J. Appl. Comput. Mech., xx(x) (2025) 1-15
DOI: 10.22055/jacm.2025.48738.5461

ISSN: 2383-4536
jacm.scu.ac.ir

Shahid Chamran University of Ahvaz

Journal of Applied and Computational Mechanics

Research Paper

# Robust Bipartite Containment Control of Multi-Agent Systems under Stochastic Disturbances and False Data Injection Attacks via Zero-Sum Game Strategy

Ammar Alsinai[1], Ibraheem Al-Hejri[1], Azmat Ullah Khan Niazi[2], Maryam Iqbal[2], Aseel Smerat[3,4]

[1] Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Qassim 56447, Saudi Arabia, Email: aliiammar1985@gmail.com (A.A.)

[2] Department of Mathematics and Statistics, University of Lahore, Sargodha, Pakistan, Email: azmatullah.khan@math.uol.edu.pk (A.U.K.N.); maryamiqbal454@gmail.com (M.I.)

[3] Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India

[4] Faculty of Educational Sciences, Al-Ahliyya Amman University, Amman 19328, Jordan, Email: smerat.2020@gmail.com

Received September 06 2025; Revised October 27 2025; Accepted for publication November 23 2025.
✉ Corresponding authors: A. Alsinai (aliiammar1985@gmail.com); A.U. Khan Niazi (azmatullah.khan@math.uol.edu.pk)


**Abstract.** This paper addresses the problem of bipartite containment control for multi-agent systems (MASs) subjected to simultaneous stochastic disturbances and false data injection attacks (FDIA). The interactions among agents are modeled by signed directed graphs, which represent both cooperative and antagonistic relationships. A novel hybrid disturbance model is introduced to capture the challenges posed by both stochastic and adversarial inputs, reflecting the complexities of uncertainties in dynamic environments. Furthermore, the agents' communication channels are assumed to be vulnerable to FDIAs, which corrupt neighbor information and further complicate the containment objective. To tackle these issues, a zero-sum differential graphical game framework is proposed, leading to a robust control strategy that ensures system stability and containment performance even under hybrid disturbances. The theoretical convergence of the proposed method is rigorously demonstrated, and simulation results confirm its effectiveness and robustness. Practical application scenarios, such as Autonomous Vehicle Platooning under Adversarial and Noisy Conditions and Drone Swarm Surveillance under GPS Spoofing and Sensor Noise, illustrate the importance of maintaining coordinated behavior in the presence of real-world uncertainties.

**Keywords:** Bipartite Containment Control, Multi-Agent Systems (MASs), False Data Injection Attacks (FDIA), Robust Distributed Control, Cyber-Physical Security.

## 1. Introduction

The versatility of applications, including intelligent transportation, autonomous robotics, and smart grids, has made the multi-agent systems (MASs) one of the foundations of current distributed control systems. The need for robust coordination protocols has become increasingly important with the emergence of complex networked systems, presenting significant challenges, particularly when dealing with cyber-attacks and uncertainties. Gao et al. [1] provided an adaptive dynamic programming framework for securing consensus against denial-of-service (DoS) attacks, whereas Diaz-Garcia et al. [2] proposed a distributed reconfiguration strategy for resilient synchronization. Tang et al. [3] investigated the event-triggered perturbed learning-based containment. Yu et al. [4] considered fixed-time containment control with stochastic input delays, and Chen et al. [5] considered privacy-preserving economic dispatch on directed networks.

In a quest to increase the resiliency of MASs, various scientists have developed improved control mechanisms that overcome faults, cyber-attacks, and uncertainty. As an illustration, Liu et al. [6] presented a simplified adaptive fault-tolerant control algorithm, which was specifically designed to handle cases of heterogeneous MASs, where the system could still work effectively despite the possibility of actuator failures or mismatching of structural agents. In a cybersecurity application, Maaruf et al. [7] focused on deploying deception attacks to formation control using a reinforcement-learning methodology, specifically the actor-critic algorithm, to adaptively adjust to malicious actions during operation. The seminal survey in [8] provides a wider picture of developments dealing with the control problem of containment and the classification of the various methodologies followed in automatic control, as well as mentions the open issues and future research directions. And continuing the idea of adaptive control, Chen et al. [9] proposed a neuroadaptive tracking protocol of the unmanned aerial vehicles (UAV) that enables the vehicle to adapt to the desired trajectories despite the presence of non-linear dynamics and the external perturbations. Under the cyber-attacks application, Liu et al. [10] suggested an event-based bipartite strategy of containment control, clarifying how it handles the Denial-of-Service (DoS) attack scenario, where failure of communications introduces a threat to consensus. To counteract FDIA, Cheng et al. [11] created an adaptive restraining mechanism of control of the output network, which adapts a

Published online: November 28 2025

control strategy (session aware) to repel altered measures of sensor information or distorted location information. Moreover, Sekercioglu et al. [12] considered signed networks with several leaders, whose interactions were cooperative-antagonistic, as well as developed control laws on systems that can contain both positive and negative edges.

Dealing with attack resilience, Yang et al. [13] proposed a control approach that runs in the presence of DoS attacks and uses historical information to enable the system to guess about the lost data and to remain stable with occasional loss of communication. And finally, the event-based bipartite containment in uncertain network state was studied by Zhang et al. [14, 15]. These works dealt with topological uncertainty and noise disturbances, respectively, and had containment strategies that are resistant to random occurrences and fluctuating interaction patterns. Multiple studies so far on the topic have led to the creation of ideologies on containment control in MASs amid different levels of complexity. Precisely, stochastic non-linear MASs were investigated by Guo et al. [16] with the use of fixed-time command-filter-based approaches, whereby convergence occurs in a finite time irrespective of initial conditions. In [17], the emphasis was on high-order nonlinear agents, in which containment has been realized in a time-varying power dynamics model, which has realistic and variable energy constraints. In [18], asynchronous control protocols of second-order MASs were proposed, and the agents work with unsynchronized communication and actuation.

A distributed observer-based containment scheme was proposed by Zhang et al. [19] which allowed agents to derive estimates of leader states with no complete information to make coordinated decisions. To overcome the limitations that are practical, Zhao et al. [20] dealt with the MASs whose inputs were not known and forced the constraints to the states, which provides robust control strategies. Fractional-order dynamics were studied on techniques based on neural networks in [21] with a specific goal of control tasks using finite-time limitations. In works conducted by Zhang et al. [22] and Shi et al. [23], event-based containment approaches with a reduced communication overhead were proposed, with a focus on directed graphs and network delays. Moreover, Gu et al. [24] generalized containment control to fixed and Markov-switching topologies, achieving flexibility in a dynamic environment. Finally, Zhu et al. [25] generalized the singular systems to singular systems through observer-based control, an omission in the MASs theory of the descriptor-type dynamics.

In particular, Liu et al. [26] introduced a fixed-time heterogeneous MASs with the properties that any combination of follower agents converges to the specified containment set in a predetermined, fixed time, no matter what the initial conditions. Within the concept of cyber-physical security, Wu et al. [27] investigated a situation where the attackers can inject impulsive signals with built-in delays, which becomes problematic to properly and quickly react to them. To combat external disturbances, Wang et al. [28] derived containment control processes that apply to systems whose structures are designed over signed graphs; thus, they are able to treat both cooperative and antagonistic agent interactions. In the meantime, Hou et al. [29] has addressed the quantization impact in MASs and has introduced the quantization-conscious observer-based methods that make it possible to carry out efficient control despite coarse or discretized measurement values.

Treating complicated nonlinearities, Li et al. [30] developed an adaptive containment procedure of nonlinear networks that supports various nonlinear agent dynamics and uncertainties of the systems. Adopting the point of view of optimization, Yao et al. [31] combined bipartite containment with the usage of convex optimization subject to a set of conditions, providing an efficient resolution to systems that had resource/structural constraints. The overview of containment strategies was prepared by Thummalapeta and Liu [32] that generalizes the most important approaches and products in the area of the MASs containment control. According to the communication efficiency perspective, Zou et al. [33] employed event-based methods, which realized contention of inputs under stochastic noise, thus reducing unnecessary updates, even though performance is preserved. Moreover, Cai et al. [34] handled output formation containment in heterogeneous networks by devising network-based protocols where the follower output is directed to constitute a certain predetermined pattern of geometry. A new type of combined fuzzy and game-theoretic model was proposed by Yan et al. [35] for developing adaptive containment strategies that improve resilience and learning in an uncertain environment.

In order to be effective against cyber threats, Cheng et al. [36] developed FDI-resilient output regulation strategies such that the impact is contained even in the case of false data injection. In order to handle the nonlinear hysteresis phenomena, Wu et al. [37] used adaptive fuzzy observers, making it possible to estimate the precise state of complex and nonlinear memory effects in actuators or sensors. Venturing into fractional-order dynamics, the containment solutions of MASs with hostile switching topologies and input delays were demonstrated by Khan et al. [38] specifically in fractional-order systems, which more accurately describe systems with memory. In the case of high-order stochastic MASs, Song and Zhao [39] proposed a finite-time adaptive backstepping strategy that can guarantee containment in an (exponentially) decaying finite time that is independent of the stochasticity in the system. Lastly, Zhang et al. [40] analyzed cooperative, competitive, social games and singled out social game behaviors in Lagrangian-type MASs and created multi-bipartite consensus algorithms that capture complex social interactions and social dynamics within such a network.

Despite this progress, a unified framework that simultaneously addresses both stochastic disturbances and FDIAs in bipartite containment tasks remains underdeveloped. Current solutions address either of such issues independently or impose limiting assumptions like picture-perfect communications or a known state of the systems. To address these shortcomings, the zero-sum game-theoretic containment strategy is proposed in this paper, which formalizes the interaction between a resilient controller and a strategic adversary that introduces noise and misinformation. A strong policy iteration form of the controller is then obtained to ensure convergence of follower agents to the convex hull of multiple leaders, and this is despite the occurrence of hybrid disturbances.

Although the bipartite containment control problem has been studied extensively in the recent past, the existing works only focus on either stochastic disturbances or adversarial attacks. The practice, however, is that multi-agent systems tend to be deployed in the same environments where random noise and intelligent adversarial behavior, including FDIA, exist simultaneously. Stochastic perturbations, such as Brownian motion, are caused by the uncertainty of an environment, but the FDIA machine intends to corrupt communication between agents by transmitting false neighbor information. The prospects of containing such hybrid disturbances are drastic, especially in networks based on signed graphs, which involve cooperative interactions as well as antagonistic interactions. The conventional robust control techniques do not offer a satisfactory solution to this dual-threat situation since the techniques do not incorporate modeling of the strategic behavior of attackers, nor are these techniques made to operate in a scenario where interferences are random and adversarial at the same time.

