

# Resilient Dynamic Average-Consensus of Multiagent Systems

Muhammad Iqbal<sup>1</sup>, Zhihua Qu<sup>2</sup>, *Fellow, IEEE*, and Azwirman Gusrialdi<sup>3</sup>, *Member, IEEE*

**Abstract**—This letter presents a distributed protocol based on competitive interaction design method to solve the dynamic average-consensus problem on strongly-connected balanced directed graphs in the presence of adversaries. The competitive interaction method allows us to design a network that protects the multi-agent systems from adversaries without requiring high network connectivity and global information about the number of adversaries. We design a resilient distributed protocol to track the average of time-varying bounded reference signals, which every agent is receiving. We show that in the presence of bounded cyber-attacks onto the communication network and actuators, the agents achieve dynamic average-consensus. Simulations are presented to illustrate our theoretical results.

**Index Terms**—Dynamic average-consensus, distributed average tracking, resilient distributed protocols.

## I. INTRODUCTION

CONSIDER a network of autonomous agents, where each agent is receiving a time-varying reference signal. The objective is to design a distributed protocol to enable agents to track the average of time-varying signals, which every agent is receiving. This problem of tracking the average of time-varying signals is called *dynamic average-consensus* or *distributed average tracking problem* [1], [2]. Dynamic average-consensus problem has received much attention for the past decade due to its applications in distributed formation control, distributed estimation, distributed unconstrained optimization and distributed resource allocation. A brief description of all the above applications can be found in

a tutorial paper [3] and the references therein. Distributed protocols are proposed in [4]–[6] to solve the *dynamic average-consensus problem* for unbounded reference signals, and with zero-steady state error [7]. However, these distributed protocols to solve the *dynamic average-consensus problem* are vulnerable to cyber-attacks, because each agent shares their local information on communication channel to track the average of time-varying reference signals. A destabilizing attack can compromise the communication channel or actuator of an agent, and prevent agents to achieve consensus. Therefore, it is important to design distributed protocols, which solve the *dynamic average-consensus problem* in the presence of cyber-attacks.

Solving resilient static consensus problem in the presence of adversaries has received considerable attention, see for example [8]–[12]. However, there is still very limited work which aims at solving the dynamic average-consensus problem in the presence of adversaries. Very recently, a decentralized resilient state-tracking problem is solved in [13] in the presence of cyber-attacks on sensor nodes. However, this letter does not consider attacks on the communication network and actuators. To our knowledge, solving the dynamic average-consensus problem in the presence of adversaries is still an open problem [14].

The contributions of this letter are twofold. First, a new dynamic average-consensus protocol based on competitive interaction [10], [11] is proposed, which enables agents to track the average of time-varying bounded reference signals (see Section III). The assumption on reference signals of being bounded can be seen in power system application [15]. Second, it is shown that the proposed dynamic-average consensus protocol is resilient against any number of bounded cyber-attacks on the communication links between agents and actuators of agents in the network (see Section IV). The proposed resilient dynamic average-consensus is illustrated via simulations in Section V.

## II. PROBLEM FORMULATION

### A. Notations and Preliminaries on Graph Theory

The Euclidean norm of a column vector  $x \in \mathbb{R}^n$  is denoted by  $\|x\|$ , and  $x^T$  is the transpose of a vector  $x$ . The  $i$ th eigenvalue of a square matrix, say  $A$ , can be written as  $\lambda_i(A) = a_i + ib_i$ , where  $a_i = \Re\{\lambda_i(A)\}$  is the real-part of  $\lambda_i(A)$ ,

Manuscript received 21 March 2022; revised 22 May 2022; accepted 14 June 2022. Date of publication 23 June 2022; date of current version 5 July 2022. The work of Muhammad Iqbal and Azwirman Gusrialdi was supported by the Academy of Finland under Project 330073. The work of Zhihua Qu work was supported in part by the U.S. Department of Energy's Awards under Grant DE-EE0007998, Grant DE-EE0009028, Grant DE-EE0009152, and Grant DE-EE0009339. Recommended by Senior Editor S. Dey. (*Corresponding author: Muhammad Iqbal.*)

Muhammad Iqbal and Azwirman Gusrialdi are with the Automation and Mechanical Engineering Unit, Tampere University, 33720 Tampere, Finland (e-mail: muhammad.iqbal@tuni.fi; azwirman.gusrialdi@tuni.fi).

Zhihua Qu is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32816 USA (e-mail: qu@ucf.edu).

Digital Object Identifier 10.1109/LCSYS.2022.3185800

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see <https://creativecommons.org/licenses/by/4.0/>

$b_i = \Im\{\lambda_i(A)\}$  is the imaginary-part of  $\lambda_i(A)$ , and  $\iota = \sqrt{-1}$ . We denote  $\mathbb{I}_n$  and  $\mathbb{O}_n$  to represent  $n \times n$  identity matrix and a zero matrix, respectively. We write  $\text{diag}(a_{11}, \dots, a_{mm})$  to denote a diagonal matrix and  $\text{blockdiag}(A, B)$  to denote a block-diagonal matrix. A column vector with  $n$  entries, all equal to 1 is denoted by  $\mathbf{1}_n$ . The time-derivative of a function  $f : t \mapsto \mathbb{R}$  is denoted by  $\dot{f}$ . The set  $\mathcal{C}^p$  contains all functions  $f$  that are  $p$ -times differentiable. A *measure of a matrix*  $A \in \mathbb{C}^{n \times n}$  is defined as [16]:

$$\mu(A) \triangleq \lim_{\theta \rightarrow 0_+} \frac{\|\mathbb{I}_n + \theta A\| - 1}{\theta}. \quad (1)$$

The solutions of a dynamical system  $\dot{x} = f(x)$  are uniformly ultimately bounded with ultimate bound  $\epsilon$  if there exists  $c > 0$ , independent of  $t_o$ , and for every  $\delta \in (0, c)$ , there is  $T \geq 0$ , dependent on  $\delta$  and  $\epsilon$  but independent of  $t_o$ , such that  $\|x(t_0)\| \leq \delta \implies \|x(t)\| \leq \epsilon, \forall t \geq t_o + T$  [17]. For detailed discussion, the readers are referred to [17].

