Bipartite containment of heterogeneous multi-agent systems under denial-of-service attacks: a historical information-based control scheme

Received: 30 June 2023 | Revised: 13 October 2023 | Accepted: 22 November 2023

DOI: 10.1002/rnc.7128

RESEARCH ARTICLE

WILEY

Bipartite containment of heterogeneous multi-agent systems under denial-of-service attacks: A historical information-based control scheme

Yize Yang[1] | **Peng Shi**[1] | **Shuoyu Wang**[2] | **Jonathon Chambers**[3,4]

[1]School of Electrical and Mechanical Engineering, The University of Adelaide, Adelaide, South Australia, Australia

[2]School of System Engineering, Kochi University of Technology, Kochi, Japan

[3]College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin, China

[4]School of Engineering, University of Leicester, Leicester, UK

Correspondence
Peng Shi, School of Electrical and Mechanical Engineering, The University of Adelaide, Adelaide, SA 5005, Australia.
Email: peng.shi@adelaide.edu.au

Abstract

A distributed control scheme based on historical information is designed to solve the problem of stable control of multi-agent systems under denial of service (DoS) attacks in this article. It achieves the control objective of bipartite output containment control, that is, the output states of the followers smoothly enter the target area. The control scheme updates the states of followers through historical information in the control protocol when agents are subjected to DoS attacks. A distributed state observer with a storage module is designed to efficiently estimate the state of followers and store the observed information as history information. The historical information of control protocol calls is not necessarily the real state information in the existence of DoS attacks. Consequently, a closed-loop feedback state compensator is designed. Then, the state compensator is converted from the time domain to the frequency domain for stability analysis using the Nyquist criterion. It is obtained that an upper bound on the amount of historical information can achieve the bipartite output trajectories containment of the controlled system. The output trajectories of the followers converge into two dynamic convex hulls, one of which is surrounded by multiple leaders, and the other is a convex hull with opposite signs of the leaders. Finally, a numerical simulation is used to verify the proposed control scheme, and the operability of the scheme is further demonstrated in a physical experiment.

KEYWORDS

bipartite output containment, denial-of-service attacks, frequency domain analysis, historical information, signed digraph

1 | INTRODUCTION

Over the past few years, the research on the containment control of multi-agent systems (MASs) has been greatly developed due to its wide application in many fields, such as unmanned aerial vehicle formation,[1] unmanned vehicle parking,[2]

Abbreviations: ANA, anti-nuclear antibodies; APC, antigen-presenting cells; IRF, interferon regulatory factor.

and multi-aircraft navigation.[3] Distributed containment control methods are used where followers can only use the information of neighbors via communication and cannot send data to leaders.[4] Previous studies have proposed a variety of approaches to implement the containment control problem, such as a fuzzy control scheme based on finite time and output feedback developed by combining an adaptive control algorithm and integral compensator technology,[5] and the event-triggered cooperative control problem investigated based on the dynamic adaptive control algorithm.[6] An adaptive formation cooperative control scheme is proposed to diagnose and compensate for operational faults in actuators,[7] based on the modified power integrator technique. Subsequently, significant results have been obtained on the output collaborative control problem of both general continuous-time and discrete-time MASs,[8,9] which were later generalized[10] and further improved.[1,11]

By developing proper control protocols with adjacent information and interaction, MASs can be driven to achieve various coordinated control and collective behaviors. The common trait of conventional MASs is that all agents are connected only by positive weights representing information transfer, that is, the communication topology considers only the interaction rules for cooperative relationships.[12] It should be pointed out that in social networks or industrial systems, there are also confrontational relationships in addition to cooperative relationships. Thus, cooperative-adversarial signed networks are proposed,[13] where the adversarial and cooperative interactions between agents are represented by negative weights and positive weights, respectively. The containment control problem with both of these relationships simultaneously is referred to as bipartite containment control. It differs from classic containment control by introducing an additional convex hull formed by the leaders' positions with opposite signs. Based on the research idea, the containment control problem for MASs with cooperation-confrontation relationship has been further developed, such as communication noise,[14] event triggering,[15] and time delay.[16] The problem of achieving bipartite consensus over a specified time interval, encompassing antagonistic relationships and time interval constraints, was addressed.[17] The necessary and sufficient conditions for achieving bipartite collaborative control are deduced and extended to the case with time intervals for continuous-time single-integrator MASs with cooperative-antagonistic relationships.[18] These results provide a foundation for understanding and solving various coordination control problems in cooperative-antagonistic MASs and have implications for a wide range of applications. A distributed control approach is utilized based on the above research work to attain a bipartite consensus. However, the above-mentioned research questions are aimed at the distributed control system, which is vulnerable to malicious cyber-attacks during signal transmission, resulting in system damage.

In transmitting information in the multi-agent system communication network, malicious attackers may carry out DoS attacks. DoS attacks have become more clearly understood over the past few years as more reachable patterns are involved. The study of communication-based autonomous vehicle network systems subject to DoS attacks has been addressed with regard to the lateral control problem.[19] The stability of cyber-physical systems based input-to-state practical experiencing malicious DoS attacks has been analyzed,[20] while a secure control problem for a kind of power systems with conventional state estimators with DoS attacks is considered.[21] In order to defend against DoS attacks, several approaches have been taken to in-depth study the security of MASs. Specifically, a distributed hybrid event triggering strategy and a multiple Lyapunov function approach have been proposed[22,23] respectively to ensure the stability of MASs with DoS attacks. A distributed control method for MASs is presented to resist distributed DoS attacks,[24] which includes a resilient observer and an adaptive control algorithm. However, there is currently no available result for the collaborative control of heterogeneous linear MASs with DoS attacks. One significant challenge in dealing with this problem is that agents are affected by DoS attacks, rendering them incapable of interacting with one another for a certain period. Therefore, it is crucial to design an effective method to resist DoS attacks and achieve the cooperative control problem.

Compared to existing literature, our study introduces a historical information retrieval method based on the generalized Nyquist criterion and devises a control scheme that involves observation before compensation. This approach guarantees the achievement of bidirectional output containment control for MASs affected by DoS attacks and communication disruptions. The main contribution is three-fold:

1. It is not feasible for agents to acquire adjacent network information in the presence of a DoS attack, which is a challenge for updating system states. Therefore, a distributed observer based on the storage module mechanism has been devised to circumvent this challenge;
2. A storage module is employed in MASs to store the state information of neighbors observed by the distributed state observer, which may have errors with the real-time real state. Thus, a full-state feedback compensator is designed to offset the possible error between the observed and real neighbor state information during DoS attacks;

3. The generalized Nyquist criterion is exploited to determine the maximum historical information of MASs with DoS attacks, and the bipartite containment control problem is realized. A more accurate description of the maximum stability operating system constraint than the commonly used Lyapunov method is provided by this approach.

To provide a structured overview, the remainder of this article is presented as follows. The essential preliminaries and the problem formulation of bipartite containment control are shown in Section 2. In Section 3, the impact of observation errors under DoS attacks is discussed and a control scheme for calling historical information from storage modules is proposed. To confirm the theoretical analysis, a numerical simulation, and a physical simulation are shown in Section 4. Finally, conclusions are given in Section 5.

2 | PRELIMINARIES AND PROBLEM FORMULATION

A heterogeneous MAS consisting of m leaders and n followers is considered in this article. The communication network of agents can be represented by a signed digraph $\mathcal{G}$ with positive and negative weights. Basic graph concepts are introduced for subsequent analysis.