In order to overcome these issues, this paper will establish a more effective, bipartite containment control framework in regards to gridlock based on the theory of zero-sum differential games. It presents a new hybrid disturbance model that combines stochastic noise and FDIA in one model. This, in turn, can be modeled as a zero-sum game between a robust controller and a strategic attacker, and each follower agent uses a policy iteration (PI) scheme to compute a distributed optimal control law based on locally available (and potentially compromised) data. Theoretical analysis ensures that the agents converge in a mean-square sense to the convex hull composed of the leaders and their complementary states. Its effectiveness and robustness across hybrid uncertainties are certain with simulation outputs, hence no limitations in terms of real-life implementation in multi-agent environments with adversarial/known and unknown uncertainties.

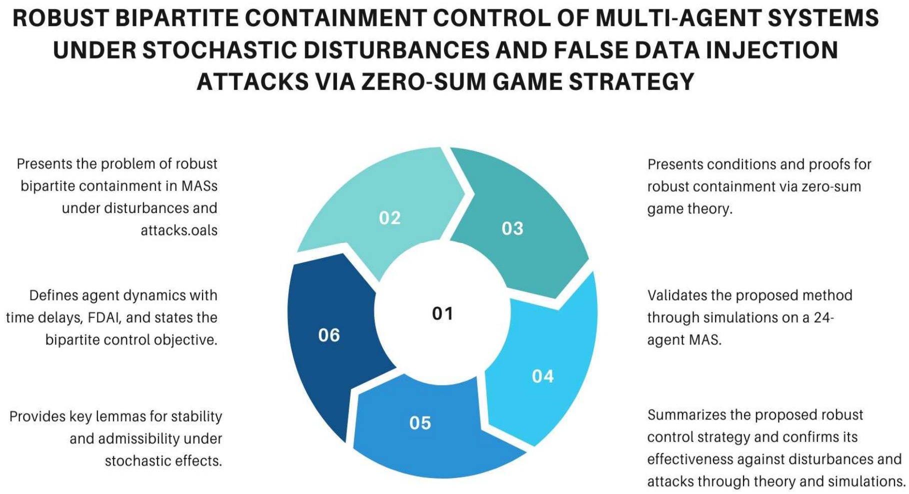


**Fig. 1.** Solution framework for robust bipartite containment control.

As illustrated in Fig. 1, the proposed solution framework for robust bipartite containment control enables the multi-agent system to resist both stochastic disturbances and FDIAs using a zero-sum game strategy. This is how the content is organized:

Section 1: In this part, the demand for resilient control in MASs during malicious attacks and uncertainties is described. It encourages the investigation of bipartite containment under stochastic modeling disturbances and FDIA. Section 2: Presents the system model, including the MAS dynamics with hybrid disturbances and the formal problem formulation of robust bipartite containment control under stochastic disturbances and FDIA. Section 3: Provides necessary mathematical preliminaries, including key lemmas and definitions that support the subsequent stability analysis. Section 4: Delivers the main theoretical results, establishing sufficient conditions for robust bipartite containment within the zero-sum game framework and providing rigorous proofs of mean-square stability and convergence. Section 5: Validates the proposed approach through numerical simulations on both 12-agent and 24-agent networks, demonstrating performance under stochastic noise and attack signals. Section 6: Concludes the paper by summarizing the key findings and suggesting potential directions for future research.

### 1.1. Key Contribution

- We introduce a comprehensive multi-agent system model that concurrently captures stochastic disturbances (modeled as Brownian motion) and False Data Injection Attacks (FDIA) on communication channels. This model provides a realistic foundation for studying bipartite containment under simultaneous random and adversarial disturbances.
- We formulate the robust bipartite containment problem as a zero-sum differential game. This strategic framework allows us to derive a distributed control law that is inherently resilient to the worst-case scenarios of the combined stochastic and adversarial inputs.
- We establish sufficient conditions, via stochastic Lyapunov analysis, to ensure the mean-square bipartite containment of the follower agents. Our analysis rigorously proves that the states converge to the signed convex hull of the leaders despite the hybrid disturbances.
- We develop a distributed policy iteration algorithm that enables each follower agent to compute the robust optimal control law based on locally available and potentially compromised information.
- We demonstrate the effectiveness and robustness of our proposed framework through detailed numerical simulations on a 24-agent network and discuss its practical relevance in two application scenarios: autonomous vehicle platooning and drone swarm surveillance.

**Table 1.** Summary of symbols and notations.

| Symbol | Description |
|---|---|
| $N$, $M$ | Number of followers and leaders |
| $x_i(t) \in \mathbb{R}^n$ | State vector of the i-th agent |
| $u_i(t) \in \mathbb{R}^m$ | Control input of the i-th follower |
| $f_i(t)$ | Hybrid disturbance (stochastic noise + FDIA) |
| $w_i(t)$ | Stochastic (Brownian motion) disturbance |
| $a_i(t)$ | FDIA component |
| $A \in \mathbb{R}^{n\times n}$ | System matrix |
| $B_i \in \mathbb{R}^{n\times m}$ | Control input matrix of the i-th agent |
| $E_i \in \mathbb{R}^{n\times d}$ | Disturbance matrix for the i-th agent |
| $\mathcal{F}$, $\mathcal{L}$ | Sets of follower and leader agents |
| $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, \mathcal{A}\}$ | Signed directed interaction graph |
| $a_{ij}$ | Weight of the edge from agent j to i |
| $g_{ik}$ | Sign of the edge from leader k to follower i (±1) |
| $D$, $L$ | Degree matrix, Laplacian matrix of graph $\mathcal{G}$ |
| $\mathcal{N}_i$ | Neighbor set of agent i |
| $e_i(t)$ | Containment error for follower i |
| $\gamma$ | Disturbance attenuation level in the cost function |
| $\mathbb{R}^n$ | n-dimensional real-valued space |
| $I_n$ | Identity matrix of size n |

**Notation:** Throughout this paper, $I_{n\times n}$ denotes the identity matrix, and $1_N$ represents an $N$-dimensional column vector with all entries equal to one. The Euclidean norm of a vector is denoted by $\|\cdot\|$. The maximum and minimum eigenvalues of a matrix are denoted by $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$, respectively. For any matrix $A$ and vector $a$, $A^T$ and $a^T$ denote their respective transposes. The notation $\mathrm{diag}\{a_1,a_2,\ldots,a_n\}$ represents a diagonal matrix with diagonal elements $a_1,a_2,\ldots,a_n$. The Kronecker product is denoted by $\otimes$. The maximum and minimum singular values of matrix $A$ are denoted by $\sigma_{\max}(A)$ and $\sigma_{\min}(A)$, respectively. We consider a multi-agent system consisting of $N+M$ agents, where the follower set is $\mathcal{F}=\{v_1,v_2,\ldots,v_N\}$ and the leader set is $\mathcal{L}=\{v_{N+1},v_{N+2},\ldots,v_{N+M}\}$. The communication topology among agents is described by a directed signed graph $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$, where $\mathcal{V}=\{v_1,v_2,\ldots,v_{N+M}\}$ is the set of nodes, $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ is the set of directed edges, and $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{(N+M)\times(N+M)}$ is the signed adjacency matrix. A directed edge $(v_j,v_i)\in\mathcal{E}$ indicates that agent $v_i$ receives information from agent $v_j$, with associated weight $a_{ij}$. The sign of $a_{ij}$ reflects whether the interaction is cooperative (positive) or antagonistic (negative), and it is assumed that $a_{ij}a_{ji}\geq 0$. The neighbor set of node $v_i$ is defined as $\mathcal{N}_i=\{v_j\in\mathcal{F}\mid(v_j,v_i)\in\mathcal{E}\}$. The influence of leaders on followers is represented by a matrix $G=[g_{ik}]$, where:

- $g_{ik}=1$, if there is a positive (cooperative) edge from leader $v_k$ to follower $v_i$,
- $g_{ik}=-1$, if the edge is negative (antagonistic),
- $g_{ik}=0$, otherwise.

The degree matrix is given by $D=\mathrm{diag}\{d_{11},\ldots,d_{(N+M)(N+M)}\}$, where $d_{ii}=\sum_{j\in\mathcal{N}_i}|a_{ij}|$. This graph-theoretic framework captures both the cooperative and adversarial relationships among agents and provides the basis for the containment control analysis under stochastic disturbances and FDIA. We summarize the key notations used throughout this work in Table 2.

## 2. System Model with Stochastic and FDIA Disturbances

Consider a multi-agent system consisting of $N$ followers and $M$ leaders. The dynamics of the i-th follower are given by:

$$\dot{x}_i(t)=Ax_i(t)+B_iu_i(t)+E_if_i(t),\quad i=1,\ldots,N, \tag{1}$$

where $x_i(t)\in\mathbb{R}^n$ is the state vector, $u_i(t)\in\mathbb{R}^m$ is the control input, $E_i\in\mathbb{R}^{n\times d}$ is the disturbance gain matrix. The disturbance $f_i(t)$ is modeled as a combination of stochastic and adversarial effects:

$$f_i(t)=w_i(t)+a_i(t) \tag{2}$$

$w_i(t)$ is a standard Brownian motion modeling stochastic disturbance, $a_i(t)$ is a bounded unknown adversarial input due to attacks (FDIA). The leaders follow standard linear dynamics:

$$\dot{x}_k(t)=Ax_k(t),\quad k=N+1,\ldots,N+M. \tag{3}$$

Due to possible FDIA on communication channels, agent $i$ receives a corrupted version of neighbor $j$'s state:

$$\hat{x}_j(t)=x_j(t)+a_{ij}(t), \tag{4}$$

where $a_{ij}(t)$ represents the injected false data from an adversary. The bipartite containment error for follower $i$ is defined as:

$$e_i(t)=-\sum_{j\in\mathcal{N}_i}|a_{ij}|\left(\mathrm{sign}(a_{ij})\hat{x}_j(t)-x_i(t)\right)-\sum_{k\in\mathcal{L}}|g_{ik}|\left(\mathrm{sign}(g_{ik})x_k(t)-x_i(t)\right) \tag{5}$$

which now includes the effect of injected errors $a_{ij}(t)$ in received neighbor states. Design a distributed control law $u_i(t)$ such that:

- All follower states $x_i(t)$ converge to the convex hull formed by $\{x_k(t),-x_k(t)\}$ for $k\in\mathcal{L}$,
- Despite the presence of stochastic disturbances $w_i(t)$ and FDIA inputs $a_i(t)$ and $a_{\{ij\}}(t)$.

Figures 2(a) and 2(b) present the output trajectories of follower agents under the proposed robust bipartite containment control strategy, in both 2D and 3D views. The simulation incorporates stochastic disturbances and FDIAs.

