Fault-tolerant Consensus of Multi-agent Systems Subject to Multiple Faults and Random Attacks

Chun Liu, *Member, IEEE*, Wanyi Wang, Bin Jiang, *Fellow, IEEE*, and Ron J. Patton, *Life Fellow, IEEE*

***Abstract*—This paper explores the consensus control problem of nonlinear multi-agent systems (MASs) under complex cyber-physical threats (CPTs), which encompass sensor/actuator faults, input/output channel noises, and random cyber-attacks. The multiple sensor/actuator faults are uniformly modeled as an exponential type, while random cyber-attacks are characterized by a Markov chain. To enhance the safety and security of MASs under CPTs, the distributed normalized observers are first developed, enabling precise estimations of unknown state and fault information. Subsequently, the distributed fault-tolerant consensus control (FTCC) scheme with a positive reconstruction mechanism is proposed to maintain resilience against attacks, compensation for faults, and robustness to noises in MASs under adverse CPTs. The two notable innovations can be outlined as follows: i) The achievement of FTCC objectives under complex CPTs, demonstrating strong algorithmic transferability in both non-attack and random attack scenarios. ii) The adoption of a double-layer distributed framework in the estimation layer and control layer, balancing computational complexity and efficiency improvements compared to a combination of decentralized and distributed approaches. Simulation results finally confirm the efficacy and feasibility of the proposed FTCC algorithm.**

***Index Terms*—Multiple faults, fault-tolerant consensus control, distributed observers, random attacks, multi-agent systems.**

I. Introduction

The subject of FTCC of MASs has garnered significant attention due to its potential in maintaining global or local expected performance in the presence of physical faults or cyber-attacks. The recent studies on FTCC strategies concerning the cyber-physical security and safety of MASs are summarized in [1]. Unlike classical FTCC schemes in linear MASs [2], the nonlinearity [3], [4] renders challenges to the reliability and robustness of MASs. Apart from unexpected physical component faults [5], malicious cyber-attacks pose significant threats to the logical security of communication links or individual nodes [6]. Hence, in the face of simultaneous CPTs, the FTCC of nonlinear MASs is required to sustain both operational capability and sustainability, at a standard or slightly diminished level.

Due to the long-term usage of the devices in diverse environments, MASs are susceptible to anomalous faults in the physical layer, such as sensor faults [7], and actuator faults [8]. Unlike addressing individual physical faults, the literature on FTCC algorithms for addressing multiple physical faults is still relatively scarce. Specifically, the fuzzy-logic-based distributed adaptive control protocol has been proposed for MASs with sensor and actuator faults [9]. The formation consensus problem is investigated for discrete-time heterogeneous MASs [10] with link failures and actuator/sensor faults, and an adaptive fault-tolerant control issue of nonlinear MASs under multiple faults is studied in [11]. To date, most studies adopt a combination of decentralized observers and distributed controllers to compensate for physical faults [5], [8]. However, the literature on the compensation mechanisms constructed by double-layer distributed architecture-based observers and controllers [12] is relatively limited. On the other hand, most studies merely consider abrupt physical faults [10], [13], while neglecting hidden incipient physical faults. It is worth noting that they bring rapid performance degradation and coordination interruption of all of the MASs due to tiny deviations induced by incipient faults spread to other agents in the unreliable network. Furthermore, the co-existence of unified abrupt-incipient physical faults and channel noises [14] makes it difficult to achieve an accurate consensus performance. Therefore, it becomes both a meaningful and challenging endeavor to devise a double-layer distributed observer-controller framework capable of effectively handling the concurrent presence of multiple sensor/actuator faults and channel noises.

Besides bolstering physical safety, mitigating the topology switching [15] or accounting for interaction interruptions [16] caused by cyber-attacks represents a viable approach for securing MASs. The logical security of MASs is commonly affected by various cyber-attacks, such as denial-of-service (DoS) attacks [17], false data injection attacks [18], and sensor and actuator attacks [19], thus the security protection mechanism of cyber-physical MASs against hostile attacks is urgent to explore. However, in rare cases, the literature has studied the integrated security of cyber-physical MASs under anomalous faults and malicious attacks. To address the FTCC problem of nonlinear cyber-physical MASs [20], the adaptive state-feedback schemes and switching mechanisms are designed to improve compensation for actuator faults and resilience to DoS attacks, respectively. The distributed anti-attack FTCC policy is proposed in [21] for MASs subject to multiple physical failures and malicious connectivity-mixed

This work was supported by National Natural Science Foundation of China (62103250, 62333011 and 62020106003); Shanghai Sailing Program (21YF1414000); Project of Science and Technology Commission of Shanghai Municipality (22JC1401401).

C. Liu is with the School of Mechatronic Engineering and Automation, and also with the School of Future Technology (Institute of Artificial Intelligence), Shanghai University, Shanghai 200444, China (e-mail: Chun_Liu@shu.edu.cn).

W. Y. Wang is with the School of Future Technology (Institute of Artificial Intelligence), Shanghai University, Shanghai 200444, China (e-mail: 2868907970@shu.edu.cn).

B. Jiang is with the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: binjiang@nuaa.edu.cn).

R. J. Patton is with the School of Engineering, University of Hull, Hull HU6 7RX, U.K. (e-mail: r.j.patton@hull.ac.uk).

attacks, and the adaptive impulsive FTCC strategy is developed in [22] for MASs with deception attacks and actuator faults. Furthermore, it is a more challenging task to address FTCC problems due to the aperiodicity [23] and unpredictability [24] of random cyber-attacks. Thus, the crucial issue is how to utilize the double-layer distributed observer-controller framework to achieve the consensus purpose of nonlinear cyber-physical MASs amidst random attacks and multiple faults.

The notable contributions are summarized as follows. (i) In contrast to handling individual physical faults [7], [8] or addressing specific and determined cyber-attacks [15], [17], this paper proposes a novel distributed FTCC scheme to achieve the safe and secure objectives of the nonlinear MASs under adverse CPTs that encompass multiple faults, channel noises, and random attacks. The FTCC strategy enables the parallel migration of algorithms by utilizing the expectation in random topology switching, applicable in both attack-free and random attack scenarios. (ii) In comparison to the decentralized and distributed combination strategy within the estimation and controller layers [5], [8], this paper employs a double-layer distributed observer-controller framework, which effectively balances computational complexity and efficiency improvements. Significantly, the distributed FTCC structure exhibits exceptional fault tolerance and attack resilience by enabling local information interaction, topological redundancy, and policy diversity, even in cases where certain nodes or links fail or are interrupted.

The rest of this paper is structured as follows. Section II presents problem formulation and model description. The main results including the double-layer distributed observer-controller framework for fault-tolerant consensus and stability analysis are provided in Section III. Simulation is illustrated to verify the feasibility and efficiency of the proposed distributed FTCC algorithm of MASs in Section IV. Section V illustrates the conclusion with future concerned investigations.

Notation: $||\cdot||$, $\mathscr{E}$ and $\otimes$ represent the Euclidean norm, mathematical expectation, and Kronecker product of matrices, respectively. $He(X)=X+X^T$, $\mathbf{R}$ is the real-number set, and $\mathbf{1}$ indicates a column vector where all elements are 1. $\lambda_{\min}$ and $\lambda_{\max}$ are the minimum and maximum eigenvalues.

II. Problem Formulation and Model Description

The dynamics of nonlinear MASs comprising N followers are expressed as follows:

$$\begin{aligned}\dot{x}_i(t)&=Ax_i(t)+Bu_i(t)+F_af_{ai}(t)+D_1\omega_{i1}(t)+\xi(x_i(t),t)\\ y_i(t)&=Cx_i(t)+F_sf_{si}(t)+D_2\omega_{i2}(t)\end{aligned}\tag{1}$$

where $x_i(t)\in\mathbf{R}^n, y_i(t)\in\mathbf{R}^p, u_i(t)\in\mathbf{R}^m$ denote the follower's state, output, and input, respectively. $f_{ai}(t)\in\mathbf{R}^{q_1}$ and $f_{si}(t)\in\mathbf{R}^{q_2}$ represent the actuator fault and sensor fault, $\omega_{i1}(t)\in\mathbf{R}^{s_1}$ and $\omega_{i2}(t)\in\mathbf{R}^{s_2}$ are the input noise and output noise on the channel, and $\xi(x_i(t),t)\in\mathbf{R}^n$ is the unknown nonlinearity item. The system-described gain matrices are represented by A,B,C, the actuator fault gain matrix and sensor fault gain matrix are denoted by F_a,F_s, and D_1,D_2 are the noise-described gain matrices. It should be noted that these gain matrices have known and appropriate dimensions.

The dynamics of the leader (labeled as 0) are expressed as

$$\begin{aligned}\dot{x}_0(t)&=Ax_0(t)+Bu_0(t)+\xi(x_0(t),t)\\ y_0(t)&=Cx_0(t)\end{aligned}\tag{2}$$

where $x_0(t)\in\mathbf{R}^n, y_0(t)\in\mathbf{R}^p$, and $\xi(x_0(t),t)\in\mathbf{R}^n$ represent the leader's state, output, and the unknown nonlinearity, respectively. Notably, $u_0(t)=-K_xx_0(t)$ denotes the control input with the state-estimation gain matrix $K_x\in\mathbf{R}^{m\times n}$.

Remark 1: The authentic physical models of the leaders and followers exhibit congruence. Nevertheless, when confronted with intricate and dynamic environments, the dynamic model of the followers incorporates considerations for composite faults in actuators/sensors and noises within input/output channels. Within homogeneous MASs [9], [11], agents conventionally engage in the communal adoption of control strategies characterized by similar structures and convergent parameters. Conversely, within heterogeneous MASs [25], [26], [27], controllers are compelled to delineate precise strategies tailored to the distinctive types, hierarchical structures, and task levels inherent to the diverse agents.

A. Multiple Fault Modeling

The abrupt and incipient actuator faults and sensor faults are modeled in a unified manner, and the distinction between abrupt and incipient faults is made by the exponential function with a decay rate. The multiple sensor and actuator faults within each element $f_{ai}^{\varrho}(t)$ and $f_{si}^{\varrho}(t)$ in the physical layer are modeled as follows:

$$\begin{aligned}f_{ai}^{\varrho}(t)&=(1-e^{-\varepsilon_a^{\varrho}(t-T_a^{\varrho})})\bar{f}_{ai}^{\varrho},t\geq T_a^{\varrho},\varrho=1,\cdots,q_1\\ f_{si}^{\varrho}(t)&=(1-e^{-\varepsilon_s^{\varrho}(t-T_s^{\varrho})})f_{si}^{\varrho},t\geq T_s^{\varrho},\varrho=1,\cdots,q_2\end{aligned}\tag{3}$$

where $f_{ai}(t)=[f_{ai}^1(t),f_{ai}^2(t),\cdots,f_{ai}^{q_1}(t)]^T$, $f_{si}(t)=[f_{si}^1(t),f_{si}^2(t),\cdots,f_{si}^{q_2}(t)]^T$. $f_{si}^{\varrho},f_{ai}^{\varrho}$ denote the unknown fault bounds in the ϱ th row elements, $\varepsilon_a^{\varrho},\varepsilon_s^{\varrho}$ denote the unknown decay rates, and $T_a^{\varrho},T_s^{\varrho}$ denote the time instants when physical faults occur. Due to the physical faults being modeled as the unified abrupt-incipient type, then multiple sensor and actuator faults are satisfied with the quick-changed decay rate ($\varepsilon_{a(s)}\geq\bar{\varepsilon}_{a(s)}$) and low-changed decay rate ($\underline{\varepsilon}_{a(s)}\leq\varepsilon_{a(s)}^{\varrho}<\bar{\varepsilon}_{a(s)}$).

