Resilient Design of Leader-Follower Consensus Against Cyber-Attacks

Mahdieh S. Sadabadi, Made Widhi Surya Atman, Anirudh Aynala, and Azwirman Gusrialdi

***Abstract*—This paper focuses on the development of a resilient cooperative control system for leader-follower consensus problems prone to external cyber-attacks. The attackers are assumed to adversely impact data integrity and privacy by (i) injecting unknown bounded exogenous signals to actuators and (ii) eavesdropping on the physical states of followers. To mitigate the adverse effects of such attacks on the consensus, privacy, and stability of leader-follower systems, we develop a resilient cooperative control system by introducing virtual states interconnected with the physical states in such a way that the leader-follower consensus is guaranteed under unknown false data injection cyber-attacks. The dynamics of the virtual states act as a dynamical output mask, which maps the physical states of followers to some virtual states that are exchanged via a communication network. A Lyapunov-based design framework is proposed to guarantee stability and the leader-follower consensus against cyber-attacks. The decentralized design of the control variables in the proposed resilient cooperative control approach facilitates creating a plug-and-play environment, where follower nodes can easily be plugged in/out. The effectiveness of the theoretical results is evaluated using several numerical examples and implementation on a planar robot experimental testbed.**

***Index Terms*—Resilient cooperative control, leader-follower consensus, cyber-attacks, privacy preservation.**

I. Introduction

Cooperative control systems, in particular leader-follower consensus, have recently been used in various applications including smart grids, intelligent transportation systems, robotics, sensor networks, and AC/DC microgrids [2]–[6]. The cooperative systems bring several potential benefits over centralized counterparts such as improved scalability, reliability, resilience to a single point of failure, and reduced cost. However, the tight coupling between cyber components (computation and communication networks) and physical systems makes the communication channel as well as the control devices become vulnerable to cyber-attacks, which may threaten the system's stability and cause damages to the physical system [7]. A real-world example of such cyber-attacks is the coordinated attack on the Ukraine power grid in 2015 that caused several hours of blackout and affected hundreds of thousands of customers [8].

The primary results of this work have been presented in European Control Conference 21 (ECC21) (see [1]).

M. S. Sadabadi is with the Department of Electrical and Electronic Engineering, University of Manchester, Manchester, United Kingdom (e-mail: mahdieh.sadabadi@manchester.ac.uk).

M. W. S. Atman, A. Aynala, and A. Gusrialdi are with the Faculty of Engineering and Natural Sciences, Tampere University, Tampere 33014, Finland (e-mail: widhi.atman@tuni.fi, anirudhaynala18@gmail.com and azwirman.gusrialdi@tuni.fi). The work of A. Gusrialdi is supported by Academy of Finland under academy project decision no. 330073.

In this paper, the main focus is on cyber-attacks on the actuator of agents in a leader-following consensus. Since cyber-attacks cannot be foreseen in advance, it is thus desirable to design a leader-follower consensus algorithm so that cooperative systems become resilient against unknown attacks.

A number of resilient leader-follower control strategies against attack on the actuators have been proposed in literature. Among those strategies, a mean subsequence reduced algorithm, see e.g., [9]–[11], has been shown to be powerful to achieve resilient leader-follower consensus without requiring any assumptions on the attacker's behavior. The main drawback of these approaches is that there is usually a restriction on the number of compromised nodes, the local number of adversarial nodes in the neighborhood of each intact node, and/or the connectivity of communication graphs.

A resilient leader-follower consensus based on an adaptive control approach in continuous-time is proposed in [12]. This work considers both actuator and sensor attacks and also a dynamic leader. Similarly, an adaptive controller is presented in [13] for achieving resilient consensus for a class of nonlinear systems in discrete-time subject to both actuator and sensor attacks. A secure observer-based consensus protocol in discrete-time is designed in [14] to estimate the attack signals and ensure the boundedness of the consensus error between the leader and followers' states under both actuator and sensor attacks. The proposed methods in [12]–[14] assume that the attack signals and their derivative are both bounded. Besides, in these methods, the design of observer gain or the control gain matrices is based on a centralized approach, which requires the full knowledge of followers. The centralized design prohibits the plug-and-play feature in the leader-follower consensus problem, as the plug-in of a new follower requires the re-design of gain matrices.

A cooperative control method, based on a virtual layer, has been proposed for the leader-follower consensus in [15]–[18] that provides resilience against attacks on communication networks and actuators. A combination of anomaly detector and adaptive attack compensator is developed in [19] to mitigate the adverse impacts of attacks on both sensors and actuators. However, these methods (and the previously mentioned strategies) rely on exchanging the physical states of followers with their neighbors. Such cooperative control strategies disclose the followers' state information and make the cooperative systems at risk of potential privacy threats. Furthermore, the primary results of this paper in [1] do not consider the privacy-preserving aspects of the leader-follower consensus problem. Note that while there exists a line of work that addresses privacy in consensus algorithms, see e.g., [20],

the resilience of the cooperative systems against cyber-attacks is not guaranteed.

In summary, the existing results on resilient cooperative control systems have limitations on the connectivity requirement of communication networks, the number of compromised nodes, the local number of malicious nodes, disclosing the state information of followers, as well as the centralized design of control parameters that might limit the plug-and-play feature of cooperative control systems. Yet, a systematic resilient cooperative control approach, which does not rely on the above-mentioned limitations and guarantees stability and consensus while under unknown external cyber-attacks, is highly desirable.

Motivated by the aforementioned challenges, this paper provides a system-theoretic framework for the leader-follower consensus problem with an emphasis on the resilience against bounded false data injection (FDI) cyber-attacks and privacy-preserving of followers' state information. The FDI attackers aim to adversely impact consensus dynamics by injecting false data into actuators (control input channels). The main objective of this paper is to develop a cooperative control strategy to ensure the leader-follower consensus and to guarantee the stability of the cooperative system against potential unknown attacks while improving the privacy of the state information of followers. Our proposed cooperative control approach consists of introducing a set of virtual states interconnected with the physical states of followers. By virtue of the Lyapunov stability theory and the graph theoretical approach, we show that by an appropriate choice of control parameters, the origin of the global closed-loop system, i.e., the interconnection of the follower/leader nodes and the virtual states, is globally asymptotically stable. The dynamics of the virtual states act as a dynamical output mask, which maps the physical states of followers to some virtual states that are exchanged via the network. The main contributions of the proposed resilient cooperative control mechanism are listed as follows:

- The proposed cooperative control strategy does not require any information about the nature and/or location of false data injection cyber-attacks and does not make any restriction on the number of malicious nodes.
- Unlike the strategies in [12]–[14], the derivative of the attacker's injection signals is not required to be bounded.
- In contrast to the methods presented in [13]–[19], by incorporating the virtual system and exchanging the virtual states instead of physical states, the proposed cooperative control approach improves the privacy of the physical state information against eavesdropping attacks.
- Unlike the proposed cooperative control system in [15]–[18], the design of controller parameters for each follower is decentralized without requiring any knowledge of the parameters of neighboring nodes or their controllers. This facilitates creating a plug-and-play environment, where follower nodes can easily be plugged in/out. Unlike the proposed cooperative control system in [15]–[18], by means of the proposed cooperative control system, an exact leader-follower consensus is guaranteed in the presence of the aforementioned attack types (refer to the consensus analysis in Theorem 1 in Subsection IV-A).

The effectiveness of the proposed resilient cooperative control strategy is demonstrated and evaluated using a planar robot experimental testbed.

Paper Organization: The rest of the paper is organized as follows: The problem statement is presented in Section II. Section III presents a novel resilient cooperative control mechanism and provides a rigorous stability analysis. The attack-resilience and privacy-preserving features of the proposed cooperative control approach are discussed in Section IV. Simulation examples and experimental verification are provided in Section V and Section VI, respectively. Finally, concluding remarks are given in Section VII.

Notation: Throughout this paper, $\mathbf{1}_n$ is an $n\times 1$ vector of ones, $\mathbf{0}_n$ is an $n\times 1$ zero vector, $\mathbf{I}_n$ is an $n\times n$ Identity matrix, and $\mathbf{0}_{n\times m}$ is a zero matrix of dimension $n\times m$. The symbols $Y=\text{diag}(X_1,\ldots,X_n)$, X^T, $X=[x_{i,j}]$, and $[x]$ respectively denote a block diagonal matrix aligning the input matrices $X_1,\ldots,X_n$ along the diagonal of Y, the transpose of matrix X, a matrix with entries $x_{i,j}$, and $[x]=\text{diag}(x_1,x_2,\ldots,x_n)$. For a symmetric matrix X, positive definite and positive semi-definite operators are respectively shown by $X\succ 0$ and $X\succeq 0$. We define $\mathbb{R}_+ := \{x\in\mathbb{R}\ \ |x>0\}$ and $\mathbb{R}_{\geq 0} := \{x\in\mathbb{R}\ \ |x\geq 0\}$.

II. Problem Statement

We consider a cooperative system consisting of $n+1$ nodes, where a leader node is labeled by 0 and follower nodes are labeled by i, $i=1,\ldots,n$. The information flow among the nodes is modeled by a directed graph $\mathscr{G}=(\mathscr{V}(\mathscr{G}),\mathscr{E}(\mathscr{G}))$, where the node set $\mathscr{V}(\mathscr{G})$ and the edge set $\mathscr{E}(\mathscr{G})$ respectively represent the nodes and the integrant information exchange links. Note that $\mathscr{V}(\mathscr{G})$ does not include the leader node. Let $x_i(t)\in\mathbb{R}$ denote the state of the node i whose dynamics are given by

$$\dot{x}_i(t)=u_i(t), \tag{1}$$

for $i\in\mathscr{V}(\mathscr{G})$, where $u_i(t)\in\mathbb{R}$ is the control input of node i. The main objective is to design the control input $u_i(t)$ such that the cooperative system in (1) reaches a consensus, i.e.,

$$\lim_{t\to\infty} x_i(t)=x_0,\ \ \forall i\in\mathscr{V}(\mathscr{G}), \tag{2}$$

where $x_0\in\mathbb{R}$ is the state of the leader node.

Remark 1. *In a multi-agent system whose individual dynamics are given by a heterogeneous nonlinear/linear system, if the individual dynamic system is input passivity-short (or can become input passivity-short by a local feedback controller), then its dynamic behaviors at the network level as well as their network control design can equivalently be transformed to the first-order dynamics in (1) [21]. Hence, in the remainder of this paper, the first-order dynamics in (1) are considered.*

A. Synchronization of Leader-Follower Systems

If node i has access to the state information of its neighbors and the leader node and the graph contains a directed spanning tree with the leader node as the root node, a solution to the consensus problem in (2) is given by [22]:

$$u_i(t)=a_{i0}\left(x_0-x_i(t)\right)+\sum_{j=1}^{n}a_{ij}\left(x_j(t)-x_i(t)\right), \tag{3}$$

for $i \in \mathscr{V}(\mathscr{G})$, where $a_{ij} \in \{0,1\}$, and $a_{ij} = 1$ if node i receives information from node j including the leader node 0; otherwise, $a_{ij} = 0$. The cooperative system with the control protocol (3) can be written in a compact form as follows:

$$\dot{\mathbf{x}}(t) = -(\mathscr{L} + \mathscr{A})\mathbf{x}(t) + (\mathscr{L} + \mathscr{A})\mathbf{1}_n x_0, \tag{4}$$

where $\mathbf{x}(t) = [x_1(t), \ldots, x_n(t)]^T$, $\mathscr{A} = \text{diag}(a_{10}, \ldots, a_{n0})$, and $\mathscr{L}$ is the Laplacian matrix associated with the communication digraph $\mathscr{G}$. As $-(\mathscr{L} + \mathscr{A})$ is Hurwitz [23], (3) guarantees the asymptotic stability of the following closed-loop system on an arbitrary digraph containing a spanning tree [22]:

$$\dot{\mathbf{e}}(t) = -(\mathscr{L} + \mathscr{A})\mathbf{e}(t), \tag{5}$$

where $\mathbf{e}(t) = \mathbf{x}(t) - \mathbf{1}_n x_0$. As a result, $\lim_{t\to\infty} \mathbf{x}(t) = \mathbf{1}_n x_0$ and the consensus objective in (2) is achieved with $\varepsilon = 0$.