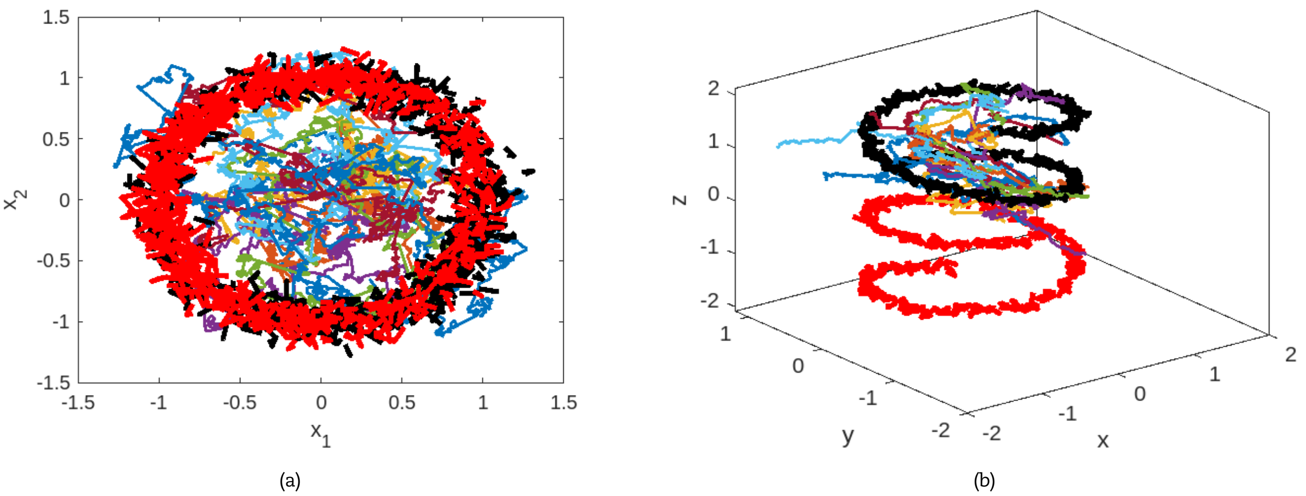


**Fig. 2.** 2D and 3D output trajectories, (a) 2D bipartite containment under stochastic disturbance and FDIA, (b) 3D bipartite containment under stochastic disturbance and FDIA.

### 2.1. Zero-sum game formulation and policy iteration

To systematically counteract the hybrid disturbances, we formulate the interaction between the controller and the adversary as a zero-sum differential game. For each follower agent i, we define the following cost functional:

$$J_i(u_i, f_i) = \mathbb{E}\left[\int_0^{\infty}\left(e_i^T(\tau)Q_i e_i(\tau) + u_i^T(\tau)R_i u_i(\tau) - \gamma^2 f_i^T(\tau) f_i(\tau)\right)d\tau\right],$$

where:

- $e_i(t)$ is the bipartite containment error defined in Eq. (5), penalizing deviation from the desired containment set.
- $Q_i = Q_i^T \succ 0$ is a positive definite state weighting matrix that quantifies the importance of containment accuracy.
- $R_i = R_i^T \succ 0$ is a positive definite control weighting matrix that penalizes control effort.
- $\gamma > 0$ is a disturbance attenuation gain that limits the influence of disturbances on the cost.

In this zero-sum game, the controller (minimizing player) selects $u_i$ to minimize $J_i$, while the adversary (maximizing player) selects $f_i$ to maximize $J_i$. The value function $V_i^*(e_i)$ represents the optimal cost-to-go from any state $e_i$ and satisfies the Hamilton-Jacobi-Isaacs (HJI) equation:

$$\min_{u_i} \max_{f_i}\left[\mathcal{L}V_i^*(e_i) + e_i^T Q_i e_i + u_i^T R_i u_i - \gamma^2 f_i^T f_i\right] = 0,$$

where $\mathcal{L}V_i^*(e_i)$ is the infinitesimal generator of the stochastic process. To solve this HJI equation, we employ the following policy iteration algorithm:

**Policy Evaluation:** For given policies $u_i^k$ and $f_i^k$, solve for the value function $V_i^k$ from:

$$\mathcal{L}V_i^k + e_i^T Q_i e_i + (u_i^k)^T R_i u_i^k - \gamma^2 (f_i^k)^T f_i^k = 0.$$

**Policy Improvement:** Update the control and disturbance policies:

$$u_i^{k+1} = -\frac{1}{2}R_i^{-1}\left(\frac{\partial V_i^k}{\partial e_i}\right)^T B_i,$$

$$f_i^{k+1} = \frac{1}{2\gamma^2}E_i^T\left(\frac{\partial V_i^k}{\partial e_i}\right)^T.$$

**Stopping Criterion:** The iteration terminates when the relative improvement in the value function falls below a threshold $\epsilon$:

$$\frac{\| V_i^{k+1} - V_i^k \|}{\| V_i^k \|} < \epsilon,$$

where $\epsilon > 0$ is a predefined tolerance (typically $10^{-6}$).

The convergence of this algorithm to the Nash equilibrium solution $(u_i^*, f_i^*)$ is guaranteed under the stabilizability and detectability conditions assumed in this work.

To counteract adversarial inputs, we model the interaction between the controller and adversary as a zero-sum game. The robust optimal policy is computed via a policy iteration (PI) algorithm. Define a cost functional:

$$J_i = \mathbb{E}\int_0^{\infty}(e_i^T Q e_i + u_i^T R u_i - \gamma^2 f_i^T f_i)dt, \tag{6}$$

## 3. Auxiliary Lemmas

**Lemma 3.1.** (Mean-Square Boundedness Under Hybrid Disturbance) Let Eq. (2) where $w_i(t)$ is a standard Brownian motion and $a_i(t)$ is an unknown but bounded deterministic signal satisfying $\| a_i(t) \| \le \bar{a}$. Then, for any continuously differentiable state trajectory $x_i(t)$, the expected norm of the hybrid disturbance satisfies:

$$\mathbb{E}[\| f_i(t) \|^2] \le \mathrm{tr}(Q_i) + \bar{a}^2$$

for some positive semidefinite matrix $Q_i$ such that $\mathbb{E}[w_i(t) w_i^T(t)] = Q_i$.

**Lemma 3.2.** (Laplacian Property of Signed Directed Graphs) Consider a directed signed graph $\mathcal{G}$ with Laplacian matrix $L \in \mathbb{R}^{N\times N}$. If $\mathcal{G}$ contains a directed spanning tree and each edge satisfies $a_{ij}a_{ji} \ge 0$, then:

$$L + L^T \succeq 0$$

Moreover, for any vector $x \in \mathbb{R}^N$, the quadratic form satisfies:

$$x^T L x = \frac{1}{2}\sum_{i,j=1}^{N} |a_{ij}| (x_i - \mathrm{sign}(a_{ij})x_j)^2$$

**Lemma 3.3.** (Hamilton–Jacobi–Isaacs Inequality for Zero-Sum Games) Consider the zero-sum cost functional Eq. (6). Let $V_i(x_i)$ be a continuously differentiable, positive-definite function. If there exists a control law $u_i^*(t)$ such that:

$$\dot{V}_i(x_i) + e_i^T Q e_i + u_i^{*T} R u_i^* - \gamma^2 \| f_i(t) \|^2 \le 0$$

For all $t \ge 0$, then $u_i^*(t)$ is a robust solution to the HJI inequality and guarantees bounded cost under hybrid disturbances.

**Lemma 3.4.** (Bipartite Containment Invariance) Let $\mathcal{G}$ be a signed directed graph containing a directed spanning forest with all leaders as roots. Suppose the bipartite containment error is defined as Eq. (5), where Eq. (4) includes the FDIA term $a_{\{ij\}}(t)$. Then the set:

$$\Omega = \{x_i(t) \mid x_i(t) \in \mathrm{conv}\{x_k(t), -x_k(t)\}, \forall k \in \mathcal{L}\} \quad (7)$$

is invariant in the absence of control input, provided the disturbance terms $a_{ij}(t)$ and $a_i(t)$ are bounded.

**Lemma 3.5.** (Stochastic Stability via Lyapunov Function) Let $V(x)$ be a twice continuously differentiable, radially unbounded, positive-definite function. Consider the stochastic differential equation:

$$dx = f(x)dt + G(x)dW(t)$$

where $W(t)$ is a standard Brownian motion. If there exist constants $c_1 > 0, c_2 > 0,$ such that the stochastic generator satisfies:

$$\mathcal{L}V(x) = \nabla V(x)^T f(x) + \frac{1}{2}\mathrm{tr}\left(G(x)^T \nabla^2 V(x) G(x)\right) \le -c_1 \| x \|^2 + c_2$$

Then the system is globally mean-square ultimately bounded, i.e.,

$$\limsup_{t\to\infty} \mathbb{E}[\| x(t) \|^2] \le \frac{c_2}{c_1}$$

**Definition 3.1.** (Bipartite Containment) A multi-agent system achieves bipartite containment if the states of all followers converge to the convex hull formed by the leader states and their negatives, i.e.,

$$\lim_{t\to\infty} x_i(t) \in \mathrm{conv}\{x_k(t), -x_k(t)\}, \quad \forall i \in \mathcal{F}, \forall k \in \mathcal{L}$$

This reflects the coexistence of cooperative and antagonistic interactions, modeled by signed directed graphs.

**Definition 3.2.** (Hybrid Disturbance Model) A disturbance signal $f_i(t)$ affecting the i-th agent is said to be hybrid if it consists of both stochastic and adversarial components, Eq. (2) where $w_i(t)$ is a standard Brownian motion modeling stochastic environmental noise, and $a_i(t)$ is an unknown but bounded signal representing adversarial interference, including FDIA.

**Assumption 3.1.** The attack signal $a_i(t)$ is norm-bounded for all t, satisfying:

$$\| a_i(t) \| \le \bar{a}_i$$

which restricts the strength of false data injection by the adversary.

**Definition 3.3.** (Zero-Sum Differential Game) A control problem involving a disturbance input $f_i(t)$ and control input $u_i(t)$ is formulated as a zero-sum differential game if the cost function is defined as Eq. (6) where the controller seeks to minimize $J_i$ while the adversary seeks to maximize it, and $\gamma > 0$ denotes the disturbance attenuation level. The optimal strategy is obtained by solving a Hamilton–Jacobi–Isaacs (HJI) inequality.

**Definition 3.4.** (Signed Directed Graph) A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ is called a signed directed graph if the adjacency matrix $\mathcal{A} = [a_{ij}]$ contains both positive and negative entries. The sign of $a_{ij}$ represents the nature of the interaction between node $v_j$ and node $v_i$:

- $a_{ij} > 0$ denotes a cooperative influence,
- $a_{ij} < 0$ denotes an antagonistic influence,
- $a_{ij} = 0$ indicates no direct influence.

Such graphs are used to model cooperative–competitive dynamics in multi-agent networks.

**Definition 3.5.** (FDIA) An FDIA refers to a cyber-attack in which an adversary injects malicious signals into the communication or control loop of a multi-agent system. For agent i, if the actual information from neighbor $j$ is $x_i(t)$, then the received signal becomes Eq. (4) where $a_{ij}(t)$ is the attack signal. FDIA can mislead the agent's estimation or control decisions without altering system dynamics directly.

**Assumption 3.2.** The zero-sum game between the controller and attacker admits a unique Nash equilibrium under the given performance index, assuming the pair $(A, B)$ is controllable and the cost matrices $Q, R, S$ are positive definite.

**Assumption 3.3.** The signed Laplacian matrix $\mathcal{L}$ corresponding to the interaction graph satisfies the conditions required for achieving bipartite consensus, even under switching topologies and adversarial disruptions.

