Adaptive consensus for heterogeneous multi-agent systems under sensor and actuator attacks ⋆

Min Meng [a], Gaoxi Xiao [a], Beibei Li [b]

[a] *School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798*

[b] *College of Cybersecurity, Sichuan University, Chengdu, P. R. China 610065*

Abstract

This study investigates the leader-following consensus problem for heterogeneous multi-agent systems subject to both sensor and actuator attacks. The attacks considered in this paper are false data injection attacks. A novel adaptive controller is proposed to guarantee that the consensus tracking is achieved with cooperative uniform ultimate boundedness for the multi-agent systems in the simultaneous presence of sensor and actuator attacks. As the whole state information is unknown, the adaptive dynamics are designed on the basis of the received compromised/uncompromised output information. Simulations are carried out to demonstrate the effectiveness of the obtained results.

Key words: Adaptive consensus, heterogeneous multi-agent systems, sensor and actuator attacks, uniform ultimate boundedness.

1 Introduction

Over the past several decades, distributed control of multi-agent systems has attracted much attention due to its wide applications in various fields, such as robotics (Bullo et al. 2009), smart grid (Tan et al. 2014), sensor networks (Ogren et al. 2004) and so on. Most existing results on distributed consensus problem (Hu et al. 2016, Li, Chen, Su & Li 2016, Li, Su & Chen 2016, Li et al. 2013, Meng et al. 2020, Olfati-Saber & Murray 2004) assume guaranteed availability of healthy local sensors, actuators of every agent and the intact communication topologies. However, as multi-agent systems are a significant subclass of cyber-physical systems that involve communications and collaborations between connected agents, they are prone to cyber-physical attacks. For example, the GPS sensors in a multi-vehicle system can be attacked and make the sensory data that the vehicles receive to be corrupted. The misleading data or false actuator input may severely affect the performance of the system and prohibit the accomplishment of system-level objectives. Therefore, design of resilient and secure architectures is of paramount importance for achieving desired coordinated goal of distributed networks under attacks.

Different methods have been proposed for detecting and mitigating deception attacks in multi-agent systems (Boem et al. 2017, Forti et al. 2018, Rahimian & Preciado 2015, Sundaram & Hadjicostis 2011, Teixeira et al. 2010), in which the sensor and/or actuator attacks were considered. There are some approaches to design mitigation techniques for addressing malicious attacks. The first one is to establish a monitor based on the discrepancy among agents and their neighbors to detect and identify attacks on neighbors, and then isolate the comprised agents (Pasqualetti et al. 2012, Sundaram & Hadjicostis 2011). Although by this means, various attacks including sensor and actuator attacks as well as attacks on communication links can be counteracted, additional assumptions on the graph connectivity and the upper bound of the fraction of adversary agents are typically needed. Also the network connectivity may be harmed by rejecting the neighbor's information. The second approach (Arabi et al. 2017, Hota & Sundaram 2018, Jin & Haddad 2019, Modares et al. 2018, Mustafa & Modares 2019, Zeng & Chow 2014, Zhu & Martínez 2013) is to design resilient distributed control protocols to mitigate the effects of attacks instead of removing compromised agents. In Zeng & Chow (2014), a reputation-based resilient control algorithm was proposed for leader-following problem of multi-agent systems in the presence of misbehaving agents. Game-theory based resilient control architecture was designed in Hota & Sundaram (2018) to mitigate the effects of adversary in-

⋆ The work was partially supported by Ministry of Education, Singapore, under contract of MOE2016-T2-1-119, the China Postdoctoral Science Foundation (No. 2019TQ0217); the Provincial Key Research and Development Program of Sichuan (No. 20ZDYF3145). Corresponding author: Gaoxi Xiao.

Email addresses: minmeng@ntu.edu.sg (Min Meng), egxxiao@ntu.edu.sg (Gaoxi Xiao), libeibei@scu.edu.cn (Beibei Li).

formation. Adaptive resilient architectures were applied to ensure that the intruded multi-agent systems under attacks achieve a cooperative goal with uniform ultimate boundedness in Arabi et al. (2017), Jin & Haddad (2019). A novel resilient distributed algorithm was presented by adopting a receding-horizon control methodology for mitigation of replay attacks (Zhu & Martínez 2013). In Mustafa & Modares (2019), a rigorous analysis of the effects of cyber attacks on discrete-time multi-agent systems was conducted and accordingly a mitigating approach for sensor and actuator attacks was proposed. Another way to protect nodes from attackers who try to steal or even alter exchanged information by hacking into the nodes or the communication channels is the digital signature based approach (Ruan et al. 2019).

However, the aforementioned references have all concentrated on homogeneous multi-agent systems under cyber attacks. In practice, it is not common that all agents in a multi-agent system have exactly the same dynamics. Usually individual agents in a multi-agent system have different dynamics and even different state dimensions. It is thus desirable to study the leader-following consensus problem for such multi-agent systems termed heterogeneous multi-agent systems in the presence of both sensor and actuator attacks.

In this paper, we apply and extend techniques from adaptive control theory to mitigate the effects of sensor and actuator attacks on leader-following consensus of heterogenous multi-agent systems. A novel adaptive cooperative controller is presented to foil the time-varying sensor and actuator attacks. The contributions of this paper are mainly as follows. i) The proposed adaptive controller guarantees the leader-following consensus with cooperative uniform ultimate boundedness (UUB). This cooperative bound can be adjusted by appropriately choosing some free parameters in the designed adaptive controller, and particularly, the bound can be sufficiently small when there are only constant sensor attacks. ii) Compared with Pasqualetti et al. (2012), Sundaram & Hadjicostis (2011), in which resilient function calculation and consensus were discussed under the constraints on the number of the malicious agents and the communication topologies, our results however do not need these assumptions. Instead, the only constraint we need is that there exist directed paths from the leader node to all the follower nodes in the communication topology (see Assumption 2). iii) We present some results ensuring that the outputs of all the followers approach the output of the leader with UUB in heterogeneous multi-agent systems under both sensor and actuator attacks while only sensor attacks or actuator attacks were considered in most literature (e.g. Arabi et al. (2017), Chen et al. (2019)). Modares et al. (2018), Mustafa & Modares (2019) present a unified approach to study resilient consensus of homogeneous/heterogeneous multi-agent systems under both sensor and actuator attacks, while however only the intact agents are ensured to achieve consensus.