The proposed solution in (3) requires that the communication digraph contains a directed spanning tree and the leader is pinned to a root node. Moreover, in the following, we show that the cooperative system in (4) is not resilient against attacks on actuators and also privacy threats disclosing the state information of followers. In this paper, we overcome these issues by developing a new resilient control approach.

B. FDI Cyber-Attack Modeling

The malicious attackers might inject unknown exogenous signals $\delta_{u_i}(t)$ to the control input channels (actuators) of the follower nodes. Such a cyber-attack can be modeled as follows:

$$\hat{u}_i(t) = u_i(t) + \lambda_{u_i}\delta_{u_i}(t), \tag{6}$$

where $\hat{u}_i(t)$ is the corrupted control input and $\lambda_{u_i} \in \{0,1\}$, where $\lambda_{u_i} = 1$ indicates the presence of an attack on the control input of the follower node i. In the presence of the false data injection cyber-attacks in (6), the cooperative system in (4) can be presented as follows:

$$\dot{\mathbf{x}}(t) = -(\mathscr{L} + \mathscr{A})\mathbf{x}(t) + (\mathscr{L} + \mathscr{A})\mathbf{1}_n x_0 + \delta(t), \tag{7}$$

where $\delta(t) = [\delta_1(t), \ldots, \delta_n(t)]^T$ and $\delta_i(t) = \lambda_{u_i}\delta_{u_i}(t)$ describes the attacks on the actuators of the followers. The above closed-loop system no longer guarantees the consensus objective in (2). In the following example, we show that the cooperative control strategy in (3) is not resilient against such attacks.

Example 1. *Consider the following multi-agent system:*

$$\dot{x}_i(t) = u_i(t), \; x_0 = 1, \tag{8}$$

for $i = 1, \ldots, 4$, where $x_i(t) \in \mathbb{R}$ and $u_i(t) \in \mathbb{R}$. The parameters of the control approach in (4) are given as follows:

$$\mathscr{L} = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & -1 & 2 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}, \; \mathscr{A} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{9}$$

In the absence of cyber-attacks, the states of the follower nodes converge to the leader state x_0, i.e., $\lim_{t\to\infty} x_i(t) = 1$ for $i = 1, \ldots, 4$ (see Fig. 1 (a)). However, as observed from Fig. 1 (b), when a constant attack $\delta_{u_i}(t) = 0.5$, $i = 1, \ldots, 4$, is injected to each node, the consensus objective in (2) is no longer satisfied.

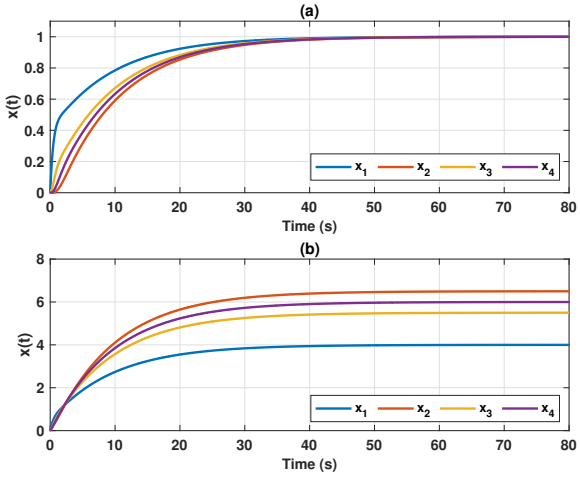


Fig. 1. Trajectories of the followers' state in Example 1: (a) no attack $\delta_u(t) = \mathbf{0}_4$ and (b) a constant attack $\delta_u(t) = 0.5 \times \mathbf{1}_4$.

C. Privacy Preserving Issue

The conventional cooperative system in (4) relies on cooperation amongst follower nodes in terms of exchanging their physical states (i.e., $\mathbf{x}(t)$) in order to achieve the leader-follower consensus objective. The information exchanges in the conventional cooperative system increase the risk of exposing the followers' sensitive information to eavesdropping adversaries, which are privacy threat. We aim to overcome the privacy issue of (3) by developing a new privacy-preserving consensus-based distributed control approach.

The main objective of this paper is to develop an attack-resilient distributed control strategy such that the objective given in (2) is guaranteed in the presence of the cyber-attacks modeled in (6) while the privacy of the follower nodes' physical states and the leader's information are preserved.

III. Resilient Cooperative Control

This section develops a new resilient cooperative control system for the cooperative system in (1). The equilibrium points, stability analysis, as well as plug-and-play capability of the proposed resilient control approach are then discussed.

A. Proposed Resilient Distributed Control Strategy

To guarantee the consensus and the leader-follower tracking performance of the cooperative system in (1) in the presence of cyber-attacks modeled in (6), we propose the following control law for node i in (1):

$$\begin{aligned}
T_{v_i}\dot{v}_i(t) =& -\alpha_i(v_i(t) - \kappa_i x_i(t)) - \frac{K}{\kappa_i}\sum_{j=1}^{n}\gamma_{j,i}(\theta_i(t) - \theta_j(t)) \\
& - \frac{\beta}{\kappa_i}\gamma_{i0}\left(\frac{v_i(t)}{\kappa_i} - x_0\right), \\
T_{\theta_i}\dot{\theta}_i(t) =& -\eta_i\theta_i(t) + \sum_{j=1}^{n}\gamma_{i,j}\left(\frac{v_i(t)}{\kappa_i} - \frac{v_j(t)}{\kappa_j}\right), \\
T_{w_i}\dot{w}_i(t) =& \alpha_i(v_i(t) - \kappa_i x_i(t)), \\
u_i(t) =& k_{1,i}\alpha_i(v_i(t) - \kappa_i x_i(t)) + k_{2,i}x_i(t) + k_{3,i}w_i(t),
\end{aligned} \tag{10}$$

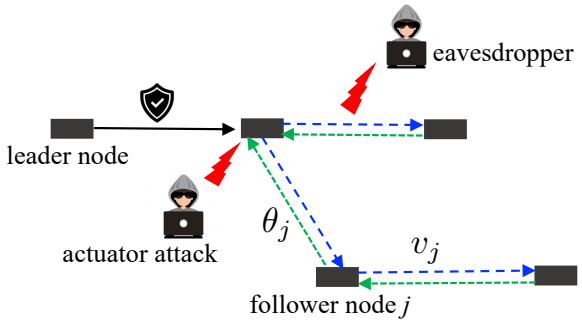


Fig. 2. Resilient design of cooperative systems in (10). The solid black line represents the secured information flow from the leader to the follower nodes. The dashed blue and green lines denote communication links in the resilient cooperative control system in (10).

for $i = 1,\dots,n$. Here, in addition to the physical state $x_i(t)$, each node also includes auxiliary states $(v_i(t), w_i(t), \theta_i(t))$. Note that the auxiliary states do not have any physical meaning and their initial values can be set to any values. Hence, we call them *virtual states*. The parameters $T_{w_i} \in \mathbb{R}_+$, $T_{v_i} \in \mathbb{R}_+$, $T_{\theta_i} \in \mathbb{R}_+$, $K \in \mathbb{R}_+$, $\kappa_i \in \mathbb{R}_+$, $\eta_i \in \mathbb{R}_+$, $\gamma_{ij} \in \mathbb{R}_{\geq 0}$, $\alpha_i \in \mathbb{R}_+$, $\beta \in \mathbb{R}_+$, and $(k_{1,i}, k_{2,i}, k_{3,i})$ are the design parameters of the distributed control protocol that can be designed to guarantee the closed-loop stability in the presence of unknown attacks. Scalar $\gamma_{i0} \in \{0,1\}$, where $\gamma_{i0} = 1$ if the node i receives information from the leader; otherwise, $\gamma_{i0} = 0$. In this work, due to the privacy of followers' state trajectories, it is assumed that the information from the leader to the follower nodes is secured as considered in related work, see e.g., [19]. This can be ensured by investing more security in the communication link between the leader to the follower node. Since the leader only requires to communicate with at least one follower node, securing this link is more reasonable than securing all links in the network. The schematic diagram of the cooperative system and its communication scheme is depicted in Fig. 2.

The dynamics of the virtual states $v_i(t)$, $w_i(t)$, and $\theta_i(t)$ are utilized to mask the local states $x_i(t)$. Thus, the physical state $x_i(t)$ is indirectly embedded in the states of the virtual nodes, i.e., instead of the physical state $x_i(t)$, the virtual states $v_i(t)$ and $\theta_i(t)$ are exchanged amongst other followers as observed from (10) and Fig. 2. However, since $v_i(t)$ asymptotically tracks $x_i(t)$, the leader-follower consensus objective in (2) is achieved. The introduction of the virtual states will also in turn preserve the privacy of the follower nodes' physical states as will be discussed in Section IV-B. Specifically, the dynamics of the virtual states including their interconnection with the physical states are designed to satisfy the following properties: (i) the convergence of the physical states of cooperative systems to the leader's value x_0 is ensured; (ii) the new cooperative system maintains leader-follower consensus objective in (2) in the presence of unknown cyber-attacks on actuators (see Lemma 1 in Section III-B); (iii) the cooperative system enhances the privacy of followers' physical states $x_i(t)$ and the leader information (refer to Section IV-B).

The global closed-loop system, i.e., the interconnection of (1) and (10) in the presence of actuator attacks in (6), can be described in a vector form as follows:

$$
\begin{aligned}
[T_v]\,\dot{\mathbf{v}}(t) =& -[\alpha]\,(\mathbf{v}(t) - [\kappa]\,\mathbf{x}(t)) - K\,[\kappa]^{-1}\,\mathscr{L}_h^T\,\theta(t) \\
& -\beta\,[\kappa]^{-1}\,\mathscr{A}_h\left([\kappa]^{-1}\,\mathbf{v}(t) - \mathbf{1}_n x_0\right), \\
[T_\theta]\,\dot{\theta}(t) =& -[\eta]\,\theta(t) + \mathscr{L}_h\,[\kappa]^{-1}\,\mathbf{v}(t), \\
\dot{\mathbf{x}}(t) =& [k_1]\,[\alpha]\,(\mathbf{v}(t) - [\kappa]\,\mathbf{x}(t)) + [k_2]\,\mathbf{x}(t) + [k_3]\,\mathbf{w}(t) + \delta(t), \\
[T_w]\,\dot{\mathbf{w}}(t) =& [\alpha]\,(\mathbf{v}(t) - [\kappa]\,\mathbf{x}(t)),
\end{aligned}
\tag{11}
$$

where $\mathbf{w}(t) = [w_1(t),\dots,w_n(t)]^T$, $\mathbf{v}(t) = [v_1(t),\dots,v_n(t)]^T$, $\theta(t) = [\theta_1(t),\dots,\theta_n(t)]^T$, $\mathscr{A}_h = \text{diag}\,(\gamma_{10},\dots,\gamma_{n0})$, and $\mathscr{L}_h$ is the Laplacian matrix associated with the communication digraph in Fig. 2, which is not necessarily equal to $\mathscr{L}$.