Assumption 1 [3], [4]: For any $i,j=0,1,\cdots,N$, there exists a positive number ρ' such that the unknown nonlinearity meets the Lipschitz condition $\parallel\xi(x_i(t),t)-\xi(x_j(t),t)\parallel\leq\rho'\parallel x_i(t)-x_j(t)\parallel$.

Assumption 2 [21]: The multiple sensor and actuator faults with an abrupt-incipient type exhibit the differentiable property after the occurrence of faults. Furthermore, $\underline{\varepsilon}_{a(s)}$ and $\bar{\varepsilon}_{a(s)}$ are the available positive constants, which denote the lower and upper boundaries of the decay rates $\varepsilon_{a(s)}^{\varrho}$, respectively.

Assumption 3 [14], [21]: The input noise (ω_{i1}) and output noise (ω_{i2}) are restricted to be upper bounded, i.e., $\parallel\omega_{i1}(t)\parallel\leq\bar{\omega}_{i1}$ and $\parallel\dot{\omega}_{i2}(t)\parallel\leq\bar{\omega}_{i2}$, respectively.

B. Random Attack Modeling

This paper establishes a type of non-periodic random cyber-attacks, which disrupt communication links among agents, altering the communication topology, and thus impacting the overall network security of the MASs. Due to the memoryless

property and the ability to capture transition relationships among random events, a Markov process denoted by the transition probability matrix $P_{pq}(t)$ is employed to represent the occurrence of random attacks and reflect the impact on the communication topology. The Markov process is defined as $P_{pq}(t) = Prob\{r(t+h) = q|r(t) = p\}$ when the topology transitions from state p to q. For $p \neq q$, the transition probability matrix $P_{pq}(t) = \gamma_{pq}h + o(h)$, conversely $P_{pq}(t) = 1 + \gamma_{pq}h + o(h)$, where γ_{pq} represents the transfer rate, and $o(h)$ signifies an infinitesimal of higher order than h such that $\lim_{h\to 0} o(h)/h = 0$. $S_1 = \{1, 2, \cdots, s\}$ is a finite state space encompassing all possibly attackable topologies. The transfer rate matrix is defined as $\gamma = \{\gamma_{pq}\}_{p,q\in S_1}$ such that for $p \neq q, \gamma_{pq} \geq 0$ and $\gamma_{pp} = 1 - \sum_{q\neq p}\gamma_{pq}$.

To facilitate the analysis of the impact of random attacks injected into MASs, the random attacks are defined to be activated in a time-varying manner within the time interval $[t_0, t)$. If $t \in [t_{2k}, t_{2k+1})$, the cyber-attacks are in the dormancy zone and the MASs are not attacked. Then, the switching sequence $\{t_{2k}\}_{k\in\mathbf{N}}$ corresponding with the initial graph $\mathcal{G}_0$ is denoted by the symbol $T_m(t_{2k}, t)$. Otherwise, if $t \in [t_{2k+1}, t_{2(k+1)})$, the cyber-attacks are in the activation zone and the MASs are subject to random cyber-attacks. Then, the switching sequence $\{t_{2k+1}\}_{k\in\mathbf{N}}$ corresponding with the swithcing graph $\mathcal{G}_{r(t)}$ is denoted by the symbol $T_p(t_{2k+1}, t)$, where $r(t)$ represents the changing state within a Markov process. Under the influence of random attacks and self-recovery mechanisms, the communication links of MASs are disrupted and reorganized, respectively. Therefore, the switching process from the initial graph $\mathcal{G}_0$ to the reorganized graph $\mathcal{G}_{r(t)}$ is called the switching topology.

Definition 1: For $t_2 > t_1 \geq 0$, define the number of random attacks as $N_a(t_1, t_2)$. Thus, denote $F_a(t_1, t_2) = N_a(t_1, t_2)/(t_2 - t_1)$ as the attack frequency over $[t_1, t_2)$.

Definition 2: For $t_2 > t_1 \geq 0$, define the total time interval of random attacks as $T_a(t_1, t_2)$. Thus, denote $\mathcal{R}_a(t_1, t_2) = T_a(t_1, t_2)/(t_2 - t_1)$ as the attack length rate over $[t_1, t_2)$.

Assumption 4 [14], [17]: Under the scenario of random attacks, it is assumed that the switching graph $\mathcal{G}_{r(t)}$ is balanced and contains a spanning tree of the union of digraphs. The switching signal $r(t)$ induced by random cyber-attacks is postulated to follow an initial time-invariant distribution $\pi_0 = [\pi_1, \cdots, \pi_s]$.

Remark 2: In complex communication environments, the topological connectivity of MASs is susceptible to intermittent cyber-attacks, such as link interruption. Hostile aggressors aim to obstruct coherent signal transmission among agents, disrupting data interactions and ultimately compromising tracking performance. However, the self-recovery mechanism of MASs enables the continuous initiation of relink requests during the dormancy interval of random cyber-attacks, persisting until the network connection is restored, which ensures communication connectivity by reconstructing the communication links in a relatively brief period. In contrast to easily detectable periodic cyber-attacks [6], [15], the energy-limited attacks executed by adversaries are non-periodic. It is assumed that the topological structure is both resilient and recoverable, and a finite number of switching topologies are completed under the constraints of attack frequency and attack length rate in Definitions 1 and 2.

Remark 3: The rationality for the mentioned assumptions is summarized as follows: 1) The Lipschitz condition contributes to the improvement of controllability and stability by imposing local constraints on unknown nonlinear terms. It is exemplified in its ability to facilitate a reasoned response to state-dependent nonlinearity encountered in the context of robot path planning and navigation [28] within intricate and unpredictable environments. 2) The original system can be augmented provided that the modeled unified abrupt-incipient type fault is differentiable, which in turn allows the design of unknown input observers to achieve estimations of unknown states and multiple faults. The predetermined decay rate boundary values are set to distinguish between abrupt-type faults and incipient-type faults, i.e., the abrupt-type faults ($\varepsilon_{a(s)} \geq \bar{\varepsilon}_{a(s)}$) and incipient-type faults ($\varepsilon_{a(s)} \leq \varepsilon^{\varrho}_{a(s)} < \bar{\varepsilon}_{a(s)}$). 3) Ensuring robustness against energy-limited external factors and interference thresholds requires constraining input/output channel noises, with the precise boundary values not necessarily needing to be entirely ascertainable. 4) The primary focus is on the connectivity of switching topologies induced by random cyber-attacks, which is a critical factor in ensuring an FTCC performance. Even when facing potential link disruptions, self-recovery mechanisms of MASs are utilized to establish new communication links. Consequently, under the influence of the Markov process, the switching topology signal $r(t)$ caused by random cyber-attacks achieves a specific switching probability aligned with the initial distribution π_0.

III. Main Results

A. Double-layer Distributed Observer-controller Framework for Fault-tolerant Consensus

The double-layer distributed observer-controller framework is constructed to achieve an asymptotic exponential consensus for nonlinear MASs subject to multiple sensor/actuator faults, channel noises, and random attacks in Fig. 1.

The procedure for normalizing the initial MASs can be outlined as follows

$$\begin{aligned}\dot{\bar{x}}_i(t) &= \bar{A}\bar{x}_i(t) + \bar{B}u_i(t) + \bar{M}\bar{d}_i(t) + \bar{\xi}(E_0\bar{x}_i(t), t)\\ y_i(t) &= \bar{C}\bar{x}_i(t)\end{aligned} \tag{4}$$

where $\bar{d}_i(t) = [\omega_{i1}^T(t)\ \dot{f}_{ai}^T(t)\ \dot{f}_{si}^T(t)\ \dot{\omega}_{i2}^T(t)]^T$ is the augmented uncertainty, $\bar{x}_i(t) = [x_i^T(t)\ f_{ai}^T(t)\ f_{si}^T(t)\ \omega_{i2}^T(t)]^T$ is the augmented state, and $\bar{\xi}(E_0\bar{x}_i(t), t) = [\xi^T(x_i(t), t)\ \ 0_{1\times q_1}\ \ 0_{1\times q_2}\ \ 0_{1\times s_2}]^T$ is the augmented nonlinearity with $E_0 = [I_n\ 0_{n\times q_1}\ 0_{n\times q_2}\ 0_{n\times s_2}]$, and the augmented matrices $\bar{A}, \bar{B}, \bar{M}$ and $\bar{C}$ are described as

$$\bar{A} = \begin{bmatrix} A & F_a & 0_{n\times q_2} & 0_{n\times s_2} \\ 0_{q_1\times n} & 0_{q_1\times q_1} & 0_{q_1\times q_2} & 0_{q_1\times s_2} \\ 0_{q_2\times n} & 0_{q_2\times q_1} & 0_{q_2\times q_2} & 0_{q_2\times s_2} \\ 0_{s_2\times n} & 0_{s_2\times q_1} & 0_{s_2\times q_2} & 0_{s_2\times s_2} \end{bmatrix}, \bar{B} = \begin{bmatrix} B \\ 0_{q_1\times m} \\ 0_{q_2\times m} \\ 0_{s_2\times m} \end{bmatrix}$$

$$\bar{M} = \begin{bmatrix} D_1 & 0_{n\times q_1} & 0_{n\times q_2} & 0_{n\times s_2} \\ 0_{q_1\times s_1} & I_{q_1} & 0_{q_1\times q_2} & 0_{q_1\times s_2} \\ 0_{q_2\times s_1} & 0_{q_2\times q_1} & I_{q_2} & 0_{q_2\times s_2} \\ 0_{s_2\times s_1} & 0_{s_2\times q_1} & 0_{s_2\times q_2} & I_{s_2} \end{bmatrix}, \bar{C} = \begin{bmatrix} C^T \\ 0_{q_1\times p} \\ F_s^T \\ D_2^T \end{bmatrix}^T$$

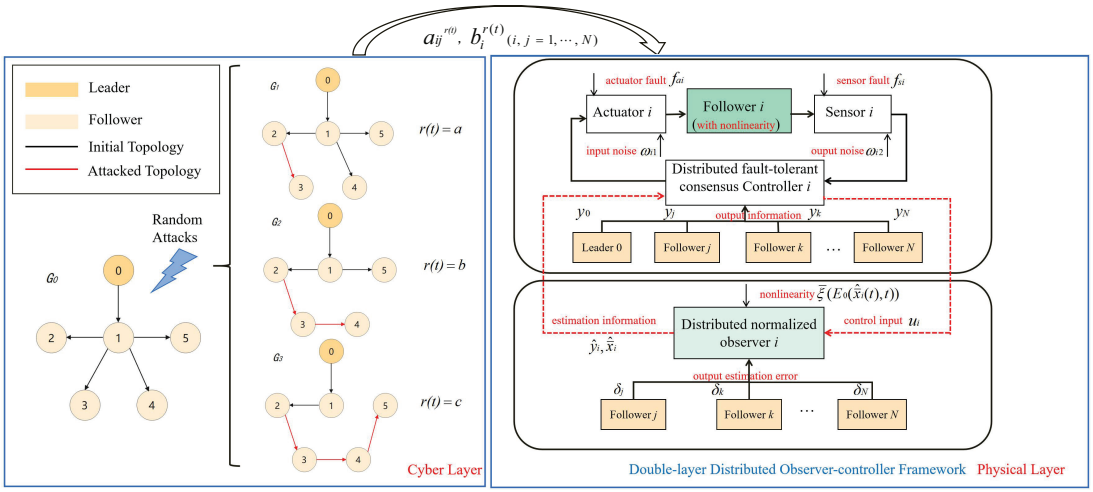

Fig. 1: Double-layer distributed observer-controller framework of nonlinear MASs subject to multiple sensor/actuator faults and channel noises in the physical layer, and random attacks in the cyber layer