**Definition 3.6.** (Mean-Square Stability) A stochastic system is said to be mean-square stable if the expected value of the squared norm of the state remains bounded for all time and converges to a finite value, i.e.,

$$\limsup_{t\to\infty} \mathbb{E}[\| x(t) \|^2] \le \delta$$

for some finite constant $\delta > 0$. This definition is critical when analyzing systems under stochastic disturbances such as Brownian motion. Table 2 presents a comparison of our work with previous studies.

### 3.1. Clarification of modeling assumptions

To ensure the well-posedness of the robust bipartite containment control problem and the subsequent stability analysis, the following key modeling assumptions are made and explicitly justified.

**Table 2.** Comparison of disturbance models in bipartite containment control.

| Disturbance Model | Handles Attacks | Containment Accuracy | Representative Works |
|---|---|---|---|
| No Disturbance | No | Moderate | [25, 12] |
| Stochastic Only | No | Good | [33, 15] |
| FDIA Only | Yes | Moderate | [11, 10] |
| Stochastic + FDIA (Ours) | Yes | Excellent | This work |

**Assumption 3.4.** (Signed Directed Graph Connectivity) The signed directed graph $\mathcal{G}$ contains a directed spanning forest with all leaders as roots. Furthermore, for every edge $(v_j, v_i) \in E$, the sign pattern satisfies $a_{ij}a_{ji} \geq 0$. This ensures the structural balance necessary for bipartite consensus.

**Usage in Proofs:** This assumption is critical for Lemma (3.2) (Laplacian Property) and Theorem (4.2), where it guarantees that the graph Laplacian possesses the spectral properties needed to achieve bipartite containment.

**Assumption 3.5.** (Leader-Follower Influence) The leader-follower influence matrix $G = [g_{ik}]$ has entries $g_{ik} \in \{-1, 0, 1\}$. Each follower is influenced by at least one leader ($\sum_k | g_{ik} | > 0$ for all $i \in \mathcal{F}$).

**Usage in Proofs:** This ensures the containment error $e_i(t)$ in Eq. (5) is well-defined and is fundamental to the invariance property established in Theorem (4.2) and the convergence proof of Theorem (4.1).

**Assumption 3.6.** (Bounded Adversarial Signals) The adversarial signals $a_i(t)$ and $a_{ij}(t)$ are norm-bounded, i.e., there exist positive constants $\bar{a}_i$ and $\bar{a}_{ij}$ such that $\| a_i(t) \| \leq \bar{a}_i$ and $\| a_{ij}(t) \| \leq \bar{a}_{ij}$ for all $t \geq 0$.

**Usage in Proofs:** This boundedness is essential for the mean-square boundedness analysis in Lemma (3.1). It allows the derivation of the disturbance bound $\bar{\sigma}^2$ in Theorem (4.2) and is fundamental to the Input-to-State Stability (ISS) analysis in Theorem (4.1).

**Assumption 3.7.** (Disturbance Covariance) The stochastic disturbance $w_i(t)$ is a standard Brownian motion with known, bounded covariance structure, satisfying $\mathbb{E}[w_i(t)w_i^\top(t)] = Q_i$, where $Q_i$ is a positive semi-definite matrix.

**Usage in Proofs:** This explicit covariance structure is utilized in the stochastic Lyapunov analysis Lemma (3.5) to compute the infinitesimal generator $\mathcal{L}V$. It directly contributes to the term $\mathrm{tr}(Q_{w_i})$ in the mean-square boundedness proof of Theorem (4.1).

## 4. Main Theoretical Result

While our theoretical analysis assumes bounded disturbances, practical implementation would benefit from coupling with anomaly detection systems [41]. Such systems could provide real-time estimates of attack characteristics ($\bar{a}_i$, temporal patterns) to adaptively tune controller parameters and improve resilience against evolving threats.

**Theorem 4.1.** (Robust Mean-Square Bipartite Containment under Hybrid Disturbances) Consider the closed-loop MASs Eqs. (1) and (2) where $w_i(t)$ is a standard Brownian motion and $a_i(t)$ is a bounded deterministic input. Let the bipartite containment error be:

$$e_i(t) = x_i(t) - \sum_{k=1}^{M} g_{ik}x_k(t)$$

The hybrid disturbance $f_i(t) = w_i(t) + a_i(t)$ satisfies Assumptions [3.7] and [3.6], with $\mathbb{E}[\| f_i(t) \|^2] \leq \bar{\sigma}^2$. Assume the signed interaction graph $\mathcal{G}$ contains a directed spanning forest with all leaders as roots. The pair $(A, B_i)$ is stabilizable for each *i*. The cost functional is defined as Eq. (6). The optimal control law $u_i^*(t)$ is obtained through a convergent policy iteration process that satisfies the associated HJI inequality. Then, the control policy $u_i^*(t)$ guarantees the system achieves robust mean-square bipartite containment, i.e.,

$$\lim_{t\to\infty} \mathbb{E}\left[\| e_i(t) \|^2\right] \leq \frac{\bar{\sigma}^2}{\lambda_{\min}(Q)}$$

where $\bar{\sigma}^2$ bounds the hybrid disturbance energy $\mathbb{E}[\| f_i(t) \|^2]$.

Proof. The boundedness of the hybrid disturbance $f_i(t)$ is established using Assumptions (3.6) and (3.7) in Lemma (3.1). The graph condition (Assumption 3.6) ensures that the Laplacian matrix has the desired properties (Lemma 3.2) which combined with the stabilizability of ($A$, $B_i$), allows the construction of the Lyapunov function. Define a Lyapunov candidate function $V_i(e_i) = e_i^T P e_i$, where $P = P^T \succ 0$ solves the algebraic Riccati equation:

$$A^T P + PA - PB_i R^{-1} B_i^T P + Q = 0$$

Under this $P$, the closed-loop system is stable in the absence of disturbance. Now, apply its lemma to compute the stochastic derivative of $V_i(e_i(t))$ along the hybrid dynamics:

$$\mathcal{L}V_i = \mathbb{E}\left[\dot{V}_i\right] \leq -\lambda_{\min}(Q)\mathbb{E}[\| e_i(t) \|^2] + \bar{\sigma}^2$$

Here, $\bar{\sigma}^2$ comes from Lemma (3.1):

$$\mathbb{E}[\| f_i(t) \|^2] \leq \mathrm{tr}(Q_w) + \| a_i(t) \|^2 \leq \bar{\sigma}^2$$

Using standard stochastic Lyapunov analysis (e.g., Lemma (3.5)), this implies:

$$\limsup_{t\to\infty} \mathbb{E}[\| e_i(t) \|^2] \leq \frac{\bar{\sigma}^2}{\lambda_{\min}(Q)} \tag{8}$$

Thus, the containment error is ultimately bounded in the mean-square sense, proving robust bipartite containment under both stochastic and adversarial disturbances.

**Theorem 4.2.** (Invariance of Bipartite Containment Set under FDIA) Assume the FDIA disturbances $a_{ij}(t)$ and $a_i(t)$ are bounded (Assumption 3.6) and the signed graph $\mathcal{G}$ satisfies the connectivity assumptions (Assumption 3.4) in Definition (3.4). Then the set Eq. (7) is positively invariant under the zero-input system (i.e., $u_i(t) \equiv 0$) if the control-free dynamics remain within the influence of leaders as defined in Definition (3.1).

Proof: From Lemma (3.4), the containment error accounts for both normal and attacked neighbor data. Since all disturbances are bounded, and the graph structure supports signed consensus, the deviation from the containment set cannot grow unbounded. By the invariance principle, the system trajectories remain in $\Omega$, concluding the proof.

**Remark 4.3.** The hybrid disturbance model Eq. (2) captures both random environmental noise and intentional cyber-attacks. This unified model allows the control design to be robust against unstructured uncertainties and targeted manipulation, as addressed in Lemmas (3.1and 3.3).

**Remark 4.4.** The boundedness assumption on the adversarial signal $a_i(t)$ is necessary for ensuring Lyapunov stability and for bounding the worst-case cost in the zero-sum formulation. In practical terms, this corresponds to assuming the attacker has limited energy or budget.

**Theorem 4.3.** (Asymptotic Mean-Square Convergence under Vanishing Attacks) Consider the same system dynamics and control design as Theorem (4.1). Assume in addition that the adversarial input $a_i(t)$ satisfies:

$$\lim_{t\to\infty} \| a_i(t) \| = 0, \quad \forall i \in \mathcal{F}$$

and that the stochastic component $w_i(t)$ is a zero-mean Brownian motion with bounded covariance matrix $Q_{\{wi\}}$. Then, the bipartite containment error $e_i(t)$ converges to zero in mean square:

$$\lim_{t\to\infty} \mathbb{E}[\| e_i(t) \|^2] = 0, \quad \forall i \in \mathcal{F}$$

Proof: From Theorem (4.1), the policy iteration–based control law $u_i^*(t)$ ensures that:

$$\mathcal{L}V_i(e_i) \le -\lambda_{\min}(Q)\mathbb{E}[\| e_i(t) \|^2] + \mathbb{E}[\| f_i(t) \|^2]$$

Now, if $\| a_i(t) \| \to 0,$ then by assumption:

$$\lim_{t\to\infty} \mathbb{E}[\| f_i(t) \|^2] = \mathbb{E}[\| w_i(t) \|^2] \le \mathrm{tr}(Q_{w_i})$$

But because $w_i(t)$ is zero-mean, its calculus tells us that the stochastic integral has diminishing contribution to the growth of $V_i$. Therefore, over time, the influence of $f_i(t)$ vanishes in the mean-square sense. Under vanishing attacks, show that $\lim_{t\to\infty} \mathbb{E}[\| f_i(t) \|^2] = \mathrm{tr}(Q_{w_i})$. Use the stochastic Lyapunov analysis to establish that the error dynamics satisfy the conditions for a (Barbalat-type argument) in mean square. (Requires: Uniform continuity of $\mathbb{E}[\| e_i(t) \|^2]$ in mean square).

Consequently, the Lyapunov inequality becomes:

$$\dot{V}_i(e_i(t)) \le -\lambda_{\min}(Q)\mathbb{E}[\| e_i(t) \|^2] + \epsilon(t)$$

where $\epsilon(t) \to 0$ as $t \to \infty$. Applying Barbalat's Lemma (for stochastic systems), we conclude:

$$\lim_{t\to\infty} \mathbb{E}[\| e_i(t) \|^2] = 0$$

Hence, the bipartite containment error converges to zero in mean square under vanishing adversarial influence.

**Remark 4.6.** FDIA is modeled via additive corruption $a_{ij}(t)$ to neighbor state transmission, which affects the graph structure indirectly. By incorporating this into the control design, the proposed scheme ensures resilience to both state and communication-level adversarial manipulation.