Next, we introduce the following assumptions on communication digraphs and actuator attacks.

Assumption 1. *It is assumed that the communication digraph in the control layer contains a rooted-out tree. As a result, rank*$(\mathscr{L}_h) = n - 1$.

Note that in Assumption 1, the root of the tree is not necessarily the leader node.

Assumption 2. *It is assumed that the attack signal $\delta(t)$ in (11) is uniformly bounded and does not depend on the physical and/or virtual states in (11).*

Note that Assumption 2 is reasonable and has also been considered in several studies, e.g., for power system applications [24] and [6], as from the attacker's perspective any intelligent attacker would aim at destabilizing the system with a bounded injection to avoid the attack detection [15]. On the other hand, from the defender's perspective, in the case of unbounded injection, simple filtering techniques can be applied to each node in order to remove excessively large signals received from its neighbors [15]. Similarly, excessively large signals observed in the actuators can be also ignored. To this end, a filtering and bad-data-rejection technique based on a threshold-based mechanism has been proposed in [15]. In the following, the existence of equilibria of the cooperative system in (11) in the absence of cyber-attacks $\delta(t)$ is discussed.

B. Existence and Uniqueness of Equilibria

First, the following lemma discusses the existence of the equilibria of the cooperative system (11) in the absence of the attack vector $\delta(t)$.

Lemma 1. *Consider the resilient cooperative system in (11) in the absence of cyber-attacks $\delta(t)$. Under Assumption 1, if $k_{3,i} \neq 0$ for $i \in \mathscr{V}(\mathscr{G})$, there exists a unique equilibrium $(\bar{\mathbf{x}}, \bar{\mathbf{v}}, \bar{\theta}, \bar{\mathbf{w}})$ satisfying*

$$
\bar{\mathbf{x}} = \mathbf{1}_n x_0,\ \bar{\mathbf{v}} = [\kappa]\,\mathbf{1}_n x_0,\ \bar{\theta} = \mathbf{0}_n,\ \bar{\mathbf{w}} = -[k_3]^{-1}\,[k_2]\,\bar{\mathbf{x}}, \tag{12}
$$

where $\bar{\mathbf{x}}$, $\bar{\mathbf{v}}$, $\bar{\mathbf{w}}$, and $\bar{\theta}$ are the equilibrium point of $\mathbf{x}(t)$, $\mathbf{v}(t)$, $\mathbf{w}(t)$, and $\theta(t)$ in (11) in the absence of cyber-attacks $\delta(t)$.

Proof. See Appendix VIII-A. ■

We then define $\mathbf{x}_{\mathbf{cl}}(t) = \left[\ \mathbf{e}_v^T(t)\quad \mathbf{e}_\theta^T(t)\quad \mathbf{e}_x^T(t)\quad \mathbf{e}_w^T(t)\ \right]^T$, where $\mathbf{e}_v(t) = \mathbf{v}(t) - \bar{\mathbf{v}}$, $\mathbf{e}_\theta(t) = \theta(t) - \bar{\theta}$, $\mathbf{e}_x(t) = \mathbf{x}(t) - \bar{\mathbf{x}}$, $\mathbf{e}_w(t) = \mathbf{w}(t) - \bar{\mathbf{w}}$. The vectors $\bar{\mathbf{x}}$, $\bar{\mathbf{v}}$, $\bar{\mathbf{w}}$, and $\bar{\theta}$ are given in (12). Finally, the cooperative system in (11) can be rewritten in the new coordinates by the following state equation:

$$\begin{aligned}\dot{\mathbf{x}}_{\mathbf{cl}}(t) &= \mathbf{A}_{\mathbf{cl}}\mathbf{x}_{\mathbf{cl}}(t)+\mathbf{B}_{\mathbf{cl}}\delta(t),\\ \mathbf{y}(t) &= \mathbf{C}_{\mathbf{cl}}\mathbf{x}_{\mathbf{cl}}(t),\end{aligned} \tag{13}$$

where $\mathbf{A}_{\mathbf{cl}}$ and $\mathbf{B}_{\mathbf{cl}}$ are defined as follows:

$$\begin{aligned}&\mathbf{A}_{\mathbf{cl}} = \tau\mathbf{A},\\ &\tau = \mathrm{diag}([T_v]^{-1},[T_\theta]^{-1},\mathbf{I}_n,[T_w]^{-1})\\ &\mathbf{A}=\begin{bmatrix} -([\alpha]+\beta[\kappa]^{-1}\mathscr{A}_h[\kappa]^{-1}) & -K[\kappa]^{-1}\mathscr{L}_h^T & [\alpha][\kappa] & \mathbf{0}_{n\times n}\\ \mathscr{L}_h[\kappa]^{-1} & -[\eta] & \mathbf{0}_{n\times n} & \mathbf{0}_{n\times n}\\ [k_1][\alpha] & \mathbf{0}_{n\times n} & [k_2]-[k_1][\alpha][\kappa] & [k_3]\\ [\alpha] & \mathbf{0}_{n\times n} & -[\alpha][\kappa] & \mathbf{0}_{n\times n}\end{bmatrix}\\ &\mathbf{B}_{\mathbf{cl}} = \begin{bmatrix}\mathbf{0}_{n\times n} & \mathbf{0}_{n\times n} & \mathbf{I}_n & \mathbf{0}_{n\times n}\end{bmatrix}^T,\\ &\mathbf{C}_{\mathbf{cl}} = \begin{bmatrix}\mathbf{0}_{n\times n} & \mathbf{0}_{n\times n} & \mathbf{I}_n & \mathbf{0}_{n\times n}\end{bmatrix}.\end{aligned} \tag{14}$$

C. Stability Analysis

The following results in Proposition 1 illustrate that for an appropriate choice of the parameters of the cooperative system in (11), the origin of the interconnected system (13) in the absence of the attack vector $\delta(t)$ is globally asymptotically stable.

Proposition 1. *Let Assumption 1 hold. If $\gamma_{i0}\geq 0$ is non-zero for at least one node and $K\in\mathbb{R}_+$, $\beta\in\mathbb{R}_+$, $[\alpha]\succ 0$, $[\kappa]\succ 0$, $[\eta]\succ 0$, $[T_v]\succ 0$, $[T_\theta]\succ 0$, $[T_w]\succ 0$, and $(k_{1,i},k_{2,i},k_{3,i})$ belongs to the following set:*

$$\mathscr{Z}_{[i]} = \left\{ k_{1,i}>0,\ k_{2,i}<0,\ 0<\frac{k_{3,i}}{T_{w_i}}<-k_{1,i}k_{2,i} \right\},\ \forall i\in\mathscr{V}(\mathscr{G}) \tag{15}$$

$\mathbf{A}_{\mathbf{cl}}$ given in (14) is a Hurwitz matrix.

Proof. See Appendix VIII-B. ■

Remark 2. *(Uniformly Ultimately Bounded (UUB) Solution of (11) in the Presence of the Cyber-attack Vector $\delta(t)$).*
As the cyber-attack vector $\delta(t)$ is assumed to be uniformly bounded and does not depend on the closed-loop system states (see Assumption 2), the existence of $\delta(t)$ does not impact the closed-loop stability provided that the parameters of the cooperative control system in (10) are selected according to the conditions given in Proposition 1.

D. Plug-and-Play Capability

One of the main features of the proposed control strategy in (10) is the potential for implementing the plug-and-play functionality of the follower nodes. Since $\mathscr{L}_h$ does not need to be connected, it facilitates a decentralized design. Furthermore, based on the results of Proposition 1, the control design for each node does not require neighboring information.

We consider that there are n follower nodes and the leader-follower consensus is achieved by means of (10) and the Laplacian matrix $\mathscr{L}_h^1$ associated with the communication graph. When a new follower node l is plugged into the cooperative system, it can randomly choose the existing follower nodes and send κ_l to the negibouring nodes or receive κ_j from them according to the new communication network with the new Laplacian matrix $\mathscr{L}_h^2$. Note that the since the adversary does not know the structure of the virtual states, then it is safe to send κ_i. In general, the plug-and-play behaviour can be characterized by a piecewise constant switching function $\sigma(t):\mathbb{R}_{\geq 0}\to\mathscr{T}$, where $\mathscr{T}=\{1,2,\ldots,q\}$ and q is the total number of possible scenarios in the communication graph due to the plug-in or plug-out of the follower nodes. Hence, the cooperative system can be cast as a switched dynamical system with the following dynamics:

$$\dot{\mathbf{x}}_{\mathbf{cl}}(t) = \mathbf{A}_{\mathbf{cl}}^{\sigma(t)}\mathbf{x}_{\mathbf{cl}}(t)+\mathbf{B}_{\mathbf{cl}}\delta(t), \tag{16}$$

where $\mathbf{A}_{\mathbf{cl}}^{\sigma(t)}$ is constructed by replacing $\mathscr{L}_h$ with $\mathscr{L}_h^{\sigma(t)}$ in $\mathbf{A}_{\mathbf{cl}}$ and $\mathbf{B}_{\mathbf{cl}}$ is given in (14).

In the following lemma, the stability of the above switched linear system is analyzed.

Lemma 2. *The origin of the switched dynamical system in (16) is globally asymptotically stable, assuming $\delta(t)=\mathbf{0}_n$.*

Proof. The Lyapunov function in (30) can be considered as a common Lyapunov function for all possible cases $\mathbf{A}_{\mathbf{cl}}^j$, $j\in\mathscr{T}$, of the switched system $\mathbf{A}_{\mathbf{cl}}^{\sigma(t)}$. The rest of the proof is similar to the proof of Proposition 1 in Subsection III-C. ■

IV. Resilience and Privacy-preserving Analysis

This section analyzes the resilient consensus and privacy-preserving feature of the proposed resilient control in (10).

A. Consensus Analysis in the Presence of FDI Cyber-attacks

The following theorem shows that using the proposed method in (11), the leader-follower consensus objective (2) is achieved in the presence of bounded FDI attacks $\delta(t)$.