Next, we provide a background of graph theory that we will use in the sequel. Consider a directed graph (digraph)  $\mathcal{G} = (\mathcal{V}, \mathcal{E})$  consisting of a finite node set  $\mathcal{V} = \{1, 2, \dots, n\}$ , an edge set  $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ . Let  $Q = [q_{ij}]$  be the adjacency matrix of the digraph  $\mathcal{G}$ , where  $q_{ij} = 1$  if node  $i$  is receiving information from node  $j$ , and  $q_{ij} = 0$  otherwise. The set  $\mathcal{N}_i^{\text{in}} = \{j \mid q_{ij} = 1, \forall j \in \mathcal{V}\} \subseteq \mathcal{V}$  contains the  $i$ th agent in-neighbors. The Laplacian matrix  $\mathcal{L} = \mathcal{L}(\mathcal{G})$  of a digraph  $\mathcal{G}$  is defined as:

$$\mathcal{L} = D - Q, \quad (2)$$

where  $D = [d_{ij}] \in \mathbb{R}^{n \times n}$  is a diagonal matrix. The diagonal entry  $d_{ii}(\mathcal{G})$  of the matrix  $D$  represents the number of in-neighbors of the  $i$ th agent. The symmetric part of the Laplacian matrix  $\mathcal{L}$  is denoted by  $\text{sym}(\mathcal{L}) = \frac{1}{2}(\mathcal{L} + \mathcal{L}^T)$ . A *directed path* from node  $v_i$  to node  $v_l$  in a digraph, is a sequence of ordered edges of the form  $(i, i+k)$ , where  $k = 1, \dots, l-1$ . A digraph  $\mathcal{G}$  is said to be *strongly connected*, if there exists a *directed path* from any node to any other node in  $\mathcal{G}$ . A *strongly connected digraph* is said to be *balanced digraph*, if  $\sum_j q_{ij} = \sum_j q_{ji}$  for all  $i \in \mathcal{V}$ .

## B. Problem Statement

Consider a group of  $n \geq 2$  agents modeled as:

$$\dot{x}_i = u_i \left( J_i, I_j^i = \left\{ I_j^i \right\}_{j \in \mathcal{N}_i^{\text{in}}} \right), \quad (3)$$

where  $u_i$  is the control input,  $J_i$  represents local state  $x_i$  and a time-varying reference signal  $r_i : (0, \infty] \rightarrow \mathbb{R}$  that each agent is receiving, and  $I_j^i$  denotes the state information coming from the in-neighbors ( $j \in \mathcal{N}_i^{\text{in}}$ ) of an  $i$ th agent as shown in Fig. 1. To achieve the *dynamic average-consensus*, the distributed protocol  $u_i$  is designed such that the state of the  $i$ th agent  $x_i(t)$  tracks  $r_{\text{avg}} = \frac{1}{n} \sum_{j=1}^n r_j$  with the following assumptions on the time-varying reference signals and the digraph  $\mathcal{G}$  representing the network topology of multi-agent systems.

*Assumption 1:* The signal  $r_i(t)$  is uniformly bounded and uniformly continuous for all  $i \in \{1, \dots, n\}$ .

*Assumption 2:* The digraph  $\mathcal{G}$  is strongly connected and balanced.

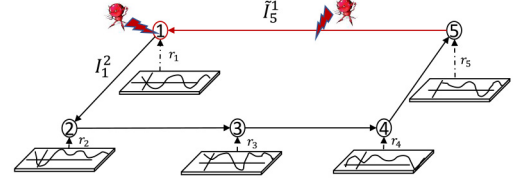


Fig. 1. A network of five agents communicating with each other: Agent  $i$  receives  $r_i$  and neighboring state information. Cyber-attacks pollute the state information exchanged through the communication links and the actuator signal.

The above setup imitates applications where agents receive time-varying reference signals, and the objective is that each agent tracks  $r_{\text{avg}}$ . For example, consider a multi-camera target tracking system, in which each camera is tracking a moving target. Due to external disturbances and measurement noise, the tracking performance of each camera might be deteriorated. To improve the tracking performance, one needs to take the average of the signals received at multiple cameras. The challenging part is to compute the average of the time-varying signals in a distributed manner because centralized unit is not present. *Dynamic-average consensus protocol* offers a solution to such problems. Many other potential applications are presented in [3], and the references therein.

In the foregoing discussion, we assumed secure communication links between agents, and secured nodes. However, in practice, communication channels and actuators are vulnerable to cyber-attacks. Therefore, we consider false-data injection attacks, which is essentially a cyber-attack onto the actuator of the  $i$ th agent, and can be modeled as given below:

$$\tilde{u}_i = u_i + \eta_{ui}(t)\delta_{ui}(t), \quad (4)$$

where  $\tilde{u}_i(t)$  is the control input together with an unknown false-data injection  $\delta_{ui}(t)$ , and  $\eta_{ui}(t) \in \{0, 1\}$  is an activation function, which is  $\eta_{ui}(t) = 1$ , in the presence of an attack.

In the case of attack onto the communication channel, agent  $i$  may not be receiving the true information from its neighbors. Thus, the feedback that agent  $i$  is receiving from its neighbor, say  $j \in \mathcal{N}_i^{\text{in}}$  takes the following form:

$$\tilde{I}_j^i = I_j^i + \eta_{fj}^i(t)\delta_{fj}^i(t), \quad j \in \mathcal{N}_i^{\text{in}}, \quad (5)$$

where  $\tilde{I}_j^i = \{\tilde{I}_j^i\}_{j \in \mathcal{N}_i^{\text{in}}}$  is the malicious information received by the  $i$ th agent from its neighbors,  $\delta_{fj}^i(t)$  is the information injected by the adversary into the communication link, and  $\eta_{fj}^i(t) \in \{0, 1\}$  is the activation function. In the presence of both actuator and communication channel attack, the dynamics of (3) can be written as:

$$\dot{x}_i = u_i \left( J_i, \tilde{I}_j^i \right) + \eta_{ui}(t)\delta_{ui}(t). \quad (6)$$

Note that  $|\delta_{fj}^i(t)|$ ,  $j \in \mathcal{N}_i^{\text{in}}$  and  $|\delta_{ui}(t)|$  for all  $i$ , are bounded. The attacker aims to generate a bounded attack signal that can destabilize (6), without having a knowledge of the agent's parameters. The bounded attacks considered in this letter are permanent [18] and can cause the system to be unstable or at least degrade the performance of the control objective. Moreover, no restrictions are made on the number of attacks.