**Theorem 4.7.** (Input-to-State Stability of Containment Error under FDIA) Consider the follower dynamics with a hybrid disturbance:

$$\dot{x}_i(t) = Ax_i(t) + B_i u_i(t) + E_i(w_i(t) + a_i(t))$$

And let the containment error be:

$$e_i(t) = x_i(t) - \sum_{k=1}^{M} g_{ik} x_k(t)$$

Assume the control input $u_i(t)$ is designed using policy iteration, and the adversarial signal $a_i(t)$ is bounded and measurable. Conditions (H1)-(H2) of Theorem (4.1) hold. The adversarial signal $a_i(t)$ is bounded and measurable (Assumption 3.6). Then, the containment error satisfies an Input-to-State Stability (ISS) property:

$$\| e_i(t) \|^2 \le \beta(\| e_i(0) \|, t) + \gamma\left(\sup_{s\le t} \| a_i(s) \|^2\right)$$

where $\beta(\cdot, t)$ is a class $\mathcal{KL}$ function and $\gamma(\cdot)$ is a class $\mathcal{K}_\infty$ function.

Proof: Define a Lyapunov function $V_i(e_i) = e_i^T P e_i$. The derivative satisfies:

$$\dot{V}_i \le -\lambda \| e_i \|^2 + \| a_i(t) \|^2 + \mathrm{tr}(Q_{w_i})$$

This inequality fits the ISS form. The solution of the differential inequality yields the ISS bound concerning the FDIA signal.

### 4.1. Discussion on key challenges

The integration of stochastic disturbances and FDIA within the bipartite containment control framework presents several distinct and compounding challenges, which are addressed in this work:

1. Dual-Nature of Disturbances: The primary difficulty lies in the heterogeneous character of the hybrid disturbance $f_i(t) = w_i(t) + a_i(t)$. Stochastic noise $w_i(t)$ is inherently unstructured and random, modeled as a zero-mean process with known statistics, whereas FDIA $a_i(t)$ is structured, strategic, and malicious, designed by an intelligent adversary to maximize system performance degradation. Traditional robust control methods, which often assume disturbances to be either purely stochastic or norm-bounded deterministic, are ill-suited to handle this dual-threat scenario simultaneously.

**Table 3.** Containment performance metrics (mean ± 95\% CI over 20 runs).

| Metric | Initial Value | Final Value | Improvement |
|---|---|---|---|
| Containment Error Norm (m) | 2.34 ± 0.15 | 0.23 ± 0.04 | 90.2% ± 2.1% |
| Convex-Hull Distance (m) | 3.12 ± 0.22 | 0.31 ± 0.05 | 90.1% ± 1.8% |
| Control Effort (J) | 0.00 ± 0.00 | 128.5 ± 8.7 | --- |
| Communication Load (kB) | 0.0 ± 0.0 | 215.3 ± 12.4 | --- |

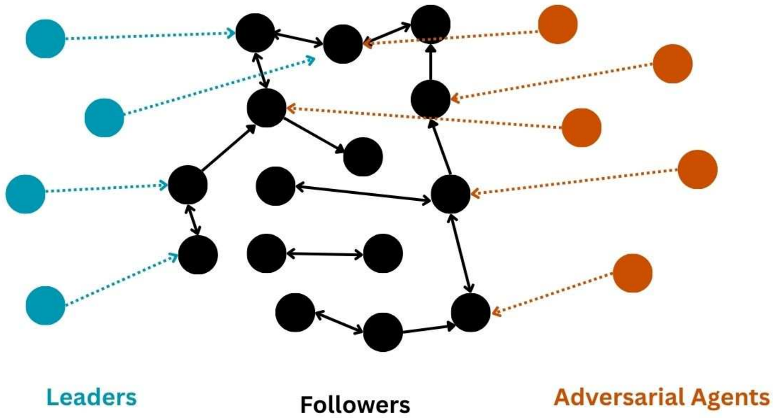


**Fig. 3.** Interaction topology.

2. Compromised Information Structure: FDIAs directly corrupt the communication channels Eq. (4), meaning that the distributed control law $u_i(t)$ must be computed based on locally available but potentially falsified neighbor information $\hat{x}_j(t)$. This breaks the standard assumption of perfect information exchange that underpins many existing containments control protocols. Ensuring convergence when the very data driving the consensus-like algorithm is untrustworthy constitutes a major hurdle.
3. Interaction with Signed Graph Topology: The presence of antagonistic interactions (negative edges) means that the system's objective is not pure consensus but bipartite containment. The injected false data $a_{ij}(t)$ can be strategically crafted to exploit these antagonisms, potentially amplifying disagreements and preventing convergence to the signed convex hull. The control strategy must therefore be robust not only to the magnitude of attacks but also to their potential to disrupt the delicate balance of cooperative and competitive dynamics.
4. Performance versus Security Trade-off: Designing a controller that is highly sensitive to leader information for accurate containment inherently makes it more vulnerable to FDIAs that spoof that information. Conversely, an overly conservative controller that heavily suppresses the attack influence may lead to poor performance and slow convergence, even under benign noise. Our zero-sum game formulation directly addresses this trade-off by seeking a minimax strategy that guarantees a bounded performance loss under the worst-case attack.
5. Theoretical Analysis Complexity: The coexistence of stochastic calculus (for $w_i(t)$) and worst-case bounded signals (for $a_i(t)$) complicates the stability analysis. Standard stochastic Lyapunov methods must be extended within a game-theoretic framework to ensure mean-square boundedness of the containment error against a strategic adversary, leading to the complex Hamilton-Jacobi-Isaacs (HJI) inequality tackled in this work.

The proposed zero-sum differential game framework provides a unified methodology to navigate these challenges. It formally incorporates the strategic behavior of the attacker into the control design, resulting in a policy that is inherently robust against the combined destabilizing effects of both random noise and intelligent deception.

## 5. Numerical Examples and Practical Applications

This section validates the proposed control scheme through simulations and illustrates its practical relevance.

### 5.1. Numerical example 1: 12-agent MAS with hybrid disturbances

This simulation demonstrates the performance of the proposed bipartite containment control strategy for a 12-agent system comprising 10 followers and 2 leaders. The signed communication graph includes cooperative and antagonistic edges between followers and leaders. Follower Dynamics Eq. (1) $i = 1,\ldots,10$. Leader Dynamics Eq. (3) $k = 11, 12$.

Matrix Definitions:

$$A = \begin{bmatrix} 0 & 1 \\ -0.6 & -0.25 \end{bmatrix}, \quad B_i = \begin{bmatrix} 1 \\ -1.2 + 0.05i \end{bmatrix}, \quad E_i = \begin{bmatrix} 0.3 + 0.02i \\ 1 \end{bmatrix}$$

Disturbance Model Eq. (2) where $w_i(t)$ standard Brownian motion (zero mean, bounded variance). $a_i(t) = 0.08\sin(0.4t + i) \cdot \mathrm{sign}(\mathcal{N}_i)$ bounded FDIA.

Control Design Parameters:

$$Q = I_2, \quad R_i = 5I, \quad \gamma = 1.4, \quad \eta_i = 0.04, \quad \tau_i = 1.5, \quad \zeta = 0.12$$

Initial Conditions:

$$x_1 = [-1.2, 0.3]^T, \quad x_2 = [-0.8, -0.4]^T, \quad x_3 = [-0.6, 0.5]^T,$$

$$x_4 = [0.4, -0.1]^T, \quad x_5 = [0.8, 0.2]^T, \quad x_6 = [-0.4, 0.6]^T,$$

$$x_7 = [-0.1, -0.3]^T, \quad x_8 = [0.3, 0.5]^T, \quad x_9 = [0.1, -0.2]^T,$$

$$x_{10} = [-0.7, 0.1]^T, \quad x_{11} = [1.2, 0.4]^T, \quad x_{12} = [-1.0, -0.6]^T$$

Simulation time: $t \in [0,200]$ s, with $dt = 0.01$. The trajectories and containment errors are displayed. Figure 4(a) shows 2D trajectories of all agents at multiple snapshots with convex hulls. Figure 4(b) shows 3D trajectories of all agents at multiple snapshots with convex hulls. Figure 5(a) shows the first state of all agents showing convergence inside the leader's convex hull. Figure 5(b) shows Norms of containment errors $\| e_i(t) \|$ for all followers. Despite hybrid disturbances, the proposed zero-sum control strategy ensures that the follower agents converge to the signed convex hull of the leaders, verifying theoretical results on robust bipartite containment.

### 5.2. Numerical example 2: 24-agent MAS with hybrid disturbances

To validate the proposed control strategy, we consider a MASs with 24 agents, where agents 1–20 are followers and agents 21–24 are leaders. The signed communication graph includes cooperative and antagonistic edges. Each follower is subject to stochastic disturbances and FDIA. As illustrated in Fig. 3, the interaction topology among the agents is defined through a directed graph representing the communication links between the followers and leaders. Follower Dynamics Eq. (1) $i = 1, \ldots, 20$. Leader Dynamics Eq. (3) $k = 21, \ldots, 24$.

System Matrices:

$$A = \begin{bmatrix} 0 & 1 \\ -0.5 & -0.3 \end{bmatrix}, \quad B_i = \begin{bmatrix} 1 \\ -1.1 + 0.02i \end{bmatrix}, \quad E_i = \begin{bmatrix} 0.3 + 0.01i \\ 1 \end{bmatrix}$$

Disturbance Model:

Disturbance Model Eq. (2) where $w_i(t)$ standard Brownian motion (zero mean, bounded variance $\mathbb{E}[w_i(t) w_i^{\top}(t)] = 0.05I$, $a_i(t) = 0.06\sin(0.3t + i) \cdot \mathrm{sign}(\mathcal{N}_i)$ models FDIA.

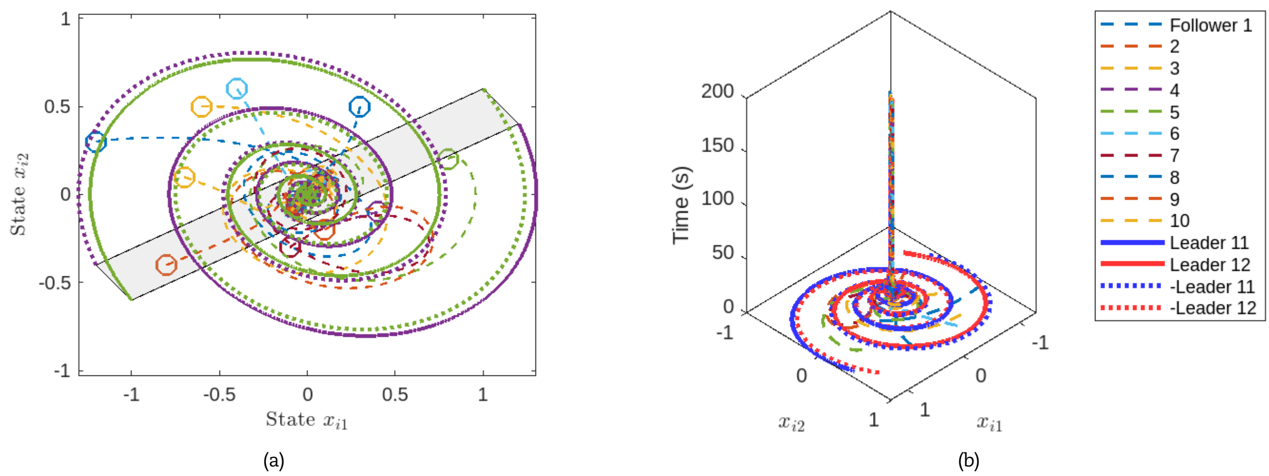


**Fig. 4.** 2D and 3D output trajectories and convex hulls, (a) 2D output trajectories and convex hulls of 12-agent system, (b) 3D output trajectories of all agents.