The rest of this paper is organized as follows. Section 2 reviews some preliminaries and formulates the studied problem. The main results of this paper are presented in Section 3. Section 4 gives an illustrative example to demonstrate the effectiveness of the obtained results, followed by a brief conclusion in Section 5.

Notations. $\mathbb{R}$ and $\mathbb{R}^{m\times n}$ denote the sets of real numbers and $m\times n$ real matrices, respectively. $\mathbf{1}_n$ ($\mathbf{0}_n$) represents an n dimensional vector with all of its elements being 1 (0). I_n is the identity matrix of dimension n. For real symmetric matrices P and Q, $P>(\geq,<,\leq)\,Q$ means that $P-Q$ is positive (positive semi-, negative, negative semi-) definite. Denote by $\|\cdot\|$ the Euclidean/induced norm for vectors/matrices. $\lambda(A)$ represents the eigenvalue of matrix A. $A\otimes B$ denotes the Kronecker product of matrices A and B. $\mathrm{diag}(a_1,a_2,\ldots,a_n)$ represents a diagonal matrix with a_i, $i=1,2,\ldots,n$, on its diagonal.

2 Preliminaries and problem formulation

In this section, some fundamentals of algebraic graph theory and the studied problem are introduced.

In a directed graph $\mathscr{G}=(\mathscr{V},\mathscr{E},\mathscr{A})$, $\mathscr{V}=\{1,2,\ldots,N\}$, $\mathscr{E}=\{(i,j):\,i,j\in\mathscr{V}\}$ and $\mathscr{A}=(a_{ij})\in\mathbb{R}^{N\times N}$ represent the vertex set, the directed edge set and the weighted adjacency matrix of $\mathscr{G}$, respectively. The weights are defined as $a_{ii}=0$, $a_{ij}>0$ if $(j,i)\in\mathscr{E}$ and $a_{ij}=0$ otherwise. A node with one edge incoming to node i is called a neighbor of node i. Denote by $\mathscr{N}_i$ the set of the neighbors of node i, then $\mathscr{N}_i=\{j|\ (j,i)\in\mathscr{E}\}$. Moreover, the Laplacian matrix $\mathscr{L}=(l_{ij})\in\mathbb{R}^{N\times N}$ is defined as $l_{ii}=\sum_{j\neq i}a_{ij}$ and $l_{ij}=-a_{ij}$, $i\neq j$. A directed path from node i_1 to node i_l is composed of a sequence of ordered edges (i_h,i_{h+1}), $h=1,2,\ldots,l-1$.

Consider a heterogeneous multi-agent system with N agents, and the dynamics of agent i, $i\in\{1,2,\ldots,N\}$, is given as

$$\begin{cases}\dot{x}_i(t)=A_ix_i(t)+B_iu_i(t),\\ y_i(t)=C_ix_i(t),\end{cases}\tag{1}$$

where $x_i(t)\in\mathbb{R}^{n_i}$, $u_i(t)\in\mathbb{R}^{m_i}$ and $y_i(t)\in\mathbb{R}^p$ are the state variable, control input and measurable output, respectively. A_i, B_i and C_i are constant real matrices with appropriate dimensions. The leader's state is assumed to be $x_0(t)\in\mathbb{R}^r$ with the following dynamics

$$\begin{cases}\dot{x}_0(t)=A_0x_0(t),\\ y_0(t)=C_0x_0(t),\end{cases}\tag{2}$$

where $x_0(t)\in\mathbb{R}^r$ is the state of the leader, $y_0(t)\in\mathbb{R}^p$ is the measurable output of the leader and A_0, C_0 are constant real matrices with appropriate dimensions. In addition, the communication topology among these follower agents in (1) is characterized by a directed graph $\mathscr{G}=(\mathscr{V},\mathscr{E},\mathscr{A})$ with $\mathscr{V}=\{1,2,\ldots,N\}$. The leader can be pinned to multiple followers, which leads to a diagonal pinning matrix $D=$

$\mathrm{diag}(d_1, d_2, \ldots, d_N) \in \mathbb{R}^{N\times N}$ with $d_i > 0$ if there is a directed edge from the leader node to the ith follower, and $d_i = 0$ otherwise. Denote $\mathscr{M} = \mathscr{L} + D$, where $\mathscr{L}$ is the Laplacian matrix of $\mathscr{G}$.

In this paper, the sensor and actuator of every agent i may be corrupted. The attack on actuators can be described as

$$u_i^c(t) = u_i(t) + u_i^a(t), \tag{3}$$

where $u_i(t) \in \mathbb{R}^{m_i}$ is the uncompromised control input, $u_i^a(t)$ is the unknown disturbance injected to the actuator of agent i, and $u_i^c(t)$ is the compromised input available to agent i in (1). The sensor attack is given as

$$y_i^c(t) = y_i(t) + y_i^a(t), \tag{4}$$

where $y_i(t)$ is the uncompromised measurable output of agent i, $y_i^a(t)$ is unknown and captures the sensor attack on agent i, and $y_i^c(t)$ is the compromised output applied to feedback. The system architecture is shown in Fig. 1.

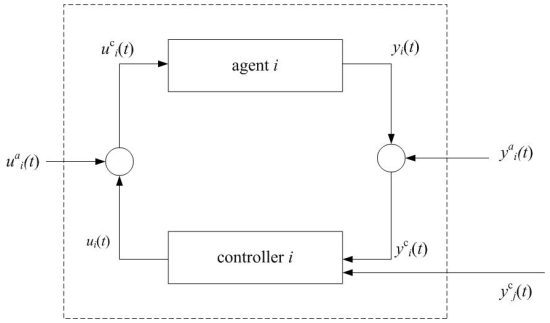

Fig. 1. System control framework of multi-agent systems in the presence of sensor and actuator attacks on agent i. Here, $j \in \mathscr{N}_i$.

Remark 1 *One can see that faults on sensors and actuators can be modeled in the same way as in (3), (4). In fact, faults and attacks have inherently different characteristics. Faults are caused randomly and unintentionally while attacks are injected intentionally by an intruder to mislead or even paralyze the whole network's behaviors. With the randomness feature, faults are easier to be detected and mitigated.*

The definition of the cooperative UUB was first defined in Das & Lewis (2010) which extends the conventional concept of UUB in Khalil & Grizzle (2002).