Theorem 1. *Let Assumption 1 and Assumption 2 hold. Moreover, let us choose $\mathscr{A}_h\succeq 0$ to have at least one positive diagonal element, $K\in\mathbb{R}_+$, $[\kappa]\succ 0$, $\beta\in\mathbb{R}_+$, $[\alpha]\succ 0$, $[T_v]\succ 0$, $[T_\theta]\succ 0$, $[T_w]\succ 0$, and $(k_{1,i},k_{2,i},k_{3,i})$ belongs to the set* (15)*. The states of the cooperative system in (11) are then bounded for any bounded adversary attack $\delta(t)$. Furthermore, $\lim_{t\to\infty}x_i(t)=x_0$, $\forall i\in\mathscr{V}(\mathscr{G})$.*

Proof. As shown in Proposition 1, $\mathbf{A}_{\mathbf{cl}}$ in (14) is a Hurwitz matrix. Hence, the linear cooperative system in (13) in the presence of the attack vector $\delta(t)$ is input-to-state stable. Since $\delta(t)$ is assumed to be bounded (see Assumption 2), the states of the cooperative system are bounded too.

From the closed-loop system in (13), the output vector $\mathbf{y}(t)$ can be obtained as follows:

$$\mathbf{y}(t) = \mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}t}\mathbf{x}_{\mathbf{cl}}(0)+\int_0^t \mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}(t-\tau)}\mathbf{B}_{\mathbf{cl}}\delta(\tau)d\tau. \tag{17}$$

where $\mathbf{x}_{\mathbf{cl}}(0)$ is the initial value of $\mathbf{x}_{\mathbf{cl}}(t)$.

Since $\delta(t)$ is assumed to be uniformly bounded (see Assumption 2), there exists a constant vector $\delta^*\in\mathbb{R}^n$ such that $\left\|\int_0^t \mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}(t-\tau)}\mathbf{B}_{\mathbf{cl}}\delta(\tau)d\tau\right\| \leq \left\|\int_0^t \mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}(t-\tau)}\mathbf{B}_{\mathbf{cl}}\delta^*d\tau\right\|$. Therefore, one can obtain that

$$\lim_{t\to\infty}\|\mathbf{y}(t)\| \leq \lim_{t\to\infty}\left\|\int_0^t \mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}(t-\tau)}\mathbf{B}_{\mathbf{cl}}\delta^*d\tau\right\|. \tag{18}$$

Hence,

$$\lim_{t\to\infty}\|\mathbf{y}(t)\| \leq \left\|-\mathbf{C}_{\mathbf{cl}}{\mathbf{A}_{\mathbf{cl}}}^{-1}\mathbf{B}_{\mathbf{cl}}\delta^*\right\|. \tag{19}$$

In (19), we have used $\lim_{t\to\infty}\left\|\mathbf{C}_{\mathbf{cl}}e^{\mathbf{A}_{\mathbf{cl}}t}\mathbf{x}_{\mathbf{cl}}(0)\right\|=0$, as $\mathbf{A}_{\mathbf{cl}}$ is Hurwitz. It can be shown that ${\mathbf{A}_{\mathbf{cl}}}^{-1}\mathbf{B}_{\mathbf{cl}}$ can be obtained as:

$${\mathbf{A}_{\mathbf{cl}}}^{-1}\mathbf{B}_{\mathbf{cl}} = \begin{bmatrix}\mathbf{0}_{n\times 3n} & [k_3]^{-1}\end{bmatrix}^T. \tag{20}$$

As a result, $\mathbf{C_{cl}}\mathbf{A_{cl}}^{-1}\mathbf{B_{cl}} = \mathbf{0}_{n\times n}$. From this result and (19), it follows that $\lim_{t\to\infty}\mathbf{y}(t) = \mathbf{0}_n$. Thus, $\lim_{t\to\infty}\mathbf{x}(t) = \bar{\mathbf{x}}$, where $\bar{\mathbf{x}} = \mathbf{1}_n x_0$ (see (12)), i.e., the consensus objective in (2) is guaranteed. ■

Remark 3. *In general, the smaller values of* $(T_{v_i}, T_{\theta_i}, T_{w_i})$ *in* (10) *lead to faster transient responses of agents' state trajectories. The value of* $k_{3,i}$ *characterizes a trade-off between the speed of the response and overshoot, i.e., a higher value of* $k_{3,i}$ *will result in a faster transient response but a higher overshoot. Furthermore, the additional term* $k_{1,i}\alpha_i(v_i(t) - \kappa_i x_i(t))$ *in* (10) *does not alter the steady state of the system, as at steady state* $\bar{v}_i = \kappa_i \bar{x}_i$ *holds. However, this term is useful to prevent the occurrence of oscillations in* $x_i(t)$*. The optimal design of* $k_{l,i}$*,* $l = 1,2,3$ *for a desired transient performance requires solving an optimization problem whose cost function is* $\mathscr{L}_2$ *gain of the dynamical system in* (13) *from* $\delta(t)$ *to* $\mathbf{y}(t)$*. The* $\mathscr{L}_2$ *gain minimization can be done via* $\mathscr{H}_\infty$ *control methods [25], thanks to the Bounded Real Lemma [26].*

Remark 4. *According to the results of Theorem 1 and the analysis of equilibria in Lemma 1, by means of the proposed resilient cooperative system in* (11)*, each node i,* $i \in \mathscr{V}(\mathscr{G})$*, is able to detect the existence of FDI integrity attacks on its actuator by checking the steady-state value of* $w_i(t)$*. In other words,* $\bar{w}_i \neq -\frac{k_{2,i}}{k_{3,i}}\bar{x}_i$ *where* $\bar{x}_i = x_0$ *(see Theorem 1) implies the existence of FDI attacks on* $u_i(t)$*.*

B. Dynamic Privacy-preserving Feature

The proposed resilient control approach in (10) does not require exchanging the physical states of follower nodes, i.e., $\mathbf{x}(t)$, amongst their neighbors. Instead, it relies upon exchanging the virtual states, i.e., $\mathbf{v}(t)$ and $\theta(t)$. The dynamics of virtual states map the physical states $\mathbf{x}(t)$ to the virtual states $\mathbf{v}(t)$ and $\theta(t)$; hence, they are called *dynamic output masks*. In particular, the virtual state $v_i(t)$, $i = 1,\ldots,n$, is a *masked output* that asymptotically tracks $\kappa_i x_i(t)$, assuming that $\kappa_i \neq 1$, $i = 1,\ldots,n$. It is worth mentioning that according to the results of Lemma 1 and Proposition 1, $\kappa_i = 1$ does not impact the closed-loop stability and the leader-follower consensus objective in the presence of FDI integrity actuator attacks. However, in this case, $v_i(t)$ asymptotically tracks $x_i(t)$ and as $v_i(t)$ are exchanged amongst agents according to a communication network, the steady-state value of $x_i(t)$ will be disclosed to eavesdropping adversaries. Therefore, for the sake of privacy, the value of $\kappa_i \neq 1$ can be considered in (11), as $\kappa_i \neq 1$ adds an obfuscation phase to the proposed distributed controller to enhance the privacy of agents' states $x_i(t)$.

The following assumptions are made on eavesdropping adversaries' knowledge about the cooperative system:

- A1: The adversaries have access to the output trajectories of follower nodes ($v_i(t)$ and $\theta_i(t)$) and transmitted information ($v_j(t)$ and $\theta_j(t)$) from their neighbors.
- A2: The value of κ_i in (10) is kept "privately" to follower node i and its neighbours. As the adversaries do not know the structure of virtual states, it is safe to send κ_i to other neighbouring followers.

As the dynamics, initial, and steady-state value of *masked output* $v_i(t)$ are different from the physical state $x_i(t)$, and also due to the unknown value of κ_i, estimating $x_i(t)$ from the system dynamics in (11) cannot be cast as a state estimation or observability problem. Therefore, there are two possible approaches to estimate $x_i(t)$ for an eavesdropping adversary. The first approach is based on system identification and then a state estimation approach; however, it requires adversaries' appropriate knowledge of the dynamics of the cooperative system in (11) and also accessing appropriate input-output data. As the adversary might not have a full knowledge of the cooperative system and also, considering that in the cooperative system in (11), the input data is the leader's state that is constant and the output data $\mathbf{v}(t)$ and $\theta(t)$ converge to constant values, the system identification-based approach might not properly work. The second approach could be based on building the dynamic solution of the cooperative system in (11). However, the adversaries' imperfect knowledge about the cooperative system would make it hard to reconstruct the private states $x_i(t)$ from $v_i(t)$ and/or $\theta_i(t)$.

Next, let us assume that the adversary knows the relationship between the steady-state value of both virtual and physical states in (12). Since the communication link from the leader is secured, i.e., it is not accessible by the eavesdropping adversary, and the parameters $\kappa_i, k_{2,i}, k_{3,i}$ are local information kept privately to node i, it would not be possible for the adversary to learn the leader information x_0 by exploiting the structure in (12). As a result, the proposed resilient control scheme in (10) would enhance the privacy of the physical states $\mathbf{x}(t)$ to eavesdropping privacy threats.

V. Simulation Results

In this section, the performance of the proposed resilient distributed control approach is verified by several examples.

Example 2. *Consider the leader-follower problem given in* **Example 1***. We assume that* $\mathscr{L}_h$ *and* $\mathscr{A}_h$ *are respectively equal to* $\mathscr{L}$ *and* $\mathscr{A}$ *given in (9). The parameters of the control layer in (11) are considered as* $[T_\theta] = 10^{-3}\times\mathbf{I}_4$*,* $[T_v] = 10^{-3}\times\mathbf{I}_4$*,* $[T_w] = 10^{-1}\mathbf{I}_4$*,* $[\eta] = \mathbf{I}_4$*,* $K = 10$*,* $[\alpha] = 10\times\mathbf{I}_4$*,* $\beta = 1$*,* $[k_1] = 11\times\mathbf{I}_4$*,* $[k_2] = -120\times\mathbf{I}_4$*, and* $[k_3] = 120\times\mathbf{I}_4$*. The performance of the proposed control technique in (10) is assessed under three cases: (i) no attack scenario* $\delta(t) = 0$*, (ii) constant attacks* $\delta(t) = 4\times\mathbf{1}_4$ *on actuators launched at* $t = 5$ *s, and (iii) cyber-attacks with the following dynamics launched at* $t = 5$ *s on actuators:*

$$\dot{\delta}(t) = A_d\delta(t) + B_d\delta_0(t), \tag{21}$$

where

$$\delta_0(t) = 4\times\mathbf{1}_4, \quad A_d = -\mathbf{I}_4, \quad B_d = \begin{bmatrix} 1 & 2 & 4 & 2 \\ -9 & 4 & 1 & 3 \\ -4 & 3 & 1 & 2 \\ 2 & 1 & 4 & 3 \end{bmatrix}. \tag{22}$$

Note that the above attack dynamics are not known to agents. The states of the follower nodes are shown in Fig. 3 (a)-(c). This figure illustrates that the effects of the cyber-attacks $\delta(t)$ *on* $\mathbf{x}(t)$ *are compensated by means of the attack-resilient cooperative system in (11). As expected from Theorem 1, the proposed resilient control framework achieves consensus in the presence of cyber-attacks; moreover, the followers track the leader node with a zero steady-state error.*