Then, the distributed normalized observers in the double-layer observer-controller framework are designed as

$$\begin{aligned}\dot{\hat{\bar{x}}}_i(t) &= \bar{A}\hat{\bar{x}}_i(t) + \bar{B}u_i(t) + \bar{R}\eta_i + \bar{\xi}(E_0(\hat{\bar{x}}_i(t),t))\\ \hat{y}_i(t) &= \bar{C}\hat{\bar{x}}_i(t)\\ \delta_i(t) &= \hat{y}_i(t) - y_i(t)\\ \eta_i &= \rho\textstyle\sum_{j=1}^{N} a_{ij}[\delta_j(t) - \delta_i(t)]\end{aligned} \tag{5}$$

where $\hat{y}_i(t)$ and $\hat{\bar{x}}_i(t) = [\hat{x}_i^T(t)\ \hat{f}_{ai}^T(t)\ \hat{f}_{si}^T(t)\ \hat{\omega}_{i2}^T(t)]^T$ represent the estimations of the output $y_i(t)$ and the augmented state $\bar{x}_i(t)$. $\delta_i(t)$ is the output estimation error of the ith agent, $\bar{R}$ is the observer gain matrix. a_{ij} is the edge coefficients between the ith and jth followers, $\bar{\xi}(E_0\hat{\bar{x}}_i(t),t) = [\xi^T(\hat{x}_i(t),t)\ 0_{1\times q_1}\ 0_{1\times q_2}\ 0_{1\times s_2}]^T$, and the coupling strength $\rho > 0$.

Taking into account the potential occurrence of random attacks on the MASs, the distributed fault-tolerant consensus controllers are intricately designed within the double-layer distributed observer-controller framework:

$$u_i(t) = \begin{cases} \alpha_1 R_1[\sum_{j=1}^{N} a_{ij}^0(y_j(t) - y_i(t)) + b_i^0(y_0(t) - y_i(t))]\\ +\alpha_1 R_1 F_s[\sum_{j=1}^{N} a_{ij}^0(\hat{f}_{sj}(t) - \hat{f}_{si}(t)) + b_i^0\hat{f}_{si}(t)]\\ +\alpha_1 R_1 D_2[\sum_{j=1}^{N} a_{ij}^0(\hat{w}_{j2}(t) - \hat{w}_{i2}(t)) + b_i^0\hat{w}_{i2}(t)]\\ -K\hat{\bar{x}}_i(t), \quad t \in T_m(t_{2k},t)\\ \alpha_2 R_2[\sum_{j=1}^{N} a_{ij}^{r(t)}(y_j(t) - y_i(t)) + b_i^{r(t)}(y_0(t) -\\ y_i(t))] + \alpha_2 R_2 F_s[\sum_{j=1}^{N} a_{ij}^{r(t)}(\hat{f}_{sj}(t) - \hat{f}_{si}(t)) +\\ b_i^{r(t)}\hat{f}_{si}(t)] + \alpha_2 R_2 D_2[\sum_{j=1}^{N} a_{ij}^{r(t)}(\hat{w}_{j2}(t) -\\ \hat{w}_{i2}(t)) + b_i^{r(t)}\hat{w}_{i2}(t)] - K\hat{\bar{x}}_i(t), \ t \in T_p(t_{2k+1},t)\end{cases} \tag{6}$$

where α_1 and α_2 are positive coupling coefficients, a_{ij}^0 and $a_{ij}^{r(t)}$ are the edge coefficients between the ith and jth followers, b_i^0 and $b_i^{r(t)}$ are the signal interaction between the leader and ith follower. R_1, R_2 are the coupling gains, and $K = [K_x\ K_b\ 0_{m\times q_2}\ 0_{m\times s_2}]$ is the compensation gain, $K_x \in \mathbf{R}^{m\times n}$ is the state-estimation gain and $K_b = B\dagger F_a \in \mathbf{R}^{m\times q_1}$ is the fault-estimation gain with the pseudo-inverse operation $\dagger$.

Define the error of augmented estimation as $e_{i1} = \bar{x}_i(t) - \hat{\bar{x}}_i(t) = [e_{xi}^T(t)\ e_{ai}^T(t)\ e_{si}^T(t)\ e_{\omega i}^T(t)]^T$, where $e_{xi}(t) = x_i(t) - \hat{x}_i(t)$, $e_{ai}(t) = f_{ai}(t) - \hat{f}_{ai}(t)$, $e_{si}(t) = f_{si}(t) - \hat{f}_{si}(t)$, $e_{\omega i}(t) = \omega_{i2}(t) - \hat{\omega}_{i2}(t)$ denote the estimation errors of the state, the actuator fault, the sensor fault, and the output channel noise, respectively.

Let $\bar{x}(t) = [\bar{x}_1^T(t),\cdots,\bar{x}_N^T(t)]^T$, $\hat{\bar{x}}(t) = [\hat{\bar{x}}_1^T(t),\cdots,\hat{\bar{x}}_N^T(t)]^T$, $u(t) = [u_1^T(t),\cdots,u_N^T(t)]^T$, and $d(t) = [d_1^T(t),\cdots,d_N^T(t)]^T$, it is obtained that

$$\begin{aligned}\dot{\bar{x}}(t) &= (I_N\otimes\bar{A})\bar{x}(t) + (I_N\otimes\bar{B})u(t) + (I_N\otimes\bar{M})d(t)\\ &\quad +\bar{\xi}(E_0(\bar{x}(t),t))\\ \dot{\hat{\bar{x}}}(t) &= (I_N\otimes\bar{A})\hat{\bar{x}}(t) + (I_N\otimes\bar{B})u(t)\\ &\quad +(I_N\otimes\bar{R})\rho(\mathcal{L}\otimes\bar{C})(\hat{\bar{x}}(t) - \hat{x}(t)) + \bar{\xi}(E_0(\hat{\bar{x}}(t),t))\end{aligned}$$

$$u(t) = \begin{cases} \alpha_1(\mathcal{L}_0\otimes R_1C)(x(t) - x_0(t)) + \alpha_1(\mathcal{L}_0\otimes R_1F_sE_s\\ +\mathcal{L}_0\otimes R_1D_2E_\omega)e_1(t) - (I_N\otimes K)\hat{\bar{x}}(t),\\ \quad t\in T_m(t_{2k},t)\\ \alpha_2(\mathcal{L}_{r(t)}\otimes R_2C)(x(t) - x_0(t)) + \alpha_2(\mathcal{L}_{r(t)}\otimes R_2\\ F_sE_s + \mathcal{L}_{r(t)}\otimes R_2D_2E_\omega)e_1(t) - (I_N\otimes K)\hat{\bar{x}}(t),\\ \quad t\in T_p(t_{2k+1},t)\end{cases} \tag{7}$$

then denote $e_1(t) = [e_{11}^T(t),\cdots,e_{N1}^T(t)]^T$, the consensus errors dynamics are obtained as:

$$\dot{e}_1(t) = \begin{cases} (I_N\otimes\bar{A} - \rho\mathcal{L}_0\otimes\bar{R}\bar{C})e_1(t) + (I_N\otimes\bar{M})\bar{d}(t)\\ \quad +\Delta\bar{\xi}(t), \quad t\in T_m(t_{2k},t)\\ (I_N\otimes\bar{A} - \rho\mathcal{L}_{r(t)}\otimes\bar{R}\bar{C})e_1(t) + (I_N\otimes\bar{M})\bar{d}(t)\\ \quad +\Delta\bar{\xi}(t), \quad t\in T_p(t_{2k+1},t)\end{cases} \tag{8}$$

where $\mathcal{L}$ is the Laplacian matrix, and $\mathcal{L}_{r(t)}$ and $\mathcal{L}_0$ are the Laplacian matrices of the switching graph $\mathcal{G}_{r(t)}$ and initial graph $\mathcal{G}_0$, respectively. $\Delta\bar{\xi}(t) = [\Delta\bar{\xi}_1^T,\cdots,\Delta\bar{\xi}_N^T]^T$ with $\Delta\bar{\xi}_i = \bar{\xi}(E_0\bar{x}_i(t),t) - \bar{\xi}(E_0\hat{\bar{x}}_i(t),t)$.

Subsequently, denote the consensus error between the leader and the ith follower as $e_{i2} = x_i(t) - x_0(t)$. Let $x(t) = [x_1^T(t),\cdots,x_N^T(t)]^T$, $f_a(t) = [f_{a1}^T(t),\cdots,f_{aN}^T(t)]^T$, and $\omega_1(t) = [\omega_{11}^T(t),\cdots,\omega_{N1}^T(t)]^T$, it is obtained that

$$\begin{aligned}\dot{x}(t) &= (I_N\otimes A)x(t) + (I_N\otimes B)u(t) + (I_N\otimes F_a)f_a(t)\\ &\quad +(I_N\otimes D_1)\omega_1(t) + \bar{\xi}(x(t),t))\\ \dot{x}_0(t) &= (I_N\otimes A)x_0(t) + (I_N\otimes B)u_0(t) + \bar{\xi}(x_0(t),t))\end{aligned} \tag{9}$$

then denote $e_2(t) = [e_{12}^T(t), \cdots, e_{N2}^T(t)]^T$, the dynamics of consensus errors are obtained as

$$\dot{e}_2(t) = \begin{cases} [I_N \otimes (A - BK_x) - \alpha_1(\mathcal{H}_0 \otimes BR_1C)]e_2(t) \\ -[\alpha_1(\mathcal{H}_0 \otimes BR_1F_sE_s) + \alpha_1(\mathcal{H}_0 \otimes BR_1D_2E_\omega) \\ -I_N \otimes BK]e_1(t) + e_\xi(t) + (I_N \otimes D_1)\omega_1(t), \\ \quad t \in T_m(t_{2k}, t) \\ [I_N \otimes (A - BK_x) - \alpha_2(\mathcal{H}_{r(t)} \otimes BR_2C)]e_2(t) \\ -[\alpha_2(\mathcal{H}_{r(t)} \otimes BR_2F_sE_s) + \alpha_2(\mathcal{H}_{r(t)} \otimes BR_2D_2 \\ E_\omega) - I_N \otimes BK]e_1(t) + e_\xi(t) + (I_N \otimes D_1)\omega_1(t), \\ \quad t \in T_p(t_{2k+1}, t) \end{cases} \tag{10}$$

where $\mathcal{H}_{r(t)}, \mathcal{H}_0$ are the information-exchange matrices of the switching graph $\mathcal{G}_{r(t)}$ and initial graph $\mathcal{G}_0$. $\mathcal{H}_{r(t)} = \mathcal{L}_{r(t)} + \mathcal{B}_{r(t)}$, and $\mathcal{B}_{r(t)} = diag\{b_1^{r(t)}, \cdots, b_N^{r(t)}\}$. Nonlinear consensus error $e_{\xi_i}(t) = \xi(x_i(t), t) - \xi(x_0(t), t)$ with $e_\xi(t) = [e_{\xi_1}^T(t), \cdots, e_{\xi_N}^T(t)]^T$. $E_s = [0_{q_2\times n}\ 0_{q_2\times q_1}\ I_{q_2}\ 0_{q_2\times s_2}]$, $E_\omega = [0_{s_2\times n}\ 0_{s_2\times q_1}\ 0_{s_2\times q_2}\ I_{s_2}]$.