Definition 1 *(Das & Lewis 2010) The leader's output $y_0(t)$ given in (2) is cooperatively uniformly ultimately bounded with respect to outputs of followers in (1) if there exists a compact set $\mathscr{C} \subset \mathbb{R}^p$ so that $y_i(t_0) - y_0(t_0) \in \mathscr{C}$ for arbitrary $i \in \{1, 2, \ldots, N\}$, then a bound ε and a time instance $t_f(\varepsilon, y_i(t_0) - y_0(t_0))$ both independent of t_0 can be found such that $\|y_i(t) - y_0(t)\| \le \varepsilon$, $\forall i$, $\forall t \ge t_0 + t_f$.*

If the conditions in Definition 1 are satisfied, we say that the leader-following consensus is achieved with cooperative UUB.

While under cyber attacks, the consensus performance can be seriously affected since even an attack on a single agent may be amplified through communications between the agent and its neighbors. As the comprised dynamics of agent i becomes

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i(u_i(t) + u_i^a(t)), \\ y_i^c(t) = C_i x_i(t) + y_i^a(t), \end{cases} \tag{5}$$

the aim of this paper is to design a distributed adaptive control protocol such that the leader-following consensus of the compromised multi-agent system (5) and (2) is achieved with cooperative UUB, that is, $\|y_i(t) - y_0(t)\|$ is uniformly ultimately bounded for every $i = 1, 2, \ldots, N$.

3 Main results

In this section, a novel distributed adaptive resilient control protocol is designed to mitigate the effects of sensor and actuator attacks, and achieve leader-following consensus with cooperative UUB.

Assumption 1 *The sensor and actuator attacks, $y_i^a(t)$ and $u_i^a(t)$, as well as their derivatives, $\dot{y}_i^a(t)$ and $\dot{u}_i^a(t)$ are bounded. Besides, the bounds are unknown.*

To achieve leader-following consensus uniformly ultimately bounded for multi-agent system (1) with the leader (2) under sensor and actuator attacks, a distributed adaptive control protocol is designed in the following form:

$$u_i(t) = K_{xi}\hat{x}_i(t) + K_{\xi i}\xi_i(t) - \hat{u}_i^a(t), \tag{6}$$

$$\dot{\xi}_i(t) = A_0\xi_i(t) + KC_0 \sum_{j\in\mathscr{N}_i} a_{ij}(\xi_i(t) - \xi_j(t)) + d_i KC_0(\xi_i(t) - x_0(t)), \tag{7}$$

$$\dot{\hat{x}}_i(t) = A_i\hat{x}_i(t) + B_i u_i(t) + F_i\tilde{y}_i(t) + B_i\hat{u}_i^a(t), \tag{8}$$

where $\xi_i(t) \in \mathbb{R}^r$ is the internal state of the controller, $\hat{x}_i(t)$ is the observer of the state $x_i(t)$, $\hat{u}_i^a(t)$ is the estimation of actuator attack $u_i^a(t)$, $\tilde{y}_i(t) := y_i^c(t) - C_i\hat{x}_i(t) - \hat{y}_i^a(t)$ with $\hat{y}_i^a(t)$ being the estimation of the sensor attack $y_i^a(t)$, and K_{xi}, $K_{\xi i}$, K, F_i are controller gains to be designed. Moreover, the dynamics of $\hat{y}_i^a(t)$ and $\hat{u}_i^a(t)$ are given as

$$\dot{\hat{y}}_i^a(t) = G_i\tilde{y}_i(t), \tag{9}$$

$$\dot{\hat{u}}_i^a(t) = -\alpha_i\hat{u}_i^a(t) + H_i\tilde{y}_i(t), \tag{10}$$

where G_i, H_i, $\alpha_i > 0$ are also unknown and to be devised. Note that the state of agent i, $x_i(t)$, cannot be fully measurable. Fortunately, the compromised output $y_i^c(t)$ is available for estimating the unknown parameters in multi-agent system (5). In view of that $\tilde{y}_i(t) = y_i^c(t) - C_i\hat{x}_i(t) - \hat{y}_i^a(t)$ can be accessible, the proposed controller in (6)–(10) is based on the local measurable output information, and thus is distributed. As most results on leader-following consensus of multi-agent systems, the following assumption is necessary.

Assumption 2

1) There exist directed paths from the leader node to all the follower nodes.
2) (A_0, C_0) is detectable.
3) (A_i, B_i) is controllable, $i = 1, 2, \ldots, N$.

Lemma 1 *(Li et al. 2015) Under 1) in Assumption 2, the matrix $\mathscr{M} = \mathscr{L} + D$ is an M-matrix, and there exists a matrix $Q = \mathrm{diag}(q_1, q_2, \ldots, q_N)$ with $q_i > 0$, $i = 1, 2, \ldots, N$, and $(q_1, q_2, \ldots, q_N)^T = \mathscr{M}^{-T}\mathbf{1}_N$ such that $Q\mathscr{M} + \mathscr{M}^T Q > 0$.*

Denote $\lambda_0 = \lambda_{\min}(Q\mathscr{M} + \mathscr{M}^T Q)$ and $q_{\max} = \max\{q_1, \ldots, q_N\}$. By recalling the existing references (Hu & Liu 2017, Meng et al. 2018, Wieland & Allgower 2009), K can be selected such that $I_N \otimes A_0 + \mathscr{M} \otimes KC_0$ is Hurwitz. In fact, by Lemma 1, K can be designed as follows:

$$K = -\mu P^{-1} C_0^T, \tag{11}$$

where $\mu \geq 2q_{\max}\lambda_0^{-1}$ and $P \in \mathbb{R}^{r\times r}$ is a positive definite matrix satisfying

$$PA_0 + A_0^T P - 2C_0^T C_0 < 0. \tag{12}$$

(12) has a solution since (A_0, C_0) is detectable (Li et al. 2010). In this setting, denote $\tilde{\xi}_i(t) = \xi_i(t) - x_0(t)$ and $\tilde{\xi}(t) = (\tilde{\xi}_1^T(t), \tilde{\xi}_2^T(t), \ldots, \tilde{\xi}_N^T(t))^T$. One can obtain the dynamics of $\tilde{\xi}(t)$ based on (7) as

$$\dot{\tilde{\xi}}(t) = (I_N \otimes A_0 + \mathscr{M} \otimes KC_0)\tilde{\xi}(t). \tag{13}$$