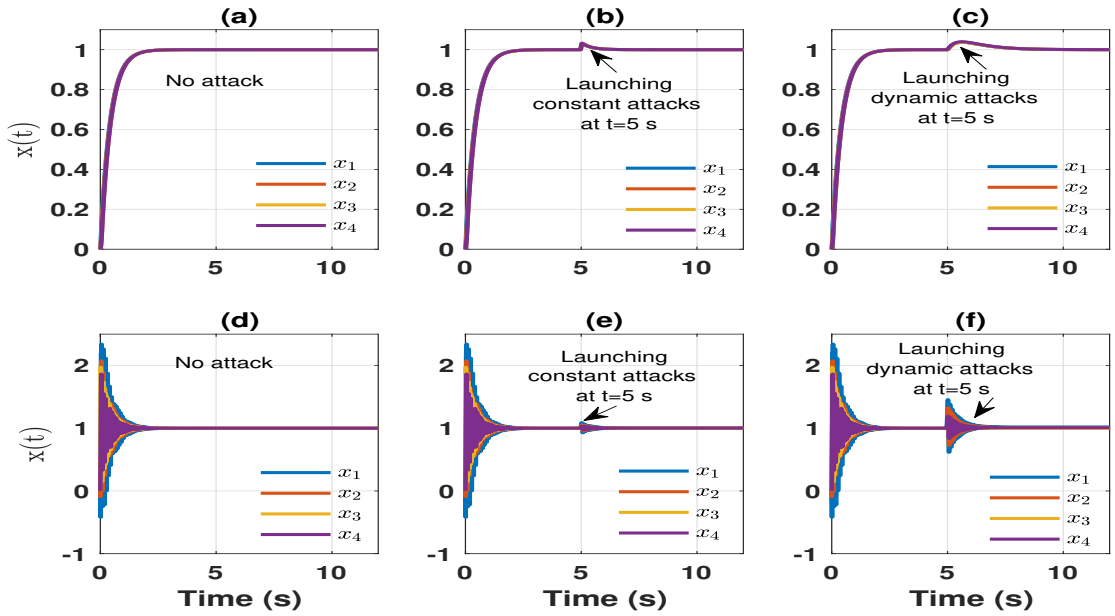


Fig. 3. State trajectories of the followers in Example 2 with the proposed resilient cooperative control system in (10) and [15]: (a) Results of (10) in the absence of cyber-attacks, (b) results of (10) in the presence of a constant attack $\delta(t) = 4 \times \mathbf{1}_4$ launched at $t = 5$ s, (c) results of (10) in the presence of attack dynamics in (21)-(22) launched at $t = 5$ s, (d) results of [15] in the absence of cyber-attacks, (e) results of [15] in the presence of a constant attack $\delta(t) = 4 \times \mathbf{1}_4$ launched at $t = 5$ s, and (f) results of [15] in the presence of attack dynamics in (21)-(22) launched at $t = 5$ s.

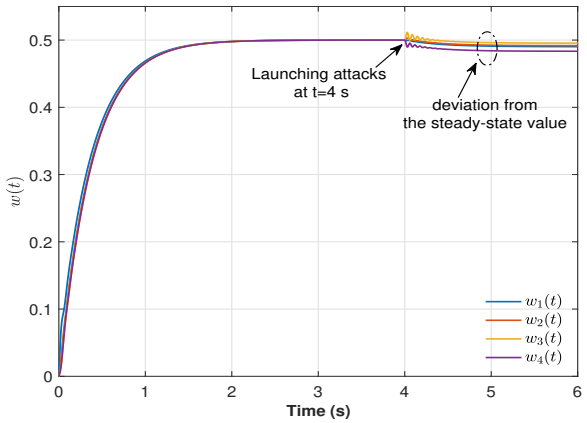


Fig. 4. Auxiliary control state $w(t)$ of the followers in Example 3 in the presence of the actuator attacks launched at $t = 4$ s.

In the following, we highlight the performance of the proposed resilient cooperative control system in (10) compared to the existing approaches. To this end, the proposed resilient virtual-layer-based cooperative control mechanism in [15] is deployed. In this control strategy, the control parameter β is chosen to be equal to 25. Note that although increasing the value of β improves leader-follower tracking performance in the presence of cyber-attacks, it makes the dynamic responses of the follower states more oscillatory. The state trajectories of the follower nodes using this control approach are depicted in Fig. 3 (d)-(f). The results in Fig. 1 and Fig. 3 show the superiority of the performance of the proposed resilient controller in (10) compared to the conventional method in (3) and the proposed resilient cooperative control in [15].

Example 3. *We consider the problem of the leader-follower over a digraph with the following Laplacian matrix:*

$$\mathscr{L}_h = \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}. \tag{23}$$

It is assumed that only follower 1 has access to the leader information $x_0 = 0.5$. In this case, the communication graph contains a rooted-out tree. The attack dynamics are considered as $\delta_1(t) = (1 + 0.2sin(0.2t))U_4(t)$, $\delta_2(t) = U_4(t)$, $\delta_3(t) = (0.5 + 0.1sin(0.1t))U_4(t)$, and $\delta_4(t) = 2U_4(t)$, where $U_4(t) = 0$ $\forall t < 4$ and $U_4(t) = 1$ $\forall t \geq 4$. Fig. 4 demonstrates the impact of the actuator attacks on deviation of the auxiliary state $w(t)$ from its steady-state values, as discussed in Remark 4.

In order to show the stability of the proposed cooperative control system in (11) in terms of the plug-in of new followers, it is assumed that a new follower node, denoted by Follower 5, is plugged into the cooperative system at $t = 6$ s. In this case, the directed communication graph is based on the following Laplacian matrix:

$$\mathscr{L}_h = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & -1 & 0 & 0 & 1 \end{bmatrix}. \tag{24}$$

Fig. 5 shows the state trajectories of all followers due to launching cyber-attacks and the plug-in of follower 5. As stated in Section III-D, the proposed resilient control strategy in (10) provides a plug-and-play environment where the followers can freely connect to the cooperative system without any requirements for modifying the control parameters of other followers.

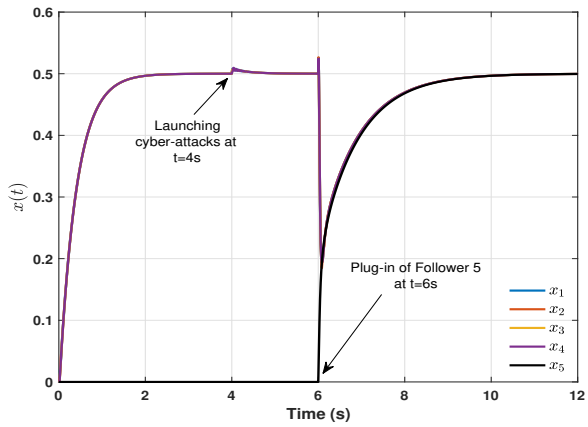


Fig. 5. State trajectories of the followers in Example 3 in the presence of attacks on the actuators of all follower nodes launched at $t = 4$ s and the plug-in of a new follower at $t = 6$ s.

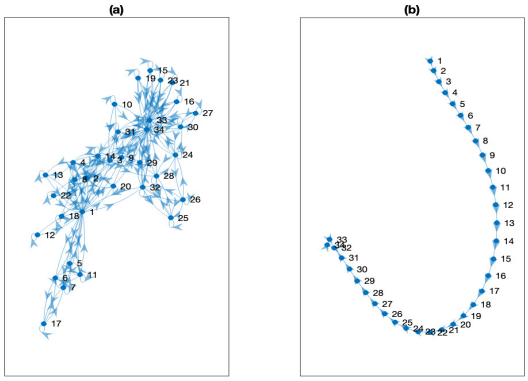


Fig. 6. Communication digraphs in Example 4 with (a) a symmetric Laplacian matrix and (b) an asymmetric Laplacian matrix.

Example 4. *In Example 4, a multi-agent system of* $n = 34$ *followers is considered. We consider two Laplacian matrices corresponding to two communication digraphs, as depicted in Fig. 6, one is assumed to be symmetric and strongly connected and the second one contains a rooted-out tree. In this example, the leader's state is* $x_0 = 1$. *It is assumed that all the actuators are subject to FDI cyberattacks* $\delta(t) = 0.5\mathbf{1}_n$ *launched at* $t = 5$ s. *The followers' state trajectories for both communication digraphs are depicted in Fig. 8.*

In this example, the control parameters in (10) *are selected as:* $\beta = 5$, $\eta_i = 10$, $T_{v_i} = 0.1$, $T_{\theta_i} = 0.1$, $T_{w_i} = 0.1$, $\kappa_i = 0.2$, $\alpha_i = 10$, $k_{1,i} = 11$, $k_{2,i} = -10$, *and* $k_{3,i} = 10$ *for* $i = 1, \ldots, 34$. *The stabilizing set* $\mathscr{Z}_{[i]}$ *in* (15) *bounds the upper bound of* $k_{3,i}$ *at the value of* 11. *Fig. 7 shows the impact of* $k_{3,i}$ *on the transient response of nodes' state* $x_i(t)$. *The higher values of* $k_{3,i}$ *leads to a faster response with larger overshoot.*

VI. Experimental Verification

Finally, we demonstrate and evaluate the implementation of the proposed resilient cooperative control algorithms on a planar robotic experimental testbed.

A. Experiment Setup

The experimental setup is illustrated in Fig. 9. In the experiment, we use Linux Ubuntu 20 as the workspace environment.

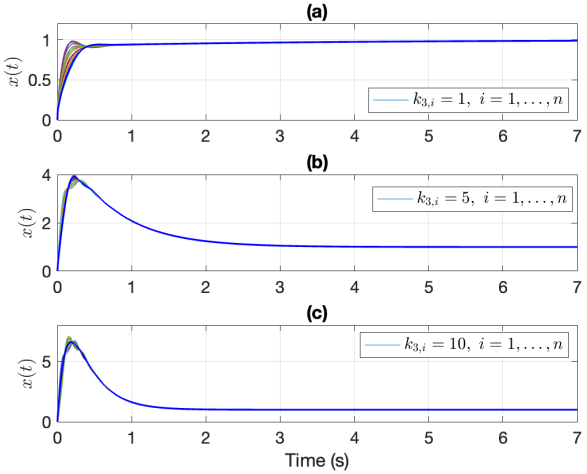


Fig. 7. State trajectories of the followers in Example 4 with a symmetric and strongly connected communication digraph for different values of $k_{3,i}$: (a) $k_{3,i} = 1$, (b) $k_{3,i} = 5$, and (c) $k_{3,i} = 10$.

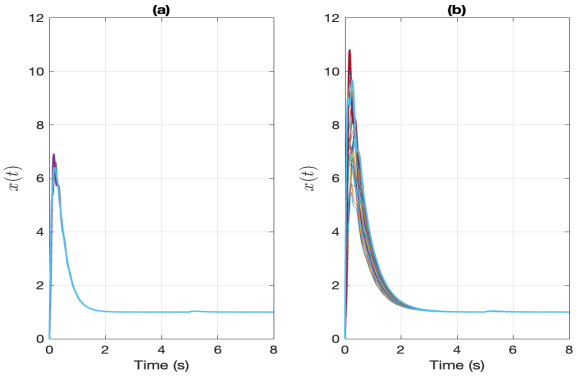


Fig. 8. State trajectories of the followers in Example 4 in the presence of FDI actuator attacks launched at $t = 5$ s in two cases: (a) a communication digraph with a symmetric Laplacian matrix and (b) a communication digraph with an asymmetric Laplacian matrix.