B. Stability Analysis

To begin with, several variables characterizing the topology switching conditions under random cyber-attacks are introduced. Denote $\pi_{\min} = \min_{p\in S_1}\{\pi_p\}, S_1 = \{1, \cdots, s\}$. Furthermore, H_{un} and $\mathcal{L}_{un}$ are denoted as the information-exchange matrix and Laplacian matrix of the union of digraphs $\mathcal{G}_{un} = \bigcup_{p\in S}\mathcal{G}_p$, where $H_{un} = \sum_{p=1}^s H_p$ and $\mathcal{L}_{un} = \sum_{p=1}^s \mathcal{L}_p$. $\hat{H}_{un}$ and $\hat{\mathcal{L}}_{un}$ are denoted as the information-exchange matrix and Laplacian matrix of the corresponding united mirror of switching graph $\mathcal{G}_{r(t)}$ under random attacks. Then, define $\tilde{H} = He(H_{un})/\lambda_{\min}(\hat{H}_{un}), \hat{H} = (H_{un}H_{un}^T)/\lambda_{\min}(\hat{H}_{un})$, $\tilde{\mathcal{L}} = He(\mathcal{L}_{un})/\lambda_{\min}(\hat{\mathcal{L}}_{un})$, and $\hat{\mathcal{L}} = (\mathcal{L}_{un}\mathcal{L}_{un}^T)/\lambda_{\min}(\hat{\mathcal{L}}_{un})$.

Theorem 1: The asymptotic exponential consensus of the nonlinear cyber-physical MASs (1) and (2) in the coexistence of multiple abrupt-incipient faults, unknown bounded channel noises, and random cyber-attacks modeled by a Markov process is achieved through the double-layer distributed observer-controller framework (5) and (6) when the following conditions hold:

(1) Given positive scalars $\chi_1, \chi_2, \chi_3, \chi_4$ and identity matrix $\mathcal{I} = I_{n+q_1+q_2+s_2}$, there exist symmetric matrices $P > 0, S > 0$ such that

$$He(PX) + \theta_{\max}(\lambda_2 PD_1D_1^TP + (1+\rho'^2)\lambda_2P^2) < -\chi_1 P \tag{11}$$

$$He(SX) + SD_1D_1^TS + (1+\rho'^2)S^2 < \chi_3 S \tag{12}$$

$$\begin{aligned} &\tfrac{1}{\tau_1}(He(\bar{A} - \rho\lambda_4\bar{R}\bar{C}) + \bar{M}\bar{M}^T + \rho'^2E_0^TE_0) + \lambda_2K^TK \\ &-\alpha_1\lambda_3(E_s^TF_s^TR_1^TR_1F_sE_s + E_\omega^TD_2^TR_1^TR_1D_2E_\omega) < -\chi_2\mathcal{I} \end{aligned} \tag{13}$$

$$\begin{aligned} &\tfrac{1}{\tau_4}(He(\bar{A}) - \bar{R}\bar{C} + \bar{M}\bar{M}^T + \rho'^2E_0^TE_0) + K^TK \\ &-\alpha_2(E_s^TF_s^TR_2^TR_2F_sE_s + E_\omega^TD_2^TR_2^TR_2D_2E_\omega) < \chi_4\mathcal{I} \end{aligned} \tag{14}$$

where $X = A - BK_x$. The coupling coefficients are satisfied with $\alpha_1 \geq \frac{\lambda_2 L}{\lambda_1+\lambda_3}$, and $\alpha_2 \geq \frac{T}{\pi_{\min}(\lambda_{\min}(\tilde{H})+\lambda_{\min}(\hat{H}))}$, where $L > 0$ and $T > 0$, $\lambda_1 = \lambda_{\min}(He(\Theta\mathcal{H}_0)), \lambda_2 = \lambda_{\min}(\Theta^2), \lambda_3 = \lambda_{\min}(\Theta\mathcal{H}_0\mathcal{H}_0^T\Theta)$, $\lambda_4 = \lambda_{\min}(\mathcal{L}_0 + \mathcal{L}_{r(t)})$, and $\rho \geq \frac{1}{\pi_{\min}(\lambda_{\min}(\tilde{\mathcal{L}})+\lambda_{\min}(\hat{\mathcal{L}}))}$. Matrix $\Theta = diag\{\theta_1^{-1}, \cdots, \theta_N^{-1}\}$ with $\theta = [\theta_1^{-1}, \cdots, \theta_N^{-1}] = (\mathcal{H}_0)^{-1}\mathbf{1}$, $\theta_{\max} = \max\{\theta_i\}$, and $\theta_{\min} = \min\{\theta_i\}$, $i = 1, \cdots, N$. Meanwhile, $\max(\frac{\epsilon_a}{\chi_2} - \sqrt{\frac{\epsilon_a^2}{\chi_2^2} - \frac{\tau_2}{\chi_2}}, \frac{\epsilon_s}{\chi_2} - \sqrt{\frac{\epsilon_s^2}{\chi_2^2} - \frac{\tau_2}{\chi_2}}) \leq \tau_1 \leq \min(\frac{\epsilon_a}{\chi_2} + \sqrt{\frac{\epsilon_a^2}{\chi_2^2} - \frac{\tau_2}{\chi_2}}, \frac{\epsilon_s}{\chi_2} + \sqrt{\frac{\epsilon_s^2}{\chi_2^2} - \frac{\tau_2}{\chi_2}})$, $0 < \tau_2 \leq \frac{\epsilon_a^2}{\chi_2}, 0 < \tau_3 \leq \frac{\epsilon_s^2}{\chi_2}$, $\tau_4 < \min(-\frac{\bar{\epsilon}_a}{\chi_4} - \sqrt{\frac{\bar{\epsilon}_a^2}{\chi_4^2} + \frac{\tau_5}{\chi_4}}, -\frac{\bar{\epsilon}_s}{\chi_4} - \sqrt{\frac{\bar{\epsilon}_s^2}{\chi_4^2} + \frac{\tau_5}{\chi_4}})$ or $\tau_4 > \max(-\frac{\bar{\epsilon}_a}{\chi_4} + \sqrt{\frac{\bar{\epsilon}_a^2}{\chi_4^2} + \frac{\tau_5}{\chi_4}}, -\frac{\bar{\epsilon}_s}{\chi_4} + \sqrt{\frac{\bar{\epsilon}_s^2}{\chi_4^2} + \frac{\tau_5}{\chi_4}})$, $\tau_5 > 0$ and $\tau_6 > 0$.

(2) The coupling gains are designed as $R_1 = L^{-1}B^TP(C^TC)^{-1}C^T, R_2 = T^{-1}B^TS(C^TC)^{-1}C^T$, the observer gain is designed as $\bar{R} = \bar{C}^T$, and the compensation gain is designed as $K_x = (B^TB)^{-1}B^TP^{-1}$. There exist constants $\gamma \in (0, \gamma^*)$ and $\gamma^* \in (0, \eta_m)$ such that the attack frequency and attack length rate are constrained within

$$\begin{cases} F_a(t_0, t) \leq \frac{1}{2}\ln^{-1}(\frac{N}{\tau_1}\mu(1+\tau_1)\bar{\omega}_1^2 + \bar{\omega}_2^2)(\gamma^* - \gamma) \\ \mathcal{R}_{T_m}(t_0, t) \geq \frac{\eta_p+\gamma^*}{\eta_m+\eta_p}, \quad \mathcal{R}_{T_p}(t_0, t) \leq \frac{\eta_m-\gamma^*}{\eta_m+\eta_p} \end{cases} \tag{15}$$

where $\mu = \max\{\theta_{\max}\lambda_{\max}(P)/\lambda_{\min}(S), -\lambda_{\max}(S)/(\theta_{\min}\lambda_{\min}(P))\} \geq 1$. $\bar{\omega}_1 = \max(\omega_{i1})$, $\bar{\omega}_2 = \max(\omega_{i2})$, $\eta_m = \min(\chi_1, \chi_2\tau_1)$, and $\eta_p = \max(\chi_3, \chi_4\tau_4)$.

Thus, the consensus error with the mathematical expectation form is achieved as follows

$$\mathscr{E}\{||e_{i2}(t)||^2\} \leq \bar{\xi}\phi e^{-\gamma(t-t_0)}\mathscr{E}\{||e_{i2}(t_0)||^2\}, i = 1, \cdots, N \tag{16}$$

with $\phi = \psi_1/\psi_2$, $\psi_1 = \max\{\lambda_{\max}(\theta_i^{-1}P^{-1}), \lambda_{\max}(S^{-1})\}$ and $\psi_2 = \min\{\lambda_{\min}(\theta_i^{-1}P^{-1}), \lambda_{\min}(S^{-1})\}$. $\bar{\xi} = \min(\xi_1, \xi_2)$, $\xi_1 = \frac{N}{\tau_1}(1+\tau_1)\bar{\omega}_1^2 + \bar{\omega}_2^2$, and $\xi_2 = \frac{N}{\tau_4}(1+\tau_4)\bar{\omega}_1^2 + \bar{\omega}_2^2$.

Proof: Due to the presence of random cyber-attacks for nonlinear cyber-physical MASs, the stability analysis is divided into two cases: non-attacks and random attacks.

(i) (Non-attacks): Choose a Lyapunov candidate as

$$V_a(t) = e_2^T(t)(\Theta \otimes P)e_2(t) \tag{17}$$

where $\Theta = diag\{\theta_1^{-1}, \cdots, \theta_N^{-1}\}$, and P is the positive definite matrix. Based on $R_1 = L^{-1}B^TP(C^TC)^{-1}C^T$, the time derivative of $V_a(t)$ in (17) is derived as

$$\begin{aligned} \dot{V}_a(t) &\leq e_2^T(t)[\Theta \otimes He(PX) + \theta_{\max}(\lambda_2PD_1D_1^TP + \lambda_2P^2) \\ &-\theta_{\min}(\alpha_1\lambda_1L^{-1} - \lambda_2 + \alpha_1\lambda_3L^{-1})PBB^TP]e_2(t) \\ &+\theta_{\max}\lambda_2e_\xi^T(t)e_\xi(t) + \mathcal{J} \leq e_2^T(t)[\Theta \otimes He(PX) \\ &+\theta_{\max}(\lambda_2PD_1D_1^TP + (1+\rho'^2)\lambda_2P^2]e_2(t) + \mathcal{J} \end{aligned} \tag{18}$$

where $\mathcal{J} = e_1^T(t)[I_N \otimes (\lambda_2K^TK - \alpha_1\lambda_3(E_s^TF_s^TR_1^TR_1F_sE_s + E_\omega^TD_2^TR_1^TR_1D_2E_\omega))]e_1(t) + \lambda_2\omega_1^T(t)\omega_1(t), X = A - BK_x$. $\theta_{\min} = \min(\theta_i), i = 1, \cdots, N. \lambda_1 = \lambda_{\min}(He(\Theta\mathcal{H}_0)), \lambda_2 = \lambda_{\max}(\Theta^2), \lambda_3 = \lambda_{\min}(\Theta\mathcal{H}_0\mathcal{H}_0^T\Theta)$, and the coupling coefficient is constrained within $\alpha_1 \geq \frac{\lambda_2 L}{\lambda_1+\lambda_3}$.