Subsequently, it can be derived that $\tilde{\xi}(t) \to 0$ as $t \to \infty$, i.e., $\tilde{\xi}_i(t) - x_0(t) \to 0$ as $t \to \infty$. To achieve the main objective of this paper, we first need to analyze the UUB of $x_i(t) - \hat{x}_i(t)$, $y_i^a(t) - \hat{y}_i^a(t)$ and $u_i^a(t) - \hat{u}_i^a(t)$. To this end, denote $\tilde{x}_i(t) := x_i(t) - \hat{x}_i(t)$, $\tilde{y}_i^a(t) := y_i^a(t) - \hat{y}_i^a(t)$ and $\tilde{u}_i^a(t) := u_i^a(t) - \hat{u}_i^a(t)$. Since $\tilde{y}_i(t) = y_i^c(t) - C_i\hat{x}_i(t) - \hat{y}_i^a(t) = C_i\tilde{x}_i(t) + \tilde{y}_i^a(t)$, we have that

$$\dot{\tilde{x}}_i(t) = (A_i - F_iC_i)\tilde{x}_i(t) - F_i\tilde{y}_i^a(t) + B_i\tilde{u}_i^a(t), \tag{14}$$
$$\dot{\tilde{y}}_i^a(t) = -G_iC_i\tilde{x}_i(t) - G_i\tilde{y}_i^a(t) + \dot{y}_i^a(t). \tag{15}$$

Define $\eta_i(t) = (\tilde{x}_i^T(t), (\tilde{y}_i^a(t))^T)^T$, then the dynamics of $\eta_i(t)$ can be obtained as

$$\dot{\eta}_i(t) = A_{Fi}\eta_i(t) + B_{i1}\tilde{u}_i^a(t) + B_{i2}\dot{y}_i^a(t), \tag{16}$$

where $A_{Fi} = \begin{bmatrix} A_i - F_iC_i & -F_i \\ -G_iC_i & -G_i \end{bmatrix}$, $B_{i1} = \begin{bmatrix} B_i \\ \mathbf{0}_{p\times m_i} \end{bmatrix}$ and $B_{i2} = \begin{bmatrix} \mathbf{0}_{n_i\times p} \\ I_p \end{bmatrix}$. Before presenting the result on the boundedness of $(\eta_i(t), \tilde{u}_i^a(t))$, another assumption is needed.

Assumption 3 *Assume that (A_i, C_iA_i) is observable for every $i = 1, 2, \ldots, N$.*

Lemma 2 *Consider the multi-agent system in (1) with the leader (2) under sensor and actuator attacks in (3) and (4). A resilient adaptive controller is given in (6)–(10). Under Assumptions 1, 3, the solution $(\eta_i(t), \tilde{u}_i^a(t))$ of the corresponding closed-loop system is uniformly ultimately bounded.*

Proof. Note that $A_{Fi} = \begin{bmatrix} A_i & \mathbf{0}_{n_i\times p} \\ \mathbf{0}_{p\times n_i} & \mathbf{0}_{p\times p} \end{bmatrix} + \begin{bmatrix} -F_i \\ -G_i \end{bmatrix} \begin{bmatrix} C_i & I_p \end{bmatrix}$. The matrix pair $(\begin{bmatrix} A_i & \mathbf{0}_{n_i\times p} \\ \mathbf{0}_{p\times n_i} & \mathbf{0}_{p\times p} \end{bmatrix}, \begin{bmatrix} C_i & I_p \end{bmatrix})$ is observable if and only if

$$\mathrm{rank}\begin{bmatrix} C_i & I_p \\ C_iA_i & \mathbf{0}_{p\times p} \\ \vdots & \vdots \\ C_iA_i^{n_i+p-1} & \mathbf{0}_{p\times p} \end{bmatrix} = n_i + p.$$

This is equivalent to

$$\mathrm{rank}\begin{bmatrix} (C_iA_i)^T & (C_iA_i^2)^T & \cdots & (C_iA_i^{n_i+p-1})^T \end{bmatrix}^T = n_i. \tag{17}$$

Since $p \geq 1$ and $A_i \in \mathbb{R}^{n_i\times n_i}$, by Cayley-Hamilton theorem, (17) is equivalent to

$$\mathrm{rank}\begin{bmatrix} (C_iA_i)^T & (C_iA_i^2)^T & \cdots & (C_iA_i^{n_i})^T \end{bmatrix}^T = n_i, \tag{18}$$

which can be implied by Assumption 3. Then one can design appropriate controller gains F_i, G_i such that there exists a positive definite matrix $P_i \in \mathbb{R}^{(n_i+p)\times(n_i+p)}$ such that

$$P_iA_{Fi} + A_{Fi}^T P_i < -P_i. \tag{19}$$

Define a Lyapunov function as

$$V_i(t) = \eta_i^T(t)P_i\eta_i(t) + (\tilde{u}_i^a(t))^T\tilde{u}_i^a(t). \tag{20}$$

Then, along the trajectory of the corresponding closed-loop system, one has

$$\begin{aligned}
\dot{V}_i(t) &= 2\eta_i^T(t)P_i\dot{\eta}_i(t) + 2(\tilde{u}_i^a(t))^T\dot{\tilde{u}}_i^a(t) \\
&= \eta_i^T(t)(P_iA_{Fi} + A_{Fi}^TP_i)\eta_i(t) + 2\eta_i^T(t)P_iB_{i1}\tilde{u}_i^a(t) \\
&\quad + 2\eta_i^T(t)P_iB_{i2}\dot{y}_i^a(t) + 2(\tilde{u}_i^a(t))^T(\dot{u}_i^a(t) - \dot{\hat{u}}_i^a(t)) \\
&\leq -\eta_i^T(t)P_i\eta_i(t) + 2\eta_i^T(t)P_iB_{i1}\tilde{u}_i^a(t) \\
&\quad + 2\eta_i^T(t)P_iB_{i2}\dot{y}_i^a(t) + 2(\tilde{u}_i^a(t))^T(\dot{u}_i^a(t) + \alpha_i\hat{u}_i^a(t)) \\
&\quad - 2(\tilde{u}_i^a(t))^TH_i\tilde{y}_i(t).
\end{aligned}$$

