases} \tag{20}$$

where $d_i(k)$ is a known exogenous signal, u_i is the primary control, v_i is the secondary control, $\varpi_i(k)$ and $\rho_i(k)$ are unknown disturbances. The measurement data received by the i-th agent was assumed to be affected by the false data injection attack. The following distributed attack detector was proposed:

$$\begin{cases} \tilde{x}_i(k+1) = A_{ii}\tilde{x}_i(k) + \displaystyle\sum_{j\in N_i} A_{ij}\bar{y}_j(k) + B_i u_i(k) \\ \qquad\qquad + M_i d_i(k) + G_i v_i(k) + L_i[y_i(k) - \tilde{y}_i(k)] \\ \tilde{y}_i(k) = \tilde{x}_i(k) \end{cases} \tag{21}$$

where $\bar{y}_j(k) = y_j(k) + \beta_j(t - T_{a_j})\vartheta_j(t)$ is contaminated by adversaries, which is similar to the model description of the fault in [54]. The detector gain L_i was simply selected such that $A_{ii} - L_i$ is Schur stable. The threshold-based distributed fault detection scheme proposed in [75] was adopted to deal with the attacks on communication channel. It was shown that the attack is detectable if the condition that $\exists \tau > T_a : \left| \sum_{k=0}^{\tau-1} \left(A_{L_i}\right)^{\tau-1-k} A_{i\hat{j}}\vartheta_{[\hat{j}]}(k) \right| > 2\bar{\gamma}_{[i]}(\tau)$ is satisified, where $\vartheta_{[\hat{j}]}(k)$ is the attack signal, $A_{L_i} = A_{ii} - L_i$ is Schur stable, and $\bar{\gamma}_{[i]}(\tau)$ is the threshold. However, it is worth mentioning that the attack may not be detected when the attack function satisfies $\vartheta_j(t) = [0\ r_j(t)\ \theta_j(t)]^T$, where $r_j(t)$ and $\theta_j(t)$ are any arbitrary functions. Later in [76], some improvement on the detector design was made to remove the limitation in [73], where a distributed UIO-based observer was designed to estimate the state and detect the attack. The main results were verified on the secondary control of direct current (DC) microgrids. The limitation is that some additional requirement must be met; see the discussions in the UIO-based fault detection in Section III. It is worth noting that the Deception attack was usually modeled as an additive fault in physical systems, see, e.g., [79]. In this case, the fault estimation, detection and diagnosis results presented in Section II and Section III can be applied. But in reality, the adversary may launch Stealthy attack that may not be detected so easily. Thus, the Deception attack cannot be simply modeled as the fault, instead sophisticated detectors may need to be designed to deal with those attacks.

VI. Secure Consensus of MASs

The secure consensus control problem of MASs has been investigated in parallel with the attack detection problem in previous years. The salient results are collected and presented in this section. A detailed categorization of cyber threats in the study of secure consensus of MASs is given in Table V.

TABLE V
A Concrete Categorization of Cyber Threats in the Study of Secure Consensus of MASs

Attack types	Reference
DoS attack	[80]−[93]
Deception attack	[94]−[102]

A. Homogeneous MASs

The synchronization control problem for a network of dynamical systems with recoverable attacks was considered in [80], where the adversary can break the communication topology completely and the network can recover from this attack after a period of time when the attack disappears. A switched system modeling method consisting of $W+1$ subsystems (one normal system plus W abnormal systems) was introduced to capture the topology switching behavior of MASs during the recoverable attacks. The energy function in the normal time interval $[t_{2k}, t_{2k+1})$, $k = 0, 1, \ldots$ is shown to be decreasing as the synchronization can be guaranteed in the absence of the attacks. On the other hand, the energy function in the abnormal time interval $[t_{2k+1}, t_{2(k+1)})$ could be increasing as the synchronization error may increase when the adversary attacks the communication topology successfully. Based on the average dwell time switching scheme, it was shown that synchronization can still be guaranteed if the attack frequency and duration are bounded. A similar analysis result can also be found in [81], where the exception is that the Itô stochastic linear dynamics were studied. Recently, the distributed consensus of linear MASs with a general DoS attack was addressed in [82], where only a portion of channels were jammed and the switched system modeling method was

also adopted. The number of overall switched systems may become very large and the computational complexity for analyzing the decay rates of the closed-loop system under different attack cases is difficult. An effective computation reduction scheme was proposed by using a uniform decay rate to replace the time-varying decay rate parameter such that a more computationally efficient controller design condition was obtained. A different framework of the Stackelberg game and the predictive control scheme was proposed in [83], and the designed predictive control scheme was able to compensate for network-induced delays and the attack-induced packet dropouts effectively by utilizing more predicted data.

Later in [84], sampled-data consensus of Lipschitz nonlinear MASs with DoS attack was investigated, where the adversary only jammed a few channels to break the connectivity such that there does not exist a directed spanning tree. A preliminary condition for the choice of the sampling interval was given as $h < \alpha/(\alpha' + v_1 + v_2)$, where α is any given scalar, $\alpha' = c\left\|\bar{L}_0\right\| \|I_{N-1} \otimes A\| + c\left\|\bar{L}_0\right\| + c^2\left\|\bar{L}_0\right\|^2$, $v_1 = c\left\|\bar{L}_0\right\| \|I_{N-1} \otimes A\| + l^2\lambda_{\max}(P_0)/\lambda_{\min}(P_0)$, and $v_2 = c^2\left\|\bar{L}_0\right\|^2$. c is the coupling strength, $\bar{L}_0$ is the modified Laplacian matrix, and l is the nonlinear bounding factor. It is noted that the sampling process is time-triggered in [84], which may waste much communication resource. The distributed event-triggered consensus of MASs with periodic DoS attack was discussed in [85], where an indicator was introduced to model the activity of the attack, i.e.,

$$a(t) = \begin{cases} 1, \text{ OFF}, & t \in [nT, nT + T_{off}^n) \\ 0, \text{ ON}, & t \in [nT + T_{off}^n, (n+1)T) \end{cases} \tag{22}$$

where T and T_{off} are the attack cycle and the length of the n-th sleep interval, respectively. By describing the MASs subject to DoS attack as a switched system as usual, and using the input time delay approach to transform the sampled-data to a time-delay term, a time-delay switched system was introduced to model the MASs with event-triggered communication mechanism and periodic DoS attack. A co-design algorithm was presented to determine the optimal event-triggered mechanism and controller gains simultaneously. However, the attack is only allowed to be periodic and the attack cycle T and the length of n-th sleep interval T_{off}^n are required to be known a prior. Very recently, distributed event-triggered secure consensus of MASs with a general DoS attack was studied in [86], where an input-based event-triggering mechanism was introduced to avoid the continuous monitoring for each agent. A link-based state estimator was first proposed to estimate the relative control input, which was transmitted under a certain event. It was proved that the consensus can be guaranteed if the attack frequency is upper bounded. Some more recent works on the secure event-based consensus of MASs with DoS attacks can also be found in [87] and [88], where co-design of the event-triggered communication mechanism and secure control protocol were addressed therein. However the attack in [87] is supposed to be periodic, which may be restrictive in reality. The aperiodic attack is studied, but the threshold of event-triggering mechanism is constant, and it may not be adequate to deal with more sophisticated attacks. Therefore, the design of effective communication mechanism to deal with the DoS attack has become a new research topic. In [89], a new stochastic communication protocol was proposed, where each agent attempts to communicate with its neighbors at any random time instant. Thus, these time instants will be unknown to the adversary. In this case, the adversary will not be able to jam the communication channels by turning on the jamming attack very timely at those instants. Then, a finite-time control approach was developed. Nevertheless, the main results were obtained for single integrator agent dynamics.