Furthermore, we use three TurtleBot3 Burger robots, which is a unicycle-like mobile robots with a maximum translational and rotational velocity of 0.22 m/s and 2.84 rad/s, respectively. Feature points with different colors are attached to the top of each robot. A camera (ZED 2) is installed on the ceiling and captures the image of the robots on the field and calculates the positions and orientations of all the robots by using a feature extraction algorithm implemented in OpenCV 4.0.

The cooperative control algorithms are implemented on ROS (Robot Operating System). Note that as the single-integrator input (1) is not directly implementable on the unicycle-like robot, we apply a transformation based on a near-identity diffeomorphism that maps the input of the single-integrator model input $(\dot{s}_i^x, \dot{s}_i^y)$ to the unicycle model input (v_i, ω_i) and vice versa. Specifically, from Fig. 11 we have [27]

$$\begin{bmatrix} s_i^x \\ s_i^y \end{bmatrix} = \begin{bmatrix} p_i^x \\ p_i^y \end{bmatrix} + \ell \begin{bmatrix} \cos(\theta_i) \\ \sin(\theta_i) \end{bmatrix}, \tag{25}$$

and the robot's body velocity can be modeled as

$$\begin{bmatrix} \dot{p}_i^x \\ \dot{p}_i^y \\ \dot{\theta}_i \end{bmatrix} = \begin{bmatrix} \cos(\theta_i) & 0 \\ \sin(\theta_i) & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v_i \\ \omega_i \end{bmatrix}. \tag{26}$$

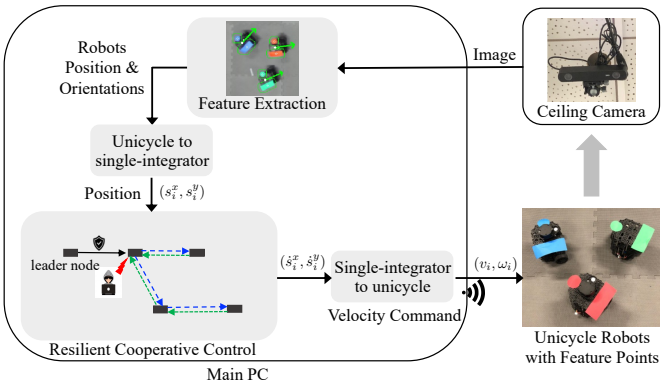


Fig. 9. Experimental system.

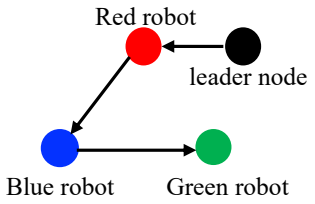


Fig. 10. The communication network topology used in the experiment consists of three follower robots, namely red, blue, and green robots.

From (25), (26) we have the following relation:

$$\begin{bmatrix} v_i \\ \omega_i \end{bmatrix} = \begin{bmatrix} \cos(\theta_i) & \sin(\theta_i) \\ -\frac{1}{\ell}\sin(\theta_i) & \frac{1}{\ell}\cos(\theta_i) \end{bmatrix} \begin{bmatrix} \dot{s}_i^x \\ \dot{s}_i^y \end{bmatrix}, \tag{27}$$

where we set $\ell = 0.06$ m in the experiment. The calculated velocity commands (v_i, ω_i) are then sent to the individual robot using Wi-Fi. As can be observed from Fig. 9, the computation of resilient cooperative control is performed in the main PC by considering the sparsity of the Laplacian matrices. This setup simplifies the implementation of the control algorithm. Distributed implementation of the resilient control algorithm by utilizing the robot's on-board computational resource is the subject of future work. In addition, since we do not explicitly take into account collision avoidance among the robots (which is not the focus of the paper), we add biases to the actual robot positions as done in [28], [29] to avoid collisions, at least in the final positions. Specifically, the bias added to the blue robot is equal to $(0.8, 0)$ m, the green robot is equal to $(-0.8, 0)$ m and the red robot is equal to $(0, 0)$ m. Hence, the positions (s_i^x, s_i^y) can be regarded as virtual/biased positions.

B. Scenarios and Results

First, we implement the conventional leader-following consensus without cyber-attacks in (4) and communication topology given in Fig. 10. The true and biased positions of the robots are shown in Fig. 12 (a) and Fig. 13 (a), respectively. As one can observe from Fig. 13 (a), the biased positions of all the follower robots converge to the position specified by the leader node (i.e., goal position) in the absence of attacks.

Next, we consider the case where an adversary inserts unknown injections starting from $t = 0\,s$ to the actuators of the blue and green robots as in (7) with $\delta(t) = [0, 0.2, -0.1]^T$ for both x-axis and y-axis directions. The true and biased positions

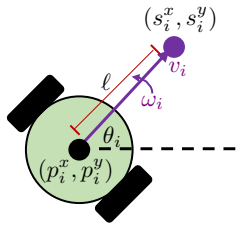


Fig. 11. The centroid position of unicycle model (p_i^x, p_i^y), its orientation θ_i and the input is given by (v_i, ω_i). The position of the corresponding single integrator model (s_i^x, s_i^y) is represented by the purple point projected at distance ℓ in the direction of velocity vector.

of the robots are shown in Fig. 12 (b) and Fig. 13 (b), respectively. As one can observe from Fig. 12 (b) and Fig. 13 (b), without the resilient control both the blue and green robots were not able to converge to the locations specified by the leader node. Finally, we implement the proposed resilient cooperative control algorithms in (11) where the Laplacian matrix $\mathscr{L}_h$ is chosen to be similar to the structure in Fig. 10 and the other parameters are set to $T_{v_i} = 1$, $T_{\theta_i} = 1$, $T_{w_i} = 1$, $k_{1,i} = 1$, $k_{2,i} = -2$ for $i = 1, 2, 3$, $k_{3,1} = 1$, $k_{3,2} = 0.25$, $k_{3,3} = 0.25$, $[\eta] = [\kappa] = \mathbf{I}_3$, $[\alpha] = 10^{-1}\mathbf{I}_3$, $\beta = 3$, $K = 1$. The true and biased positions of the robots are shown in Fig. 12 (c) and Fig. 13 (c), respectively. As can be observed from Fig. 13 (c), the biased positions of all three robots converge to the position specified by the leader node in the presence of cyber-attacks. For comparison, we also implement the resilient cooperative control proposed in [15] with the gain $\beta = 1.5$ and whose resulting trajectories are shown in Fig. 12 (d) and Fig. 13 (d). It can be observed from Fig. 13 (c) and Fig. 13 (d) that in comparison to the method presented in [15], even though the proposed resilient control yields a larger overshoot, the steady-state error is zero and the robots' trajectories are also smoother (less oscillatory). The videos of the experiments are available via the following link: `https://youtu.be/mQMrcyroplk`

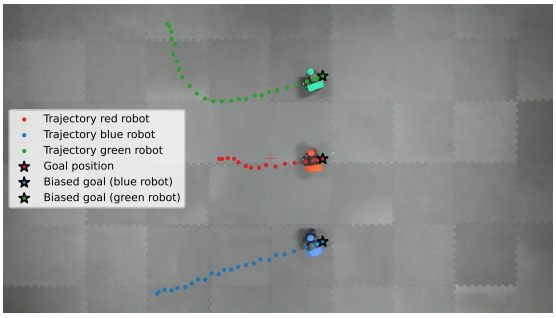
VII. Conclusion

In this paper, a resilient cooperative control strategy for the leader-follower consensus problem in the presence of cyber-attacks is proposed. The attacks are assumed to infiltrate actuators by injecting bounded false data. An attack-resilient cooperative control framework is developed and investigated under unknown bounded attacks. In contrast to the existing literature, our proposed solution does not require the connectivity of communication graphs and also does not rely on exchanging the physical states of followers; hence, enhancing the privacy of followers' state information. By virtue of the Lyapunov stability method and network control theory, a concise stability certificate is derived and the leader-follower consensus is guaranteed against attacks. Illustrative examples and implementation on experimental testbed verify the effectiveness of the proposed cooperative control strategy. The future directions of this work include the extension of results to (i) higher-order systems, (ii) time-varying leader states, and (iii) cyber-attacks in communication networks.

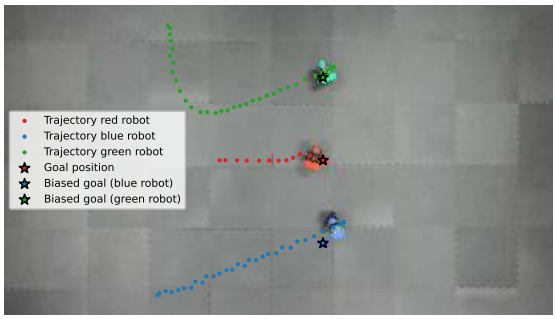
VIII. Appendices

A. Proof of Lemma 1

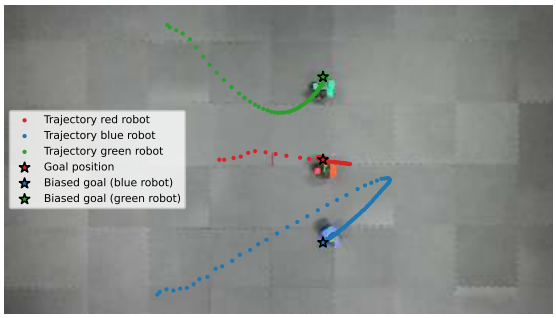
Consider the cooperative system in (11). The equilibria of (11) in the absence of cyber-attacks, i.e., $\delta(t) = 0$, can be



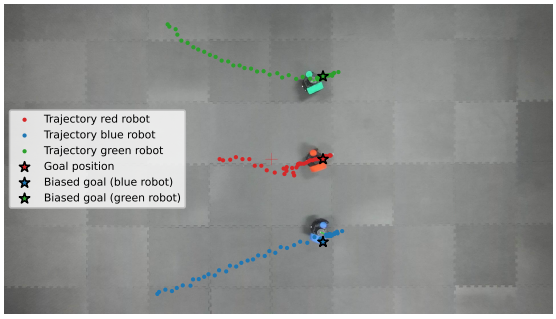
(a) Standard leader-follower consensus in the absence of attacks.



(b) Leader-follower consensus algorithm in presence of attacks.



(c) Proposed resilient cooperative control in presence of attacks.



(d) Resilient cooperative control proposed in [15] with $\beta = 1.5$.