Note that

$$
\begin{aligned}
2\eta_i^T(t)P_iB_{i1}\tilde{u}_i^a(t) &\le \frac{1}{6}\eta_i^T(t)P_i\eta_i(t)+6(\tilde{u}_i^a(t))^TB_{i1}^TP_iB_{i1}\tilde{u}_i^a(t),\\
2\eta_i^T(t)P_iB_{i2}\dot{y}_i^a(t) &\le \frac{1}{6}\eta_i^T(t)P_i\eta_i(t)+6(\dot{y}_i^a(t))^TB_{i2}^TP_iB_{i2}\dot{y}_i^a(t),\\
2(\tilde{u}_i^a(t))^T\dot{u}_i^a(t) &\le \frac{\alpha_i}{2}(\tilde{u}_i^a(t))^T\tilde{u}_i^a(t)+\frac{2}{\alpha_i}(\dot{u}_i^a(t))^T\dot{u}_i^a(t),\\
2\alpha_i(\tilde{u}_i^a(t))^T\hat{u}_i^a(t) &= 2\alpha_i(\tilde{u}_i^a(t))^Tu_i^a(t)-2\alpha_i(\tilde{u}_i^a(t))^T\tilde{u}_i^a(t),\\
&\le 2\alpha_i(u_i^a(t))^Tu_i^a(t)-\frac{3}{2}\alpha_i(\tilde{u}_i^a(t))^T\tilde{u}_i^a(t),\\
-2(\tilde{u}_i^a(t))^TH_i\tilde{y}_i(t) &= -2(\tilde{u}_i^a(t))^TH_i[C_i\ I_p]\eta_i(t)\\
&\le \frac{1}{6}\eta_i^T(t)P_i\eta_i(t)\\
&\quad +6(\tilde{u}_i^a(t))^TH_i[C_i\ I_p]P_i^{-1}[C_i\ I_p]^TH_i^T\tilde{u}_i^a(t).
\end{aligned}
$$

With the above derivations, we obtain that

$$
\begin{aligned}
\dot{V}_i(t) \le & -\frac{1}{2}\eta_i^T(t)P_i\eta_i(t)-\alpha_i(\tilde{u}_i^a(t))^T\tilde{u}_i^a(t)\\
&+6(\tilde{u}_i^a(t))^TB_{i1}^TP_iB_{i1}\tilde{u}_i^a(t)+6(\dot{y}_i^a(t))^TB_{i2}^TP_iB_{i2}\dot{y}_i^a(t)\\
&+\frac{2}{\alpha_i}(\dot{u}_i^a(t))^T\dot{u}_i^a(t)+2\alpha_i(u_i^a(t))^Tu_i^a(t)\\
&+6(\tilde{u}_i^a(t))^TH_i[C_i\ I_p]P_i^{-1}[C_i\ I_p]^TH_i^T\tilde{u}_i^a(t).
\end{aligned}
$$

Take α_i as $\alpha_i = a_{i1}+6\|B_{i1}^TP_iB_{i1}\|+6\|H_i[C_i\ I_p]P_i^{-1}[C_i\ I_p]^TH_i^T\|$ with a_{i1} being any positive number. Let $b_i=\min\{1/2,a_{i1}\}$ and $c_i(t) = 6(\dot{y}_i^a(t))^TB_{i2}^TP_iB_{i2}\dot{y}_i^a(t)+\frac{2}{a_i}(\dot{u}_i^a(t))^T\dot{u}_i^a(t)+2\alpha_i(u_i^a(t))^Tu_i^a(t)$. From Assumption 1, we can suppose that a bound of $c_i(t)$ exists and is $\bar{c}_i$. Hence,

$$
\dot{V}_i(t) \le -b_iV_i(t)+\bar{c}_i, \tag{21}
$$

that is,

$$
V_i(t) \le (V_i(0)-\frac{\bar{c}_i}{b_i})e^{-b_it}+\frac{\bar{c}_i}{b_i}. \tag{22}
$$

Since e^{-b_it} approaches zero as $t\to\infty$, there exists a positive number T_i such that for any $t\ge T_i$, $e^{-b_it} < \frac{\bar{c}_i}{b_i|V_i(0)-\frac{\bar{c}_i}{b_i}|}$ when $V_i(0)-\frac{\bar{c}_i}{b_i}$ is nonzero. Hence, it can be obtained that for any $t\ge T_i$, $V_i(t)\le\frac{2\bar{c}_i}{b_i}$. Note that $\|\eta_i(t)\|^2$ is less than $\lambda_{\min}^{-1}(P_i)V_i(t)$, and $\|\tilde{u}_i^a(t)\|^2\le V_i(t)$. One can thus derive that $(\eta_i(t),\tilde{u}_i^a(t))$ is uniformly ultimately bounded. ■

From Lemma 2, we can see that $\hat{x}_i(t)$, $\hat{y}_i^a(t)$, $\hat{u}_i^a(t)$ are the estimations of $x_i(t)$, $y_i^a(t)$, $u_i^a(t)$, respectively, with slight error bounds, which lay a paramount foundation for ensuring leader-following consensus with UUB.

On the other hand, $\xi_i(t)$ for $i=1,2,\ldots,N$, are viewed as internal states of the designed controller and aim to estimate the leader's state from the perspective of every agent, i.e., $\xi_i(t)$ is the estimation of $x_0(t)$ for agent i. In order to assure that the output of agent i, $y_i(t)$, goes to the leader's output $y_0(t)$, $\xi_i(t)$ also needs to satisfy another principle by appropriately designing controller gains K_{xi} and $K_{\xi i}$. By 3) in Assumption 2, select K_{xi} to make the real part of every eigenvalue of $A_i+B_iK_{xi}$ be less than -1, and then take $K_{\xi i}$ as $K_{\xi i}=Y_i-K_{xi}X_i$, where (X_i,Y_i), $i=1,2,\ldots,N$, are the solutions to the following equations, called regulated equations:

$$
A_iX_i+B_iY_i = X_iA_0, \tag{23}
$$

$$
C_iX_i = C_0,\ i=1,2,\ldots,N. \tag{24}
$$

Lemma 3 *Consider the multi-agent system in (1) with the leader (2) under sensor and actuator attacks in (3) and (4). A resilient adaptive controller is given in (6)–(10). Under Assumptions 1–3, by choosing appropriate K, K_{xi}, $K_{\xi i}$, the trajectory of $\varepsilon_i(t):=\hat{x}_i(t)-X_i\xi_i(t)$ is uniformly ultimately bounded.*