2.1 | Graph theory

A heterogeneous MAS associated with the digraph $\mathcal{G}$ of signed communications is considered. The interaction relationship among n agents is called the topology of MAS, which can be represented by a communication structure digraph. The leader exhibits autonomous behavior and cannot receive information, that is, there is no edge pointing to the leader. The followers can receive information from leaders as well as direct information from neighbor followers. The communication structure sub-digraph $\mathcal{G}_0$ of followers and the topology of multiple leaders constitute a complete heterogeneous MAS, which consists of n followers and m leaders with an interaction relationship described by the signed digraph $\mathcal{G}$ with positive and negative weights. The sub-digraph $\mathcal{G}_0 = (\mathcal{N}, \mathcal{E}, \mathcal{A})$, where the set of follower nodes denotes $\mathcal{N} = \{n_1, n_2, n_3, \dots\}$ and the set of interaction relationship denotes $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$.

An edge $(n_j, n_i) \in \mathcal{E}$ indicates that node i and node j are neighbors such that they can exchange states information or data information. An adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$ related to graph $\mathcal{G}$ is given such that $a_{ij} = 1$ if $(n_j, n_i) \in \mathcal{E}$ while $a_{ij} = 0$ otherwise. Denote a directed line from node i to node j in the form $\{(n_i, n_{i+1}), (n_{i+1}, n_{i+2}), \dots, (n_{j-1}, n_j)\}$. The diagonal matrix $G_k = diag(g_i) \in \mathbb{R}^{n\times n}$ are pinning gains, where $g_i = \sum_{k=n+1}^{k=n+m} g_{ij}$. Kronecker product is denoted by $\otimes$. Let $\mathbb{R}^q$, $\mathbb{R}^{p\times q}$ be the q dimensional and $p \times q$ dimensional Euclidean spaces, respectively. Denote $n \times n$ dimensional identity matrix by I_n. The Laplacian matrix $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{n\times n}$ is given as $l_{ij} = \sum_{i\neq j} a_{ij}$ while $l_{ij} = -a_{ij}$ for $i \neq j$, there are no self-loops $a_{ii} = 0$. The degree of agent is $D = diag\left[\sum_{j\in N_i} |a_{ij}|\right]$.

Definition 1 (13). The general Laplacian matrix and the signed Laplacian matrix are denoted as $\mathcal{L} = D - \mathcal{A}$ and $\overline{\mathcal{L}} = D - \overline{\mathcal{A}}$, where $\overline{\mathcal{A}} = [|a_{ij}|] \in \mathbb{R}^{n\times n}$ is the adjacency matrix of a signed digraph $\overline{\mathcal{G}}$.

Lemma 1 (13). *Suppose that there is a directed spanning forest for the signed sub-digraph $\mathcal{G}_0$. Subsequently, the following results are equivalent*:

(i) The $\mathcal{G}_0$ is called structural balance;
(ii) The associated digraph $\mathcal{G}_0(\mathcal{A}_u)$ is structurally balanced, then a matrix $\mathcal{A}_u = (\mathcal{A} + \mathcal{A}^{\mathrm{T}})/2$ is hold.
(iii) The signature matrix set $\mathcal{Q} = diag(\sigma_i)$, $\sigma_i \in \{1, -1\}$, such that $\overline{\mathcal{A}} = [|a_{ij}|] = Q\mathcal{A}Q$, where $Q = Q^{\mathrm{T}} = Q^{-1} \in \mathcal{Q}$.

Remark 1. According to the results of Reference 13, a structurally balanced signed digraph can choose a suitable Q so that $Q\mathcal{A}Q$ is non-negative. Furthermore, the MASs associated with the signed digraph can achieve the bipartite consensus. Therefore, Assumption 3 being true is a prerequisite for Lemma 2. Otherwise, there is no suitable Q such that $Q\mathcal{A}Q$ is non-negative.

2.2 | System description

The research object of this article is the general linear heterogeneous dynamic MASs, which consist of m leaders and n followers, each with dynamic behavior and differing dimensions. The dynamics of the followers are given as follows

$$\begin{cases} \dot{r}_i(t) = A_i r_i(t) + B_i u_i(t) \\ y_i(t) = C_i r_i(t) \end{cases}, \qquad i = 1, \dots, n, \tag{1}$$

where the input state, control protocol, and output state of the ith follower are denoted by $r_i(t) \in \mathbb{R}^p$, $u_i \in \mathbb{R}^n$, and $y_i(t) \in \mathbb{R}^q$, respectively. The state matrix and control protocol matrix are represented by Ai and B_i, respectively. The dynamics of the leaders are given as follows

$$\begin{cases} \dot{\xi}_k(t) = S\xi_k(t) \\ y_k(t) = R\xi_k(t) \end{cases}, \qquad k = n+1, \dots, n+m, \tag{2}$$

where the input and output state of the kth leader are denoted by $\xi_k(t) \in \mathbb{R}^p$ and $y_k(t) \in \mathbb{R}^q$, respectively. The constant matrices $S \in \mathbb{R}^{q\times q}$ and $R \in \mathbb{R}^{p\times q}$ need to be designed.

The subsequent technical outcomes are crucial prerequisites for the principal findings.

Definition 2 (13). A signed subdigraph $\mathcal{G}_0$ is considered structural balance if there exists a bipartition of its nodes $\mathcal{N}_1$, $\mathcal{N}_2$ such that $\mathcal{N}_1 \bigcup \mathcal{N}_2 = \mathcal{V}$, $\mathcal{N}_1 \bigcap \mathcal{N}_2 = 0$, and $a_{ij} \geq 0$, for any $n_i, n_j \in \mathcal{N}_z$, where $z \in \{1, 2\}$. Moreover, $a_{ij} \leq 0$ for any $\forall n_i \in \mathcal{N}_z$ and $n_j \in \mathcal{N}_r$ with $z \neq c, z, c \in 1, 2$, then $\mathcal{G}_0$ is structurally unbalanced.

Assumption 1. For a follower i, there exists a directed line in the signed digraph $\mathcal{G}$ from the leader k that can transfer information called g_{ik}.

Assumption 2. The real parts of all eigenvalues of the constant matrix S are nonnegative.

Assumption 3. The signed sub-digraph $\mathcal{G}_0$ is known as the so-called structural balance and has a spanning tree.

Assumption 4. For every follower i, the pair (A_i, B_i) is stabilizable and the pair (A_i, C_i) is detectable.

Remark 2. It is important to note that Assumption 4 is critical in control system design because an unstable state can lead to unpredictable results such as system loss of control or unstable oscillation, which can have negative impacts on the system's performance and reliability. Similarly, if a system is undetectable, state feedback controllers cannot be used to design the control system. These assumptions are utilized in References 25 and 26.

2.3 | DoS attacks model

DoS attacks are a class of malicious attacks by destroy or block the communication channel, which can interrupt the communication between agents, thereby destroying the system to achieve the goal of cooperative control. In principle, such malicious effects can affect the communication channels between agents in MASs. Inspired by Reference 27, we model the DoS attack by its launching time instants and durations.