Some other researchers studied the DoS effect on MASs from the Markovian jumping system point of view. For example, the secure consensus of linear MASs with random attack was studied in [90], where the attack was driven by a Markov process. A state feedback secure consensus protocol consisting of two controllers was proposed for different time intervals, where one controller was designed for the MAS subject to attacks and the other one was designed for the normal MAS without attacks, i.e.,

$$u_i = \begin{cases} \alpha K\left[\sum_{j\in N_i} a_{ij}^0\left(x_j - x_i\right) + b_i^0\left(x_0 - x_i\right)\right] \\ \qquad t \in [t_{2k}, t_{2k+1}) \\ \beta H\left[\sum_{j\in N_i} a_{ij}^{\lambda(t)}\left(x_j - x_i\right) + b_i^{\lambda(t)}\left(x_0 - x_i\right)\right] \\ \qquad t \in [t_{2k+1}, t_{2(k+1)}) \end{cases} \tag{23}$$

where $\lambda(t)$ is a switching signal obeying the Markov transition process. α and β are the coupling strengths for the MASs without attack and with attack, respectively. K and H are the two controller gains that were determined based on the solution of an algebraic Riccati equation and an algebraic Riccati inequality, respectively, i.e., $K = R^{-1}B^T P$ and $H = T^{-1}B^T S$ with

$$\begin{cases} PA + A^T P - PB^{-1}B^T P + Q = 0 \\ SA + A^T S - SBT^{-1}BS - \delta S < 0 \end{cases}$$

where $\delta > 0$ is any given scalar, and P, R, S, and T are positive definite matrices.

The similar analysis method was later extended to the observer-based control protocol in [91]. However, the attack distribution information must be known a prior for consensus protocol design, which may not be an easy task due to the fact that the adversaries would try to hide their attack strategies. On the other hand, the adversaries may inject some false data into the packet to mislead the agent as the price of launching the DoS attack may be very high. Now, we pay our attention to the case of Deception attack. The recent advances are summarized in the following.

The secure consensus of MASs with Deception attack was investigated in [94], where the received data by the i-th agent was modeled as $\tilde{y}_i(k) = \sum_{j\in N_i} a_{ij}y_{ij}(k) + \beta_i(k)(\delta_i(k) - \sum_{j\in N_i} a_{ij}y_{ij}(k))$, where $y_{ij}(k)$ is the relative output measurement, $\beta_i(k) \in \{0, 1\}$ is a binary stochastic variable indicating whether the attack

occurs or not, and $\|\delta_i(k)\|^2 \le \delta_i$ is the data injected by the adversary. Due to the fact that the data was not eliminated in the consensus protocol, the consensus error can only be guaranteed to be bounded rather than decaying to zero. The similar modeling method was also adopted in [95], where the distributed impulsive control protocol was designed. Different from these two works, the Deception attack signal was modeled as a locally state-dependent nonlinear function $g_i(x_i(t_k))$ in [96], and it was assumed to satisfy the Lipschitz condition $\|g_i(a)-g_i(b)\| \le \theta_i^2\|a-b\|$. Thus the consensus error system was shown to be mean-square asymptotically stable provided that some matrix inequalities are satisfied.

Note that most of the above works did not eliminate the effects of Deception attacks, which can only lead to the bounded consensus error. Very recently, an adaptive filter was proposed to compensate for the Deception attack effect in [97], and the filter was given by

$$\begin{cases} \dot{\psi}_i(t) = E\psi_i(t) + \hat{g}_i(t) \\ \dot{\hat{g}}_i(t) = -\hat{g}_i(t) + g_{q,i}^a(t) + v_{a,i}(t) \end{cases}$$

where $\psi_i(t)$ and $\hat{g}_i(t)$ are the states of the observer and filter, respectively. $g_{q,i}^a(t)$ is the relative observation, and $v_{a,i}(t) = \sum_{j\in N_i} a_{ij} v_{a,ij}(t)$ is the compensation term, which was designed as follows:

$$v_{a,ij}(t) = -\frac{F_i^T \hat{g}_i(t)\hat{\delta}_{a,ij}^2(t)}{\left\|F_i^T \hat{g}_i(t)\right\|\hat{\delta}_{a,ij}(t) + \vartheta_{ij}(t)}$$

where $\dot{\hat{\delta}}_{a,ij}(t) = -\lambda\sigma_{ij}(t)\hat{\delta}_{a,ij}(t) + \lambda\left\|F_i^T\hat{g}_i(t)\right\|$, $\sigma_{ij}(t)$ is a bounded signal. $\hat{\delta}_{a,ij}(t)$ is the estimate of the Deception attack signal. Based on the above elimination mechanism, the consensus error can decay to zero asymptotically.

In [98], the content modification attack (a form of Deception attack) was investigated for consensus of MASs with double-integrator dynamics, where the received information by the j-th agent was described by

$$\begin{cases} \tilde{p}_i = p_i + \bar{p}_{ij},\ \bar{p}_{ij} = K_{ij}^p\left[(O_a p)^T,\ (O_a \dot{p})^T\right]^T \\ \tilde{\dot{p}}_i = \dot{p}_i + \bar{\dot{p}}_{ij},\ \bar{\dot{p}}_{ij} = K_{ij}^v\left[(O_a p)^T,\ (O_a \dot{p})^T\right]^T \end{cases} \tag{24}$$

where p_i is the position of the i-th agent, and K_{ij}^p and K_{ij}^v are the two positive attack gains. $O_a = \mathrm{diag}\{\bar{A}1_n\}$ is the attack operator, where $\bar{A}$ is the adjacency matrix of the compromised agents. It was shown that the attack can be detected if $\tilde{\dot{p}}_i(t) \ne \dot{\tilde{p}}_i(t)$ is satisfied by the fact that the received velocities and positions would not be coherent when agents are attacked. Once the attack is detected, the agent would transmit $(p_i, 0)$ instead of $(p_i, \dot{p}_i)$, and the following observer-based controller would be triggered:

$$\begin{cases} u_i = -\sum_{j\in N_i}\left(p_i - p_j\right) - \rho\dot{\tilde{z}}_i \\ \dot{\tilde{z}}_i = -\tau\tilde{z}_i + \sum_{j\in N_i}\left(p_i - p_j\right) \end{cases} \tag{25}$$

where ρ and τ are positive scalars. Based on the above mitigation method, the consensus of MASs with double-integrator dynamics can be achieved.