Fig. 12. Trajectories (positions) of the robots in the experiment. The goal position is specified by the leader node.

obtained by solving the following algebraic equations:

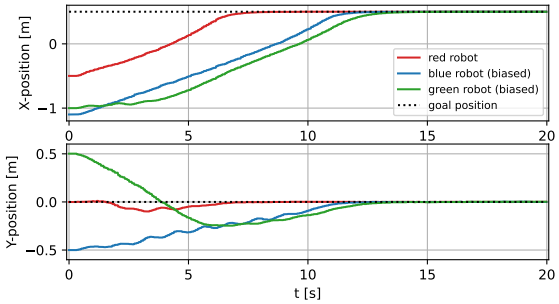
$$\mathbf{0}_n = -[\eta]\,\bar{\theta} + \mathscr{L}_h\,[\kappa]^{-1}\,\bar{\mathbf{v}}, \tag{28a}$$

$$\mathbf{0}_n = [\alpha]\,(\bar{\mathbf{v}} - [\kappa]\,\bar{\mathbf{x}}), \tag{28b}$$

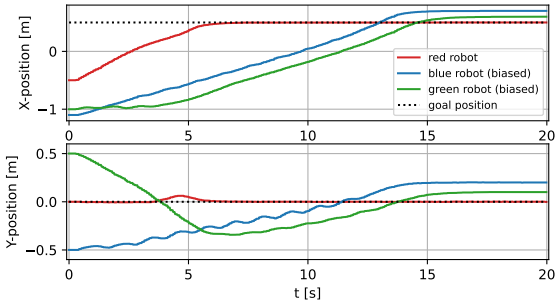
$$\mathbf{0}_n = -[\alpha]\,(\bar{\mathbf{v}} - [\kappa]\,\bar{\mathbf{x}}) - K\,[\kappa]^{-1}\,\mathscr{L}_h^T\,\bar{\theta} - \beta\,[\kappa]^{-1}\,\mathscr{A}_h([\kappa]^{-1}\,\bar{\mathbf{v}} - \mathbf{1}_n x_0), \tag{28c}$$

$$\mathbf{0}_n = [k_1]\,[\alpha]\,(\bar{\mathbf{v}} - [\kappa]\,\bar{\mathbf{x}}) + [k_2]\,\bar{\mathbf{x}} + [k_3]\,\bar{\mathbf{w}}. \tag{28d}$$

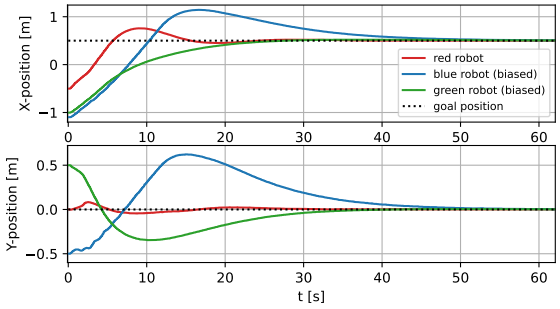
From (28a) and (28b), one obtains that $\bar{\theta} = [\eta]^{-1}\,\mathscr{L}_h\,[\kappa]^{-1}\,\bar{\mathbf{v}}$ and $\bar{\mathbf{x}} = [\kappa]^{-1}\,\bar{\mathbf{v}}$. By replacing $\bar{\mathbf{x}}$ and $\bar{\theta}$ with $[\kappa]^{-1}\,\bar{\mathbf{v}}$ and $[\eta]^{-1}\,\mathscr{L}_h\,[\kappa]^{-1}\,\bar{\mathbf{v}}$ in (28c), one obtains that



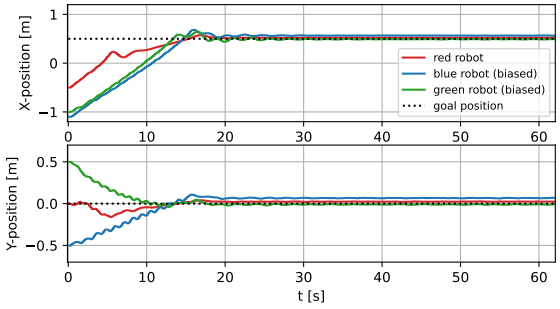
(a) Standard leader-follower consensus in the absence of attacks.



(b) Leader-follower consensus algorithm in presence of attacks.



(c) Proposed resilient cooperative control in presence of attacks.



(d) Resilient cooperative control proposed in [15] with $\beta = 1.5$.

Fig. 13. Biased positions of the robots in the experiment. Biased positions of the robots converge to the desired position specified by the leader node in presence of cyber-attacks.

$$-[\kappa]^{-1}\left(K\mathscr{L}_h^T\,[\eta]^{-1}\,\mathscr{L}_h\,[\kappa]^{-1}\,\bar{\mathbf{v}} + \beta\mathscr{A}_h\left([\kappa]^{-1}\,\bar{\mathbf{v}} - \mathbf{1}_n x_0\right)\right) = \mathbf{0}_n.$$

Using the properties of the Laplacian $\mathscr{L}_h$ as $\mathscr{L}_h\mathbf{1}_n = \mathbf{0}_n$ (see Assumption 1), from the above equation, it follows that

$$\underbrace{\left(K\mathscr{L}_h^T\,[\eta]^{-1}\,\mathscr{L}_h + \beta\mathscr{A}_h\right)}_{\mathscr{X}}\left([\kappa]^{-1}\,\bar{\mathbf{v}} - \mathbf{1}_n x_0\right) = \mathbf{0}_n. \tag{29}$$

Since $\mathscr{L}_h^T\,[\eta]^{-1}\,\mathscr{L}_h \succeq 0$, $\mathscr{A}_h \succeq 0$, and $rank(\mathscr{L}_h^T\,[\eta]^{-1}\,\mathscr{L}_h) = n-1$, it can be shown that $\mathscr{X} \succ 0$. Hence, $\mathscr{X}$ is invert-

ible. Therefore, (29) results in $[\kappa]^{-1}\bar{\mathbf{v}} = \mathbf{1}_n x_0$. As a result, $\bar{\mathbf{x}} = [\kappa]\bar{\mathbf{v}} = \mathbf{1}_n x_0$. By replacing $\bar{\mathbf{x}}$ and $\bar{\mathbf{v}}$ in (28d), it follows that $\bar{\mathbf{w}} = -[k_3]^{-1}[k_2]\bar{\mathbf{x}}$. Note that since $k_{3,i}$ is assumed to be non-zero (see (15)), $[k_3]^{-1}$ exists. Furthermore, from $\bar{\theta} = [\eta]^{-1}\mathscr{L}_h[\kappa]^{-1}\bar{\mathbf{v}}$ and $\bar{\mathbf{v}} = [\kappa]\mathbf{1}_n x_0$, one obtains that $\bar{\theta} = \mathbf{0}_n$.

B. Proof of Proposition 1

Let $\delta(t) = \mathbf{0}_n$ in (13). Then, in order to show that $\mathbf{A_{cl}}$ in (14) is Hurwitz, it suffices to show that the origin in (13) is globally asymptotically stable. To this end, the following quadratic-type Lyapunov function is considered:

$$\begin{aligned}\mathscr{V}(\mathbf{x_{cl}}(t)) = &\frac{1}{2}\mathbf{e}_v^T(t)[T_v]\mathbf{e}_v(t) + \frac{K}{2}\mathbf{e}_\theta^T(t)[T_\theta]\mathbf{e}_\theta(t)\\ &+\frac{1}{2}\sum_{i=1}^{n}[e_{x_i}(t)\ e_{w_i}(t)]P_i[e_{x_i}(t)\ e_{w_i}(t)]^T,\end{aligned} \tag{30}$$

where $P_i \in \mathbb{R}^{2\times 2}$ is defined as follows:

$$P_i = \kappa_i\begin{bmatrix}\rho_i & -\frac{1}{T_{w_i}}\rho_i\nu_i\\ -\frac{1}{T_{w_i}}\rho_i\nu_i & \nu_i(1+\frac{1}{T_{w_i}^2}\rho_i\nu_i)\end{bmatrix}, \tag{31}$$

where ρ_i and ν_i are determined based on any values of $(k_{1,i}, k_{2,i}, k_{3,i}, T_{w_i})$ in $\mathscr{Z}_{[i]}$ given in (15) as follows:

$$\rho_i = \frac{k_{2,i}}{k_{2,i}k_{1,i} + \frac{1}{T_{w_i}}k_{3,i}},\ \nu_i = -T_{w_i}\frac{k_{3,i}}{k_{2,i}}. \tag{32}$$

According to the set $\mathscr{Z}_{[i]}$ in (15), $\rho_i \in \mathbb{R}_+$ and $\nu_i \in \mathbb{R}_+$. Moreover, since $trace(P_i) > 0$, $det(P_i) > 0$, and $P_i \in \mathbb{R}^{2\times 2}$, it can be shown that P_i is a positive-definite matrix, i.e., $P_i \succ 0$. The time derivative of $\mathscr{V}(\mathbf{x_{cl}}(t))$ in (30) along the closed-loop trajectories in (13) is expressed as follows:

$$\begin{aligned}\dot{\mathscr{V}}(\mathbf{x_{cl}}(t)) = &-0.5\left(\mathbf{e}_v^T(t)[\alpha](\mathbf{e}_v(t) - [\kappa]\mathbf{e}_x(t))\right)\\ &-0.5\left((\mathbf{e}_v(t) - [\kappa]\mathbf{e}_x(t))^T[\alpha]\mathbf{e}_v(t)\right) - K\mathbf{e}_\theta^T(t)[\eta]\mathbf{e}_\theta(t)\\ &-0.5K\left(\mathbf{e}_v^T(t)[\kappa]^{-1}\mathscr{L}_h^T\mathbf{e}_\theta(t) + \mathbf{e}_\theta^T(t)\mathscr{L}_h[\kappa]^{-1}\mathbf{e}_v(t)\right)\\ &-0.5K\mathbf{e}_v^T(t)\left([\kappa]^{-1}\mathscr{A}_h[\kappa]^{-1} + [\kappa]^{-1}\mathscr{A}_h^T[\kappa]^{-1}\right)\mathbf{e}_v(t)\\ &+0.5K\left(e_\theta^T(t)\mathscr{L}_h[\kappa]^{-1}\mathbf{e}_v(t) + \mathbf{e}_v^T(t)[\kappa]^{-1}\mathscr{L}_h^T\mathbf{e}_\theta(t)\right)\\ &+0.5\sum_{i=1}^{n}[e_{x_i}(t)\ e_{w_i}(t)]Q_i[e_{x_i}(t)\ e_{w_i}(t)]^T\\ &+0.5\sum_{i=1}^{n}\alpha_i[e_{x_i}(t)\ e_{w_i}(t)]P_iH_i(e_{v_i}(t) - \kappa_i e_{x_i}(t))\\ &+0.5\sum_{i=1}^{n}\alpha_i(e_{v_i}(t) - \kappa_i e_{x_i}(t))^T H_i^T P_i[e_{x_i}(t)\ e_{w_i}(t)]^T,\end{aligned} \tag{33}$$

where

$$Q_i = P_i\begin{bmatrix}k_{2,i} & k_{3,i}\\ 0 & 0\end{bmatrix} + \begin{bmatrix}k_{2,i} & k_{3,i}\\ 0 & 0\end{bmatrix}^T P_i,\ H_i = \begin{bmatrix}k_{1,i} & \frac{1}{T_{w_i}}\end{bmatrix}^T.$$

In the next step, we will show that $\dot{\mathscr{V}}(\mathbf{x_{cl}}) \le 0$. By direct calculations and taking into account (31)-(32), it follows that

$$\rho_i(k_{1,i} - \frac{1}{T_{w_i}^2}\nu_i) = 1,\ Q_i = 2\kappa_i\rho_i\begin{bmatrix}k_{2,i} & -\frac{k_{2,i}}{T_{w_i}}\nu_i\\ -\frac{k_{2,i}}{T_{w_i}}\nu_i & \frac{\nu_i^2}{T_{w_i}^2}k_{2,i}\end{bmatrix},\ P_iH_i = \begin{bmatrix}\kappa_i\\ 0\end{bmatrix}$$