The objective of this letter is to design a distributed resilient control law  $u_i$  given in (3) such that the state  $x_i(t)$  tracks the average signal  $r_{avg}$  in the presence of cyber-attacks; that is

$$|x_i(t) - r_{avg}| < \epsilon, \text{ for all } t \geq T, i \in \mathcal{V}, \quad (7)$$

where  $T < \infty$  is a finite value,  $\epsilon$  is sufficiently small positive value.

### III. COMPETITIVE INTERACTION BASED RESILIENT DYNAMIC AVERAGE CONSENSUS

In this section, we aim to design a new distributed protocol based on competitive interaction method [11] to solve the *dynamic average-consensus problem* for strongly connected balanced digraphs. Later in this letter, we will show that the designed *dynamic average-consensus protocol* is resilient to cyber-attacks.

We propose the following resilient dynamic average consensus protocol to enable each agent to track the average of time-varying reference signals that each agent is receiving:

$$\begin{aligned} \dot{x}_i &= \alpha(r_i - x_i) - \alpha\beta \sum_{j \in \mathcal{N}_i^{in}} (x_i - x_j) + \beta \sum_{j \in \mathcal{N}_i^{in}} (z_i - z_j) + v_{r_i} \\ \dot{z}_i &= \alpha(r_i - z_i) - \beta \sum_{j \in \mathcal{N}_i^{in}} (x_i - x_j) - \alpha\beta \sum_{j \in \mathcal{N}_i^{in}} (z_i - z_j) + v_{r_i}, \end{aligned} \quad (8)$$

where  $v_{r_i} = \dot{r}_i$ , and  $r_i(t) \in \mathcal{C}^2$  is a time-varying signal that the  $i$ th agent is receiving,  $z_i \in \mathbb{R}$  is a state of the  $i$ th agent,  $\alpha$  and  $\beta$  are positive scalar gains.

*Remark 1:* The design of  $\alpha$  and  $\beta$  relies on the eigenvalues of  $\mathcal{L}$ , which implies that the network topology must be known a priori. However, the implementation is distributed because every agent is taking decisions based on local and neighboring information.

Let  $J_i = \{J_i^1, J_i^2\}$ , then in the context of (6),  $J_i^1 = \{\alpha x_i, \alpha r_i, \alpha\beta x_i, \beta z_i, v_{r_i}\}$  and  $J_i^2 = \{\alpha z_i, \alpha r_i, \alpha\beta z_i, \beta x_i, v_{r_i}\}$  represent local information. Similarly, letting  $I_j^i = \{I_j^{x_i}, I_j^{z_i}\}$ , then for each  $i$ th agent, the information available from its neighbors through the communication network is  $I_j^{x_i} = \{\alpha\beta x_j - \beta z_j, j \in \mathcal{N}_i^{in}\}$  and  $I_j^{z_i} = \{\alpha\beta z_j + \beta x_j, j \in \mathcal{N}_i^{in}\}$ .

Writing (8) in a compact vector form:

$$\begin{aligned} \dot{x} &= \alpha(r - x) - \alpha\beta \mathcal{L}x + \beta \mathcal{L}z + v_r \\ \dot{z} &= \alpha(r - z) - \beta \mathcal{L}x - \alpha\beta \mathcal{L}z + v_r, \end{aligned} \quad (9)$$

where  $r = [r_1, \dots, r_n]^T$ ,  $z = [z_1, \dots, z_n]^T$  and  $v_r = [v_{r_1}, \dots, v_{r_n}]^T$ . To show that (9) achieve dynamic average-consensus, we show that  $e_{x_i} = x_i - \frac{1}{n} \sum_{j=1}^n r_j$  and  $e_{z_i} = z_i - \frac{1}{n} \sum_{j=1}^n r_j$  converge to an  $\epsilon$ -sized hyperball around the origin as  $t \rightarrow \infty$ . To that end, we have the following transformation:

$$e_x = x - \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T r, \quad e_z = z - \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T r. \quad (10)$$

Note that  $\mathcal{L}e_x = \mathcal{L}x$  and  $\mathcal{L}e_z = \mathcal{L}z$ . Taking the time-derivative of (10), we have

$$\dot{e}_x = \alpha(r - x) - \alpha\beta \mathcal{L}e_x + \beta \mathcal{L}e_z + v_r - \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T v_r,$$

$$\dot{e}_z = \alpha(r - z) - \beta \mathcal{L}e_x - \alpha\beta \mathcal{L}e_z + v_r - \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T v_r. \quad (11)$$

After algebraic manipulation, we have the following convenient form of (11):

$$\begin{aligned} \dot{e}_x &= -(\alpha \mathbb{I}_n + \alpha\beta \mathcal{L})e_x + \beta \mathcal{L}e_z + \Pi_n(\alpha r + v_r) \\ \dot{e}_z &= -\beta \mathcal{L}e_x - (\alpha \mathbb{I}_n + \alpha\beta \mathcal{L})e_z + \Pi_n(\alpha r + v_r), \end{aligned} \quad (12)$$

where  $\Pi_n = \mathbb{I}_n - \frac{1}{n} \mathbf{1}_n \mathbf{1}_n^T$ . Writing (12) in a compact vector form:

$$\dot{\zeta} = \Xi \zeta + \Upsilon(\alpha r, v_r), \quad (13)$$

where  $\zeta = [e_x^T, e_z^T]^T$ ,  $\Upsilon(\alpha r, v_r) = [1, 1]^T \otimes \Pi_n(\alpha r + v_r)$ , and

$$\Xi = \begin{bmatrix} -(\alpha \mathbb{I}_n + \alpha\beta \mathcal{L}) & \beta \mathcal{L} \\ -\beta \mathcal{L} & -(\alpha \mathbb{I}_n + \alpha\beta \mathcal{L}) \end{bmatrix}. \quad (14)$$

Next, we study the stability properties of (13). To do so, first we check the stability of the zero-system of (13). Thus, for  $r(t) = 0$ , (13) can be written as:

$$\dot{\zeta} = \Xi \zeta. \quad (15)$$

In the following result, we show that the system (15) is stable.