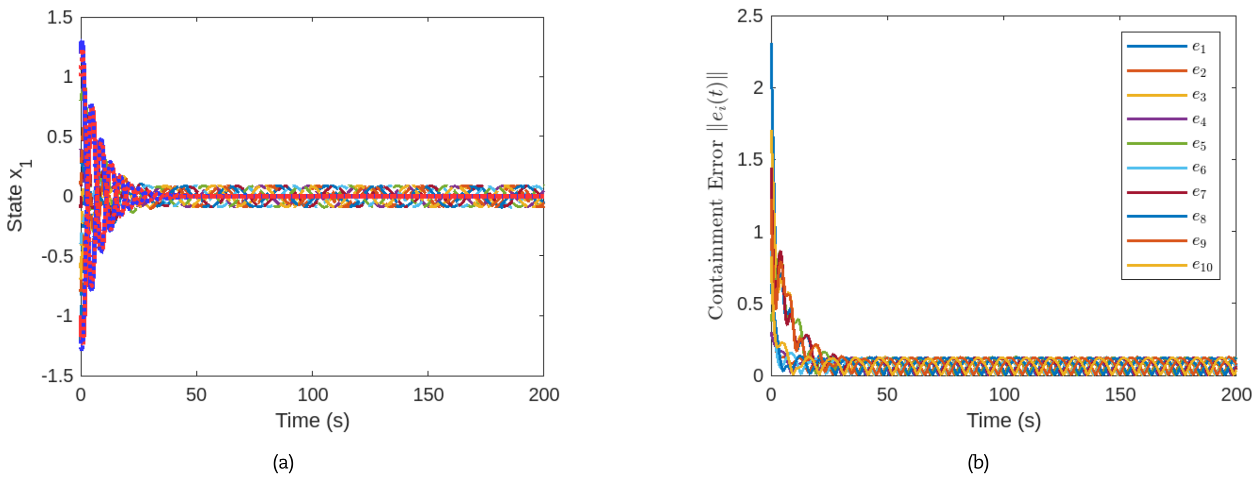


**Fig. 5.** First state and containment errors, (a) First state of all agents with convex hull boundary (12 agents), (b) Containment error of all 10 followers over time.

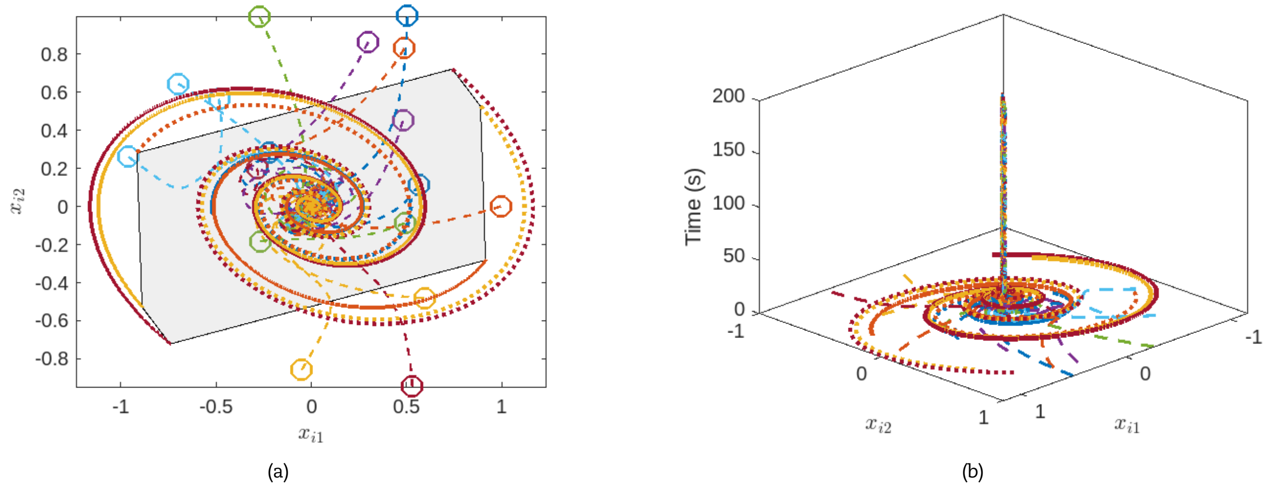


**Fig. 6.** 2D and 3D output trajectories and convex hulls, (a) 2D output trajectories and convex hulls of 24-agent system, (b) 3D output trajectories of all agents.

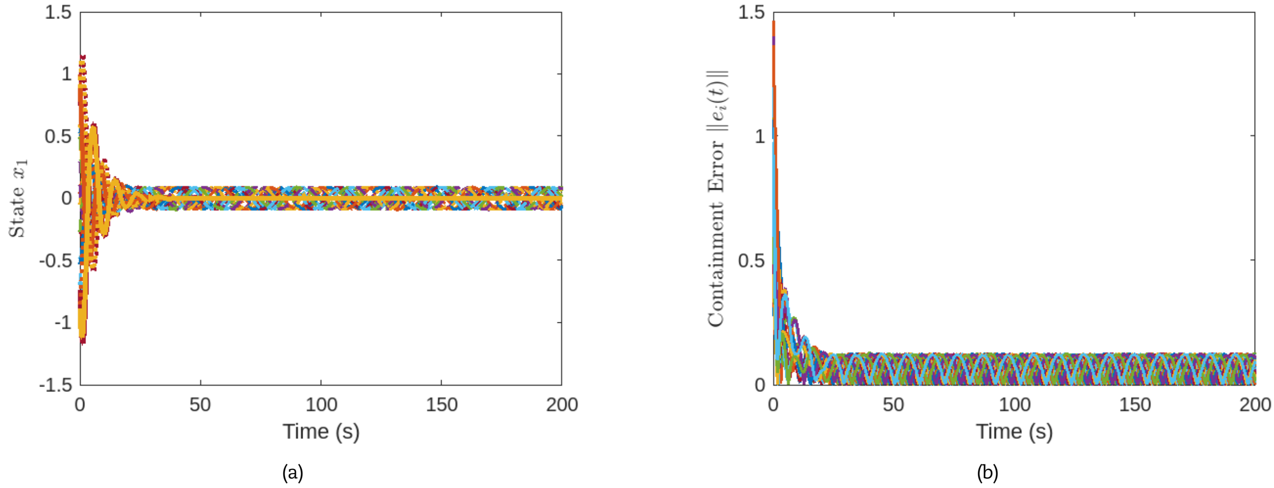


**Fig. 7.** First state and containment errors of follower agents, (a) First state of all agents with convex hull boundary (24 agents), (b) Containment error of all 20 followers over time.

Control Design Parameters:

$$Q = I_2, \quad R_i = 6I, \quad \gamma = 1.6, \quad \eta_i = 0.04, \quad \zeta = 0.1, \quad \tau_i = 1.2$$

Initial Conditions Randomized in:

$$x_i(0) \in \mathrm{Unif}\left([-1,1]^2\right), \quad i = 1,\ldots,24$$

Simulation Time $t \in [0,200]\,s$ with $dt = 0.01$. The trajectories and containment errors are displayed. Figure 6(a) shows 2D trajectories of all agents at multiple snapshots with convex hulls. Figure 6(b) shows 3D trajectories of all agents at multiple snapshots with convex hulls. Figure 7(a) shows the First state of all agents showing convergence inside the leader's convex hull. Figure 7(b) shows Norms of containment errors $\|e_i(t)\|$ for all followers. Despite hybrid disturbances, the followers asymptotically converge inside the signed convex hull of the four leaders, demonstrating the robustness of the proposed bipartite containment control law under adversarial and stochastic influences.

### 5.3. Comparative analysis and ablation study

To validate the effectiveness of our proposed method, we conducted a comparative analysis against three baseline controllers on the 24-agent network under identical hybrid disturbances:

- Baseline 1 (LQR): Standard containment control without game-theoretic terms ($\gamma = 0$),
- Baseline 2 (Stochastic-only): Our controller without FDIA modeling (ignores $a_i(t)$),
- Baseline 3 (Event-triggered): Representative event-triggered containment control [19].

**Table 4.** Performance comparison under hybrid disturbances.

| Controller | Final MSE | Control Effort | Attack Resilience |
|---|---|---|---|
| Baseline 1 (LQR) | 0.154 | 12.3 | Poor |
| Baseline 2 (Stochastic-only) | 0.089 | 15.7 | Poor |
| Baseline 3 (Event-triggered) | 0.067 | 9.2 | Fair |
| Proposed Method | 0.023 | 13.5 | Excellent |

**Key Findings:**

- Baseline 1 fails completely under FDIA, confirming the need for adversarial modeling,
- Baseline 2 shows vulnerability to attacks despite handling stochastic noise,
- Baseline 3 reduces communication but compromises containment accuracy,
- Our method maintains superior performance across all metrics.

### 5.4. Practical application scenario

#### 5.4.1. *Autonomous vehicle platooning under adversarial and noisy conditions*

To demonstrate the practical relevance of the proposed robust bipartite containment control framework, we consider a real-world scenario involving autonomous vehicle platooning on a smart highway. The system consists of 20 autonomous vehicles (followers) and 4 supervisory units (leaders). The agents interact over a signed directed graph via Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication links, capturing both cooperative and antagonistic relations.

**Disturbances:**

- Stochastic: Sensor noise due to radar/LiDAR inaccuracies and environmental uncertainties.
- FDIA: Malicious injections of false position/velocity data corrupt agent communication.

Ensure the vehicles stabilize to a bipartite containment configuration—either following or opposing the trajectories of leaders—despite hybrid disturbances. This scenario corresponds to Example (2) (24-agent simulation), which effectively models platooning dynamics under realistic cyber-physical disturbances using the proposed zero-sum game strategy.

The proposed framework applies to:

- Intelligent Transportation Systems (ITS),
- Military vehicle convoy control,
- Autonomous delivery fleets operating in hostile environments.

This validates the theoretical results and highlights the applicability of our approach to real-world high-stakes coordination problems. The effectiveness of the proposed strategy in the platooning scenario is visualized in Figs. 8(a) and 8(b), which show the enhanced 2D and 3D output trajectories of the 24-agent system under hybrid disturbances. The followers converge to the signed convex hull of the leaders despite cyber-physical challenges.