In [99], the resilient consensus problem was considered for a class of general linear MASs with Deception attack, where the attack signal $w_i(t)$ was injected to affect the local state dynamics. It was revealed that the intact agents (those agents which are not subject to attacks) affected by the i-th agent can not follow the leader when the attack on the i-th agent is generated by $\dot{w}_i(t) = Tw_i(t)$, where the eigenvalues of T are the subset of the eigenvalues of the state matrix A. In order to prevent the agent from the attack, a trust-confidence-based consensus protocol was proposed from the H_∞ control point of view. Then, the nonhomogeneous game algebraic Riccati equations were derived to solve the H_∞ optimal consensus problem. The off-policy reinforcement learning method was also introduced when the agent dynamics are not completely known a prior.

In [100], the Kullback-Liebler (KL) divergence based criterion was proposed to detect the misbehaving agents, where the attacks on the actuator and sensor of the i-th agent were respectively modeled as $u_i^c = u_i + \beta_i u_i^d$ and $x_i^c = x_i + \alpha_i x_i^d$, where u_i^d and x_i^d are the disrupted signal injected into the actuator and sensor, respectively. By defining the following two error sequences λ_i and τ_i based on the local information exchange for the i-th agent:

$$\begin{cases} \lambda_i = \left\|\sum_{j\in N_i} a_{ij}\left(x_j^c - x_i^c + \varpi_{ij}\right)\right\| \\ \tau_i = \sum_{j\in N_i}\left\|a_{ij}\left(x_j^c - x_i^c + \varpi_{ij}\right)\right\| \end{cases} \tag{26}$$

where ϖ_{ij} denotes the Gaussian-type communication noise. The attack can be detected easily by the KL-divergence method because τ_i would go to zero for intact agents despite the attack. However, λ_i would not converge to zero in the presence of an attack; instead its statistical distribution depends on the statistical information of the communication noise and the attack signal. If the attack is detected in one agent, it would reduce its trustworthiness level about its own data and informs its neighbors about the confidence of its communicated information. The agent only accepts information from its neighbors with high level of confidence. Based on the above mitigation mechanism and adopting trust and self-belief values, the consensus error can be guaranteed to converge to zero asymptotically.

In [101], an adaptive control strategy was introduced for the resilient (secure) consensus of discrete-time linear MASs with actuator and sensor attacks, where the attack models were the same as the ones in [100]. The designed controller was described as $u_i(k) = u_{1i}(k) + u_{2i}(k)$, where $u_{1i}(k) = cK(1+h_i)^{-1} \times \sum_{j\in N_i} a_{ij}\left(x_j(k) - x_i(k)\right)$ is the normal control input. c is the coupling strength, h_i is the entry of in-degree matrix of the network. The controller gain $K = R^{-1}B^T PA$, where R is a positive definite matrix to be designed, and P is a solution of $A^T PA - A - A^T PB(R + B^T PB)^{-1}B^T PA = Q$. $u_{2i}(k) = cK\bar{\varepsilon}_i(k) - d_i(k)$ is the compensation term, with $d_i(k+1) = \theta cK(\hat{\varepsilon}_i(k) - \bar{\varepsilon}_i(k)) + \theta d_i(k)$, where $\bar{\varepsilon}_i(k) = (1+h_i)^{-1}\sum_{j\in N_i} a_{ij}\left(x_j^c(k) - x_i^c(k)\right)$, $\hat{\varepsilon}_i(k) = (1+h_i)^{-1}\sum_{j\in N_i} a_{ij}\left(\hat{x}_j(k) - \hat{x}_i(k)\right)$ with $\hat{x}_i(k+1) = A\hat{x}_i(k) + cBK(1+h_i)^{-1}\sum_{j\in N_i} a_{ij}\left(\hat{x}_j(k) - \hat{x}_i(k)\right)$. $x_i^c(k)$ is the contami-

nated data, where $x_i^c(k) = x_i(k) + \alpha_i x_i^a(k)$, with $\alpha_i \in \{0,1\}$ and unknown $x_i^a(k)$. $\theta > 0$ is a designed parameter. It was proved that the consensus error bound can be made arbitrarily small by appropriate selection of θ with a cost of high-gain input. Most of the existing studies focus on the linear agent systems. Recently in [102], the secure bipartite consensus control problem of a class of nonlinear MASs with sensor attacks was addressed, where a neural network was adopted to approximate the unknown nonlinear functions, and a secure measurement preselector was designed to filter out the attacked sensor signals. Nevertheless, the nonlinear functions need to satisfy the bounded condition.

B. Heterogeneous MASs

The secure output consensus of heterogeneous MASs with aperiodic sampling and DoS attack was studied in our earlier work [92], where the input-hold mechanism was adopted when DoS attack occurs. In our work [102], both of the communication channels of agent-satellite and agent-agent were broken when attack occurs. By introducing a piece-wise signal to describe the nonuniform sampling phenomenon, a stochastic variable to characterize the occurrence of the attack and the time-delay term to model the attack duration, a stochastic switched-time delay system was derived that is capable of modeling the MASs subject to nonuniform sampling and random DoS attack. With the help of Lyapunov stability theory, some sufficient conditions were proposed such that the output consensus error system was guaranteed to be exponentially stable in the mean-square sense and achieved a prescribed H_∞ performance level. Some matrix manipulation techniques were also introduced to derive the controller gain matrices. Note that the secure control protocol design was based on the precise attack probability, which is a limitation in reality. Recently, a new switched system approach was proposed for the secure consensus of heterogeneous MASs with DoS attack in [93], where a piece-wise switching signal indicating different attack duration was proposed to characterize the attack strategy variation, i.e., the local position signal can be modeled as

$$\tilde{y}_i(k) = \begin{cases} y_i(k), & d(k) = 0 \\ y_i(k-1), & d(k) = 1 \\ \vdots & \\ y_i(k-N), & d(k) = N \end{cases} \tag{27}$$

where $d(k) \in \{0, 1, 2, \ldots, N\}$ is a switching signal indicating the different attack durations. The similar modeling method was also adopted for the communication interaction of agent i and its neighbors. In this case, the attack probability is not involved in the system modeling and analysis. A major limitation is that the adversary could jam all the communication channels, while in reality the adversary may only have the ability to jam a few channels as the system size is usually large.

Recently, the Markovian jumping system approach was proposed to model the partially unknown and uncertain attack in secure consensus of heterogenous MASs in [103], where the agents are communicating with each other periodically when there is no attack. A nonuniform sampled-data system was introduced when the attack occurs, the attack duration and probability are transformed into the number of sampling periods and transition probability of Markovian jumping system, respectively by assuming that the attack strategy follows a Markov chain as in [90].