Therefore, considering the above equations, $\dot{\mathscr{V}}(\mathbf{x_{cl}}(t))$ in (33) can be rewritten as

$$\begin{aligned}\dot{\mathscr{V}}(\mathbf{x_{cl}}(t)) = &-\beta\frac{K}{2}\mathbf{e}_v^T(t)\left([\kappa]^{-1}\mathscr{A}_h[\kappa]^{-1} + [\kappa]^{-1}\mathscr{A}_h^T[\kappa]^{-1}\right)\mathbf{e}_v(t)\\ &+\frac{1}{2}\sum_{i=1}^{n}[e_{x_i}(t)\ e_{w_i}(t)]Q_i[e_{x_i}(t)\ e_{w_i}(t)]^T - K\mathbf{e}_\theta^T(t)[\eta]\mathbf{e}_\theta(t)\\ &-(\mathbf{e}_v(t) - [\kappa]\mathbf{e}_x(t))^T[\alpha](\mathbf{e}_v(t) - [\kappa]\mathbf{e}_x(t)).\end{aligned}$$

In can be shown that the eigenvalues of Q_i are $\lambda_{i,1} = 0$ and $\lambda_{i,2} = 2\rho_i\kappa_i k_{2,i}(1 + \frac{v_i^2}{T_{w_i}^2}) < 0$; thus, $Q_i \preceq 0$. As $Q_i \preceq 0$, $[\alpha] \succ 0$, and $[\kappa]^{-1}\mathscr{A}_h[\kappa]^{-1} + [\kappa]^{-1}\mathscr{A}_h^T[\kappa]^{-1} \succeq 0$, $\dot{\mathscr{V}}(\mathbf{x_{cl}}) \le 0$. In the final step, we use the LaSalle's Invariance Principle to show the globally asymptotic stability of the origin in (13) with $\delta(t) = \mathbf{0}_n$. To this end, we define $\mathscr{S} = \{\mathbf{x_{cl}}(t) :\ \dot{\mathscr{V}}(\mathbf{x_{cl}}(t)) = \mathbf{0}_n\}$. If $\dot{\mathscr{V}}(\mathbf{x_{cl}}(t)) = 0$, then $\mathbf{e}_v = [\kappa]\mathbf{e}_x$, $\mathbf{e}_\theta = \mathbf{0}_n$, $[\kappa]^{-1}\mathscr{A}[\kappa]^{-1}\mathbf{e}_v = 0$, and $[e_{x_i}(t)\ e_{w_i}(t)]^T \in ker(Q_i)$, $i \in \mathscr{V}(\mathscr{G})$. The null-space of Q_i is characterized as $e_{x_i}(t) = T_{w_i}^{-1}\nu_i e_{w_i}(t)$. Taking into account $\mathscr{S}$, the closed-loop trajectories in (13) imply $\mathscr{L}_h[\kappa]^{-1}\mathbf{e}_v = \mathbf{0}_n$. Therefore, $\mathbf{e}_v = \mathbf{e}_x = \mathbf{0}_n$ and $\mathbf{e}_w = \mathbf{0}_n$. Thus, the only solution that stays identically in $\mathscr{S}$ is $\mathbf{x_{cl}}(t) = \mathbf{0}_{4n}$. Hence, the origin in (13) in the absence of $\delta(t)$ is globally asymptotically stable. As a result, $\mathbf{A_{cl}}$ in (14) is Hurwitz.

REFERENCES

[1] M. S. Sadabadi and A. Gusrialdi, "On resilient design of cooperative systems in presence of cyber-attacks," in *European Control Conference (ECC21)*, June-July 2021.

[2] A. Maknouninejad and Z. Qu, "Realizing unified microgrid voltage profile and loss minimization: A cooperative distributed optimization and control approach," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1621–1630, 2014.

[3] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 215–233, 2007.

[4] Wei Ren, R. W. Beard, and E. M. Atkins, "A survey of consensus problems in multi-agent coordination," in *Proceedings of the 2005, American Control Conference, 2005.*, vol. 3, 2005, pp. 1859–1864.

[5] M. S. Sadabadi, "A distributed control strategy for parallel DC-DC converters," *IEEE Control Systems Letters*, vol. 5, no. 4, pp. 1231–1236, Oct. 2021.

[6] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "A fully resilient cyber-secure synchronization strategy for AC microgrids," *IEEE Transactions on Power Electronics*, vol. 36, no. 12, pp. 13 372–13 378, Dec. 2021.

[7] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of cps security," *Annual reviews in control*, vol. 47, pp. 394–411, 2019.

[8] T. Pultarova, "Ukraine grid hack is wake-up call for network operators [news briefing]," *Eng. Technol.*, vol. 11, no. 1, pp. 12–13, 2005.

[9] H. Ishii, Y. Wang, and S. Feng, "An overview on multi-agent consensus under adversarial attacks," *Annual Reviews in Control*, 2022.

[10] H. Rezaee, T. Parisini, and M. M. Polycarpou, "Resiliency in dynamic leader–follower multiagent systems," *Automatica*, vol. 125, p. 109384, 2021.

[11] J. Usevitch and D. Panagou, "Resilient leader-follower consensus to arbitrary reference values," in *2018 Annual American Control Conference (ACC)*. IEEE, 2018, pp. 1292–1298.

[12] M. Meng, G. Xiao, and B. Li, "Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks," *Automatica*, vol. 122, p. 109242, 2020.

[13] R. Gao and J. Huang, "Leader-following consensus of uncertain strict feedback multiagent systems subject to sensor and actuator attacks," *International Journal of Robust and Nonlinear Control*, vol. 30, no. 17, pp. 7635–7654, 2020.

[14] S. Huo, H. Wu, and Y. Zhang, "Secure consensus control for multi-agent systems against attacks on actuators and sensors," *International Journal of Robust and Nonlinear Control*, 2022.

[15] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3159–3166, Sept. 2018.

[16] H. Dong, C. Li, and Y. Zhang, "Resilient consensus of multi-agent systems against malicious data injections," *Journal of the Franklin Institute*, vol. 357, no. 4, pp. 2217–2231, 2020.

[17] S. Zuo and D. Yue, "Resilient output formation containment of heterogeneous multigroup systems against unbounded attacks," *IEEE Transactions on Cybernetics*, pp. 1–9, 2020.

[18] Z. Li, Z. Li, and Y. Liu, "Resilient control design of the third-order discrete-time connected vehicle systems against cyber-attacks," *IEEE Access*, vol. 8, pp. 157 470–157 481, 2020.

[19] A. Mustafa and H. Modares, "Attack analysis and resilient control design for discrete-time distributed multi-agent systems," *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 369–376, 2020.

[20] H. Xu, Y.-H. Ni, Z. Liu, and Z. Chen, "Privacy-preserving leader-following consensus via node-augment mechanism," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 6, pp. 2117–2121, 2021.

[21] Z. Qu and M. A. Simaan, "Modularized design for cooperative control and plug-and-play operation of networked heterogeneous systems," *Automatica*, vol. 50, no. 9, p. 2405–2414, Sept. 2014.

[22] H. Zhang, F. L. Lewis, and A. Das, "Optimal design for synchronization of cooperative systems: State feedback, observer and output feedback," *IEEE Transactions on Automatic Control*, vol. 56, no. 8, pp. 1948–1952, Aug. 2011.

[23] Z. Qu, *Cooperative Control of Dynamical Systems: Applications to Autonomous Vehicles*. Springer-Verlag, 2009.

[24] M. Shi, X. Chen, M. Shahidehpour, Q. Zhou, and J. Wen, "Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded ac microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1953–1963, 2021.

[25] K. Zhou and J. C. Doyle, *Essentials of robust control*. N.Y.: Prentice-Hall, 1998.

[26] A. Isidori, *Lectures in Feedback Design for Multivariable Systems*. Springer, 2016.

[27] S. Wilson, P. Glotfelter, L. Wang, S. Mayya, G. Notomista, M. Mote, and M. Egerstedt, "The robotarium: Globally impactful opportunities, challenges, and lessons learned in remote-access, distributed control of multirobot systems," *IEEE Control Systems Magazine*, vol. 40, no. 1, pp. 26–44, 2020.

[28] M. W. S. Atman, T. Hatanaka, Z. Qu, N. Chopra, J. Yamauchi, and M. Fujita, "Motion synchronization for semi-autonomous robotic swarm with a passivity-short human operator," *International Journal of Intelligent Robotics and Applications*, vol. 2, no. 2, pp. 235–251, 2018.

[29] C. Yoshioka and T. Namerikawa, "Formation control of nonholonomic multi-vehicle systems based on virtual structure," in *Proc. of 17th IFAC World Congress*, 2008, pp. 5149–5154.

Mahdieh S. Sadabadi (Senior Member, IEEE) is currently an Assistant Professor at the Department of Electrical and Electronic Engineering, University of Manchester, Manchester, United Kingdom. Previously, she held academic positions at Queen Mary University of London and the University of Sheffield. She was a Postdoctoral Research Associate at the Department of Engineering, the University of Cambridge and a Postdoctoral Fellow in the Division of Automatic Control at the Department of Electrical Engineering, Linkoping University in Sweden. She received her Ph.D. in Control Systems from Automatic Control Laboratory, Swiss Federal Institute of Technology in Lausanne (EPFL), Switzerland in February 2016. She was a Visiting Scholar at the Electrical Engineering Department, Ecole Polytechnique de Montreal, QC, Canada, Methods and Algorithms for Control (MAC) group, LAAS-CNRS in Toulouse, France, and HHMI Janelia Research Campus in Ashburn, VA, USA. Her research interests are generally centered on robust fixed-structure control of large-scale uncertain systems, networked control systems, and their applications in power-electronics-based power systems.

Made Widhi Surya Atman (Member, IEEE) received the B.Eng and M.Sc degrees in electrical engineering from the Institut Teknologi Bandung, Indonesia, in 2011 and 2014, respectively. In 2017 and 2020, he received the M.Eng degree in mechanical and control engineering and the D.Eng degree in systems and control engineering from the Tokyo Institute of Technology. Since 2020, he has been a postdoctoral research fellow with the Automation Technology and Mechanical Engineering, at Tampere University. His research interests include human-swarm interaction, passivity-based control, and distributed control of networked systems.

Anirudh Aynala completed his B.Tech at SRM Institute of Science and Technology in 2015 and obtained his Masters in Factory Automation and Industrial Engineering from Tampere University in 2021. His research interests include, primarily focusing on control system development for mobile robots, with a specialization in application-specific navigation and behavior.

Azwirman Gusrialdi (Member, IEEE) received the B.Eng and M.Eng degrees in mechanical & control engineering from the Tokyo Institute of Technology, Japan, in 2006 and 2008 respectively, and the Dr.-Ing. degree in control engineering from Technische Universitat Munchen, Germany, in 2012. He was a postdoctoral researcher at the Department of Electrical and Computer Engineering, University of Central Florida (UCF), Orlando. Since 2019, he has been an assistant professor with the Automation Technology and Mechanical Engineering unit, Tampere University, Finland, and leading the Intelligent Networked Systems group. His research interests include the design of resilient networked systems, cooperative control, and distributed optimization for networked cyber-physical systems.