With the scalars $\tau_1 > 0, \tau_2 > 0, \tau_3 > 0$, another Lyapunov function is designed as

$$V_b(t) = \tfrac{1}{\tau_1}e_1^T(t)e_1(t) + \tfrac{1}{\tau_2}\dot{f}_a^T(t)\dot{f}_a(t) + \tfrac{1}{\tau_3}\dot{f}_s^T(t)\dot{f}_s(t) \tag{19}$$

The second-order derivatives of the multiple actuator/sensor faults $f_{ai}^\varrho(t), f_{si}^\varrho(t)$ corresponding with the unified abrupt-incipient fault type are represented as

$$\begin{aligned} \ddot{f}_{ai}^\varrho(t) &= -(\varepsilon_a^\varrho)^2e^{-\varepsilon_a^\varrho(t-T_a^\varrho)}\bar{f}_{ai}^\varrho = -\varepsilon_a^\varrho\dot{f}_{ai}^\varrho(t), \varrho = 1, \cdots, q_1 \\ \ddot{f}_{si}^\varrho(t) &= -(\varepsilon_s^\varrho)^2e^{-\varepsilon_s^\varrho(t-T_s^\varrho)}\bar{f}_{si}^\varrho = -\varepsilon_s^\varrho\dot{f}_{si}^\varrho(t), \varrho = 1, \cdots, q_2 \end{aligned} \tag{20}$$

Subsequently, the time derivative of $V_b(t)$ is acquired as

$$\begin{aligned}&\dot{V}_b(t) \leq \tfrac{1}{\tau_1} e_1^T(t)[I_N \otimes He(\bar{A} - \rho\lambda_4 \bar{R}\bar{C}) + \bar{M}\bar{M}^T \\ &+\rho'^2 E_0^T E_0]e_1(t) + \tfrac{1+\tau_1}{\tau_1}\omega_1^T(t)\omega_1(t) + \tfrac{1}{\tau_1}\dot{\omega}_2^T(t)\dot{\omega}_2(t) \\ &+(\tfrac{1}{\tau_1} - \tfrac{2\varepsilon_a}{\tau_2})\dot{f}_a^T(t)\dot{f}_a(t) + (\tfrac{1}{\tau_1} - \tfrac{2\varepsilon_s}{\tau_3})\dot{f}_s^T(t)\dot{f}_s(t)\end{aligned} \tag{21}$$

where $\lambda_4 = \lambda_{\min}(\mathcal{L}_0 + \mathcal{L}_{r(t)})$, and define $V_1(t) = V_a(t) + V_b(t)$, and according to the inequalities (11) and (13), the time derivative of $V_1(t)$ is derived as

$$\begin{aligned}&\dot{V}_1(t) \leq -\chi_1 V_a(t) - \chi_2\tau_1 V_b(t) + \mathcal{M} + (\tfrac{\chi_2\tau_1 - 2\varepsilon_a}{\tau_2} + \tfrac{1}{\tau_1}) \\ &\dot{f}_a^T(t)f_a(t) + (\tfrac{\chi_2\tau_1 - 2\varepsilon_s}{\tau_3} + \tfrac{1}{\tau_1})\dot{f}_s^T(t)f_s(t) \\ &\leq -\min(\chi_1, \chi_2\tau_1)V_1(t) + \mathcal{M}\end{aligned} \tag{22}$$

where $\mathcal{M} = \frac{1+\tau_1}{\tau_1}\omega_1^T(t)\omega_1(t) + \frac{1}{\tau_1}\dot{\omega}_2^T(t)\dot{\omega}_2(t)$, $\frac{\chi_2\tau_1 - 2\varepsilon_a}{\tau_2} + \frac{1}{\tau_1} \leq 0$, $\frac{\chi_2\tau_1 - 2\varepsilon_s}{\tau_3} + \frac{1}{\tau_1} \leq 0$ based on the constraints of scalars τ_1, τ_2 and τ_3.

Let $\eta_m = \min(\chi_1, \chi_2\tau_1)$ and $\xi_1 = \frac{N}{\tau_1}(1+\tau_1)\bar{\omega}_1^2 + \bar{\omega}_2^2$ with $\bar{\omega}_1 = \max(\omega_{i1})$, and $\bar{\omega}_2 = \max(\omega_{i2})$, it follows that

$$V_1(t) \leq \xi_1 e^{-\eta_m(t-t_0)}V_1(t_0) + \tfrac{\xi}{\eta_m} \tag{23}$$

ii (Random attacks): Select stochastic Lyapunov functions

$$V_c^p(t) = \mathscr{E}[e_2^T(t)(I_N \otimes S)e_2(t)\Gamma_p] \tag{24}$$

$$V_d^p(t) = \mathscr{E}[\frac{1}{\tau_4}e_1^T(t)e_1(t) + \frac{1}{\tau_5}\dot{f}_a^T(t)\dot{f}_a(t) + \frac{1}{\tau_6}\dot{f}_s^T(t)\dot{f}_s(t)\Gamma_p] \tag{25}$$

where $\tau_4 > 0, \tau_5 > 0, \tau_6 > 0$. $V_c^p(t)$ and $V_d^p(t)$ denote the stochastic types of the Lyapunov functions $V_c(t)$ and $V_d(t)$ when $r(t) = p, p \in S_1$. $r(t)$ represents the topology switching signal inspired by random cyber-attacks, and when $r(t) = p, \Gamma_p = 1$, conversely $\Gamma_p = 0$.

Then, the derivative of $V_c^p(t)$ is obtained as

$$\begin{aligned}&\mathscr{E}\{\dot{V}_c^p(t)\} = \mathscr{E}\{2e_2^T(t)(I_N \otimes S)\dot{e}_2(t) + \sum_{q=1}^{s}\gamma_{pq}V_c^p(t)dt \\ &+o(dt)\}\end{aligned} \tag{26}$$

and according to Assumptions 4 and 5, the coupling coefficient is chosen as $\alpha_2 \geq \frac{T}{\pi_{\min}(\lambda_{\min}(\tilde{H}) + \lambda_{\min}(\hat{H}))}$, $\pi_{\min} = \min_{p\in S_1}\{\pi_p\}$, and the gain matrix is chosen as $R_2 = T^{-1}B^TS(C^TC)^{-1}C^T$, it follows that

$$\begin{aligned}&\mathscr{E}\{\dot{V}_c(t)\} \leq \mathscr{E}\{e_2^T(t)[I_N \otimes He(SX) + SD_1D_1^TS + S^2 \\ &-\pi_{\min}\alpha_2(T^{-1}(\lambda_{\min}(\tilde{H}) + \lambda_{\min}(\hat{H})) - 1)SBB^TS]e_2(t) \\ &+e_\xi^T(t)e_\xi(t) + \mathcal{J}_1\} \\ &\leq \mathscr{E}\{e_2^T(t)[I_N \otimes He(SX) + SD_1D_1^TS + (1+\rho'^2)S^2]e_2(t) \\ &+\mathcal{J}_1\}\end{aligned} \tag{27}$$

with $\mathcal{J}_1 = e_1^T(t)[I_N \otimes (K^TK - \alpha_1(E_s^TF_s^TR_2^TR_2F_sE_s + E_\omega^TD_2^TR_2^TR_2D_2E_\omega))]e_1(t) + \omega_1^T(t)\omega_1(t)$, $\tilde{H} = He(H_{un})/\lambda_{\min}(\hat{H}_{un})$, and $\hat{H} = (H_{un}H_{un}^T)/\lambda_{\min}(\hat{H}_{un})$.

Similar to (27), the derivative of $V_d(t)$ is obtained that

$$\begin{aligned}&\mathscr{E}\{\dot{V}_d(t)\} \leq \mathscr{E}\{\tfrac{1}{\tau_4}e_1^T(t)[I_N \otimes He(\bar{A}) - \rho He(\mathcal{L}_p \otimes \bar{R}\bar{C}) \\ &+\bar{M}\bar{M}^T + \rho'^2E_0^TE_0]e_1(t) + (\tfrac{1}{\tau_4} - \tfrac{2\varepsilon_a}{\tau_5})\dot{f}_a^T(t)\dot{f}_a(t) + \tfrac{1+\tau_4}{\tau_4} \\ &\omega_1^T(t)\omega_1(t) + \tfrac{1}{\tau_4}\dot{\omega}_2^T(t)\dot{\omega}_2(t) + (\tfrac{1}{\tau_4} - \tfrac{2\varepsilon_s}{\tau_6})\dot{f}_s^T(t)\dot{f}_s(t)\} \\ &\leq \mathscr{E}\{\tfrac{1}{\tau_4}e_1^T(t)[I_N \otimes He(\bar{A}) - \bar{R}\bar{C} + \bar{M}\bar{M}^T \\ &+\rho'^2E_0^TE_0]e_1(t) + \tfrac{1+\tau_4}{\tau_4}\omega_1^T(t)\omega_1(t) + \tfrac{1}{\tau_4}\dot{\omega}_2^T(t)\dot{\omega}_2(t)\} \\ &+(\tfrac{1}{\tau_4} - \tfrac{2\varepsilon_a}{\tau_5})\dot{f}_a^T(t)\dot{f}_a(t) + (\tfrac{1}{\tau_4} - \tfrac{2\varepsilon_s}{\tau_6})\dot{f}_s^T(t)\dot{f}_s(t)\}\end{aligned} \tag{28}$$

with the coupling strength $\rho \geq \frac{1}{\pi_{\min}(\lambda_{\min}(\tilde{\mathcal{L}}) + \lambda_{\min}(\hat{\mathcal{L}}))}$. $\tilde{\mathcal{L}} = He(\mathcal{L}_{un})/\lambda_{\min}(\hat{\mathcal{L}}_{un})$, $\hat{\mathcal{L}} = (\mathcal{L}_{un}\mathcal{L}_{un}^T)/\lambda_{\min}(\hat{\mathcal{L}}_{un})$.

Denote $V_2(t) = V_c(t) + V_d(t)$, based on (12) and (14), the derivative of $V_2(t)$ is obtained that

$$\begin{aligned}&\mathscr{E}\{\dot{V}_2(t)\} \leq \mathscr{E}\{\chi_3V_c(t) + \tau_4\chi_4V_d(t) + \mathcal{M}_1 + (-\tfrac{\chi_4\tau_4 + 2\varepsilon_a}{\tau_5} \\ &+\tfrac{1}{\tau_4})\dot{f}_a^T(t)\dot{f}_a(t) + (-\tfrac{\chi_4\tau_4 - 2\varepsilon_s}{\tau_6} + \tfrac{1}{\tau_4})\dot{f}_s^T(t)\dot{f}_s(t)\} \\ &\leq \mathscr{E}\{\max(\chi_3, \chi_4\tau_4)V_2(t) + \mathcal{M}_1\}\end{aligned} \tag{29}$$

where $\mathcal{M}_1 = \frac{1+\tau_4}{\tau_4}\omega_1^T(t)\omega_1(t) + \frac{1}{\tau_4}\dot{\omega}_2^T(t)\dot{\omega}_2(t)$, $-\frac{\chi_4\tau_4 + 2\varepsilon_a}{\tau_5} + \frac{1}{\tau_4} \leq 0$, $-\frac{\chi_4\tau_4 - 2\varepsilon_s}{\tau_6} + \frac{1}{\tau_4} \leq 0$ based on the constrains of scalars τ_4, τ_5 and τ_6.