As for the Deception attacks, the research on secure consensus of heterogeneous MASs is yet to be reported. Compared with the results on secure consensus of homogeneous systems, the regulator equation [104] is usually necessary to derive the consensus protocols, see, e.g., [92], [93], [103].

VII. Conclusions and Future Work

We have presented an overview of recent advances on the physical safety and cyber security issues of MASs in this paper. In particular, we have presented the results on physical fault estimation, detection and diagnosis, fault-tolerant control, cyber attack detection, and secure control under two typical kinds of attacks: the DoS attack and the Deception attack. Although many significant results have been reported on the security issue of MASs from various perspectives, the increasing complex security situation and higher security demand have brought many new challenges to the protection of MASs. Some potential research directions are recommended as follows.

A. Consensus With Sophisticated Attacks

In most of existing works, usually only one attack phenomenon is studied, i.e., the DoS attack and the Deception attack were usually investigated separately. A sole attack behavior may be easier to be detected and eliminated by a well designed detection system. In order to avoid being detected, the adversary would try to launch more sophisticated attacks such as a combination of the DoS attacks, Deception attacks, Replay attacks [105], Stealth attack [106] etc. In this scenario, how can we design the secure consensus protocol? The main challenge is that it is usually hard to precisely capture the dynamic behavior of adversaries precisely. Furthermore, with the rapid development of artificial intelligence, some well designed attacks may have the learning ability to evolve and mutate to avoid being detected [107]. Modeling of such a sophisticated attack is a difficult task [108]. This may be one of the potential reasons that very few works on secure consensus of heterogeneous MASs with Deception attack have been reported, not to mention a more sophisticated attack. A possible method to deal with those sophisticated attacks is from the game-theory perspective, which has been shown to be effective in dealing with the attacks in smart grids [109], [110]. Note that it is possible to design a perfect defense system only when the attacker's dynamic behavior can be predicted and modeled accurately. Thus, the security analysis of MASs subject to more sophisticated attacks deserves further research attention as it is the first stage to deal with attacks.

B. Consensus With Physical and Cyber Securities

A successful working MAS relies on healthy components

and a secure communication environment. However, most of current attention has only focused on the physical safety or cyber security individually, instead of both simultaneously. With the development of network and communication technologies, the boundaries between the physical world and the cyber world have been blurred. Furthermore, the adversaries may exploit security vulnerabilities to gain control over some of the sensors and actuators, MASs may crash quickly when they are subject to physical and cyber threats at the same time [111]. Therefore, a collaborative defense strategy must be established from both the physical and cyber levels to better protect MASs, which could be a second potential research direction. However, it is a challenging task, because we have not fully understood the physical world, let alone the cyber world. A possible method to deal with unknown physical and cyber securities is to use the current advanced artificial intelligence technology by collecting the large amount of running data; see the recent survey papers [112], [113].

C. Finite-Time Attack Detection and Secure Consensus

The MASs are safety-critical systems that should be designed with time-efficient attack detection and defense. In other words, malicious attack signals should be detected in a timely manner. However, most of current researchers only focused on whether malicious attack signals can be detected or not, with very little attention being paid on how fast malicious signals can be detected. The survey paper [9] has presented a few interesting results on finite-time consensus of MASs, which may be helpful to provide a new insight for development of time-efficient defense approaches for MASs with desirable detection speed and performance. To the best of our knowledge, such a kind of finite-time malicious signal detection and secure consensus is still not solved yet, which could be a good research direction in this area.

D. Real Testbed Design and System-Level Application

In most existing works, only theoretical results are reported with some simulations. For example, a simulation study was performed for the protection of power system in [114]. These results are still far away from real applications. Designing a real testbed to verify the effectiveness of existing theoretical results is an urgent task as this is the first step in developing practical techniques to protect actual systems. Note that some testbeds have been designed for industrial cyber-physical systems, see the water distribution testbed [115], power generation station testbed [116], the teleoperation system [96], etc. But, the development of the system testbeds is still very limited and the focus is only paid on detecting the attack without designing any defense mechanism. It should also be a challenge when the physical threats and cyber threats are simultaneously considered in the design of testbeds and defense strategies, which could be a fourth potential research direction.

REFERENCES

[1] Y. Y. Tan, M. C. Zhou, Y. Y. Wang, X. W. Guo, and L. Qi, "A hybrid MIP-CP approach to multistage scheduling problem in continuous casting and hot-rolling processes," *IEEE Trans. Autom. Sci. Eng.*, vol. 16, no. 4, pp. 1860–1869, Oct. 2019.

[2] L. Huang, M. C. Zhou, K. R. Hao, and E. Hou, "A survey of multi-robot regular and adversarial patrolling," *IEEE/CAA J. Autom. Sinica*, vol. 6, no. 4, pp. 894–903, Jul. 2019.

[3] Y. Duan, W. F. Li, X. W. Fu, Y. Luo, and L. Yang, "A methodology for reliability of WSN based on software defined network in adaptive industrial environment," *IEEE/CAA J. Autom. Sinica*, vol. 5, no. 1, pp. 74–82, Jan. 2018.

[4] T. Wang, M. Hu, and Y. L. Zhao, "Consensus control with a constant gain for discrete-time binary-valued multi-agent systems based on a projected empirical measure method," *IEEE/CAA J. Autom. Sinica*, vol. 6, no. 4, pp. 1052–1059, Jul. 2019.

[5] M. J. Morshed, " A nonlinear coordinated approach to enhance the transient stability of wind energy-based power systems," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 4, pp. 1087–1097, Jul. 2020.

[6] S. B. Li, Y. Zheng, K. Q. Li, Y. J. Wu, J. K. Hedrick, F. Gao, and H. W. Zhang, "Dynamical modeling and distributed control of connected and automated vehicles: Challenges and opportunities," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 3, pp. 46–58, Jul. 2017.

[7] L. Ding, Q. L. Han, X. H. Ge, and X. M. Zhang, " An overview of recent advances in event-triggered consensus of multiagent systems," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1110–1123, Apr. 2018.

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

[9] Z. Y. Zuo, Q. L. Han, B. D. Ning, X. H. Ge, and X. M. Zhang, "An overview of recent advances in fixed-time cooperative control of multiagent systems," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2322–2334, Jun. 2018.

[10] A. Dorri, S. S. Kanhere, and R. Jurdak, " Multi-agent systems: A survey," *IEEE Access*, vol. 6, pp. 28573–28593, Apr. 2018.

[11] P. Stone and M. Veloso, " Multiagent systems: A survey from a machine learning perspective," *Auton. Robots*, vol. 8, no. 3, pp. 345–383, Jun. 2000.

[12] L. Chen and C. Englund, " Cooperative intersection management: A survey," *IEEE Trans. Intell. Transp. Syst.* , vol. 17, no. 2, pp. 570–586, Feb. 2016.

[13] A. Trivedi, D. Srinivasan, K. Sanyal, and A. Ghosh, " A survey of multiobjective evolutionary algorithms based on decomposition," *IEEE Trans. Evol. Comput.*, vol. 21, no. 3, pp. 440–462, Jun. 2017.