The case of DoS simultaneously affecting the communication channels from leaders to followers and among followers is considered in this article. It is assumed that data transmission is impossible in the presence of DoS attacks. The attacker can interrupt communication channels during active periods that vary over time. Considering real-world resource limitations, DoS attacks from malicious attackers are typically constrained, which means that the duration of each communication blockage within the system is limited. The sequence $\{\vartheta_n\}_{n\in N_+}$ denotes the transitions of the DoS attacks from normal communication to communication interruption, that is, DoS off/on transitions. Therefore, for a given time $t \geq \Delta n \in \mathbb{R}$, the sets of time instants where DoS time-interval can be expressed as follows[28–30]:

$$K_n := \{\vartheta_n\} \bigcup [\vartheta_n, \vartheta_n + \Delta_n]$$

represents the nth communication is disrupted, which lasts for a duration of $\Delta_n \geq 0$, during which encountered DoS attacks. If $\Delta_n = 0$, the nth DoS attack takes the form of a single signal at time ϑ_n. The agent updates the state and sends information to neighbors based on recently received control instructions. For a given time $t \geq t_0 \geq 0$, the sets of time intervals when DoS attacks lead to communication failure and normal communication without attacks are denoted as

$$\Xi(t_0, t) = \bigcup_{n \in N} K_n,$$
$$\Theta(t_0, t) = [t_0, t] \setminus \Xi[t_0, t].$$

Consider DoS attacks on communication can be expressed as

$$\alpha(t) = \begin{cases} 0, & if \Theta(0, t) \neq \emptyset, \\ 1, & otherwise, \end{cases}$$

where $\alpha(t) = 1$ implies the MASs subject to DoS attacks, and $\alpha(t) = 0$ implies no DoS attacks.

Remark 3. In this article, all the communication relationships between agents are vulnerable to malicious DoS attacks. In particular, malicious attackers are capable of interrupting multiple or all communication transmissions within each time interval.

2.4 | Problem formulation

In order to clarify the bipartite output containment control problem studied in this article, it is necessary to introduce the following definition for the explanation.

Definition 3 (31). There exists a distance from $r \in \mathbb{R}^n$ to $\varpi \in \mathbb{R}^n$ is defined as follows:

$$dist(r, \varpi) = \inf_{y \in \varpi} \|r - y\|_2,$$

where $|\cdot|_2$ denotes the Euclidean norm.

Definition 4 (32). There exists a set $\varpi \in \mathbb{R}^n$ is convex if $(1 - \kappa)r + \kappa y \in \varpi$ for all $r, y \in \varpi$ and all $\kappa \in (0, 1)$. The set of output trajectories of leaders and sign-reversed output trajectories is expressed as $Y_{\mathcal{L}}(t) = \{y_{n+1}, y_{n+2}, \ldots, y_{n+m}\}$. The extended convex hull $CO(Y_{\mathcal{L}})$ can be thought of as a convex set containing all minimal agents in $Y_{\mathcal{L}}$. In other words, for $\sum_{k=n+1}^{n+m}(\alpha_k y_k - \beta_k y_k)$, it has

$$CO(Y_{\mathcal{L}}) = \left\{ \alpha_k \geq 0, \beta_k \geq 0, \sum_{k=n+1}^{n+m} (\alpha_k + \beta_k) = 1 \right\},$$

where the convex hull of $CO(Y_{\mathcal{L}})$ is the minimal convex set of all combinations of $\sum_{k=n+1}^{n+m} \beta_k y_k$ in $Y_{\mathcal{L}}$.

Lemma 2 (26). *For the system of equations given by*

$$\begin{cases} A_i \Pi_i + B_i \Gamma_i = \Pi_i S \\ C_i \Pi_i = R \end{cases}, \tag{3}$$

For each i ranging from 1 to n, it is ensured that there is a distinct solution (Π_i, Γ_i).

The control objective of this article is to achieve bipartite output containment control for heterogeneous MASs subject to DoS attacks, where the followers and leaders have different dimensional states and communication may be blocked. The main design objectives are listed below. First, a heterogeneous MAS composed of agents with different dimensional states is considered. Second, there is information transmission between the leader and followers, and DoS attacks may

be encountered in this process. Finally, the communication topology associated with MASs includes negative weights in addition to positive weights.

To achieve the above objectives, a control scheme that invokes the historical information in the state observer and state compensator is designed, which can be adapted to common intelligent systems. The objective of the bipartite output containment control problem is to develop a novel distributed control protocol u_i such that the output trajectory y_i of the followers asymptotically converges to the convex hull formed by the trajectories of the leaders, one of which is the true convex hull y_k and the sign-reversed unrealistic convex hull $-y_k$ of the leader, that is,

$$\lim_{t\to\infty} dist(y_i(t), Co(Y_{\mathcal{L}}(t))) = 0, \qquad i = 1, \dots, n. \tag{4}$$

The above provides the foundational definitions, lemmas, and notions that are necessary for addressing the problem in this article. The following section will introduce the main research results.

3 | MAIN RESULTS

In this section, a novel control protocol is proposed to address the state update problem under DoS attacks and achieve bipartite output inclusion control for heterogeneous MAS.

The output signed containment error of heterogeneous MAS is defined as follows,

$$\begin{aligned} e_{y_i}(t) = &\sum_{j=1}^{n} a_{ij}\left[y_j(t) - sgn\left(a_{ij}\right)y_i(t)\right] \\ &+ \sum_{k=n+1}^{n+m} g_{ik}\left[y_k(t) - sgn(g_{ik})y_i(t)\right], \end{aligned} \tag{5}$$

the following error can be obtained by further derivation

$$\begin{aligned} e_{y_i}(t) = &\sum_{j=1}^{n}\left[a_{ij}y_j(t) - \left|a_{ij}\right|y_i(t)\right] \\ &+ \sum_{k=n+1}^{n+m}\left[g_{ik}y_k(t) - \left|g_{ik}\right|y_i(t)\right] \\ = &\sum_{k=n+1}^{n+m} g_{ik}y_k(t) - \sum_{k=n+1}^{n+m}\left|g_{ik}\right|y_i(t) \\ &+ \sum_{j=1}^{n}\left[a_{ij}y_j(t) - \left|a_{ij}\right|y_i(t)\right]. \end{aligned} \tag{6}$$

Let $\Phi_k = \frac{1}{m}\mathcal{L} + \overline{G}$, then The output signed containment error (6) can be obtained as

$$\begin{aligned} e_y(t) = &\left(G_k \otimes I_q\right)Y_2 \\ &- \left[(D - \mathcal{A}) \otimes I_q + \left(\overline{G}_k \otimes I_q\right)\right]Y_1 \\ = &\left(G_k \otimes I_q\right)Y_2 - \left(\Phi_k \otimes I_q\right)Y_1, \end{aligned} \tag{7}$$

where $e_y(t) = \left[e_{y_1}(t), , e_{y_n}(t)\right]^{\mathrm{T}}$, $Y_1 = [y_1(t), \dots, y_n(t)]^{\mathrm{T}}$ and $Y_2 = [y_{n+1}(t), \dots, y_{n+m}(t)]^{\mathrm{T}}$.

Considering the DoS attacks model, the cooperative control tracking error in the above case can be defined as

$$\tilde{e}_y(t) = (1 - \alpha(t))e_y(t) + \alpha(t)e_y(t - \tau(t)), \tag{8}$$

where $\tau(t)$ represents the history of information transmitted in communication between agents. Because of DoS attacks, historical information is time-varying and satisfies $0 < \tau(t) \leq h$, h means the maximum historical information that can be saved.