Let $\eta_p = \max(\chi_3, \chi_4\tau_4)$, and $\xi_2 = \frac{N}{\tau_4}(1+\tau_4)\bar{\omega}_1^2 + \bar{\omega}_2^2$ with $\bar{\omega}_1 = \max(\omega_{i1})$, and $\bar{\omega}_2 = \max(\omega_{i2})$, it follows that

$$\mathscr{E}\{V_2(t)\} \leq \xi_2 e^{\eta_p(t-t_0)}\mathscr{E}\{V_2(t_0)\} - \tfrac{\xi}{\eta_p} \tag{30}$$

To analyze the overall stability of the cyber-physical MASs, choose a piece-wise Lyapunov function as

$$V(t) = \begin{cases} V_1(t), & t \in T_m(t_{2k}, t) \\ V_2(t), & t \in T_p(t_{2k+1}, t) \end{cases} \tag{31}$$

where $V_1(t)$ represents the MASs that remain unaffected by attacks during the time period $T_m(t_{2k}, t)$, while $V_2(t)$ represents the MASs that experience random cyber-attacks within the time period $T_p(t_{2k+1}, t)$.

Let $\bar{\xi} = \min(\xi_1, \xi_2)$, according to (23) and (30), the piece-wise Lyapunov function (31) with expectation is acquired as

$$\mathscr{E}\{V(t)\} < \bar{\xi}e^{\eta_pT_p(t_{2k+1},t) - \eta_mT_m(t_{2k},t)}\mathscr{E}\{V(t_{2k})\} \tag{32}$$

It is derived that the number of random attacks $N_a(t_0, t) = k$ for $t \in T_m(t_{2k}, t)$ and $N_a(t_0, t) = k+1$ for $t \in T_p(t_{2k+1}, t)$ from Definition 2. Therefore, for any $t \geq t_0$, it holds that

$$\begin{aligned}&\mathscr{E}\{V(t)\} < \bar{\xi}e^{\eta_pT_p(t_{2k+1},t) - \eta_mT_m(t_{2k},t)}\mathscr{E}\{V(t_{2k})\} \\ &< \bar{\xi}^2\mu e^{\eta_pT_p(t_{2k},t) - \eta_mT_m(t_{2k-1},t)}\mathscr{E}\{V(t_{2k-1})\} \\ &< \cdots < \bar{\xi}^{2k+1}\mu^{2k}e^{\eta_pT_p(t_0,t) - \eta_mT_m(t_0,t)}\mathscr{E}\{V(t_0)\} \\ &= \bar{\xi}e^{2N_a(t_0,t)\ln(\bar{\xi}\mu) + \eta_pT_p(t_0,t) - \eta_mT_m(t_0,t)}\mathscr{E}\{V(t_0)\}\end{aligned} \tag{33}$$

According to the inequalities (15), it is derived as $2N_a(t_0, t)\ln(\bar{\xi}\mu) \leq (\gamma^* - \gamma)(t - t_0)$ and $\eta_pT_p(t_0, t) - \eta_mT_m(t_0, t) \leq -\gamma^*(t - t_0)$. Then, it is obtained that

$$e^{2N_a(t_0,t)\ln(\bar{\xi}\mu) + \eta_pT_p(t_0,t) - \eta_mT_m(t_0,t)} \leq e^{-\gamma(t-t_0)} \tag{34}$$

and substituting (34) into (33) yields that

$$\mathscr{E}\{V(t)\} < \bar{\xi}e^{-\gamma(t-t_0)}\mathscr{E}\{V(t_0)\} \tag{35}$$

Finally, the consensus error expectation is expressed as

$$\mathscr{E}\{||e_{i2}(t)||^2\} \leq \bar{\xi}\phi e^{-\gamma(t-t_0)}\mathscr{E}\{||e_{i2}(t_0)||^2\} \tag{36}$$

From (36), it can be seen that the exponential convergence of consensus error is achieved, and also illustrates that $x_i(t) \to x_0(t)$ as $t \to +\infty$. That is the consensus control purpose of nonlinear MASs under complex CPTs is achieved through the double-layer distributed observer-controller algorithm.

Remark 4: In addressing the FTCC issue in leader-follower MASs, it is customary to furnish predetermined anticipated states for the leader, concurrently accounting for follower coordination to trace the leader and engage in collaborative endeavors. The existence of a faulty leader not only impinges upon FTCC among followers but also necessitates the incorporation of supplementary fault compensation terms into the leader's controller. Moreover, the absence of fault-tolerant mechanisms for the leader engenders task failure or degradation. In contrast to the introduction of faults, the methodology of suppressing input/output channel noises in the leader's model bears a resemblance to the noise-resistant strategy applied to the follower's model. In instances where both leader and follower channel noise errors persist and are unknown but bounded, the proposed double-layer distributed FTCC algorithm can be deployed for resolution. Under these circumstances, the bounded conditions are stipulated as follows: for $c_1, c_2 > 0$, it is asserted that $||\Delta_{\omega_1}|| \leq c_1$ and $||\Delta_{\dot{\omega}_2}|| \leq c_2$, where ω_{01} and ω_{02} denote the input and output noise of the leader, and $\Delta_{\omega_1} = \omega_{01} - \omega_{i1}$, $\Delta_{\dot{\omega}_2} = \dot{\omega}_{02} - \dot{\omega}_{i2}$.

IV. Simulation Results

In this section, the effectiveness and validity of the comparative analysis (decentralized observer and distributed controller framework [29] and the proposed double-layer distributed observer-controller framework) is demonstrated through the presentation of two simulation cases. Case 1 pertains to the multi- unmanned aerial vehicles (UAVs) systems, while case 2 focuses on the multi-machine power systems.

A. Case 1: multi-UAV systems

A simulation case of UAVs with five followers and a leader is carried out. The dynamic behavior corresponds to the lateral dynamics of the UAV as follows [30]:

$$A = \begin{bmatrix} -0.0277 & 0 & 3.29 & 0.981 \\ -0.0103 & -0.8325 & 0.375 & 0 \\ 0.0365 & 0 & -0.0639 & 0 \\ 0 & 0.1 & 0 & 0 \end{bmatrix},$$
$$B = \begin{bmatrix} -0.543 & 0 \\ 0 & -2.864 \\ -0.949 & 0 \\ 0 & 0 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (37)$$

The input channel noise $\omega_{i1}(t)$ and output channel noise $\omega_{i2}(t)$ are set as $\omega_{i1}(t) = 0.9\sin(0.8t), \omega_{i2}(t) = 0.5\cos(1.5t)$, and the noise-described gain matrices are settled as $D_1 = [0.8, 0.9, 1, 0]^T, D_2 = [0.85, 0.95]^T$, respectively. The Lipschitz state-depended nonlinearity is given as $\xi(x_i(t), t) = \sum_{j=1}^{5} \sin(x_{i1} - x_{j1})$. The actuator fault gain matrix is selected as $F_a = [-5.432, 0, -9.49, 0]^T$, and the sensor fault gain matrix is selected as $F_s = [1.5, 0.8]^T$. Define the upper and lower boundaries of the decay rates as $\bar{\varepsilon}_{a(s)} = 0.5, \underline{\varepsilon}_{a(s)} = 0.05$. Then the multiple unified actuator/sensor faults $f_{ai}(t), f_{si}(t)$ are set as

$$f_{ai}(t) = \begin{cases} 0, 0s \leq t < 10s \\ 2(1 - e^{10-t}), 10s \leq t < 30s \\ 2(1 - e^{-20}) - 4(1 - e^{30-t}), 30s \leq t < 50s \end{cases}$$
$$f_{si}(t) = \begin{cases} 2(1 - e^{-0.5t}), 0s \leq t < 15s \\ 2, 15s \leq t < 30s \\ 2 - 2(1 - e^{1.5-0.05t}), 30s \leq t < 50s \end{cases} \quad (38)$$

The random cyber-attacks are modeled by the Markov process, where the initial distribution is $\pi_0 = [0.6, 0.15, 0.25]$, and the generator matrix is set as $\Xi = \begin{bmatrix} -0.1 & 0.02 & 0.08 \\ 0.3 & -0.5 & 0.2 \\ 0.1 & 0.1 & -0.2 \end{bmatrix}$.

The control parameters of Theorem 1 are configured as $\alpha_1 = 15, \alpha_2 = 10, \rho = -3$. Scalar values $L = 100$, $T = 0.05$, $Q = 2I$, and $\bar{\tau} = 0.1$ are selected, and control gain matrices are determined through the application of the Riccati equation ($PA + A^TP - PBL^{-1}B^TP + Q = 0$) and Riccati inequality ($SA + A^TS - SBT^{-1}B^TS - \bar{\tau}S < 0$). The fault-estimation gain is denoted as $K_b = [0.7534, 0]^T$, while the coupling gains R_1, R_2, and the state-estimation gain K_x are computed by implementing the formulas stipulated in Theorem 1:

$$R_1 = \begin{bmatrix} 0.0946 & 0.0142 & -0.8273 & 0.2492 \\ -0.0062 & -0.0539 & 0.0464 & -0.2063 \end{bmatrix},$$
$$R_2 = \begin{bmatrix} 0.0198 & 0.0360 & -1.0318 & 0.3678 \\ -0.0067 & -0.0220 & 0.1049 & -0.2277 \end{bmatrix},$$
$$K_x = \begin{bmatrix} -0.2490 & -0.0022 & -0.0410 & -0.0012 \\ -0.0079 & -0.3051 & 0.0036 & 0.0322 \end{bmatrix}.$$

The topology switching signal $r(t)$ depicted in Fig. 2 illustrates the stochastic variations in the communication topology among $\mathcal{G}_1, \mathcal{G}_2$, and $\mathcal{G}_3$ under random cyber-attacks for the time interval $t \in [0s, 50s]$. Fig. 3 demonstrates the precise estimation results of multiple actuator and sensor faults using the

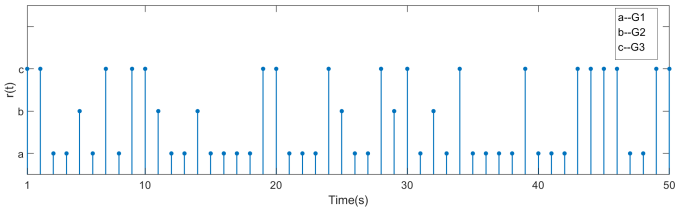

Fig. 2: Topology switching signal $r(t)$

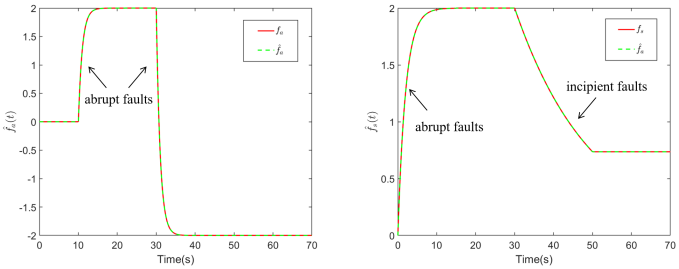

Fig. 3: Estimation of unified abrupt-incipient actuator faults and sensor faults

proposed distributed normalized observer. The plot illustrates the exact jump times for both actuator faults (occurring at 10s and 30s) and sensor faults (occurring at 15s and 30s).