[14] S. V. Albrecht and P. Stone, " Autonomous agents modelling other agents: A comprehensive survey and open problems," *Artif. Intell.*, vol. 258, pp. 66–95, May 2018.

[15] Q. Sun, K. W. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Inform.*, vol. 16, no. 7, pp. 4920–427, Jul. 2020.

[16] D. Zhang, W. A. Zhang, L. Yu, and Q. G. Wang, "Distributed fault detection for a class of large-scale systems with multiple incomplete measurements," *J. Franklin Inst.* , vol. 352, no. 9, pp. 3730–3749, Sep. 2015.

[17] W. K. V. Chan and C. L. Philip Chen, " Consensus control with failure—wait or abandon?" *IEEE Trans. Cybern.* , vol. 46, no. 1, pp. 75–84, Jan. 2016.

[18] Y. Jung, M. Kim, A. Masoumzadeh, and J. B. D. Joshi, "A survey of security issue in multi-agent systems," *Artif. Intell. Rev.*, vol. 37, no. 3, pp. 239–260, Mar. 2012.

[19] H. Yang, Q. L. Han, X. H. Ge, L. Ding, Y. G. Xu, B. Jiang, and D. H. Zhou, " Fault-tolerant cooperative control of multiagent systems: A survey of trends and methodologies," *IEEE Trans. Ind. Inform.*, vol. 16, no. 1, pp. 4–17, Jan. 2020.

[20] E. Semsar-Kazerooni and K. Khorasani, " Team consensus for a network of unmanned vehicles in presence of actuator faults," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 5, pp. 1155–1161, Sep. 2010.

[21] S. J. Qin, " Survey on data-driven industrial process monitoring and diagnosis," *Annu. Rev. Control*, vol. 36, no. 2, pp. 220–234, Dec. 2012.

[22] Z. Q. Ge, "Review on data-driven modeling and monitoring for plant-wide industrial processes," *Chemom. Intell. Lab. Syst.* , vol. 171, pp. 16–25, Dec. 2017.

[23] Y. C. Jiang, S. Yin, and O. Kaynak, "Data-driven monitoring and safety control of industrial cyber-physical systems: Basics and beyond," *IEEE Access*, vol. 6, pp. 47374–47384, Aug. 2018.

[24] P. P. Menon and C. Edwards, "Robust fault estimation using relative information in linear multi-agent networks," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 477–482, Feb. 2014.

[25] C. Mellucci, P. P. Menon, C. Edwards, and A. Ferrara, "Second-order sliding mode observers for fault reconstruction in power networks," *IET Control Theory Appl.*, vol. 11, no. 16, pp. 2772–2782, Nov. 2017.

[26] K. Zhang, B. Jiang, and P. Shi, " Adjustable parameter-based distributed fault estimation observer design for multiagent systems with directed graphs," *IEEE Trans. Cybern.*, vol. 47, no. 2, pp. 306–314, Feb. 2017.

[27] K. Zhang, B. Jiang, and V. Cocquempot, "Distributed fault estimation observer design for multi-agent systems with switching topologies," *IET Control*, *Theory Appl.*, vol. 11, no. 16, pp. 2801–2807, Nov. 2017.

[28] J. P. Xia, B. Jiang, and K. Zhang, "Dissipativity-based robust reduced-order fault estimation observer design of multi-agent systems," *Int. J. Control Autom. Syst.*, vol. 15, no. 6, pp. 2619–2627, Dec. 2017.

[29] J. L. Chen, H. J. Chu, Q. Fan, and Y. Y. Cao, " Fault estimation observer design for a class of nonlinear multiagent systems in finite-frequency domain," *Int. J. Robust Nonlinear Control* , vol. 29, no. 10, pp. 2777–2798, Jul. 2019.

[30] W. X. Han, Z. H. Wang, Y. Shen, and W. B. Xie, " Robust fault estimation in the finite-frequency domain for multi-agent systems," *Trans Inst Meas Control*, vol. 41, no. 11, pp. 3191–3181, Jul. 2019.

[31] J. W. Zhu and G. H. Yang, "Robust distributed fault estimation for a network of dynamical systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 14–22, Mar. 2018.

[32] X. H. Liu, X. W. Gao, and J. Han, "Distributed fault estimation for a class of nonlinear multiagent systems," *IEEE Trans. Syst.*, *Man*, *Cybern.*: *Syst.*, vol. 50, no. 9, pp. 3382–3390, Sep. 2020.

[33] K. Hashimoto, M. S. Chong, and D. V. Dimarogonas, "Distributed ℓ_1-state-and-fault estimation for multiagent systems" *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 2, pp. 699–710, Jun. 2020.

[34] M. Gao, S. Yang, and L. Sheng, "Distributed fault estimation for time-varying multi-agent systems with sensor faults and partially decoupled disturbances," *IEEE Access*, vol. 7, pp. 147905–147913, Oct. 2019.

[35] K. Zhang, G. S. Liu, and B. Jiang, "Robust unknown input observer-based fault estimation of leader-follower linear multi-agent systems," *Circuits*, *Syst.*, *Signal Process.*, vol. 36, no. 2, pp. 525–542, Feb. 2017.

[36] H. J. Ma and L. X. Xu, " Cooperative fault diagnosis for uncertain nonlinear multiagent systems based on adaptive distributed fuzzy estimators," *IEEE Trans. Cybern.*, vol. 50, no. 4, pp. 1739–1751, Apr. 2019.

[37] J. F. C. Mota, J. M. F. Xavier, P. M. Q. Aguiar, and M. Puschel, "Distributed basis pursuit," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1942–1956, Apr. 2012.

[38] T. Wang, G. X. Zhang, J. B. Zhao, Z. Y. He, J. Wang, and M. Pérez-Jiménez, " Fault diagnosis of electric power systems based on fuzzy reasoning spiking neural P systems," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1182–1194, May 2015.

[39] H. Zhang and J. M. Wang, "Active steering actuator fault detection for an automatically-steered electric ground vehicle," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3685–3702, May 2017.

[40] M. T. Amin, S. Imtiaz, and F. Khan, "Process system fault detection and diagnosis using a hybrid technique," *Chem. Eng. Sci.* , vol. 189, pp. 191–211, Nov. 2018.

[41] I. Shames, A. M. H. Teixeira, H. Sandberg, and K. H. Johansson, "Distributed fault detection for interconnected second-order systems," *Automatica*, vol. 47, no. 12, pp. 2757–2764, Dec. 2011.

[42] X. H. Liu, X. W. Gao, and J. Han, "Robust unknown input observer based fault detection for high-order multi-agent systems with disturbances," *ISA Trans.*, vol. 61, pp. 15–28, Mar. 2016.

[43] X. W. Gao, X. H. Liu, and J. Han, "Reduced order unknown input observer based distributed fault detection for multi-agent systems," *J. Franklin Inst.*, vol. 354, pp. 1464–1483, Feb. 2017.