DoS attacks can attack all communication channels, blocking the transmission signals between agents and preventing them from receiving real-time data, resulting in reduced system performance. To determine the agent state of the last received normal communication information, the distributed state observer is designed as

$$\begin{cases} \dot{\hat{r}}_i(t) = A_i\hat{r}_i(t) + B_iu_i(t) - D_i(y_i(t) - \hat{y}_i(t)) \\ \hat{y}_i(t) = C_i\hat{r}_i(t) \end{cases}, \tag{9}$$

where $\hat{r}_i$ is the observation state and D_i is the observation gain matrix that needs to be adjusted. Then, the state observation errors under DoS attacks can be defined as follows

$$\tilde{r}(t) = r(t) - \hat{r}(t), \tag{10}$$

where $\tilde{r}(t) = [\tilde{r}_1(t), \tilde{r}_2(t), \ \dots \ , \tilde{r}_n(t)]^{\mathrm{T}}$ and $\hat{r}(t) = \left[\hat{r}_1(t), \hat{r}_2(t), \ \dots \ , \hat{r}_n(t)\right]^{\mathrm{T}}$.

Lemma 3. *For given the followers' dynamics (1) and the leaders' dynamics (2) and assuming that Assumptions 1–4 are satisfied, the state observer can asymptotically achieve tracking of the follower r_i under DoS attacks. It holds that $\lim_{t\to\infty} \tilde{r}(t) = 0$ if D_i is adjusted such that $A_i + D_iC$ is stable.*

Proof. It is noted by (9) and (10) that

$$\begin{aligned} \dot{\tilde{r}}(t) &= \dot{r}(t) - \dot{\hat{r}}(t) \\ &= diag(A_i)r(t-h) + diag(B_i)u(t-h) \\ &\quad - \left[diag(A_i)\hat{r}(t-h) + diag(B_i)u(t-h)\right] \\ &\quad - \left[diag(D_i)(y_i(t-h) - \hat{y}_i(t-h))\right] \\ &= diag(A_i + D_iC_i)\tilde{r}(t-h). \end{aligned} \tag{11}$$

The state observer tracking error $\lim_{t\to\infty} \tilde{x}(t) = 0$ can be achieved if D_i is designed such that $A_i + D_iC_i$ is stable. This means that the state observer can effectively track the system's state even in the presence of DoS attacks. ∎

Remark 4. When a multi-agent system encounters DoS attacks, followers are typically unable to receive state update information from the leader. Hence, a distributed state observer is designed to provide state observation information for the system affected by the aforementioned issues. Lemma 3 gives the condition for effective observation by the distributed state observer. It is worth emphasizing that, due to the existence of a storage module, when a DoS attack occurs, the distributed state observer actually tracks the historical state information, that is, $r(t-h)$. The historical state information stored in the storage module may be different from the true state information. For general intelligent systems, the controller will not be attacked by DOS when calling historical information from the storage module.

To eliminate the aforementioned error and enable the followers to achieve the desired state under DoS attacks, a feedback compensator needs to be designed. According to Lemma 2, the following full-state feedback compensator is designed as follows

$$\begin{aligned} \dot{\xi}_i(t) = S\xi_i(t) &+ \sum_{j=1}^{n} \left(a_{ij}\xi_j(t) - \left|a_{ij}\right|\xi_i(t)\right) \\ &+ \sum_{k=n+1}^{n+m} (g_{ik}\xi_k(t) - |g_{ik}|\xi_i(t)). \end{aligned} \tag{12}$$

Consider the MAS subject to DoS attacks, $\tilde{e}_y(t)$ in (8) can be reformulated as

$$\begin{aligned}
\tilde{e}_y(t) &= e_y(t-\tau(t)) \\
&= -\left(\Phi_k \otimes I_q\right)\Big[Y_1(t-\tau(t)) \\
&\quad -\left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)Y_2(t-\tau(t))\Big] \\
&= -\left(\Phi_k \otimes I_q\right)\Big[diag(C_i)r(t-\tau(t)) \\
&\quad -\left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)(I_n \otimes R)\bar{\xi}(t-\tau(t))\Big] \\
&= -\left(\Phi_k \otimes I_q\right)\Big[diag(C_i)r(t-\tau(t)) \\
&\quad -diag(C_i\Pi_i)\left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)\bar{\xi}(t-\tau(t))\Big] \\
&= -\left(\Phi_k \otimes I_q\right)\big\{diag(C_i)[r(t-\tau(t)) \\
&\quad -diag(\Pi_i)\delta(t-\tau(t))]\big\} \\
&= -\left(\Phi_k \otimes I_q\right)\big\{diag(C_i)[r(t-\tau(t)) \\
&\quad +\gamma(t-\tau(t)) + diag(\Pi_i)\delta(t-\tau(t))]\big\},
\end{aligned} \tag{13}$$

where $\delta(t) = \xi(t) - \left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)\bar{\xi}(t)$ is denoted by the full-state feedback signed compensator errors. The current $\tilde{e}_y$ represents the cooperative control tracking error under DoS attacks. It will now be demonstrated that bipartite containment control of MASs under DoS attacks is achieved by $u_i(t)$, which utilizes the history information from state observers and feedback compensators in followers.

The state observation signed containment errors under DoS attacks are defined as follows,

$$\gamma(t) = \hat{r}(t) - diag(\Pi_i)\xi(t), \tag{14}$$

where $\gamma(t) = [\gamma_1(t), \gamma_2(t), \ldots, \gamma_n(t)]^{\mathrm{T}}$ and $\xi(t) = [\xi_1(t), \xi_2(t), \ldots, \xi_n(t)]^{\mathrm{T}}$.

Lemma 4. *The signed compensator errors (14) can converge to zero under Assumptions 1–3, that is,* $\lim_{t\to\infty} \delta(t) = 0$, *if historical information h is satisfied*

$$h < \frac{\pi}{2\lambda_{\max}(\varphi)}, \tag{15}$$

where $\lambda_{\max}(\varphi)$ *is denoted as the maximum eigenvalue of* φ.

Proof. According to the signed compensator errors (14), we can obtain

$$\begin{aligned}
\dot{\delta}(t) &= \dot{\xi}(t) - \left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)\dot{\bar{\xi}}(t) \\
&= (I_n \otimes S)\xi(t-h) - \left(\Phi_k \otimes I_q\right)\delta(t-h) \\
&\quad - \left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)\bar{\xi}(t-h) \\
&= (I_n \otimes S)\xi(t-h) - \left(\Phi_k \otimes I_q\right)\delta(t-h) \\
&\quad - (I_n \otimes S)\left(\Phi_k \otimes I_q\right)^{-1}\left(\overline{G}_k \otimes I_q\right)\bar{\xi}(t-h) \\
&= \left[(I_n \otimes S) - \left(\Phi_k \otimes I_q\right)\right]\delta(t-h).
\end{aligned} \tag{16}$$

Let $\varphi = (I_n \otimes S) - \left(\Phi_k \otimes I_q\right)$, one has

$$\dot{\delta}(t) = \varphi\delta(t-h). \tag{17}$$

Then, it can be obtained by applying the Laplace transform to the above equation,

$$s\delta(s) - \delta(0) = \varphi e^{-sh}\delta(s). \tag{18}$$

From $|sI - \varphi e^{-sh}| = 0$, the system (18) will converge when s has roots in the negative plane. The former formula can be written as $\left|I - \varphi \frac{e^{-sh}}{s}\right| = 0$, $s \neq 0$. Let $s = j\omega$, according to the Nyquist criterion, if $\frac{|\lambda(\varphi)|e^{-j\omega h}}{j\omega}$ varies with ω and does not pass through any point in $(-1, 0)$, the system will converge, where $\lambda(\varphi)$ denotes the eigenvalues of φ.