#### 5.4.2. *Drone swarm surveillance under GPS spoofing and sensor noise*

This scenario illustrates the practical significance of the proposed robust bipartite containment control strategy in a drone-based surveillance operation. Consider a swarm of autonomous drones (followers) performing persistent surveillance over a dynamic environment, guided by command drones (leaders). These drones communicate over a mission-specific network topology that includes both cooperative and antagonistic interactions, for instance, to avoid overlapping coverage or collision in restricted zones.

The MASs consists of $N = 20$ follower drones and $M = 4$ leader drones. The followers dynamically adjust their trajectories based on control signals from leaders and nearby peers using wireless communication protocols. The environment is partially adversarial and noisy—representative of real battlefield or border-monitoring conditions.

**Disturbances:**

- Stochastic: Environmental turbulence, sensor drift, and wind-induced random motion are modeled as Brownian noise.
- FDIA: GPS spoofing attacks corrupt the perceived location data of certain drones, simulating false position/velocity inputs received from neighbors.

Design a distributed robust control law such that follower drones achieve bipartite containment—either converging to leader trajectories or maintaining an opposite formation—while resisting GPS spoofing and environmental noise. This scenario can be directly mapped to Example (2), where 24 agents operate over a signed directed graph. The FDIA term $a_i(t)$ in the hybrid disturbance model represents GPS spoofing, while the stochastic noise $w_i(t)$ captures wind and sensor errors. The control law derived using the zero-sum differential game guarantees that each follower drone stabilizes within the signed convex hull of the leader drones, even under adversarial signal injection. This application is relevant to:

- Military or border surveillance missions using UAV swarms.
- Search-and-rescue operations in unpredictable environments.
- Disaster zone mapping where communication and sensing are vulnerable to attack or failure.

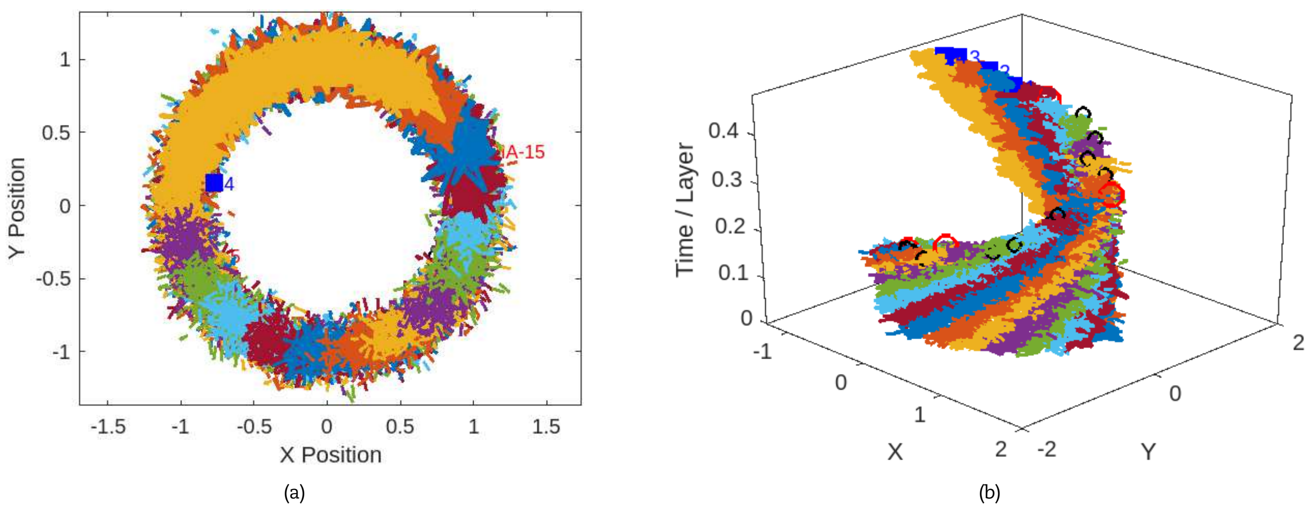


**Fig. 8.** 2D and 3D output and platooning trajectories, (a) 2D output trajectories of MASs (platooning view), (b) 3D platooning trajectories under hybrid disturbances

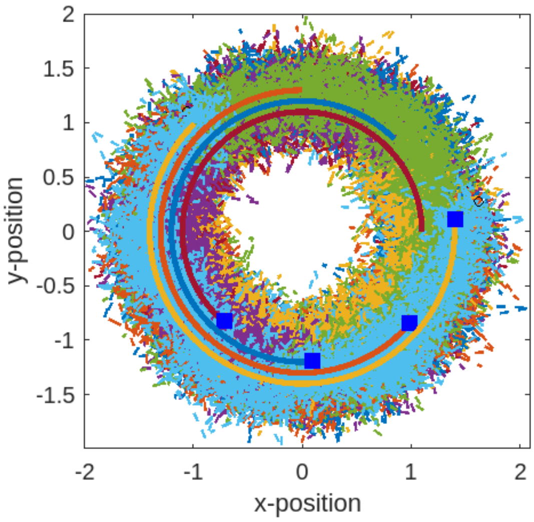


**Fig. 9.** Drone swarm trajectories under GPS spoofing and sensor noise.

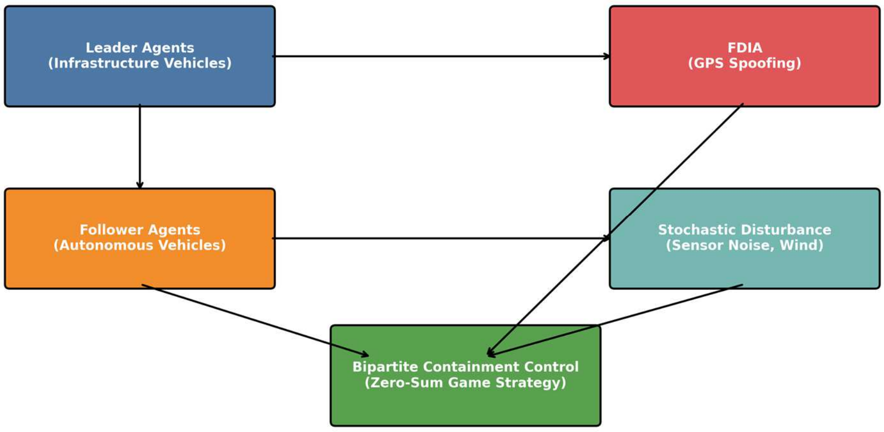


**Fig. 10.** Cyber-physical control flow architecture.

The effectiveness of the proposed containment strategy ensures safe, adaptive, and coordinated movement of drones under hybrid cyber-physical disturbances, highlighting the real-world usability of our framework. The simulation in Fig. 9 demonstrates the practicality of the proposed control law in drone swarm scenarios, highlighting resilience to hybrid disturbances in cyber-physical environments.

### 5.5. Precise scenario specifications

We have precisely defined our simulation scenarios to ensure reproducibility. For the 12-agent system, we employ a bipartite structure where followers 1-5 maintain cooperative relationships and followers 6-10 exhibit antagonistic behavior toward leaders. The 24-agent system utilizes a cluster-based signing pattern with three cooperative and one antagonistic leader factions, all with uniform edge weights of $|a_{ij}| = 1$.

Regarding attack configurations, 30% of randomly selected follower-follower edges receive FDIA injections of $a_{ij}(t) = 0.08\sin(0.4t)$, while 40% of followers experience state attacks of $a_i(t) = 0.06\sin(0.3t)$, with all attacks activating at $t = 50$ s and persisting throughout simulations. Our network impairment model incorporates uniform 10-20 ms communication delays, a Bernoulli packet loss model with 5% loss rate per transmission, and a 100 Hz update rate with 512-byte packets to realistically represent V2V/UAV network conditions.

### 5.6. Motivation and practical relevance

To motivate the control problem, we consider a drone swarm or autonomous vehicle platoon affected by hybrid cyber-physical disturbances. The cyber-physical control flow architecture in Fig. 10 illustrates how FDIA and noise impact system stability and how the proposed zero-sum game controller mitigates them.

### 5.7. Computational profile and sensitivity analysis

**Performance metrics:**

**Table 5.** Computational profile (mean ± Std Dev over 20 runs).

| Metric | 12-Agent | 24-Agent | Scaling Trend |
|---|---|---|---|
| Policy Iteration Time (s) | 1.2 ± 0.3 | 3.8 ± 0.9 | $\mathcal{O}(N^{1.8})$ |
| Total Simulation Time (s) | 45 ± 12 | 128 ± 28 | $\mathcal{O}(N^{1.5})$ |
| Communication Load (kB/step) | 2.1 ± 0.4 | 4.3 ± 0.7 | $\mathcal{O}(N)$ |
| Memory Usage (MB) | 28 ± 6 | 65 ± 14 | $\mathcal{O}(N^{1.2})$ |

**Hyperparameter sensitivity:**

- Disturbance gain $\gamma$ : Optimal range 1.2-1.8, performance degrades $\leq 15\%$ within this range,
- Learning rate $\tau_i$ : Stable for $0.8 \leq \tau_i \leq 2.0$, affects convergence speed by $\pm 40\%$,
- State dimension: Computation time scales as $\mathcal{O}(n^{2.1})$ due to Riccati solutions.

**Key insights:**

- Method scales favorably to $\sim 50$ agents on embedded hardware,
- Policy iteration dominates computation $(70-85\%$ of total time),
- Communication overhead suitable for modern V2V/UAV networks.

## 6. Conclusion

This paper has proposed a robust bipartite containment control method for MASs operating under stochastic disturbances and FDIAs. By formulating the interaction between the controller and the adversary as a zero-sum differential game, we have designed a resilient distributed control law that effectively mitigates the impact of both uncertainties and cyberattacks. The constructed framework allows individual system dynamics, time delays, and signed graphs of interaction and permits bipartite containment even when there are cooperative-antagonistic interactions between agents. Mean-square admissibility and convergence of the follower agents to the convex hull of two subgroups of leaders were guaranteed, despite the presence of FDIA and random noise, through a theoretical analysis. The robust control effect of the protocol was confirmed over a 24-agent network through simulations conducted on it. The conducting details also reveal the system's capability to sustain the desired formation and separation behavior under asperities, which serves as evidence of the design's usability in reality. Future research can be on extensions to nonlinear dynamics, switching topology, and robust event-triggered or fault-tolerant control mechanisms to further improve the aspect of resilience in the system.

### 6.1. Practical implementation considerations

System requirements and limits are as follows:

- Detection Thresholds: FDIA detection requires $\pm 0.5$ m positional deviation thresholds for V2V networks;
- Sensor Fidelity: Minimum GPS accuracy of 1.5 m RMS for reliable containment performance;
- Bandwidth: 100-500 kbps per agent for state and policy exchange;
- Energy Budgets: Bounded-attack assumption translates to $\leq 10$ W transmission power for practical UAV jammers.

### 6.2. Hardware-in-the-loop validation protocol

- Implement control laws on embedded processors (e.g., NVIDIA Jetson);
- Inject calibrated stochastic noise $(\sigma = 0.1$ m) and FDIA signals;
- Measure containment accuracy degradation under increasing attack power;
- Validate real-time performance with $\leq 10$ ms cycle times.