[44] Z. H. Zhang and G. H. Yang, "Distributed fault detection and isolation for multiagent systems: An interval observer approach," *IEEE Trans. Syst.*, *Man Cybern.*: *Syst.*, vol. 50, no. 6, pp. 2220–2230, Jun. 2020.

[45] 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.

[46] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Trans. Cybern.* , vol. 44, no. 11, pp. 2024–2037, Nov. 2014.

[47] D. Zhao, M. Chi, Z. H. Guan, Y. H. Wu, and J. Chen, "Distributed estimator-based fault detection for multi-agent networks," *Circuits*, *Syst.*, *Signal Process.*, vol. 37, no. 1, pp. 98–111, Jan. 2018.

[48] Y. Li, H. Fang, J. Chen, and C. P. Yu, "Distributed cooperative fault detection for multiagent systems: A mixed H_∞/H_2 optimization approach," *IEEE Trans. Ind. Electron.* , vol. 65, no. 8, pp. 6468–6477, Aug. 2018.

[49] M. Davoodi, N. Meskin, and K. Khorasani, " Simultaneous fault detection and consensus control design for a network of multi-agent systems," *Automatica*, vol. 66, pp. 185–194, Apr. 2016.

[50] S. Hajshirmohamadi, F. Sheikholeslam, and N. Meskin, "Distributed simultaneous fault detection and leader-following consensus control for multi-agent systems," *ISA Trans.*, vol. 87, pp. 129–142, Apr. 2019.

[51] M. R. Davoodi, K. Khorasani, H. Ali Talebi, and H. R. Momeni, "Distributed fault detection and isolation filter design for a network of heterogeneous multiagent systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 3, pp. 1061–1069, May 2014.

[52] Z. Q. Zuo, J. Zhang, and Y. J. Wang, "Adaptive fault-tolerant tracking control for linear and lipschitz nonlinear multi-agent systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3923–3931, Jun. 2015.

[53] S. Chen, D. W. C. Ho, L. L. Li, and M. Liu, "Fault-tolerant consensus of multi-agent system with distributed adaptive protocol," *IEEE Trans. Cybern.*, vol. 45, no. 10, pp. 2142–2155, Oct. 2015.

[54] D. Ye, M. M. Chen, and H. J. Yang, " Distributed adaptive event-triggered fault-tolerant consensus of multiagent systems with general linear dynamics," *IEEE Trans. Cybern.* , vol. 49, no. 3, pp. 757–767, Mar. 2019.

[55] G. Chen and Y. D. Song, " Fault-tolerant output synchronisation control of multi-vehicle systems," *IET Control Theory Appl.* , vol. 8, no. 8, pp. 574–584, May 2014.

[56] J. W. Zhu, G. H. Yang, W. A. Zhang, and L. Yu, "Cooperative fault tolerant tracking control for multiagent systems: An intermediate estimator-based approach," *IEEE Trans. Cybern.* , vol. 48, no. 10, pp. 2972–2980, Oct. 2018.

[57] C. Deng and G. H. Yang, "Cooperative adaptive output regulation for linear multi-agent systems with actuator faults," *IET Control Theory Appl.*, vol. 11, no. 14, pp. 2396–2402, Sep. 2017.

[58] C. Deng and G. H. Yang, "Distributed adaptive fault-tolerant control approach to cooperative output regulation for linear multi-agent systems," *Automatica*, vol. 103, pp. 62–68, May 2019.

[59] J. Zhang, D. W. Ding, and C. J. An, " Fault-tolerant containment control for linear multi-agent systems: An adaptive output regulation approach," *IEEE Access*, vol. 7, pp. 89306–89315, Jul. 2019.

[60] M. E. Dehshalie, M. B. Menhaj, and M. Karrari, " Fault tolerant cooperative control for affine multi-agent systems: An optimal control approach," *J. Franklin Inst.*, vol. 356, no. 3, pp. 1360–1378, Feb. 2019.

[61] S. Chen, B. Chen, and F. Shi, " Distributed fault-tolerant consensus protocol for fuzzy multi-agent systems," *Circuits*, *Syst.*, *Signal Process.*, vol. 38, no. 2, pp. 611–624, Feb. 2019.

[62] W. M. Shi, W. H. Chen, L. X. Gao, and J. P. Hu, " Adaptive fault-tolerant tracking control for singular multi-agent systems," in *Proc. 11th Asian Control Conf.*, Gold Coast, Australia, 2017, pp. 2358–2363.

[63] A. Ghasemi, J. Askari, and M. B. Menhaj, "Distributed fault tolerant control for multi-agent systems with complex-weighted directed communication topology subject to actuator faults," *Int. J. Control*, *Autom. Syst.*, vol. 17, no. 2, pp. 415–424, Feb. 2019.

[64] Y. J. Wang, Y. D. Song, and F. L. Lewis, " Robust adaptive fault-tolerant control of multiagent systems with uncertain nonidentical dynamics and undetectable actuation failures," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3978–3988, Jun. 2015.

[65] M. Khalili, X. D. Zhang, M. M. Polycarpou, T. Parisini, and Y. C.

Cao, " Distributed adaptive fault-tolerant control of uncertain multi-agent systems," *Automatica*, vol. 87, pp. 142–151, Jan. 2018.

[66] C. Deng, W. N. Gao, and W. W. Che, " Distributed adaptive fault-tolerant output regulation of heterogeneous multi-agent systems with coupling uncertainties and actuator faults," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 4, pp. 1098–1106, Jul. 2020.

[67] L. Cao, H. Y. Li, G. W. Dong, and R. Q. Lu, " Event-triggered control for multiagent systems with sensor faults and input saturation," *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published.

[68] B. Yan, C. F. Wu, and P. Shi, "Formation consensus for discrete-time heterogeneous multi-agent systems with link failures and actuator/sensor faults," *J. Franklin Inst.* , vol. 356, no. 12, pp. 6547–6570, Aug. 2019.

[69] P. A. Ioannou and J. Sun, *Robust Adaptive Control*. Upper Saddle River, USA: PTR Prentice-Hall, 1996.

[70] H. Yang, M. Staroswiecki, B. Jiang, and J. Y. Liu, " Fault tolerant cooperative control for a class of nonlinear multi-agent systems," *Syst. Control Lett.*, vol. 60, no. 4, pp. 271–277, Apr. 2011.

[71] Y. Chen, S. Kar, and J. M. F. Moura, "Resilient distributed estimation through adversary detection," *IEEE Trans. Signal Process.* , vol. 66, no. 9, pp. 2455–2469, May 2018.

[72] N. Forti, G. Battistelli, L. Chisci, S. Q. Li, B. L. Wang, and B. Sinopoli, " Distributed joint attack detection and secure state estimation," *IEEE Trans. Signal Inf. Proce. Netw.*, vol. 4, no. 1, pp. 96–110, Mar. 2018.