Note that

$$\frac{|\lambda(\varphi)|\left(\cos^{\omega h} - j\sin^{\omega h}\right)\cdot j}{\omega} = -\frac{|\lambda(\varphi)|\sin^{\omega h}}{\omega} - j\frac{|\lambda(\varphi)|\cos^{\omega h}}{\omega}, \tag{19}$$

then, such that $\frac{|\lambda(\varphi)|\cos^{\omega h}}{\omega} = 0$ and $-\frac{|\lambda(\varphi)|\sin^{\omega h}}{\omega} = 0$, it can be obtained $\tau(t) < \min\left(\frac{\pi}{2|\lambda(\varphi)|}\right)$, which is equivalent to $h < \frac{\pi}{2\left|\lambda_{\max}(\varphi)\right|}$. ∎

Remark 5. In Lemma 4, a frequency-domain-based stability analysis method and the Nyquist criterion are used to analyze the distribution of characteristic roots in the complex plane, thereby determining the convergence characteristics of the system state. Compared with commonly used Lyapunov and LMI methods, the frequency-domain-based method used in this article can more intuitively reveal the influence of historical information on the control protocol and better reveal the robust characteristics and controllability of the system. If the φ matrix is designed to be Hurwitz, Equation (17) can be stabilized when δ is in the complex plane. The stability range matches the range obtained using the Lyapunov method and is not the maximum stability range. The frequency-domain method can be employed to determine the maximum stable range, which represents the maximum historical information that can be utilized.

According to the full-state feedback compensator and the distributed state observer, a control protocol that invokes historical information from state observers and state compensators is proposed to drive MASs to achieve bipartite output containment control,

$$u_i(t) = H_i\hat{r}_i(t) + (\Gamma_i - H_i\Pi_i)\xi_i(t), \tag{20}$$

where $\xi_i(t)$ is the feedback compensation parameter and H_i is a constant gain matrix that needs to be adjusted.

Theorem 1. *Consider a heterogeneous MAS consisting of the followers' dynamics (1) and the leaders' dynamics (2) subject to DoS attacks with Assumptions 1–4, the distributed dynamic control protocol (20) can achieve the bipartite output containment, that is,* $\lim_{t\to\infty} \tilde{e}_y(t) = 0$ *if the following two statements hold for each follower*,

(i) H_i *is adjusted to ensure the stability of* $A_i + B_iH_i$, *and* D_i *is adjusted to ensure the stability of* $A_i + D_iC_i$;
(ii) The historical information satisfies $\tau(t) < \frac{\pi}{2\left|\lambda_{\max}(\varphi)\right|}$.

Proof. By applying the distributed control protocol in (12), it can derive from (14), then

$$\begin{aligned}
\dot{\gamma}(t) &= \dot{\hat{r}}(t) - diag(\Pi_i)\dot{\xi}(t)\\
&= diag(A_i)\hat{r}(t-h) + diag(B_i)u\\
&\quad - diag(D_iC_i)\tilde{r}(t-h)\\
&\quad - diag(\Pi_i)\left[(I_n \otimes S)\xi(t-h)\right.\\
&\quad \left.-\left(\Phi_k \otimes I_q\right)\delta(t-h)\right]\\
&= diag(A_i + B_iH_i)\gamma(t-h)\\
&\quad - diag(D_iC_i)\tilde{r}(t-h)\\
&\quad + diag(\Pi_i)\left(\Phi_k \otimes I_q\right)\delta(t-h).
\end{aligned} \tag{21}$$

Let $\Lambda = diag(A_i + B_iH_i)$, $\Psi = diag(\Pi_i)\left(\Phi_k \otimes I_q\right)$ and $\Upsilon = diag(A_i + D_iC_i)$, then the closed-loop signed state error dynamics of MAS is

$$\begin{bmatrix} \dot{\gamma}(t) \\ \dot{\delta}(t) \\ \dot{\tilde{r}}(t) \end{bmatrix} = \begin{bmatrix} \Lambda & \Psi & -diag(D_iC_i) \\ 0 & \varphi & 0 \\ 0 & 0 & \Upsilon \end{bmatrix} \begin{bmatrix} \gamma(t-\tau(t)) \\ \delta(t-\tau(t)) \\ \tilde{r}(t-\tau(t)) \end{bmatrix}. \tag{22}$$

According to Lemma 4, if $\tau(t) < \frac{\pi}{2\left|\lambda_{\max}(\varphi)\right|}$, then $\delta(t)$ goes to zero. If Υ is stable, then $\tilde{r}(t)$ goes to zero. If Λ is stable, then $\gamma(t)$ goes to zero. Therefore, The output signed containment error $\lim_{t\to\infty} \tilde{e}_y(t) = 0$, which the proof is completed. ∎

Remark 6. The above is the theoretical framework of this article, aiming to address the problem of DoS attacks on MASs in achieving output bipartite containment control. The proposed control protocol utilizes observation and feedback compensation information stored in the storage module to drive MASs to achieve output bipartite containment control under DoS attacks. In comparison with the works of References 33 and 34, which are also aimed at stable control of MASs when communication is blocked, the work of this article does not significantly affect the motion process of the agents because the control protocol drives the MASs by utilizing the information stored in the storage module. According to the research motivation of the problem, the control scheme proposed in this article will be applied to real physical systems, such as unmanned cars and drones, where the motion process of the controlled vehicles is stable and smooth. The following simulation section will verify this conclusion on both numerical and physical simulation platforms, and the simulation results will also prove the above conclusion.

Corollary 1. *Consider the heterogeneous MASs composed of the followers' dynamics (1) and the leaders' dynamics (2), the bipartite containment problem can be solved if Assumptions 1 and 2 are satisfied, such that* $\lim_{t\to\infty} \tilde{e}_y(t) = 0$.

Remark 7. The proof process for Corollary 1 is similar to that of Lemma 1, hence omitted here. Note that the bipartite containment control without DoS attacks can be realized by using the historical information-based control scheme in this article. When there are no DoS attacks, the control protocol only needs to call the real-time or latest information to update the agents' state, that is, the kth or $(k-1)$th information transmission.

Remark 8. Compared with References 34 and 35, which addresses the consensus control problem based on the leader-follower system, we examine more intricate engineering problems of cooperative regulation. Moreover, References 34 and 36 only account for cooperative interactions among agents, where the communication weight is positive. A more comprehensive and complex scenario with both cooperative and competitive relationships is considered in this article. Furthermore, it should be noted that Reference 37 also investigates heterogeneous MASs with adversarial relations, but the more challenging case of encountering DoS attacks is further explored in this article.

4 | SIMULATION RESULTS

A numerical simulation is performed in this section to demonstrate the effectiveness of the designed control scheme. Furthermore, to validate the applicability of the scheme, we conducted a physical experiment.