In the presence of simultaneous sensor faults, actuator faults, input channel noise, and output channel noise in the physical layer, the consensus errors of the five followers depicted in Fig. 4 - Fig. 7 demonstrate that each state element of $e_{i2}(t) = x_i(t) - x_0(t)$ can ultimately reach consensus and convergence in suitable time. The continuously fluctuating trend observed in the consensus error state is undeniably influenced by channel noises and their configuration. Additionally, the variations in the peak values of the state variables can be attributed to the occurrence of multiple abrupt-incipient sensor/actuator faults in the following three scenarios: firstly, only sensor faults exist from 0s to 10s; secondly, sensor faults coexist with actuator faults from 10s to 50s; and finally, no faults are present from 50s to 70s.

Taking further into consideration the influence of random cyber-attacks on the consensus control of nonlinear MASs, Figs. 8 - 11 illustrate the concurrent impact of multiple CPTs (sensor/actuator fault, input/output noises, and random cyber-attacks). As depicted in Fig. 2, alterations in the communication topology lead to irregular fluctuations in the consensus errors. Specifically, when the communication topology undergoes continuous changes, these fluctuations become more pronounced, whereas they remain relatively minor otherwise. These findings offer further evidence that the security and safety performance, as well as the consensus control indicators of the nonlinear MASs, can be effectively maintained even when faced with the occurrence of aperiodic random attacks, multiple physical faults, and simultaneous channel noises.

B. Case 2: multi-machine power systems

The state of the i-th machine ($i = 1, \cdots, 5$) within the dynamic model of the power system is articulated as $x_i = [\Delta\sigma_i^T, \Delta\omega_i^T, \Delta P_{mi}^T, \Delta X_{ei}^T]^T$, where $\Delta\sigma_i$, $\Delta\omega_i$, ΔP_{mi}, and ΔX_{ei} denote the deviation of rotor angular velocity, relative speed, mechanical power, and steam valve aperture, respectively. Moreover, the consensus error between the leader and followers is expressed as $e_i = [e_{i2}^{\sigma}, e_{i2}^{\omega}, e_{i2}^{P}, e_{i2}^{X}]^T$. Thus, the matrix delineating the dynamic behavior of the multi-machine power systems is as follows [21]:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -0.2941 & 30.7999 & 0 \\ 0 & 0 & -2.8571 & 2.8571 \\ 0 & 0.6366 & 0 & -10 \end{bmatrix},$$
$$B = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 10 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad (39)$$

In both cases 1 and 2, consistent physical models are maintained, resulting in parallel configurations for input/output noises and actuator/sensor faults. Case 2 mirrors the choices made in Case 1, encompassing dynamic models and associated matrix information. A focused comparative analysis of FTCC effectiveness against noises and faults in the physical layer is

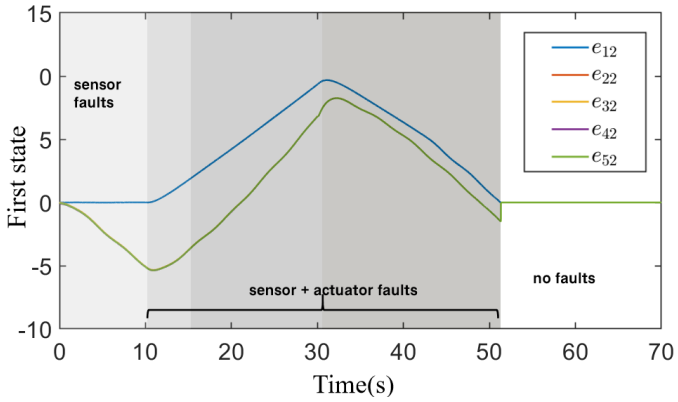

Fig. 4: First state of the consensus error with non-attacks

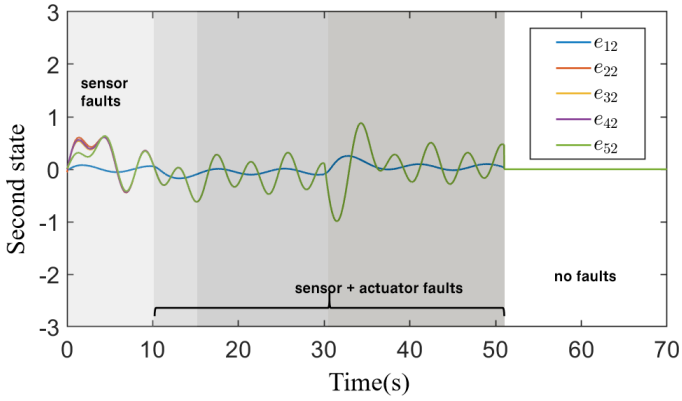

Fig. 5: Second state of the consensus error with non-attacks

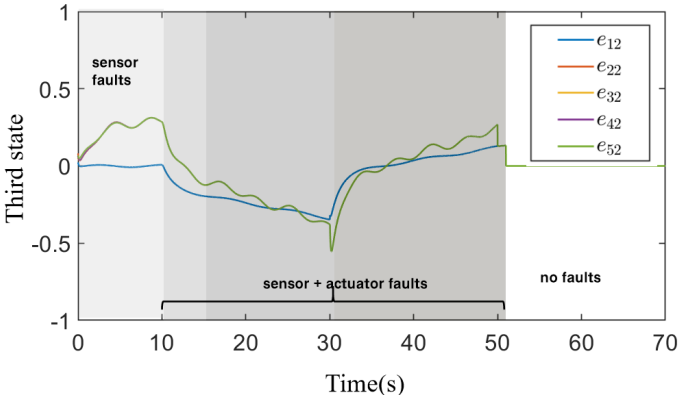

Fig. 6: Third state of the consensus error with non-attacks

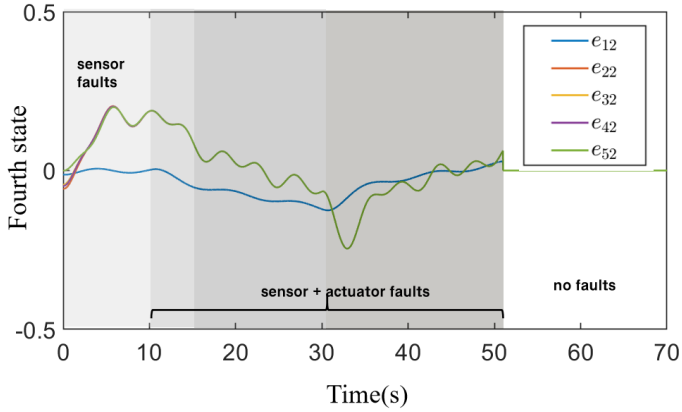

Fig. 7: Fourth state of the consensus error with non-attacks

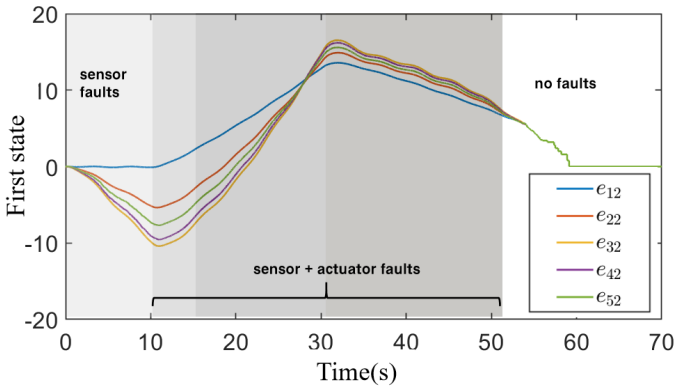

Fig. 8: First state of consensus error with random attacks

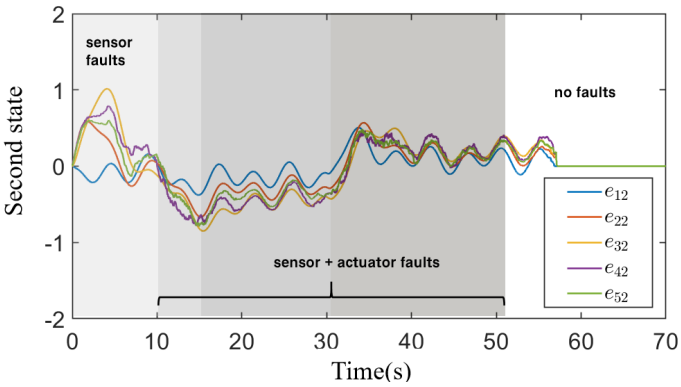

Fig. 9: Second state of consensus error with random attacks

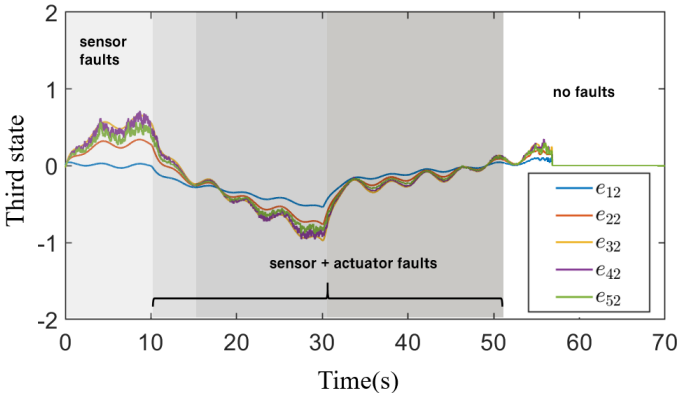

Fig. 10: Third state of consensus error with random attacks

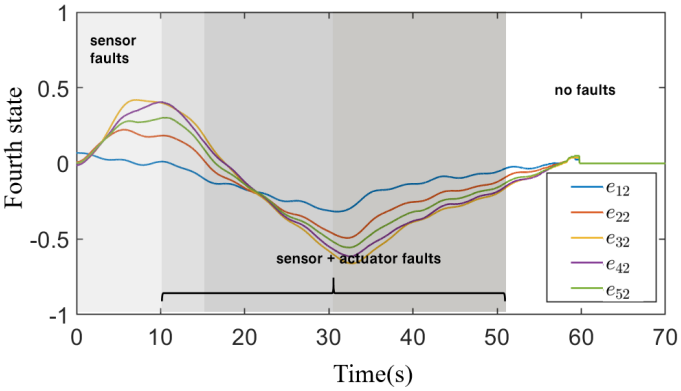

Fig. 11: Fourth state of consensus error with random attacks

conducted, which is motivated by the alignment between the employed attack modeling concept and principles discussed in [29]. In accordance with the stipulated requirements, the prescribed control parameters manifest as $\alpha_1 = 0.5$, $\rho = -5$, and $\bar{R} = \begin{bmatrix} 0.1 & 0 & 0.5 & 0.8 & 0 & 1.8 & 2.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^T$. Thus, the matrices of control gain, state-estimation gain, and fault-estimation gain are derived as $R_1 = [0.1414, 0.2651, 1.7536, 0.42198]$, $K_x = [0.0137, 0.3339, -0.2297, 0.7632]$, and $K_b = [0.15]$.