[73] M. Deghat, V. Ugrinovskii, I. Shames, and C. Langbort, "Detection and mitigation of biasing attacks on distributed estimation networks," *Automatica*, vol. 99, pp. 369–381, Jan. 2019.

[74] F. Pasqualetti, A. Bicchi, and F. Bullo, " Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan. 2012.

[75] R. M. G. Ferrari, T. Parisini, and M. M. Polycarpou, "Distributed fault detection and isolation of large-scale discrete-time nonlinear systems: An adaptive approximation approach," *IEEE Trans. Autom. Control*, vol. 57, no. 2, pp. 275–290, Feb. 2012.

[76] A. J. Gallo, M. S. Turan, P. Nahata, F. Boem, T. Parisini, and G. Ferrari-Trecate, " Distributed cyber-attack detection in the secondary control of DC microgrids," in *Proc. European Control Conf.*, Limassol, Cyprus, 2018, pp. 344–349.

[77] R. Merco, Z. A. Biron, and P. Pisu, " Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Proc. Annual American Control Conf.*, Milwaukee, USA, 2018, pp. 5582–5587.

[78] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[79] F. Boem, A. J. Gallo, G. Ferrari-Trecate, and T. Parisini, "A distributed attack detection method for multi-agent systems governed by consensus-based control," in *Proc. IEEE 56th Annu. Conf. Decision and Control*, Melbourne, Australia, 2017, 5961–5966.

[80] Y. W. Wang, H. O. Wang, J. W. Xiao, and Z. H. Guan, "Synchronization of complex dynamical networks under recoverable attacks," *Automatica*, vol. 46, no. 1, pp. 197–203, Jan. 2010.

[81] Z. Feng, G. Q. Hu, and G. H. Wen, "Distributed consensus tracking for multi-agent systems under two types of attacks," *Int. J. Robust Nonlinear Control*, vol. 26, no. 5, pp. 896–918, Mar. 2016.

[82] A. Y. Lu and G. H. Yang, " Distributed consensus control for multi-agent systems under denial-of-service," *Inf. Sci.* , vol. 439–440, pp. 95–107, May 2018.

[83] H. J. Yang, S. Ju, Y. Q. Xia, and J. H. Zhang, "Predictive cloud control for networked multiagent systems with quantized signals under DoS attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published.

[84] W. B. Zhang, Z. D. Wang, Y. R. Liu, D. R. Ding, and F. E. Alsaadi, "Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks," *Int. J. Robust Nonlinear Control* , vol. 28, no. 1, pp. 53–67, Jan. 2018.

[85] Z. H. Cheng, D. Yue, S. L. Hu, H. Ge, and L. Chen, "Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks," *Neurocomputing*, vol. 400, pp. 458–466, Aug. 2020.

[86] Y. Xu, M. Fang, Z. G. Wu, Y. J. Pan, M. Chadli, and T. W. Huang, "Input-based event-triggering consensus of multiagent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 50, no. 4, pp. 1455–1464, Apr. 2020.

[87] Y. Xu, M. Fang, P. Shi, and Z. G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3468–3476, Aug. 2020.

[88] Z. Feng and G. Q. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

[89] A. Cetinkaya, K. Kikuchi, T. Hayakawa, and H. Ishii, "Randomized transmission protocols for protection against jamming attacks in multi-agent consensus," *Automatica*, vol. 117, Article No. 108960, Jul. 2020. DOI: 10.1016/j.automatica.2020.108960.

[90] Z. Feng, G. H. Wen, and G. Q. Hu, " Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1273–1284, May 2017.

[91] Y. Yang, H. W. Xu, and D. Yue, " Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks," *IEEE Trans. Circ. Syst. I: Regul. Pap.*, vol. 66, no. 8, pp. 3089–3099, Aug. 2019.

[92] D. Zhang, L. Liu, and G. Feng, " Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.

[93] D. Zhang and G. Feng, " A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with DoS attack," *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published.

[94] D. R. Ding, Z. D. Wang, D. W. C. Ho, and G. L. Wei, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks," *IEEE Trans. Cybern.* , vol. 47, no. 8, pp. 1936–1947, Aug. 2017.

[95] W. L. He, X. Y. Gao, W. M. Zhong, and F. Qian, " Secure impulsive synchronization control of multi-agent systems under deception attacks," *Inf. Sci.*, vol. 459, pp. 354–368, Aug. 2018.

[96] Y. Cui, Y. R. Liu, W. B. Zhang, and F. E. Alsaadi, "Sampled-based consensus for nonlinear multiagent systems with deception attacks: The decoupled method," *IEEE Trans. Syst., Man, Cybern.: Syst.*, to be published.

[97] X. Huang and J. X. Dong, " Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst., Man, Cybern.: Syst.* , vol. 50, no. 1, pp. 89–99, Jan. 2020.

[98] Y. M. Dong, N. Gupta, and N. Chopra, "False data injection attacks in bilateral teleoperation systems," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 1168–1176, May 2020.

[99] R. Moghadam and H. Modares, " Resilient autonomous control of distributed multiagent systems in contested environments," *IEEE Trans. Cybern.*, vol. 49, no. 11, pp. 3957–3967, Nov. 2019.

[100] A. Mustafa, H. Modares, and R. Moghadam, "Resilient synchronization of distributed multi-agent systems under attacks," *Automatica*, vol. 115, Article No. 108869, May 2020. DOI: 10.1016/j.automatica.2020.108869.

[101] A. Mustafa and H. Modares, " Attack analysis and resilient control design for discrete-time distributed multi-agent systems," *IEEE Robot. Autom. Lett.*, vol. 5, no. 2, pp. 369–376, Apr. 2020.

[102] Y. Yang, Q. D. Liu, Y. Qian, D. Yue, and X. H. Ding, "Secure bipartite tracking control of a class of nonlinear multi-agent systems with nonsymmetric input constraint against sensor attacks," *Inf. Sci.*, vol. 539, pp. 504–521, Oct. 2020.

[103] Z. H. Xu, H. J. Ni, H. R. Karimi, and D. Zhang, "A markovian jump system approach to consensus of heterogeneous multiagent systems with partially unknown and uncertain attack strategies," *Int. J. Robust Nonlinear Control*, vol. 30, no. 7, pp. 3039–3053, May 2020.

[104] J. Huang, *Nonlinear Output Regulation: Theory and Applications*. Philadelphia, USA: Society for Industrial and Applied Mathematics, 2004.

[105] A. Sonnino, S. Bano, M. Al-Bassam, and G. Danezis, "Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers," arXiv: 1901.11218, Sep. 2020.

[106] L. Faramondi, R. Setola, and G. Oliva, "Performance and robustness of discrete and finite time average consensus algorithms," *Int. J. Syst.*

Sci., vol. 49, no. 12, pp. 2704–2724, Aug. 2018.

[107] Satori is the latest Mirai botnet variant that is targeting Huawei HG532 home routers. [Online]. Available: https://securityaffairs.co/wordpress/67040/malware/satori-botnet-mirai-variant.html. Accessed on: Oct. 2019.