The heterogeneous MAS considered consists of 3 leaders and 4 followers, and the communication topology structure digraph $\mathcal{G}$ of MAS is shown in Figure 1. A positive weight value represents a cooperative communication relationship, and a negative weight value represents a competitive relationship. The larger the value, the closer/farther the two agents are. The bipartition nodes are $\mathcal{N}_1 = \{n_1, n_2\}$ and $\mathcal{N}_2 = \{n_3, n_4\}$, it can be known that the $\mathcal{G}_0$ is structural balance and has a spanning tree. The bipartite output states of agents are illustrated in the Cartesian coordinate system, where the horizontal and vertical axes are represented as $(y_{\text{hor}}, y_{\text{ver}})$. Consider the initial states are $y_5 = (4.7, 2.5)$, $y_6 = (4.7, 1.5)$ and $y_7 = (5.6, 2)$ for the dynamics (2) of the leaders for $k = 5, 6, 7$ and the initial input states are $r_1 = (0, 4)$, $r_2 = (0, -1)$, $r_3 = (0, 2)$ and $r_4 = (0, -3)$ for the dynamics (1) of the followers in a two-dimensional graph. The system matrices of each follower are

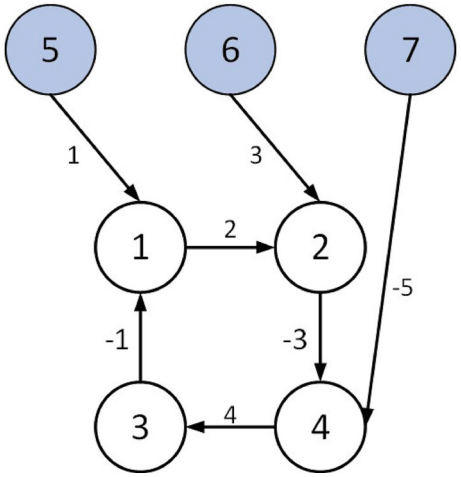

FIGURE 1 Communication structure digraph of the MAS.

described by (1) with

$$A_1 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & -1 \\ 2 & -2 \end{bmatrix},$$
$$A_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & -1 \end{bmatrix}, A_4 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 2 & 4 & -1 \end{bmatrix},$$
$$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix},$$
$$B_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, B_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix},$$
$$C_1 = C_2 = \begin{bmatrix} -1 & 0 \end{bmatrix}, C_3 = C_4 = \begin{bmatrix} -1 & 0 & 0 \end{bmatrix}.$$

The constant matrices and control signals are defined as

$$S = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}, \ R = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$
$$D_1 = D_2 = \begin{bmatrix} 8 & 0 \\ 0 & 8 \end{bmatrix}, D_3 = D_4 = \begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix},$$
$$H_1 = H_2 = \begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}, H_3 = H_4 = \begin{bmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix}.$$

The performance of the distributed observer (9) under DoS attacks is shown in Figure 2. The bipartite state trajectories of MAS with the feedback compensator (12) and control protocol (20) subject to DoS attacks are depicted in Figure 3.

It can be seen that the state observation errors of agents converge rapidly to zero in Figure 3, indicating that the distributed observer can effectively observe the state information of the agents even when communication is blocked. The

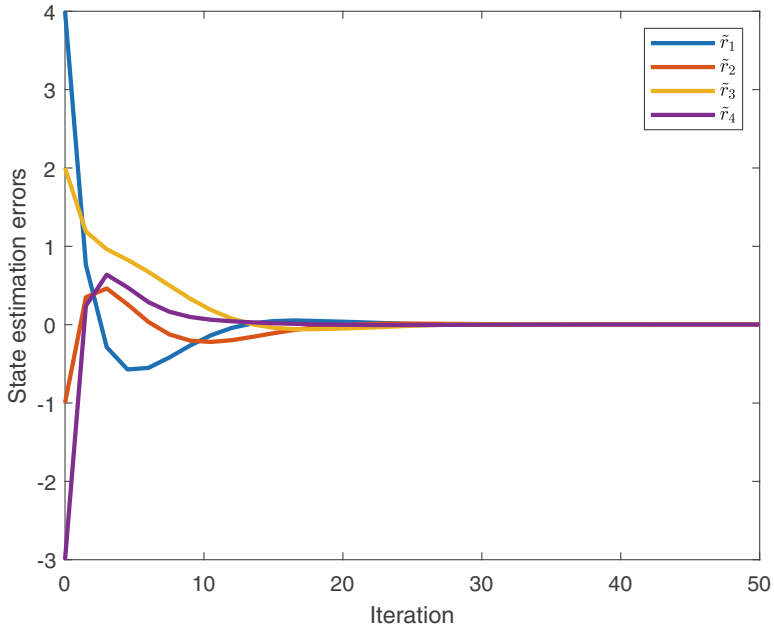

FIGURE 2 State observation errors of the followers.

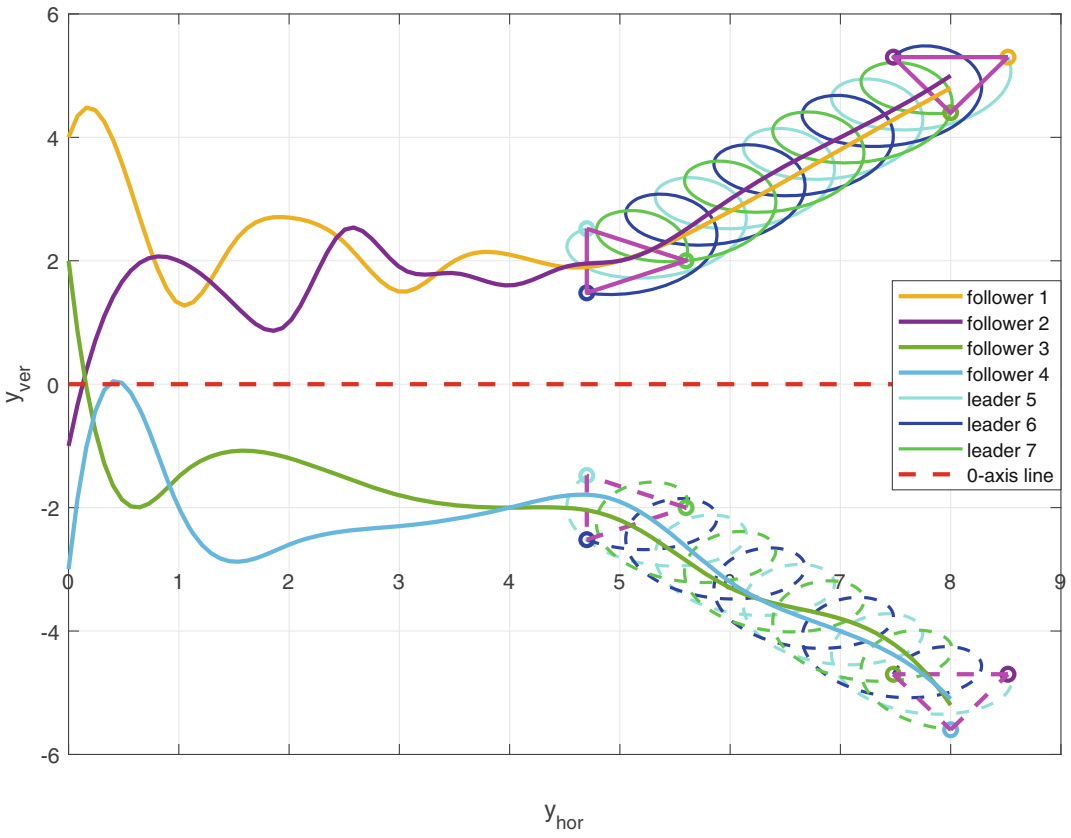

FIGURE 3 Output States of all agents.