Proof. As analyzed previously, with the designed K in (11), we have $\lim_{t\to\infty}(\xi_i(t)-x_0(t))=0$. That is, for any $\nu>0$, a positive number T^1 exists such that for $t\ge T^1$, $\|\tilde{\xi}(t)\|^2<\nu$, where $\tilde{\xi}(t)=(\tilde{\xi}_1^T(t),\tilde{\xi}_2^T(t),\ldots,\tilde{\xi}_N^T(t))^T$ with $\tilde{\xi}_i(t)=\xi_i(t)-x_0(t)$, $i=1,2,\ldots,N$. Denote $\varepsilon(t)=(\varepsilon_1^T(t),\varepsilon_2^T(t),\ldots,\varepsilon_N^T(t))^T$ and $\tilde{y}(t)=(\tilde{y}_1^T(t),\tilde{y}_2^T(t),\ldots,\tilde{y}_N^T(t))^T$, then

$$
\dot{\varepsilon}(t) = (A+BK_x)\varepsilon(t)+F\tilde{y}(t)-X(\mathscr{M}\otimes KC_0)\tilde{\xi}(t), \tag{25}
$$

where $\Upsilon=\mathrm{diag}(\Upsilon_1,\Upsilon_2,\ldots,\Upsilon_N)$ for $\Upsilon_i=A_i,B_i,K_{xi},K_{\xi i},F_i,X_i$, $i=1,2,\ldots,N$. Define a Lyapunov function as

$$
V_\varepsilon(t)=\varepsilon^T(t)P_x\varepsilon(t), \tag{26}
$$

where $P_x=\mathrm{diag}(P_{x1},P_{x2},\ldots,P_{xN})$ with P_{xi} being a positive definite matrix satisfying

$$
P_{xi}(A_i+B_iK_{xi})+(A_i+B_iK_{xi})^TP_{xi} < -2P_{xi}, \tag{27}
$$

for $i=1,2,\ldots,N$. Therefore the derivative of $V_\varepsilon(t)$ is

$$
\begin{aligned}
\dot{V}_\varepsilon(t) &= 2\varepsilon^T(t)P_x\dot{\varepsilon}(t)\\
&\le -2\varepsilon^T(t)P_x\varepsilon(t)+2\varepsilon^T(t)P_xF\tilde{y}(t)\\
&\quad -2\varepsilon^T(t)P_xX(\mathscr{M}\otimes KC_0)\tilde{\xi}(t)\\
&\le -\varepsilon^T(t)P_x\varepsilon(t)+2\tilde{y}^T(t)F^TP_xF\tilde{y}(t)\\
&\quad +2\tilde{\xi}^T(t)(\mathscr{M}\otimes KC_0)^TX^TP_xX(\mathscr{M}\otimes KC_0)\tilde{\xi}(t),
\end{aligned}
$$

where the second inequality was obtained by $2a^Tb\le 1/2a^Ta+2b^Tb$. For $t\ge\max\{T_1,T_2,\ldots,T_N,T^1\}$ where T_i, $i=1,2,\ldots,N$, are given in the proof of Lemma 2, one has that $\dot{V}_\varepsilon(t)\le -V_\varepsilon(t)+\bar{b}$, where $\bar{b}$ is $4N\|F^TP_xF\|(\|C\|^2+1)\max_{i=1,2,\ldots,N}\{\frac{2\bar{c}_i}{\lambda_{\min}(P_i)b_i}\}+2\|(\mathscr{M}\otimes KC_0)^TX^TP_xX(\mathscr{M}\otimes KC_0)\|\nu$, i.e., a bound of $2\tilde{y}^T(t)F^TP_xF\tilde{y}(t)+2\tilde{\xi}^T(t)(\mathscr{M}\otimes$

$KC_0)^T X^T P_x X(\mathscr{M}\otimes KC_0)\tilde{\xi}(t)$ from the proof of Lemma 2, since

$$\begin{aligned}&\tilde{y}^T(t)F^T P_x F\tilde{y}(t)+\tilde{\xi}^T(t)(\mathscr{M}\otimes KC_0)^T X^T P_x X(\mathscr{M}\otimes KC_0)\tilde{\xi}(t)\\&\le 2\|F^T P_x F\|(\|C\|^2\|\tilde{x}(t)\|^2+\|\tilde{y}^a(t)\|^2)\\&\quad+\|(\mathscr{M}\otimes KC_0)^T X^T P_x X(\mathscr{M}\otimes KC_0)\|\nu.\end{aligned}$$

Similar to the proof of Lemma 2, there exists a positive number $T\ge\max\{T_1,T_2,\ldots,T_N,T^1\}$ such that $\|\varepsilon(t)\|^2\le 2\lambda_{\min}^{-1}(P_x)\bar{b}$ for any $t\ge T$. Thus, we can claim that $\varepsilon(t)$ is uniformly ultimately bounded. ■

Equipped with the above results, now we are in a position to present the conditions to ensure the leader-following consensus is achieved with cooperative UUB.

Theorem 1 *Consider the multi-agent system in (1) with the leader (2) under sensor and actuator attacks in (3) and (4). A resilient adaptive controller is given in (6)–(10). Under Assumptions 1–3, by choosing appropriate controller gains, leader-following consensus of multi-agent system (1) with the leader (2) is achieved with cooperative UUB.*

Proof. Note that

$$\begin{aligned}&\|y_i(t)-y_0(t)\|^2\\&=\|C_ix_i(t)-C_i\hat{x}_i(t)+C_i\hat{x}_i(t)-C_iX_i\xi_i(t)+C_iX_i\xi_i(t)-C_0x_0(t)\|^2\\&\le 3\|C_i\|^2\|\tilde{x}_i(t)\|^2+3\|C_i\|^2\|\varepsilon_i(t)\|^2+3\|C_0\|^2\|\tilde{\xi}_i(t)\|^2.\end{aligned}$$

By Lemmas 2 and 3, for any $t\ge T$ where T is in the proof of Lemma 3, one can claim that $y_i(t)-y_0(t)$ is uniformly ultimate bounded. That is, the leader-following consensus for the studied multi-agent system is achieved with cooperative UUB. ■

From the proofs, we conclude that the desired controller gains in (6)–(10) can be designed according to the following procedures:

i) Compute K in (7) via (11) based on the Laplacian matrix $\mathscr{L}$ of the followers' communication topology $\mathscr{G}$, the pinning matrix D, and a solution to the linear matrix inequality (LMI) in (12).
ii) Determine K_{xi} such that the LMI in (27) holds.
iii) Let $K_{\xi i}=Y_i-K_{xi}X_i$, where a set of (X_i,Y_i), $i=1,2,\ldots,N$, is the solution to (23) and (24).
iv) Select F_i,G_i such that the Lyapunov equation (19) has a solution $P_i>0$.
v) Take $\alpha_i=a_{i1}+6\|B_{i1}^T P_i B_{i1}\|+6\|H_i[C_i\ I_p]P_i^{-1}[C_i\ I_p]^T H_i^T\|$, where $a_{i1}>0$, $B_{i1}=\begin{bmatrix}B_i^T & \mathbf{0}_{m_i\times p}\end{bmatrix}^T$, $H_i\in\mathbb{R}^{m_i\times P}$, and P_i is a positive definite matrix satisfying (19).