[108] J. L. Liu, T. T. Yin, D. Yue, H. R. Karimi, and J. D. Cao, "Event-based secure leader-following consensus control for multiagent systems with multiple cyber attacks," *IEEE Trans. Cybern.*, to be published.

[109] A. Sanjab and W. Saad, "Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2038–2049, Jul. 2016.

[110] A. Sanjab and W. Saad, "On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection," in *Proc. Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids*, Vienna, Austria, 2016, pp. 1–6.

[111] L. Zhao and G. H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with DoS attacks," *Inf. Sci.*, vol. 536, pp. 39–53, Jul. 2020.

[112] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Commun. Surv. Tutorials* , vol. 21, no. 1, pp. 686–728, 2019.

[113] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 640–660, 2019.

[114] W. Chen, D. R. Ding, H. L. Dong, and G. L. 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.

[115] C. M. Ahmed, V. R. Palleti, and A. P. Mathur, "WADI: A water distribution testbed for research in the design of secure cyber physical systems," in *Proc. 3rd Int. Workshop on Cyber-Physical Systems for Smart Water Networks*, Pittsburgh, USA, 2017, pp. 25–28.

[116] E. Korkmaz, A. Dolgikh, M. Davis, and V. Skormin, "Industrial control systems security testbed," in *Proc. 11th Annu. Symp. Information Assurance*, Albany, USA, 2016.

Dan Zhang (SM' 20) received the B.E. degree in automation and the Ph.D. degree in control theory and control engineering from the Zhejiang University of Technology, China, in 2007 and 2013, respectively. He is currently an Associate Professor with the Department of Automation, Zhejiang University of Technology. He was a Research Fellow with Nanyang Technological University, Singapore, from 2013 to 2014, the National University of Singapore, Singapore, from 2016 to 2017, and City University of Hong Kong, from 2017 to 2019. respectively. His research interests are in the area of networked control systems, robust control, and filtering.

He is a Senior Member of IEEE, an Associate Editor of *ISA Transactions*, *International Journal of Uncertainty*, *Fuzziness and Knowledge-based Systems*, and *International Journal of Control*, *Automation and Systems*, and was an Associate Editor of *Neurocomputing*.

Gang Feng (SM'95−F'05) received the Ph.D. degree in electrical engineering from the University of Melbourne, Australia. He has been with City University of Hong Kong since 2000 after serving as lecturer/senior lecturer at School of Electrical Engineering, University of New South Wales, Australia, from 1992 to 1999. He is now Chair Professor of Mechatronic Engineering. He has been awarded an Alexander von Humboldt Fellowship, the IEEE Transactions on Fuzzy Systems Outstanding Paper Award, Changjiang Chair Professorship from Education Ministry of China, and CityU Outstanding Research Award. He is listed as a SCI highly cited researcher by Clarivate Analytics. His current research interests include multi-agent systems and control, intelligent systems and control, and networked systems and control.

He is a Fellow of IEEE, an Associate Editor of *IEEE Trans. Fuzzy Systems and Journal of Systems Science and Complexity*, and was an Associate Editor of *IEEE Trans. Automatic Control*, *IEEE Trans. Systems, Man & Cybernetics, Part C*, *Mechatronics* , and *Journal of Control Theory and Applications*. He is on the Advisory Board of *Unmanned Systems*.

Yang Shi (SM'09–F' 17) received the B.Sc. and Ph.D. degrees in mechanical engineering and automatic control from Northwestern Polytechnical University, Xi'an, China, in 1994 and 1998, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Alberta, Edmonton, AB, Canada in 2005. From 2005 to 2009, he was an Assistant Professor and Associate Professor in the Department of Mechanical Engineering, University of Saskatchewan, Saskatoon, SK, Canada. In 2009, he joined the University of Victoria, and now he is a Professor in the Department of Mechanical Engineering, University of Victoria, Victoria, BC, Canada. His current research interests include networked and distributed systems, model predictive control (MPC), cyber-physical systems (CPS), robotics and mechatronics, navigation and control of autonomous systems (AUV and UAV), and energy system applications.

He received the University of Saskatchewan Student Union Teaching Excellence Award in 2007, and the Faculty of Engineering Teaching Excellence Award in 2012 at the University of Victoria (UVic). He is the recipient of the JSPS Invitation Fellowship (short-term) in 2013, the UVic Craigdarroch Silver Medal for Excellence in Research in 2015, the 2017 *IEEE Transactions on Fuzzy Systems* Outstanding Paper Award, the Humboldt Research Fellowship for Experienced Researchers in 2018. Currently he serves as a member of the IEEE Industrial Electronics Society (IES) Administrative Committee, the Chair of IEEE IES Technical Committee on Industrial Cyber-Physical Systems, and Co-Editor-in-Chief for *IEEE Transactions on Industrial Electronics*. He also serves as Associate Editor for *Automatica*, *IEEE Transactions on Control Systems Technology*, *IEEE/ASME Transactions on Mechatronics*, *IEEE Transactions on Cybernetics*, etc. He is General Chair of the 2019 International Symposium on Industrial Electronics (ISIE) and the 2021 International Conference on Industrial Cyber-Physical Systems (ICPS). He is a Fellow of IEEE, American Society of Mechanical Engineers (ASME), Canadian Society of Mechanical Engineers (CSME), and Engineering Institute of Canada (EIC), and a registered Professional Engineer in British Columbia, Canada.

Dipti Srinivasan (SM'02−F' 20) received the M.Eng. and Ph.D. degrees in electrical engineering from the National University of Singapore, in 1991 and 1994, respectively. She is a Professor in the Department of Electrical & Computer Engineering at the National University of Singapore, where she also heads the Centre for Green Energy Management & Smart Grid (GEMS). Her recent research projects are in the broad areas of optimization and control, wind and solar power prediction, electricity price prediction, deep learning, and development of multi-agent systems for system operation and control. Her current research focuses on the development of novel computational intelligence-based models and methodologies to aid the integration of the new Smart Grid technologies into the existing infrastructure so that power grid can effectively utilize pervasive renewable energy generation and demand-side management programs, while accommodating stochastic load demand. She is the author of four books and over 400 journal and conference papers in the field of computational intelligence, renewable energy and smart grids which have been published in top tier journals.

She is a Fellow of IEEE, and was awarded the IEEE Power & Energy Society (PES) Outstanding Engineer Award in 2010. She is an Associate Editor of *IEEE Transactions on Smart Grid*, *IEEE Transactions on Sustainable Energy*, *IEEE Transactions on Evolutionary Computation*, *IEEE Transaction on Neural Networks and Learning Systems*, and *IEEE Computational Intelligence magazine*. At the Electrical & Computer Engineering (ECE) Department of National University of Singapore, she teaches courses in the areas of sustainable energy systems, smart grid, and computational intelligence methods. She is the recipient of NUS Annual Teaching Excellence Award and Engineering Educator Award.