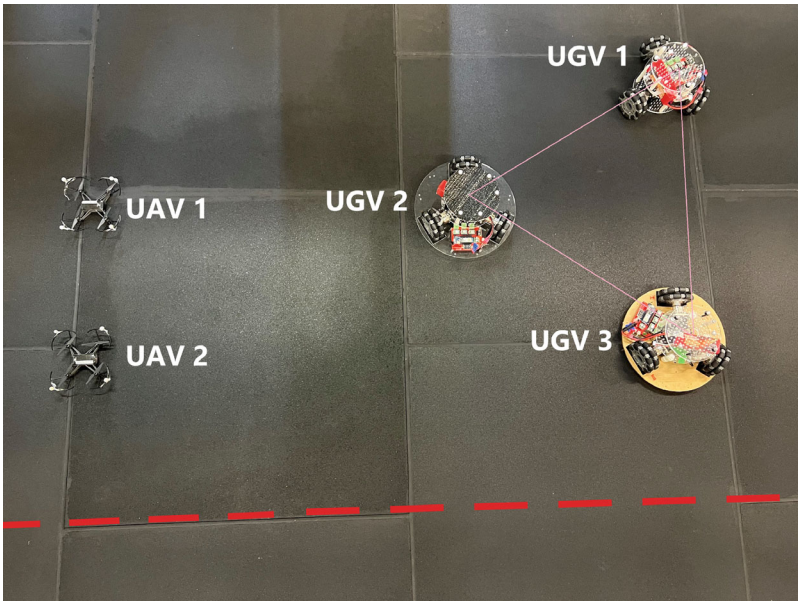

FIGURE 4 The heterogeneous system consisting of UGVs and UAVs.

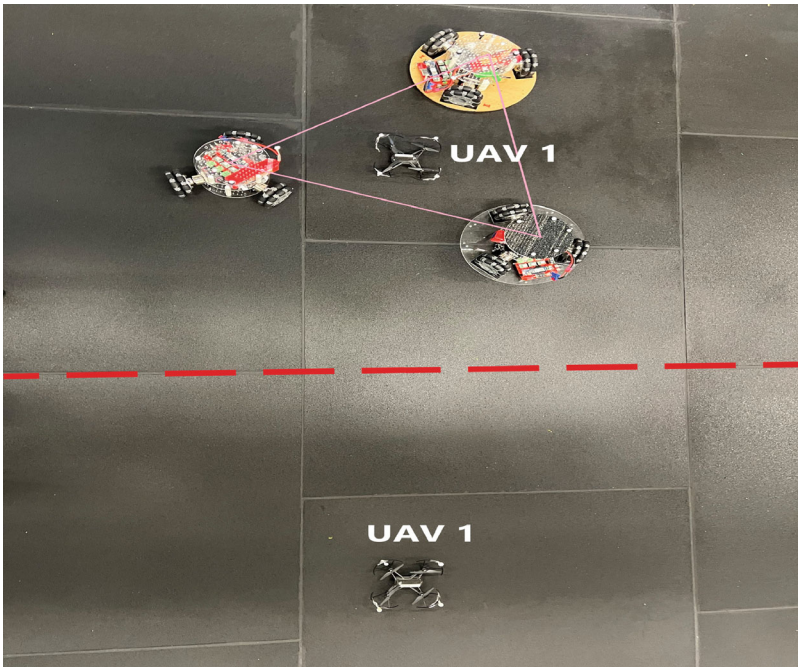

FIGURE 5 The performance of the physical heterogeneous system.

control protocol (12) drives the MASs based on the observed state history information and compensator feedback history information. In Figure 3, the solid-lined triangular region represents the true convex hull composed of three leaders. Followers 3 and 4 eventually enter the unrealistic convex hull depicted by dashed lines, which have the opposite sign of the true convex hull entered by followers 1 and 2. This indicates that the heterogeneous MASs with the proposed control protocol (12) can achieve bipartite output containment control under DoS attacks.

In addition to numerical simulations, we also conducted physical simulations. The heterogeneous multi-agent system consists of 3 UGVs and 2 UAVs, as shown in Figure 4. We note that both UGV and UAV are independent nonlinear systems vehicles. The simulation platform based on Python and ROS can control them through information interaction and state

feedback, and verify the algorithm in this article. The positions of the UGVs form a triangle representing the target convex hull enclosed by the three leaders. The UGVs move along predetermined trajectories and provide position feedback. The position trajectory of the kth UAV is given as follows

$$\xi_k(t) = \left[\cos\left(0.08t + \frac{\pi}{3}\right), \sin\left(0.08t + \frac{\pi}{3}\right), 0.2 + 0.2t\right]^{\mathrm{T}}.$$

The UAVs receive discontinuous and periodically uncertain feedback, simulating an environment in which the system is subjected to DoS attacks. The performance of the physical heterogeneous system is given in Figure 5, where it can be observed that UAV1 eventually enters the convex hull enclosed by the 3 UGVs, while UAV2 lands in the opposite position. The dashed line represents the axis of symmetry at $y_{\mathrm{ver}} = 0$. This proves that the proposed control protocol (12) can drive physical heterogeneous multi-agent systems subject to DoS attacks to achieve bipartite output containment control.

5 | CONCLUSION

This article addresses the state update problem of heterogeneous MASs when the communication in the system is blocked and achieves bipartite output containment control. A distributed state observer design was proposed to estimate the agents' states, considering the impact of malicious DoS attacks on system communication. To attain the objective of achieving bipartite output containment control, a novel distributed control scheme was developed that incorporated historical information in the state update process. Graph theory, matrix processing techniques, and the Nyquist criterion were utilized to derive the maximum constraint condition on historical information. A numerical simulation result demonstrates the reliability of the control scheme proposed in this article, and engineering verification is carried out on a heterogeneous physical platform composed of UGVs and UAVs. Further research aims to apply the research ideas and theoretical conclusions of this article to complex systems with different types of attack models and to study fault detection and fault-tolerant systems caused by cyber-attacks.

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

ACKNOWLEDGMENT

Open access publishing facilitated by The University of Adelaide, as part of the Wiley - The University of Adelaide agreement via the Council of Australian University Librarians.

ORCID

Yize Yang https://orcid.org/0009-0009-8026-7998
Peng Shi https://orcid.org/0000-0001-8218-586X

REFERENCES

1. Dong X, Hua Y, Zhou Y, Ren Z, Zhong Y. Theory and experiment on formation-containment control of multiple multirotor unmanned aerial vehicle systems. *IEEE Trans Autom Sci Eng*. 2019;16(1):229-240.
2. Cao Y, Stuart D, Ren W, Meng Z. Distributed containment control for multiple autonomous vehicles with double-integrator dynamics: Algorithms and experiments. *IEEE Trans Control Syst Technol*. 2011;19(4):929-938.
3. Gong Y, Cao L, Pan Y, Lu Q. Adaptive containment control of nonlinear multi-agent systems about privacy preservation with multiple attacks. *Int J Robust Nonlinear Control*. 2023;33(11):6103-6120.
4. Wang FY, Ni YH, Liu ZX, Chen ZQ. Containment control for general second-order multiagent systems with switched dynamics. *IEEE Trans Cybern*. 2020;50(2):550-560.
5. Li Y, Qu F, Tong S. Observer-based fuzzy adaptive finite-time containment control of nonlinear multiagent systems with input delay. *IEEE Trans Cybern*. 2021;51(1):126-137.