*Lemma 1:* Let  $\mathcal{L}$  given in (14), be the Laplacian matrix associated with a digraph that holds Assumption 2. Let  $\lambda_i(\mathcal{L}) = \delta_i + \omega_i$  be the  $i$ th eigenvalue of  $\mathcal{L}$ . Let  $\alpha > 0$  and  $\beta > 0$  in (14) be the gains, the system (15) is asymptotically stable if and only if  $\alpha > \frac{\beta|\omega_i|}{1+\beta\delta_i}$  for all  $i \in \mathcal{V}$ .

*Proof:* To show the stability of (15), we diagonalize the matrix  $\Xi$ . To that end, we use the following transformation:

$$\zeta = TS\bar{\zeta}, \quad T = \begin{bmatrix} \mathbb{I}_n & -\mathbb{I}_n \\ \mathbb{I}_n & \mathbb{I}_n \end{bmatrix}, \quad S = \text{blockdiag}(V, V), \quad (16)$$

where  $\bar{\zeta} = [\hat{\zeta}_1, \tilde{\zeta}_1, \tilde{\zeta}_2, \dots, \tilde{\zeta}_{n-1}, \hat{\zeta}_2, \tilde{\zeta}_n, \dots, \tilde{\zeta}_{2n-2}]^T$ , and  $V$  is a matrix containing the generalized left-eigenvectors of  $\mathcal{L}$ . Taking the time-derivative of (16) with  $r(t) = 0$  yields

$$\dot{\zeta} = \Lambda \bar{\zeta}, \quad \Lambda = \text{blockdiag}(\mathbb{I}_n + \alpha\beta J + \iota\beta J, -\alpha \mathbb{I}_n + \alpha\beta J - \iota\beta J), \quad (17)$$

where  $J = \text{blockdiag}(0, \tilde{J})$  is the Jordan normal form of  $-\mathcal{L}$ , that is,  $-\mathcal{L} = VJV^{-1}$ , and  $\tilde{J} \in \mathbb{C}^{n-1 \times n-1}$ . Note that  $\lambda_i(J) = -\lambda_i(\mathcal{L})$  for all  $i \in \mathcal{V}$ . Thus, the eigenvalues of  $\Xi$  can be written as:

$$\lambda_i(\Xi) = -\alpha - \alpha\beta\delta_i \pm \beta\omega_i + \iota(\beta\delta_i \pm \alpha\beta\omega_i), \quad \forall i \in \mathcal{V},$$

which shows that stability of (15) is guaranteed if and only if

$$\alpha + \alpha\beta\delta_i > \beta|\omega_i|.$$

This completes the proof.  $\blacksquare$

Next, we show that the protocol presented in (9) achieve dynamic average-consensus. To that end, we apply the same transformation given in (16) to the system given in (13) where  $r(t) \neq 0$  to factor out the dynamics associated with the zero eigenvalue of the Laplacian matrix  $\mathcal{L}$  of  $\mathcal{G}$  that holds Assumption 2. Thus, we write (13) in the following equivalent form:

$$\dot{\zeta} = \Gamma \hat{\zeta}, \quad \text{with } \Gamma = \text{diag}(-\alpha, -\alpha), \quad (18a)$$

$$\dot{\zeta} = \tilde{\Lambda} \tilde{\zeta} + \tilde{\Upsilon}(\alpha r, v_r), \quad (18b)$$

where  $\hat{\zeta} = [\hat{\zeta}_1, \hat{\zeta}_2]^T$ ,  $\tilde{\zeta} = [\tilde{\zeta}_1, \dots, \tilde{\zeta}_{2n-2}]^T$ ,  $\tilde{\Upsilon}(\alpha r, v_r) = [\tilde{\Upsilon}_1, \dots, \tilde{\Upsilon}_{2n-2}]^T$ , and

$$\tilde{\Lambda} = \text{blockdiag}(-\alpha \mathbb{I}_{n-1} + \alpha \beta \tilde{J} + \iota \beta \tilde{J}, -\alpha \mathbb{I}_{n-1} + \alpha \beta \tilde{J} - \iota \beta \tilde{J}).$$

Note that the first and the  $(n+1)$ th elements of  $TS\Upsilon(\alpha r, v_r)$  are zero, because the first row vector of  $V$  is the left-eigenvector of  $\mathcal{L}$  associated with the strongly connected balanced digraph  $\mathcal{G}$ . To facilitate the discussion in the sequel, we split  $\tilde{\Lambda} = M + \beta \Omega$ , where  $\Omega = \text{blockdiag}(\iota \tilde{J}, -\iota \tilde{J})$ , and

$$M = \text{blockdiag}(-\alpha \mathbb{I}_{n-1} + \alpha \beta \tilde{J}, -\alpha \mathbb{I}_{n-1} + \alpha \beta \tilde{J}).$$

Next, we show the Input-to-State Stability (ISS) of (13).

*Theorem 1:* Consider a network of  $n$  agents given in (9), where  $\mathcal{L}$  be the Laplacian matrix associated with a digraph that holds Assumption 2, and each  $r_i(t)$  satisfies Assumption 1. Then the norm of the solution  $\zeta$  of (13) is uniformly bounded and uniformly ultimately bounded by  $\epsilon > 0$  if  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$  and sufficiently large  $\beta > 0$ , for all  $i \in \mathcal{V}$ . Moreover  $\sum_{i=1}^n e_{x_i}$  approaches to zero asymptotically.

The conditions  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{x_i} \rightarrow 0$  and  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{z_i} \rightarrow 0$  entail that the average of time-varying signals stays within the states' trajectories because  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{x_i}$  implies  $\lim_{t \rightarrow \infty} |\frac{1}{n} \sum_{i=1}^n x_i(t) - r_{\text{avg}}|$ . Therefore, the states' trajectories enclose  $r_{\text{avg}}$  in their convex hull, asymptotically.