Remark 2 *From Theorem 1, the leader-following consensus with cooperative UUB is independent of the upper number of compromised agents, and it is enough that the communication topologies satisfy condition 1) in Assumption 2.*

Remark 3 *The cooperative uniform ultimate bound of $\|y_i(t)-y_0(t)\|$ depends on the bounds of the derivatives of the sensor and actuator attacks. However, the designed adaptive cooperative controller, equivalently the desired controller gains, make no reference to the bounds of the sensor and actuator attacks along with their derivatives. In fact, one bound of $y_i(t)-y_0(t)$ can be specifically as*

$$6\|C_i\|^2\lambda_{\min}^{-1}(P_i)\frac{\bar{c}_i}{b_i}+6\|C_i\|^2\lambda_{\min}^{-1}(P_x)\bar{b}+3\|C_0\|^2\nu. \quad (28)$$

From the proofs in this section, if there are only constant sensor attacks, then the designed adaptive controller is still applicable by deleting the terms relying on $u_i^a(t)$, $\dot{u}_i^a(t)$, $\dot{y}_i^a(t)$. In this case, the upper bound in (28) becomes $3\|C_0\|^2\nu$. As $\nu>0$ can be sufficiently small, therefore, the leader-following consensus can be achieved exactly, i.e., the error $y_i(t)-y_0(t)$ approaches zero as $t\to\infty$ for $i=1,2,\ldots,N$.

Remark 4 *The condition in Assumption 3 can be replaced by another condition on the multi-agent system: (A_i,C_i) is controllable and A_i is nonsingular for every $i=1,2,\ldots,N$. This condition can ensure that Assumption 3 is satisfied.*

Remark 5 *Our method can be extended to the case of multi-agent systems under actuator dynamics as follows (Dogan et al. 2017, 2019):*

$$\begin{cases}\dot{z}_i(t)=-M_iz_i(t)+v_i(t)\\ u_i(t)=M_iz_i(t)\end{cases} \quad (29)$$

where $z_i(t)\in\mathbb{R}^{m_i}$ is the state of the actuator dynamics, $M_i\in\mathbb{R}^{m_i\times m_i}$ is a positive definite diagonal matrix with its entries representing the actuator bandwidths of each control channel of agent i, and $v_i(t)$ is the feedback control input.

4 Example

In this section, we give a numeriacal example to illustrate the obtained results. Consider a heterogeneous multi-agent system with the dynamics matrices as (Wieland et al. 2011)

$$A_i=\begin{bmatrix}-1&1&0\\0&0&a_i\\0&-c_i&d_i\end{bmatrix},\ B_i=\begin{bmatrix}0&0\\0&0\\b_{i1}&b_{i2}\end{bmatrix},\ C_i=\begin{bmatrix}1&0&0\end{bmatrix},$$

where $a_i>0,b_{i1}>0,b_{i2}>0,c_i>0$ and $d_i>0$ for $i=1,2,\ldots,N$. The leader's system matrices are assumed to be

$$A_0=\begin{bmatrix}0&1\\-1&0\end{bmatrix},\ C_0=\begin{bmatrix}1&1\end{bmatrix}.$$

Consider $N=6$ and $(a_i,b_{i1},b_{i2},c_i,d_i)$ is chosen as $(1,1,1,0,1)$, $(1,1,1,1,2)$, $(1,1,1,1,2)$, $(1,1,1,10,1)$,

$(1,1,2,0,1)$, $(1,1,2,1,2)$. The communication topology among the leader and the followers is depicted as in Fig. 2. When this multi-agent system is subject to sensor and actuator attacks, take $y_i^a(t) = 0.1 * \cos(t)$ and $u_i^a(t) = (0.5 * \sin(t), 0.2 * \cos(t))^T$ as an example. It can be

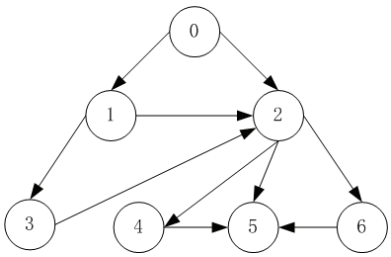

Fig. 2. The communication topology among the leader and the followers.

easily verified that Assumptions 1–3 are satisfied. Based on the distributed controller in (6)–(10), the output error trajectories between the followers and the leader are shown in Fig. 3, from which one can see that the leader-following consensus is achieved with cooperative UUB.

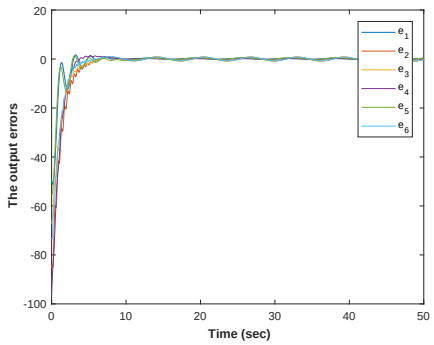

Fig. 3. The output errors $e_i(t) = y_i(t) - y_0(t)$, $i = 1,2,\ldots,6$.

5 Conclusion

In this paper, we addressed the adaptive distributed leader-following consensus for a kind of heterogeneous multi-agent systems under sensor and actuator attacks. Novel resilient distributed controllers were given by extending the adaptive methods and can be designed to ensure the leader following consensus with cooperative UUB for the studied multi-agent systems. Future research interest is to study resilient consensus of heterogeneous multi-agent systems under actuator dynamics and attacks without the assumption of their bounded derivatives.

References

Arabi, E., Yucelen, T., & Haddad, W. M. (2017). Mitigating the effects of sensor uncertainties in networked multi-agent systems. *Journal of Dynamic Systems, Measurement, and Control*, *139*(4), 041003.