6. Zhou Q, Wang W, Ma H, Li H. Event-triggered fuzzy adaptive containment control for nonlinear multiagent systems with unknown Bouc–wen hysteresis input. *IEEE Trans Fuzzy Syst*. 2021;29(4):731-741.
7. Xiao W, Ren H, Zhou Q, Li H, Lu R. Distributed finite-time containment control for nonlinear multiagent systems with mismatched disturbances. *IEEE Trans Cybern*. 2022;52(7):6939-6948.
8. Liu H, Cheng L, Tan M, Hou ZG. Containment control of continuous-time linear multi-agent systems with aperiodic sampling. *Automatica*. 2015;57:78-84.
9. Liu Y, Fan Y, Ao Y, Jia Y. An iterative learning approach to formation control of discrete-time multi-agent systems with varying trial lengths. *Int J Robust Nonlinear Control*. 2022;32(17):9332-9346.
10. Xiong Q, Zhang Q, Lin P, Ren W, Gui W. Containment problem for multiagent systems with nonconvex velocity constraints. *IEEE Trans Cybern*. 2021;51(9):4716-4721.
11. Yan B, Shi P, Lim CC. Robust formation control for nonlinear heterogeneous multiagent systems based on adaptive event-triggered strategy. *IEEE Trans Autom Sci Eng*. 2022;19(4):2788-2800.
12. Zhu ZH, Hu B, Guan ZH, Zhang DX, Cheng XM. Containment control for general second-order multiagent systems with switched dynamics. *IEEE Trans Netw Sci Eng*. 2021;8(4):3099-3112.
13. Altafini C. Consensus problems on networks with antagonistic interactions. *IEEE Trans Automat Contr*. 2013;58(4):935-946.
14. Du Y, Wang Y, Zuo Z, Zhang W. Stochastic bipartite consensus with measurement noises and antagonistic information. *J Frankl Inst*. 2021;358(15):7761-7785.
15. Yu H, Chen X, Chen T, Hao F. Event-triggered bipartite consensus for multiagent systems: A Zeno-free analysis. *IEEE Trans Automat Contr*. 2020;65(11):4866-4873.
16. Ding TF, Ge MF, Xiong CH, Park JH, Li M. Second-order bipartite consensus for networked robotic systems with quantized-data interactions and time-varying transmission delays. *ISA Trans*. 2021;108:178-187.
17. Meng D, Du M, Jia Y. Interval bipartite consensus of networked agents associated with signed digraphs. *IEEE Trans Automat Contr*. 2016;61(12):3755-3770.
18. Ma CQ, Xie L. Necessary and sufficient conditions for leader-following bipartite consensus with measurement noise. *IEEE Trans Syst Man Cybern Syst*. 2020;50(5):1976-1981.
19. Lian Z, Shi P, Lim CC, Yuan X. Fuzzy-model-based lateral control for networked autonomous vehicle systems under hybrid cyber-attacks. *IEEE Trans Cybern*. 2023;53(4):2600-2609.
20. Ma R, Shi P, Wu L. Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks. *IEEE Trans Cybern*. 2021;51(5):2306-2318.
21. Chen W, Ding D, Dong H, Wei G. Distributed resilient filtering for power systems subject to denial-of-service attacks. *IEEE Trans Syst Man Cybern Syst*. 2019;49(8):1688-1697.
22. Tang Y, Zhang D, Shi P, Zhang W, Qian F. Event-based formation control for nonlinear multiagent systems under DoS attacks. *IEEE Trans Automat Contr*. 2021;66(1):452-459.
23. Zhao R, Zuo Z, Wang Y. Event-triggered control for switched systems with denial-of-service attack. *IEEE Trans Automat Contr*. 2022;67(8):4077-4090.
24. Zhang D, Deng C, Feng G. Resilient cooperative output regulation for nonlinear multiagent systems under DoS attacks. *IEEE Trans Automat Contr*. 2023;68(4):2521-2528.
25. Zuo S, Song Y, Lewis FL, Davoudi A. Adaptive output containment control of heterogeneous multi-agent systems with unknown leaders. *Automatica*. 2018;92:235-239.
26. Castro RS, Flores JV, Salton AT. Robust practical output regulation of rational nonlinear systems via numerical approximations to the regulator equations. *Int J Robust Nonlinear Control*. 2022;32(3):1229-1255.
27. De Persis C, Tesi P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans Automat Contr*. 2015;60(11):2930-2944.
28. Li Y, Wang J, Wang R, Gao DW, Sun Q, Zhang H. A switched Newton–Raphson-based distributed energy management algorithm for multienergy system under persistent DoS attacks. *IEEE Trans Autom Sci Eng*. 2022;19(4):2985-2997.
29. Zhang Y, Wang G, Sun J, Li H, He W. Distributed observer-based adaptive fuzzy consensus of nonlinear multiagent systems under DoS attacks and output disturbance. *IEEE Trans Cybern*. 2023;53(3):1994-2004.
30. Shi L, Cheng Y, Xilin Z, Jinliang S. Consensus tracking control of discrete-time second-order agents over switching signed digraphs with arbitrary antagonistic relations. *Int J Robust Nonlinear Control*. 2020;30:4826-4838.
31. Zuo S, Song Y, Lewis F, Davoudi A. Bipartite output containment of general linear heterogeneous multi-agent systems on signed digraphs. *IET Control Theory Appl*. 2018;12(9):1180-1188.
32. Wang YW, Liu XK, Xiao JW, Shen Y. Output formation-containment of interacted heterogeneous linear systems by distributed hybrid active control. *Automatica*. 2018;93:26-32.
33. Ma YS, Che WW, Deng C, Wu ZG. Observer-based event-triggered containment control for MASs under DoS attacks. *IEEE Trans Cybern*. 2022;52(12):13156-13167.
34. Zhang Y, Wu ZG, Shi P. Resilient event-/self-triggering leader-following consensus control of multiagent systems against DoS attacks. *IEEE Trans Industr Inform*. 2023;19(4):5925-5934.
35. Li D, Li T. Cooperative output feedback tracking control of stochastic linear heterogeneous multiagent systems. *IEEE Trans Automat Contr*. 2023;68(1):47-62.
36. Zuo S, Yue D. Resilient output formation containment of heterogeneous multigroup systems against unbounded attacks. *IEEE Trans Cybern*. 2022;52(3):1902-1910.

37. Zuo S, Lewis FL, Davoudi A. Resilient output containment of heterogeneous cooperative and adversarial multigroup systems. *IEEE Trans Automat Contr*. 2020;65(7):3104-3111.

How to cite this article: Yang Y, Shi P, Wang S, Chambers J. Bipartite containment of heterogeneous multi-agent systems under denial-of-service attacks: A historical information-based control scheme. *Int J Robust Nonlinear Control*. 2023;1-16. doi: 10.1002/rnc.7128