*Proof:* To show the ISS of (13), we show the ISS of the equivalent system given in (18b). Note that (18a) is asymptotically stable for any  $\alpha > 0$ . From Lemma 1, we know that for  $\alpha > 0$ ,  $\beta > 0$  and  $\alpha > \frac{\beta|\omega_i|}{1+\beta\delta_i}$ ,  $\tilde{\Lambda}$  is Hurwitz. Thus, the solution of (13) can be written as:

$$\tilde{\zeta}(t) = \underbrace{\exp(t\tilde{\Lambda})\tilde{\zeta}(0)}_{\text{zero-input response}} + \int_0^t \exp((t-\tau)\tilde{\Lambda})\tilde{\Upsilon}(\alpha r, v_r) d\tau. \quad (19)$$

Invoking the inequality in [16, Th. 27], that is  $\|\exp(t\tilde{\Lambda})\| \leq \exp(\mu(\tilde{\Lambda})t)$ , where  $\mu(\tilde{\Lambda})$  is the *measure of the matrix*  $\tilde{\Lambda}$ , we estimate the solution by

$$\|\tilde{\zeta}(t)\| \leq \exp(\mu(\tilde{\Lambda})t) \|\tilde{\zeta}(0)\| + \int_0^t \exp(\mu(\tilde{\Lambda})(t-\tau)) \|\tilde{\Upsilon}\| d\tau. \quad (20)$$

Next, using the properties of  $\mu(\cdot)$ , that is  $\mu(\tilde{\Lambda}) = \mu(M + \beta\Omega) \leq \mu(M) + \mu(\beta\Omega)$ ,  $\mu(\beta\Omega) = \beta\mu(\Omega)$ , and  $\mu(-\alpha\mathbb{I}_{n-1}) = -\alpha$  given in [16, Th. 27], we have

$$\|\tilde{\zeta}(t)\| \leq \exp(-\lambda t) \|\tilde{\zeta}(0)\| + \frac{1}{\lambda} \sup_{0 \leq \tau \leq t} \|\tilde{\Upsilon}(\alpha r, v_r)\|, \quad \forall t \in \mathbb{R}_{\geq 0}, \quad (21)$$

where  $\lambda = \alpha + \alpha\beta\lambda_2(\text{sym}(\mathcal{L})) - \beta\mu(\Omega)$ , and  $\mu_2(\alpha\beta\tilde{J}) = -\alpha\beta\lambda_2(\text{sym}(\mathcal{L}))$  [16, Th. 24]. Choosing  $\alpha$  and  $\beta$  such that  $\alpha + \alpha\beta\lambda_2(\text{sym}(\mathcal{L})) > \beta\mu(\Omega)$ , the zero-input response in (19) corresponds to zero-error as it approaches to zero, exponentially. It is apparent from (21) that, for any valid choice of  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$ , the ultimate bound on error decreases monotonically to zero as  $\beta$  increases.

Next pre-multiplying  $\dot{e}_x$  and  $\dot{e}_z$  given in (12) by  $\mathbf{1}_n^T$ , and by exploiting the balanced property of the digraph  $\mathcal{G}$ , we have

$$\sum_{i=1}^n \dot{e}_{x_i} = -\alpha \sum_{i=1}^n e_{x_i}, \quad \sum_{i=1}^n \dot{e}_{z_i} = -\alpha \sum_{i=1}^n e_{z_i}. \quad (22)$$

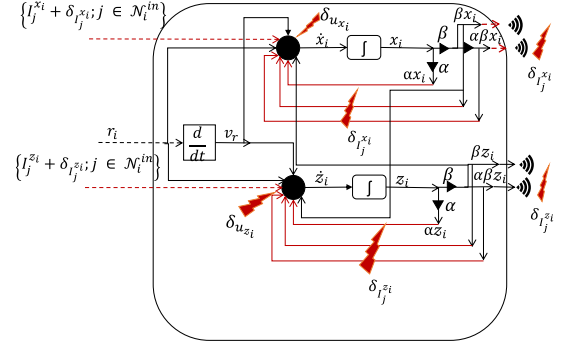


Fig. 2. Model of the  $i$ th agent together with cyber-attacks. (Red lines show vulnerability to cyber-attacks. All arrows show directional information flow, whereas triangle arrowhead represents gain.)

Thus, the average of the time-varying reference signals  $r_{\text{avg}} = \sum_{i=1}^n r_i$  stays within the agents states  $x_i$  and  $z_i$  for all  $i \in \{1, 2, \dots, n\}$ . This completes the proof. ■

#### IV. RESILIENT CONSENSUS IN THE PRESENCE OF CYBER-ATTACKS

In this section, we consider bounded cyber-attacks on communication network and on actuators as shown in (6). In the context of (6), the dynamics of (8) can be written as given below:

$$\begin{aligned} \dot{x}_i &= u_{x_i} \begin{pmatrix} J_i^1 \\ I_j^{x_i} \end{pmatrix} + d_i(t), \\ \dot{z}_i &= u_{z_i} \begin{pmatrix} J_i^2 \\ I_j^{z_i} \end{pmatrix} + d'_i(t), \end{aligned} \quad (23)$$

where

$$\begin{aligned} d_i(t) &= \eta_{u_{x_i}}(t) \delta_{u_{x_i}}(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}} \eta_{I_j^{x_i}}(t) \delta_{I_j^{x_i}}(t), \quad j \in \mathcal{N}_i^{\text{in}} \\ d'_i(t) &= \eta_{u_{z_i}}(t) \delta_{u_{z_i}}(t) + \sum_{j \in \mathcal{N}_i^{\text{in}}} \eta_{I_j^{z_i}}(t) \delta_{I_j^{z_i}}(t), \quad j \in \mathcal{N}_i^{\text{in}}. \end{aligned} \quad (24)$$

We see from Fig. 1 and Fig. 2 that  $d_i(t)$  represents malicious information added to the actuator signal, denoted by  $\delta_{u_{x_i}}(t)$ , and malicious information added to the neighboring state information, denoted by  $\delta_{I_j^{x_i}}(t)$ . Similarly,  $d'_i(t)$  represents malicious information added to the actuator signal, denoted by  $\delta_{u_{z_i}}(t)$ , and malicious information added to the neighboring state information, denoted by  $\delta_{I_j^{z_i}}(t)$ . Note that, in general, an adversary can manipulate the shared information differently for different neighbors, which is known as *Byzantine adversary* [19]. A detailed model for the  $i$ th agent is shown in Fig. 2. In the general case as shown in (24), the adversary may or may not attack the local feedback signals, and the links  $(i, j)$ ,  $(i, k)$  can be manipulated differently for maximum damage.