Boem, F., Gallo, A. J., Ferrari-Trecate, G., & Parisini, T. (2017). A distributed attack detection method for multi-agent systems governed by consensus-based control. In *IEEE 56th Annual Conference on Decision and Control (CDC)* (pp. 5961–5966).

Bullo, F., Cortes, J., & Martinez, S. (2009). *Distributed control of robotic networks: A mathematical approach to motion coordination algorithms*. Princeton University Press, New Jersey, USA.

Chen, C., Xie, K., Lewis, F. L., Xie, S., & Davoudi, A. (2019). Fully distributed resilience for adaptive exponential synchronization of heterogeneous multiagent systems against actuator faults. *IEEE Transactions on Automatic Control*, *64*(8), 3347–3354.

Das, A., & Lewis, F. L. (2010). Distributed adaptive control for synchronization of unknown nonlinear networked systems. *Automatica*, *46*(12), 2014–2021.

Dogan, K. M., Gruenwald, B. C., Yucelen, T., Muse, J. A., & Butcher, E. A. (2017). Distributed adaptive control of networked multiagent systems with heterogeneous actuator dynamics. In *2017 American Control Conference (ACC)* (pp. 5605–5610).

Dogan, K. M., Gruenwald, B. C., Yucelen, T., Muse, J. A., & Butcher, E. A. (2019). Distributed adaptive control and stability verification for linear multiagent systems with heterogeneous actuator dynamics and system uncertainties. *International Journal of Control*, *92*(11), 2620–2638.

Forti, N., Battistelli, G., Chisci, L., Li, S., Wang, B., & Sinopoli, B. (2018). Distributed joint attack detection and secure state estimation. *IEEE Transactions on Signal and Information Processing over Networks*, *4*(1), 96–110.

Hota, A., & Sundaram, S. (2018). Interdependent security games on networks under behavioral probability weighting. *IEEE Transactions on Control of Network Systems*, *5*(1), 262–273.

Hu, W., & Liu, L. (2017). Cooperative output regulation of heterogeneous linear multi-agent systems by event-triggered control. *IEEE Transactions on Cybernetics*, *47*(1), 105–116.

Hu, W., Liu, L., & Feng, G. (2016). Consensus of linear multi-agent systems by distributed event-triggered strategy. *IEEE Transactions on Cybernetics*, *46*(1), 148–157.

Jin, X., & Haddad, W. M. (2019). An adaptive control architecture for leader-follower multiagent systems with stochastic disturbances and sensor and actuator attacks. *International Journal of Control*, *92*(11), 2561–2570.

Khalil, H. K., & Grizzle, J. W. (2002). *Nonlinear systems*. Prentice hall New Jersey.

Li, X., Chen, M. Z. Q., Su, H., & Li, C. (2016). Consensus networks with switching topology and time-delays over finite fields. *Automatica*, *68*, 39–43.

Li, X., Su, H., & Chen, M. Z. Q. (2016). Consensus networks with time-delays over finite fields. *International Journal of Control*, *89*(5), 1000–1008.

Li, Z., Duan, Z., Chen, G., & Huang, L. (2010). Consensus of multiagent systems and synchronization of complex networks: A unified viewpoint. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *57*(1), 213–224.

Li, Z., Ren, W., Liu, X., & Fu, M. (2013). Consensus of multi-agent systems with general linear and Lipschitz nonlinear dynamics using distributed adaptive protocols. *IEEE Transactions on Automatic Control*, *58*(7), 1786–1791.

Li, Z., Wen, G., Duan, Z., & Ren, W. (2015). Designing fully distributed consensus protocols for linear multi-agent systems with directed graphs. *IEEE Transactions on Automatic Control*, *60*(4), 1152–1157.

Meng, M., Li, X., & Xiao, G. (2020). Synchronization of networks over finite fields. *Automatica*, *115*, 108877.

Meng, M., Liu, L., & Feng, G. (2018). Adaptive output regulation of heterogeneous multiagent systems under Markovian switching topologies. *IEEE Transactions on Cybernetics*, *48*(10), 2962–2971.

Modares, H., Moghadam, R., Lewis, F. L., & Davoudi, A. (2018). Static output-feedback synchronisation of multi-agent systems: A secure and unified approach. *IET Control Theory & Applications*, *12*(8), 1095–1106.

Mustafa, A., & Modares, H. (2019). Attack analysis and resilient control design for discrete-time distributed multi-agent systems. *IEEE Robotics and Automation Letters*, *5*(2), 369–376.

Ogren, P., Fiorelli, E., & Leonard, N. E. (2004). Cooperative control of mobile sensor networks: Adaptive gradient climbing in a distributed environment. *IEEE Transactions on Automatic control*, *49*(8), 1292–1302.

Olfati-Saber, R., & Murray, R. M. (2004). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, *49*(9), 1520–1533.

Pasqualetti, F., Bicchi, A., & Bullo, F. (2012). Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, *57*(1), 90–104.

Rahimian, M. A., & Preciado, V. M. (2015). Detection and isolation of failures in directed networks of LTI systems. *IEEE Transactions on Control of Network Systems*, *2*(2), 183–192.

Ruan, M., Gao, H., & Wang, Y. (2019). Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, *64*(10), 4035–4049.

Sundaram, S., & Hadjicostis, C. N. (2011). Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*, *56*(7), 1495–1508.

Tan, Z., Yang, P., & Nehorai, A. (2014). An optimal and distributed demand response strategy with electric vehicles in the smart grid. *IEEE Transactions on Smart Grid*, *5*(2), 861–869.

Teixeira, A., Sandberg, H., & Johansson, K. H. (2010). Networked control systems under cyber attacks with applications to power networks. In *Proceedings of American Control Conference (ACC)* (pp. 3690–3696).

Wieland, P., & Allgower, F. (2009). An internal model principle for consensus in heterogeneous linear multi-agent systems. In *Proceedings of the 1st IFAC Workshop Distributed Estimation and Control in Networked Systems* (pp. 7–12).

Wieland, P., Sepulchre, R., & Allgöwer, F. (2011). An internal model principle is necessary and sufficient for linear output synchronization. *Automatica*, *47*(5), 1068–1074.

Zeng, W., & Chow, M. Y. (2014). Resilient distributed control in the presence of misbehaving agents in networked control systems. *IEEE Transactions on Cybernetics*, *44*(11), 2038–2049.

Zhu, M., & Martínez, S. (2013). On distributed constrained formation control in operator-vehicle adversarial networks. *Automatica*, *49*(12), 3571–3582.