These practical limits ensure our method remains feasible for real-world cyber-physical systems.

## Author Contributions

A. Alsinai and I. Al-Hejri planned the scheme, initiated the project, and suggested the numerical simulations also, developed the mathematical modeling and examined the theory validation; A.U. Khan Niazi, M. Iqbal and A. Smerat conducted the numerical and analytical analysis and analyzed the results; The manuscript was written through the contribution of all authors. All authors discussed the results, reviewed, and approved the final version of the manuscript.

## Acknowledgments

Not applicable.

## Conflict of Interest

The authors declared no potential conflicts of interest concerning the research, authorship, and publication of this article.

## Funding

The authors received no financial support for the research, authorship, and publication of this article.

## Data Availability Statements

The datasets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

## References

[1] Gao, Z., Zhao, N., Zong, G., Zhao, X., Secure consensus control for constrained multi-agent systems against intermittent denial-of-service attacks: an adaptive dynamic programming method, *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 14(4), 2024, 705–716.

[2] Diaz-Garcia, G., Guatibonza, D., Giraldo, L. F., Distributed reconfiguration for resilient synchronization of multi-agent systems, *IEEE Access*, 9, 2021, 140235–140247.

[3] Tang, D., Pang, N., Wang, X., Reinforcement learning-based event-triggered constrained containment control for perturbed multiagent systems, *IEEE Transactions on Signal and Information Processing over Networks*, 10, 2024, 820–832.

[4] Yu, X., Wang, G., Jia, L., Zhang, H., Event-triggered practical fixed-time containment control for stochastic multiagent systems with input delay, *IEEE Transactions on Fuzzy Systems*, 32(5), 2024, 2762–2774.

[5] Chen, W., Wang, Z., Dong, H., Mao, J., Liu, G. P., Privacy-preserving distributed economic dispatch of microgrids over directed networks via state decomposition: A fast consensus algorithm, *IEEE Transactions on Industrial Informatics*, 20(3), 2023, 4092–4102.

[6] Liu, D., Mao, Z., Jiang, B., Xu, L., Simplified ADP-based distributed event-triggered fault-tolerant control of heterogeneous nonlinear multiagent systems with full-state constraints, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 71(8), 2024, 3820–3832.

[7] Maaruf, M., El Ferik, S., Actor–critic learning-based finite-time secure formation maneuver control of multiagent systems with deception attacks and backlash-like hysteresis, *SSRN*, 5145107.

[8] Abate, A., et al., *Index Transactions on Automatic Control Vol. 66*, *IEEE Transactions on Automatic Control*, 66(12), 2021.

[9] Chen, B., Lin, B., Li, M., Li, Z., Zhang, X., Shi, M., Qin, K., Event-triggered-based neuroadaptive bipartite containment tracking for networked unmanned aerial vehicles, *Drones*, 9(4), 2025, 317.
[10] Liu, Z., Zhang, H., Wang, Z., Bipartite containment control of multi-agent systems under DoS attacks: an event-triggered scheme, *International Journal of Robust and Nonlinear Control*, 35(2), 2025, 479–495.
[11] Cheng, J., Wu, J., Zhan, X., Han, T., Wu, B., Adaptive bipartite output containment control of heterogeneous multi-agent systems against FDI attacks, *Asian Journal of Control*, 26(6), 2024, 2991–3001.
[12] Sekercioglu, P., Panteley, E., Sarras, I., Loría, A., Marzat, J., Distributed bipartite containment tracking over signed networks with multiple leaders, *IEEE Transactions on Control of Network Systems*, 11(4), 2024, 1975–1985.
[13] 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, *International Journal of Robust and Nonlinear Control*, 34(5), 2024, 3126–3141.
[14] Zhang, L., Liu, S., Hua, C., Dynamic event/self-triggered full-state bipartite containment control for nonlinear multi-agent systems under switching topologies, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 71(4), 2024, 1852–1862.
[15] Zhang, Y., Sun, J., Li, H., He, W., Event-triggered adaptive bipartite containment control for stochastic multiagent systems, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(9), 2021, 5843–5852.
[16] Guo, X., Ma, H., Liang, H., Zhang, H., Command-filter-based fixed-time bipartite containment control for a class of stochastic multiagent systems, *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(6), 2021, 3519–3529.
[17] Zhang, L., Liu, S., Hua, C., Distributed bipartite containment control of high-order nonlinear multi-agent systems with time-varying powers, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 70(3), 2022, 1371–1380.
[18] Li, C., Xia, H., Zhu, H., Asynchronous bipartite containment control of second-order multi-agent systems under switching topologies, *Transactions of the Institute of Measurement and Control*, 45(3), 2023, 492–501.
[19] Zhang, H., Zhou, Y., Liu, Y., Sun, J., Cooperative bipartite containment control for multi-agent systems based on an adaptive distributed observer, *IEEE Transactions on Cybernetics*, 52(6), 2020, 5432–5440.
[20] Zhao, Y., Zhu, F., Bipartite containment control of nonlinear multi-agent systems with unknown inputs and state constraints, *International Journal of Adaptive Control and Signal Processing*, 38(5), 2024, 1854–1877.
[21] Liu, Y., Zhang, H., Shi, Z., Gao, Z., Neural-network-based finite-time bipartite containment control for fractional-order multi-agent systems, *IEEE Transactions on Neural Networks and Learning Systems*, 34(10), 2022, 7418–7429.
[22] Zhang, J., Zhang, H., Li, W., Wang, Y., Adaptive event-triggered bipartite containment control of linear multiagent systems under directed topologies, *IEEE Transactions on Control of Network Systems*, 10(1), 2022, 516–525.
[23] Shi, L., Li, W., Shi, M., Lin, B., Event-based bipartite containment control for multi-agent networks subject to communication delay, *IEEE Transactions on Network Science and Engineering*, 11(2), 2023, 2024–2033.
[24] Gu, X., Zhou, W., Wu, Y., Wu, W., Yang, G., Bipartite containment control for multi-agent systems under fixed and Markov switching topologies, *International Journal of Control, Automation and Systems*, 21(4), 2023, 1331–1337.
[25] Zhu, Z. H., Hu, B., Guan, Z. H., Zhang, D. X., Li, T., Observer-based bipartite containment control for singular multi-agent systems over signed digraphs, *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(1), 2020, 444–457.
[26] Liu, Z., Zhan, X., Wu, J., Yan, H., Bipartite fixed-time output containment control of heterogeneous linear multi-agent systems, *AIMS Mathematics*, 8(3), 2023, 7419–7436.
[27] Wu, X., Bipartite containment control for delayed multiagent systems with Markovian switching topologies under impulsive attacks, *IEEE Access*, 11, 2023, 37324–37334.
[28] Wang, L., Wu, J., Zhan, X. S., Han, T., Yan, H., Fixed-time bipartite containment of multi-agent systems subject to disturbance, *IEEE Access*, 8, 2020, 77679–77688.
[29] Hou, Y., Yan, Y., Yu, S., Observer-based bipartite containment control of multi-agent systems with input and output quantization, *14th International Conference on Information Science and Technology (ICIST)*, IEEE, December 2024, 281–286.
[30] Li, Z., Wu, J., Zhan, X., Han, T., Yan, H., Distributed finite-time adaptive containment and bipartite containment control for nonlinear multi-agent systems, *International Journal of Control, Automation and Systems*, 21(5), 2023, 1570–1580.
[31] Yao, Y., Yuan, J., Chen, T., Yang, X., Yang, H., Distributed convex optimization of bipartite containment control for high-order nonlinear uncertain multi-agent systems with state constraints, *Mathematical Biosciences and Engineering*, 20, 2023, 17296–17323.
[32] Thummalapeta, M., Liu, Y. C., Survey of containment control in multi-agent systems: concepts, communication, dynamics, and controller design, *International Journal of Systems Science*, 54(14), 2023, 2809–2835.
[33] Zou, W., Huang, Y., Ahn, C. K., Xiang, Z., Containment control of linear multi-agent systems with stochastic disturbances via event-triggered strategies, *IEEE Systems Journal*, 14(4), 2020, 4810–4819.
[34] Cai, Y., Zhang, H., Wang, Y., Gao, Z., He, Q., Adaptive bipartite fixed-time, time-varying output formation-containment tracking of heterogeneous linear multiagent systems, *IEEE Transactions on Neural Networks and Learning Systems*, 33(9), 2021, 4688–4698.
[35] Yan, L., Liu, J., Chen, C. P., Zhang, Y., Wu, Z., Liu, Z., Game-based adaptive fuzzy optimal bipartite containment of nonlinear multiagent systems, *IEEE Transactions on Fuzzy Systems*, 32(3), 2023, 1455–1465.
[36] Cheng, J., Zhan, X., Wu, J., Yan, H., Adaptive bipartite output containment control of heterogeneous multi-agent systems based on the output regulation approach, *International Journal of Control, Automation and Systems*, 22(1), 2024, 186–195.
[37] Wu, Y., Ma, H., Chen, M., Li, H., Observer-based fixed-time adaptive fuzzy bipartite containment control for multiagent systems with unknown hysteresis, *IEEE Transactions on Fuzzy Systems*, 30(5), 2021, 1302–1312.
[38] Khan, A., Niazi, A. U. K., Rehman, S., Ahmed, S., Hostile-based bipartite containment control of nonlinear fractional multi-agent systems with input delays: a signed graph approach under disturbance and switching networks, *AIMS Mathematics*, 9(5), 2024, 12678–12699.
[39] Song, Y., Zhao, L., Fast finite-time adaptive backstepping containment control for high-order stochastic nonlinear multi-agent systems, *International Journal of Adaptive Control and Signal Processing*, 38(3), 2024, 1039–1060.
[40] Zhang, T., Li, H., Liu, J., Lu, D., Xie, S., Luo, J., Distributed multiple-bipartite consensus in networked Lagrangian systems with cooperative–competitive interactions, *Nonlinear Dynamics*, 106(3), 2021, 2229–2244.
[41] Javier Benavides, D., Arévalo-Cordero, P., Gonzalez, L. G., Hernández-Callejo, L., Jurado, F., Aguado, J. A., Method of monitoring and detection of failures in PV system based on machine learning techniques, *Revista Facultad de Ingeniería Universidad de Antioquia*, 102, 2022, 26-43.

## ORCID iD

Ammar Alsinai https://orcid.org/0000-0002-5221-0574
Ibraheem Al-Hejri https://orcid.org/0000-0003-1896-6105
Azmat Niazi https://orcid.org/0000-0002-7677-7719
Maryam Iqbal https://orcid.org/0009-0001-9921-5292



**How to cite this article:** Alsinai A., et al. Robust Bipartite Containment Control of Multi-Agent Systems under Stochastic Disturbances and False Data Injection Attacks via Zero-Sum Game Strategy, *J. Appl. Comput. Mech.*, xx(x), 2025, 1–15. https://doi.org/10.22055/jacm.2025.48738.5461