As such, (9) takes the following form under cyber-attacks:

$$\begin{aligned} \dot{x} &= \alpha(r - x) - \alpha\beta\mathcal{L}x + \beta\mathcal{L}z + v_r + d(t) \\ \dot{z} &= \alpha(r - z) - \beta\mathcal{L}x - \alpha\beta\mathcal{L}z + v_r + d'(t), \end{aligned} \quad (25)$$

where  $d(t) = [d_1, \dots, d_n]^T$  and  $d'(t) = [d'_1, \dots, d'_n]^T$  are uniformly bounded attacks:

$$\|d(t)\| < U < \infty, \quad \|d'(t)\| < U^* < \infty, \quad (26)$$

where  $U$  and  $U^*$  are positive constants. In the following, we show that agents achieve the *resilient dynamic average-consensus* in the presence of adversarial attacks on communication network and on actuators.

**Theorem 2:** Consider an interconnected system (25) where  $\mathcal{L}$  is the Laplacian matrix associated with a digraph satisfying Assumption 2, and the attack vectors  $d(t)$ ,  $d'(t)$  are bounded. Then for sufficiently large  $\beta > 0$  and  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$ , for all  $i \in \mathcal{V}$ , the multi-agent system in (25) solve the resilient dynamic average-consensus problem, that is, the state vector  $x(t) \in \mathbb{R}^n$  and  $z(t) \in \mathbb{R}^n$  converge to a small neighborhood of  $r_{avg} = \frac{1}{n} \sum_{j=1}^n r_j$ , where each  $r_j$  satisfies Assumption 1.

*Proof:* Again, let  $e_{x_i} = x_i - r_{avg}$  and  $e_{z_i} = z_i - r_{avg}$ . Taking the time derivative of  $e_x = [e_{x_1}, \dots, e_{x_n}]^T$  and  $e_z = [e_{z_1}, \dots, e_{z_n}]^T$ , we get

$$\begin{aligned}\dot{e}_x &= -(\alpha\mathbb{I}_n + \alpha\beta\mathcal{L})e_x + \beta\mathcal{L}e_z + \Pi_n(\alpha r + v_r) + d(t) \\ \dot{e}_z &= -\beta\mathcal{L}e_x - (\alpha\mathbb{I}_n + \alpha\beta\mathcal{L})e_z + \Pi_n(\alpha r + v_r) + d'(t),\end{aligned}$$

Letting  $\zeta = [e_x^T, e_z^T]^T$ , we have

$$\dot{\zeta} = \Xi\zeta + \Upsilon(\alpha r, v_r) + \Delta(d, d'), \quad (27)$$

where  $\Delta(d, d') = [d^T; d'^T]^T$ . Next, using the coordinate transformation given in (16), (27) takes the following form:

$$\dot{\hat{\zeta}} = \Gamma\hat{\zeta} + \hat{\Delta}(d, d'), \quad (28a)$$

$$\dot{\tilde{\zeta}} = \tilde{\Lambda}\tilde{\zeta} + \tilde{\Upsilon}(\alpha r, v_r) + \tilde{\Delta}(d, d'), \quad (28b)$$

where  $\hat{\Delta}(d, d') = [\hat{\Delta}_1, \hat{\Delta}_2]^T$ , with  $\hat{\Delta}_1$  and  $\hat{\Delta}_2$  to be the first and  $(n+1)$ th elements of  $TS\Delta(d, d')$ , respectively, and  $\tilde{\Delta}(d, d') = [\tilde{\Delta}_1, \dots, \tilde{\Delta}_{2n-2}]^T$  contains the rest of the entries of  $TS^{-1}\Delta(d, d')$ . To show that (27) is input-to-state stable, we show ISS of the equivalent system (28a)-(28b). For  $\alpha > 0$ ,  $\Gamma$  is Hurwitz, therefore the solution of (28a) can be estimated by

$$\|\hat{\zeta}(t)\| \leq \exp(-\alpha t) \|\hat{\zeta}(0)\| + \frac{1}{\alpha} \sup_{0 \leq \tau \leq t} \|\hat{\Delta}(d, d')\|, \quad \forall t \in \mathbb{R}_{\geq 0}. \quad (29)$$

We see from (29), that the ultimate bound on  $\|\hat{\zeta}(t)\|$  decreases monotonically to zero as  $\alpha$  increases. Next, we show that (28b) is input-to-state stable. To that end, we choose  $\alpha > 0$ ,  $\beta > 0$  such that  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$ , and invoke the properties of  $\mu(\cdot)$  mentioned in Theorem 1 in estimating the solution of (28b) by

$$\begin{aligned}\|\tilde{\zeta}(t)\| &\leq \exp(-\lambda t) \|\tilde{\zeta}(0)\| \\ &+ \frac{1}{\lambda} \sup_{0 \leq \tau \leq t} \left( \|\tilde{\Upsilon}(\alpha r, v_r)\| + \|\tilde{\Delta}(d, d')\| \right), \quad \forall t \in \mathbb{R}_{\geq 0}.\end{aligned} \quad (30)$$

As  $\alpha + \alpha\beta\lambda_2(\text{sym}(\mathcal{L})) > \beta\mu(\Omega)$ , the zero-input response in (30) corresponds to zero-error as it approaches to zero, exponentially. From (30), we see that, for any valid choice of  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$ , the ultimate bound on error decreases monotonically to zero as  $\beta$  increases. ■