With the existence of multiple physical faults and channel noises in the physical layer, substantial fluctuations in rotor angular velocity, relative speed, mechanical power, and steam valve aperture deviation errors manifest during fault occurrences, as depicted in Figs. 12 - 15. Nevertheless, the double-layer distributed observer-controller framework adeptly achieves efficient and expeditious convergence. Noteworthy are two salient observations: 1) Abrupt faults at 10s and 30s of actuators/sensors markedly influence the consensus error signal. Specifically, faults characterized by larger amplitudes and faster rates tend to manifest spikes at each fault occurrence moment. Owing to highly robust compensation mechanism of FTCC law, multiple physical faults at 0s and 15s, concomitant with channel noises, are effectively attenuated to insignificance. 2) The double-layer distributed observer-controller framework proposed in this paper demonstrates superior convergence speed, reduced oscillation amplitudes, and heightened robustness to sinusoidal noises when compared with the decentralized observer and distributed controller framework [29]. Additionally, as time progresses, the convergence trend of the consensus error demonstrates a more desirable behavior with fluctuations around a value in proximity to zero.

V. Conclusion

A novel double-layer observer-controller framework operating in a distributed strategy for fault-tolerant consensus is proposed to ensure the safety and security performance of nonlinear MASs, even in the presence of complex and adverse CPTs. These CPTs encompass unified abrupt and incipient sensor/actuator faults, channel noises, and random cyber-attacks. To achieve consensus, distributed normalized observers are devised to estimate sensor/actuator faults and output noise by leveraging local output information. Moreover, the distributed FTCC law is developed, incorporating both estimation and reconstruction information, thereby enabling compensation for physical faults, robustness against channel noises, and resilience against random cyber-attacks. In future investigations, particular emphasis is placed on addressing the challenges faced by the fully distributed FTCC issue in linear/nonlinear heterogeneous MASs, specifically those arising from cyber-physical threats, such as composite faults, data incompleteness due to deception attacks, or information leakage caused by privacy attacks.

References

[1] 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 Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

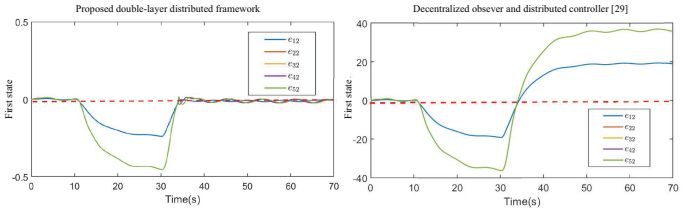

Fig. 12: Comparative results in consensus errors e_{i2}^{σ}

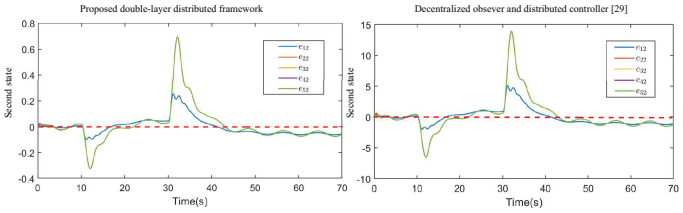

Fig. 13: Comparative results in consensus errors e_{i2}^{ω}

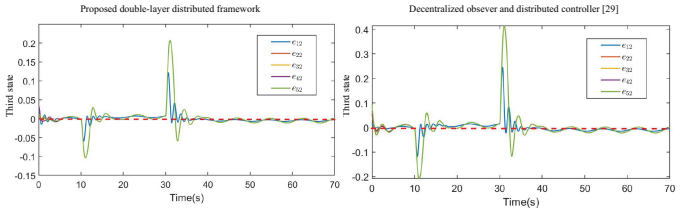

Fig. 14: Comparative results in consensus errors e_{i2}^{P}

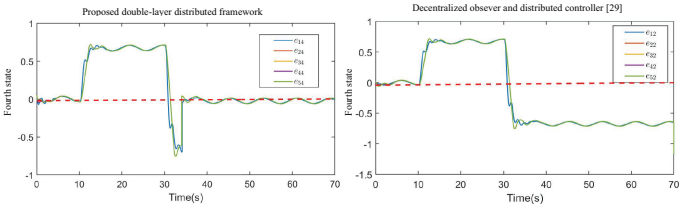

Fig. 15: Comparative results in consensus errors e_{i2}^{X}

[2] W. Zhang, D. Xu, B. Jiang and P. Shi, "Virtual-sensor-based model-free adaptive fault-tolerant constrained control for discrete-time nonlinear systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 10, pp. 4191–4202, 2022.

[3] C. Deng, X. Jin, Z. Wu, and W. Che, "Data-driven-based cooperative resilient learning method for nonlinear MASs under DoS attacks," *IEEE Transactions on Neural Networks and Learning Systems*, 2023, doi.org/10.1109/TNNLS.2023.3252080.

[4] X. Song, J. Man, S. Song and C. K. Ahn, "Finite-time fault estimation and tolerant control for nonlinear interconnected distributed parameter systems with markovian switching channels," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 3, pp. 1347–1359, 2022.

[5] S. Li, Y. Chen, and J. Zhan, "Simultaneous observer-based fault detection and event-triggered consensus control for multi-agent systems," *Journal of the Franklin Institute*, vol. 358, no. 6, pp. 3276–3301, 2021.

[6] C. Ying, N. Zheng, Y. Wu, M. Xu, and W. A. Zhang, "Privacy-preserving adaptive resilient consensus for multi-agent systems under cyber attacks," *IEEE Transactions on Industrial Informatics*, 2023, doi:10.1109/TII.2023.3280318.

[7] S. Xiong and Z. Hou, "Data-driven formation control for unknown MIMO nonlinear discrete-time multi-agent systems with sensor fault," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 7728–7742, 2022.

[8] W. Yang, W. X. Zheng, and W. Yu, "Observer-based event-triggered adaptive fuzzy control for fractional-order time-varying delayed MIMO systems against actuator faults," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 12, pp. 5445–5459, 2022.

[9] Y. Wu, J. Liu, Z. Wang, and Z. Ju, "Distributed resilient tracking of multiagent systems under actuator and sensor faults," *IEEE Transactions on Cybernetics*, vol. 53, no. 7, pp. 4653–4664, 2023.

[10] B. Yan, C. Wu, and P. Shi, "Formation consensus for discrete-time heterogeneous multi-agent systems with link failures and actuator/sensor faults," *Journal of The Franklin Institute-Engineering and Applied Mathematics*, vol. 356, no. 12, pp. 6547–6570, 2019.

[11] X. Wang, Y. Zhou, T. Huang, and P. Chakrabarti, "Event-triggered adaptive fault-tolerant control for a class of nonlinear multiagent systems with sensor and actuator faults," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 10, pp. 4203–4214, 2022.

[12] Y. Y. Qian, L. Liu, and G. Feng, "Cooperative output regulation of linear multiagent systems: An event-triggered adaptive distributed observer approach," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, pp. 833-840, 2021.

[13] Y. Wang, Y. Song, M. Krstic, and C. Wen, "Fault-tolerant finite time consensus for multiple uncertain nonlinear mechanical systems under single-way directed communication interactions and actuation failures," *Automatica*, vol. 63, pp. 374–383, 2016.

[14] M. Li and F. Deng, "Cluster consensus of nonlinear multi-agent systems with markovian switching topologies and communication noises," *ISA Transactions*, vol. 116, pp. 113–120, 2021.

[15] X. Jin, Y. Shi, Y. Tang, H. Werner and J. Kurths, "Event-triggered fixed-time attitude consensus with fixed and switching topologies," *IEEE Transactions on Automatic Control*, vol. 67, no. 8, pp. 4138–4145, 2022.

[16] L. Zeng, D. Qiu, and M. Sun, "Resilience enhancement of multi-agent reinforcement learning-based demand response against adversarial attacks," *Applied Energy*, vol. 324, p. 119688, 2022.

[17] C. Deng, W. Gao, C. Wen, Z. Chen and W. Wang, "Data-driven practical cooperative output regulation under actuator faults and DoS attacks," *IEEE Transactions on Cybernetics*, vol. 53, no. 11, pp. 7417-7428, 2023.

[18] J. Zhou, W. Yang, H. Zhang, W. X. Zheng, Y. Xu, and Y. Tang, "Security analysis and defense strategy of distributed filtering under false data injection attacks," *Automatica*, vol. 138, p. 110151, 2022.

[19] Y. Gao, G. Sun, J. Liu, Y. Shi, and L. Wu, "State estimation and self-triggered control of cpss against joint sensor and actuator attacks," *Automatica*, vol. 113, p. 108687, 2020.

[20] L. Zhao and G. H. Yang, "Adaptive fault-tolerant control for nonlinear multi-agent systems with DoS attacks," *Information Sciences*, vol. 526, pp. 39–53, 2020.

[21] C. Liu, J. Zhao, B. Jiang, and R. J. Patton, "Fault-tolerant consensus control of multi-agent systems under actuator/sensor faults and channel noises: A distributed anti-attack strategy," *Information Sciences*, vol. 623, pp. 1–19, 2023.

[22] L. Zhao and G. H. Yang, "Cooperative adaptive fault-tolerant control for multi-agent systems with deception attacks," *Journal of the Franklin Institute*, vol. 357, no. 6, pp. 3419–3433, 2020.

[23] X. G. Guo, P. M. Liu, J. L. Wang, and C. K. Ahn, "Event-triggered adaptive fault-tolerant pinning control for cluster consensus of heterogeneous nonlinear multi-agent systems under aperiodic DoS attacks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1941–1956, 2021.

[24] J. Wu, F. He, H. Shen, S. Ding, and Z. G. Wu, "Adaptive NN fixed-time fault-tolerant control for uncertain stochastic system with deferred output constraint via self-triggered mechanism," *IEEE Transactions on Cybernetics*, 2022,

[25] W. Cheng, K. Zhang, B. Jiang, and S. X. Ding, "Fixed-time fault-tolerant formation control for heterogeneous multi-agent systems with parameter uncertainties and disturbances," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 5, pp. 2121-2133, 2021.

[26] M. Yadegar and N. Meskin, "Fault-tolerant control of nonlinear heterogeneous multi-agent systems," *Automatica*, vol. 127, p. 109514, 2021.

[27] G. Y. Bao, L. F. Ma, and X. J. Yi, "Recent advances on cooperative control of heterogeneous multi-agent systems subject to constraints: a survey," *Systems Science & Control Engineering*, vol. 10, no. 1, pp. 539–551, 2022.

[28] C. Rösmann, A. Makarow, and T. Bertram, "Online motion planning based on nonlinear model predictive control with non-euclidean rotation groups," *2021 European Control Conference (ECC)*, pp. 1583-1590, 2021.

[29] Y. Yang, H. Xu, and D. Yue, "Observer-based distributed secure consensus control of a class of linear multi-agent systems subject to random attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 8, pp. 3089-3099, 2019.

[30] S. K. Mudge and R. J. Patton, "Analysis of the technique of robust eigenstructure assignment with application to aircraft control," *IEE Proceedings D Control Theory and Applications*, vol. 135, no. 4, pp. 275–281, 1988.