Next, we consider a special case of cyber-attacks, where the attacks in (25) take the form  $d(t) = \mathcal{L}\bar{d}(t)$  and  $d'(t) = \mathcal{L}\bar{d}'(t)$ , because the attack on agent  $i$  is polluting the transmitting information by the same amount. Moreover, we assume that the same malicious information is added to the local feedback

signals  $x_i$  and  $z_i$  as well [11]. Note that the adversary is not Byzantine, as it is polluting the neighbors in a similar manner. In addition, the states  $x_i$  and  $z_i$  are amplified first and thereafter used as a local feedback. Thus, (25) can be written in the following form:

$$\begin{aligned}\dot{x} &= \alpha(r - x) - \alpha\beta\mathcal{L}x + \beta\mathcal{L}z + v_r + \mathcal{L}\bar{d}(t) \\ \dot{z} &= \alpha(r - z) - \beta\mathcal{L}x - \alpha\beta\mathcal{L}z + v_r + \mathcal{L}\bar{d}(t).\end{aligned} \quad (31)$$

Next, we show that  $x_i$  for all  $i \in \mathcal{V}$ , tracks  $r_{avg}$ . To that end, we show the ultimate boundedness on the norm of error signals  $e_x, e_z$ , and  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{x_i}$ ,  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{z_i}$  approach to zero. Following the similar path of coordinate transformation in Section III, define  $e_x$  and  $e_z$  and taking its time-derivative yields:

$$\begin{aligned}\dot{e}_x &= -(\alpha\mathbb{I}_n + \alpha\beta\mathcal{L})e_x + \beta\mathcal{L}e_z + \Pi_n(\alpha r + v_r) + \mathcal{L}\bar{d}(t) \\ \dot{e}_z &= -(\alpha\mathbb{I}_n + \alpha\beta\mathcal{L})e_z - \beta\mathcal{L}e_x + \Pi_n(\alpha r + v_r) + \mathcal{L}\bar{d}(t),\end{aligned} \quad (32)$$

Letting  $\zeta(t) = [e_x^T, e_z^T]^T$  and using the coordinate transformation  $\zeta = T\bar{\zeta}$  given in (16), (32) takes the following form:

$$\dot{\hat{\zeta}} = \Gamma\hat{\zeta}, \quad (33a)$$

$$\dot{\tilde{\zeta}} = \tilde{\Lambda}\tilde{\zeta} + \tilde{\Upsilon}(\alpha r, v_r) + \tilde{\Delta}(\mathcal{L}\bar{d}(t), \mathcal{L}\bar{d}'(t)), \quad (33b)$$

where  $\tilde{\Delta}(\mathcal{L}\bar{d}(t), \mathcal{L}\bar{d}'(t)) = [\tilde{\Delta}_1, \dots, \tilde{\Delta}_{2n-2}]^T$  contains the elements of  $TS\tilde{\Delta}(\mathcal{L}\bar{d}(t), \mathcal{L}\bar{d}'(t))$ , excluding the first and the  $(n+1)$ th entries.

The following result shows that the resilient dynamic average-consensus can be achieved in the presence of unknown bounded attacks on the communication network.

**Corollary 1:** Consider an interconnected system as given in (31) where  $\mathcal{L}$  is the Laplacian matrix associated with a digraph satisfying Assumption 2, and each  $r_i(t)$  satisfies Assumption 1. Let the attack vectors  $\bar{d}(t)$ ,  $\bar{d}'(t)$  be bounded. (a) Then for  $\alpha > \max\{\frac{\beta|\omega_i|}{1+\beta\delta_i}, \frac{\mu(\Omega)}{\lambda_2(\text{sym}(\mathcal{L}))}\}$  and sufficiently large  $\beta > 0$ , for all  $i \in \mathcal{V}$ , the norm of the error vector  $\zeta(t)$  in (32) is uniformly bounded and uniformly ultimately bounded by  $\epsilon > 0$ . (b) Moreover,  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{x_i}$  and  $\lim_{t \rightarrow \infty} \sum_{i=1}^n e_{z_i}$  approach to zero, for all  $i \in \mathcal{V}$ .

*Proof:*

(a) For any  $\alpha > 0$ , (33a) is asymptotically stable. We see that  $\tilde{\Delta}(d, d')$  in (28b) and  $\tilde{\Delta}(\mathcal{L}\bar{d}(t), \mathcal{L}\bar{d}'(t))$  in (33b) are both bounded. Thus, the proof follows from Theorem 2.

(b) Next pre-multiplying  $\dot{e}_x$  and  $\dot{e}_z$  given in (32) by  $1_n^T$ , and by exploiting the balanced property of the digraph  $\mathcal{G}$ , we have

$$\sum_{i=1}^n \dot{e}_{x_i} = -\alpha \sum_{i=1}^n e_{x_i}, \quad \sum_{i=1}^n \dot{e}_{z_i} = -\alpha \sum_{i=1}^n e_{z_i}. \quad (34)$$

Thus, the average of the time-varying reference signals  $r_{avg} = \frac{1}{n} \sum_{i=1}^n r_i$  stays within the agents states trajectories  $x_i$  and  $z_i$  for all  $i \in \{1, 2, \dots, n\}$ . This completes the proof. ■

**Remark 2:** Theorem 2 does not quantify that  $r_{avg}$  stays in between the state trajectories, whereas Corollary 1 quantifies this fact.

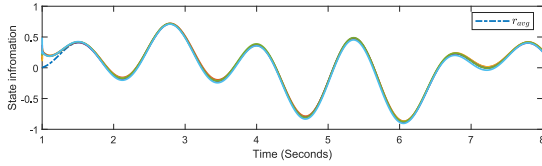


Fig. 3. Resilient dynamic average-consensus: attack on communication network.

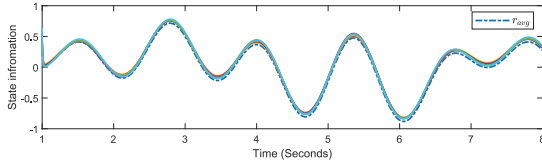


Fig. 4. Resilient dynamic average-consensus: attack on both communication network and on actuators with high gains ( $\alpha = 110$  and  $\beta = 50$ ).

## V. SIMULATION RESULTS

Consider the Laplacian matrix  $\mathcal{L}$  of the digraph given in Fig. 1. Agents receive the following time-varying bounded reference signals:

$$\begin{aligned} r_1(t) &= -\cos(t), \quad r_2(t) = \sin(t), \quad r_3(t) = -\cos(3t), \\ r_4(t) &= -\cos(4t), \quad r_5(t) = 2\sin(5t). \end{aligned} \quad (35)$$

First, we demonstrate how agents achieve dynamic average-consensus in the presence of cyber-attack on communication network as given in (31). One can always design a destabilizing bounded attack, which can destabilize a MAS. For example, the strategy of the attacker in (31) is given below:

$$\dot{\tilde{d}}(t) = F_1 \tilde{d} + d_o \quad (36a)$$

$$\dot{\bar{d}}(t) = F_2 \bar{d} + d_o, \quad (36b)$$

where  $F_1 = -\mathbb{I}$ ,  $F_2 = -2\mathbb{I}$ , and  $d_o = [9.9, 7.7, 5.5, 4.4, 2.2]^T$ . The norm of the solution vector  $\tilde{d}(t)$  of (36a) is bounded because  $F_1$  is Hurwitz and that  $d_o$  is bounded. Similarly, the norm of the solution vector  $\bar{d}(t)$  of (36b) is bounded because  $F_2$  is Hurwitz. The bounded signals  $\tilde{d}_i$  and  $\bar{d}_i$ , which are the linear combination of actuator and communication attacks as shown in (24), are added to the state information that Agent  $i$  is receiving and also added to the actuator signal of Agent  $i$ , representing the cyber-attacks  $d_i(t)$  and  $d'_i(t)$  given in (24), respectively. The competitive interaction based distributive protocol given in (9) solves the dynamic-average consensus problem in the presence of attack onto the communication network as shown in Fig. 3. Note that  $r_{avg}$  stays in between the state trajectories.

Next, we demonstrate how competitive interaction based design method enables agents to track the average of time-varying reference signals in the presence of cyber-attacks on the communication network and actuators as shown in (25), where the attack injections  $d(t)$  and  $d'(t)$  have the same dynamics as  $\tilde{d}(t)$  and  $\bar{d}(t)$ , respectively, as given in (36a) and (36b). We choose  $\alpha = 110$  and  $\beta = 50$  so that

$\alpha + \alpha\beta\lambda_2(\text{sym}(\mathcal{L})) \gg \beta\mu(J)$ . We see in Fig. 4 that state trajectories track the average signal  $r_{avg}$ .

## VI. CONCLUSION

We have designed a competitive interaction based distributed protocol to solve the dynamic average-consensus problem in the presence of adversaries. We considered attack on the communication network and actuators of the agents in a network. The cyber-attack considered in this letter is a general form of bounded attacks. We showed that agents track the average of the time-varying bounded reference signals, which each agent is receiving, in the presence of attack on the communication network and the actuators of agents.

## REFERENCES

- [1] D. P. Spanos, R. Olfati-Saber, and R. M. Murray, "Dynamic consensus on mobile networks," in *Proc. IFAC World Congr.*, 2005, pp. 1–6.
- [2] F. Chen, Y. Cao, and W. Ren, "Distributed computation of the average of multiple time-varying reference signals," in *Proc. Amer. Control Conf.*, 2011, pp. 1650–1655.
- [3] S. S. Kia, B. Van Scoy, J. Cortes, R. A. Freeman, K. M. Lynch, and S. Martinez, "Tutorial on dynamic average consensus: The problem, its applications, and the algorithms," *IEEE Control Syst. Mag.*, vol. 39, no. 3, pp. 40–72, Jun. 2019.
- [4] S. S. Kia, J. Cortés, and S. Martinez, "Dynamic average consensus under limited control authority and privacy requirements," *Int. J. Robust Nonlinear Control*, vol. 25, no. 13, pp. 1941–1966, 2015.
- [5] J. George and R. A. Freeman, "Robust dynamic average consensus algorithms," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4615–4622, Nov. 2019.
- [6] A. Sen, S. R. Sahoo, and M. Kothari, "Distributed algorithm for higher-order integrators to track average of unbounded signals," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2903–2908, 2020.
- [7] R. Aldana-López, R. Aragüés, and C. Sagüés, "EDCHO: High order exact dynamic consensus," *Automatica*, vol. 131, Sep. 2021, Art. no. 109750.
- [8] C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of partial synchrony," *J. ACM*, vol. 35, no. 2, pp. 288–323, 1988.
- [9] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, Apr. 2013.
- [10] B. Gharehifard and T. Başar, "Resilience in consensus dynamics via competitive interconnections," *IFAC Proc. Vol.*, vol. 45, no. 26, pp. 234–239, 2012.
- [11] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Robust design of cooperative systems against attacks," in *Proc. Amer. Control Conf.*, 2014, pp. 1456–1462.
- [12] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Trans. Autom. Control*, vol. 63, no. 9, pp. 3159–3166, Sep. 2018.
- [13] Y. Mao and P. Tabuada, "Decentralized resilient state-tracking," in *Proc. 60th IEEE Conf. Decis. Control (CDC)*, 2021, pp. 3480–3485.
- [14] J. George, M. L. Elwin, R. A. Freeman, and K. M. Lynch, "Distributed fault detection and accommodation in dynamic average consensus," in *Proc. Annu. Amer. Control Conf. (ACC)*, 2018, pp. 5019–5024.
- [15] D. Chowdhury and H. K. Khalil, "Dynamic consensus and extended high gain observers as a tool to achieve practical frequency synchronization in power systems under unknown time-varying power demand," *Automatica*, vol. 131, Art. Sep. 2021, no. 109753.
- [16] C. A. Desoer and M. Vidyasagar, *Feedback Systems: Input-Output Properties*. Philadelphia, PA, USA: SIAM, 2009.
- [17] H. K. Khalil, *Nonlinear Systems*, vol. 3. Upper Saddle River, NJ, USA: Prentice Hall, 2002.
- [18] B. Gerard, H. Voos, Y. Li, and M. Darouach, "Effects of permanent bounded cyber-attacks on networked control systems," in *Proc. 23rd Mediterr. Conf. Control Autom. (MED)*, 2015, pp. 877–882.
- [19] 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.