AIMS Mathematics, 10(6): 12956–12979.
DOI:10.3934/math.2025583
Received: 18 February 2025
Revised: 24 March 2025
Accepted: 17 April 2025
Published: 05 June 2025

https://www.aimspress.com/journal/Math

Research article

Robust neural network-driven control for multi-agent formation in the presence of Byzantine attacks and time delays

Asad Khan[1], Azmat Ullah Khan Niazi[2,*], Saadia Rehman[2], Saba Shaheen[2], Taoufik Saidani[3], Adnan Burhan Rajab[4,5], Muhammad Awais Javeed[6] and Yubin Zhong[7,*]

[1] Metaverse Research Institute, School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China

[2] Department of Mathematics and Statistics, The University of Lahore, Sargodha 40100, Pakistan

[3] Center for Scientific Research and Entrepreneurship, Northern Border University, Arar 73213, Saudi Arabia

[4] Department of Computer Engineering, College of Engineering, Knowledge University, Erbil 44001, Iraq

[5] Department of Computer Engineering, Al-Kitab University, Altun Kupri, Iraq

[6] School of Transportation, Southeast University, Nanjing 211189, Jiangsu, China

[7] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China

* **Correspondence:** Email: azmatullah.khan@math.uol.edu.pk, zhong_yb@gzhu.edu.cn.

Abstract: This paper presents an adaptive leader-follower formation control strategy for second-order nonlinear multi-agent systems with unknown dynamics. To handle system uncertainties, we used neural networks (NNs) to approximate and compensate for nonlinear effects. A key feature of our approach is its ability to deal with Byzantine attacks and time delays, which can disrupt coordination among agents. Unlike existing methods, our control strategy actively accounts for these challenges while ensuring stable formation tracking. Using Lyapunov stability theory, we proved that all system errors remain within a bounded range. Numerical simulations confirmed the effectiveness of our approach, showing that it successfully maintains formation control even in the presence of adversarial attacks and delays.

Keywords: Byzantine attack and time delay; multi-agent system; second-order nonlinear dynamics; formation control; adaptive neural networks; framework for leader-follower; Lyapunov stability
Mathematics Subject Classification: 34H05, 93C10, 93D09

1. Introduction

Formation control plays a vital role in the coordinated management of multi-agent systems (MAS), largely due to its extensive range of real-world applications [1–3]. MAS comprises multiple intelligent agents that interact to create sophisticated group behaviors by sharing information within their local networks. A key focus in formation control is developing robust control protocols that enable agents to reach and maintain specified geometric configurations necessary for accomplishing specific tasks.

Among the diverse approaches to formation control in MAS, the leader-follower strategy [4, 5] has emerged as a widely favored method. This approach is valued for its straightforward design, dependable performance, and ease of scalability, making it a popular and effective choice for researchers and practitioners. More recently, neighbor-based formation control [6, 7] methods have gained traction. These approaches enhance efficiency by requiring each agent to communicate with only a few nearby agents, reducing overall communication needs while maintaining effective coordination. In recent years, considerable research has focused on identifying and addressing the vulnerabilities of networked multi-agent systems in the presence of diverse cyber threats. These threats include denial-of-service (DoS) attacks [8], which aim to overwhelm the system to hinder normal operations, replay attacks, where attackers maliciously resend authentic messages, false-data injection (FDI) attacks [9], designed to introduce deceptive information camouflage attacks [10], which mask malicious actions as standard operational behavior and deception attacks [11]. Among these, Byzantine attacks, stand out as a particularly subtle and dangerous type of threat.

Malicious Byzantine attacks and operating time delays pose significant obstacles to MAS [12, 13], jeopardizing system dependability. Byzantine attacks are especially pernicious because they enable adversaries to introduce hidden flaws, using agent cooperation and trust to manipulate the system's operation. The challenge is made worse by time delays [14], a problem in real-world MAS because they prevent the timely sharing of information needed for coordinated control. Because second-order formation control [15,16] has to handle the velocity and position variables, it is particularly susceptible to delays and Byzantine errors.

Finite-time synchronization and energy optimization have been considered in multilayer fractional-order networks [17, 18] to obtain some practical conclusions about synchronization time and control energy consumption. The effect of stochastic disturbances such as Lévy noise and Markov switching in delayed MASs has been analyzed for achieving robust exponential synchronization [19]. These findings emphasize the significance of modeling uncertainties in MASs, which agrees with our approach to designing attack resilient formation control mechanisms.

Agents exhibit behavior governed by nonlinear functions, which are either well-defined or satisfy a Lipschitz-type condition to ensure specific smoothness characteristics. Recently, there has been significant progress in developing adaptive consensus methods for nonlinear systems, utilizing neural networks (NN) [20, 21] to harness their capacity for managing complex, uncertain interactions.

Neural networks have been efficiently used for robust control of nonlinear and multi-agent systems against uncertainties, disturbances, and time delays. Recent studies have considered neural network-based observers for output feedback control, hybrid models for precise parameter identification, and adaptive fuzzy controllers for the multi-disturbance environment. These enhancements show the neural networks in improving the system stability and performance [22–24].

These advanced approaches aim to help agents reach consensus or shared objectives, even amidst

the challenges of nonlinear dynamics.

Researchers have increasingly focused on ensuring that multi-agent formations remain stable despite adversarial challenges. [25] explored motion coordination in high-precision systems, while [26] studied navigation methods for constrained environments, which are useful for maintaining formation control under disruptions like Byzantine attacks. To improve reliability, [27] developed an adaptive filtering approach for cooperative localization, addressing issues such as sensor failures and unpredictable noise. While these studies offer important advancements, they do not fully address the challenge of maintaining stable formations when facing Byzantine attacks and time delays. This work seeks to close this gap by developing a robust adaptive control framework that ensures secure and reliable coordination among agents. Taking Byzantine attacks and communication delays into consideration, this study addresses these issues by proposing a robust adaptive formation control [28, 29] approach for nonlinear multi-agent systems having double-integral unknowing dynamics. Utilizing neural networks' (NNs) versatility, the approach successfully tackles the unidentified dynamics while integrating a strong framework to manage time delays and lessen the impact of vicious attackers. A numerical simulation demonstrates the suggested method's capacity to sustain robust formation control in the face of communication delays and Byzantine attacks [30].

To address the effects of Byzantine attacks, secure communication protocols [31] ensure that the information shared between agents remains accurate and trustworthy, thereby preventing malicious agents from introducing deceptive data into the system. Additionally, robust control techniques are applied to create control laws capable of maintaining system stability despite the presence of compromised agents. By incorporating these approaches into the adaptive formation control method, the system becomes more resilient to Byzantine attacks, while sustaining its performance and stability.

The research [32] investigates a leader-follower multi-agent system subjected to communication failures and Byzantine attacks. To address these challenges, a robust consensus protocol was introduced [33, 34] incorporating an optimal H_0 strategy. The stability and performance of multi-agent systems are crucial to guarantee time-delay compensation. A Padé approximation-based repetitive control strategy was proposed by [35] to enhance the tracking accuracy under delays. Despite having made significant robust control, loopholes exist in addressing actuator faults, external disturbances, and Byzantine attacks in multi-agent systems. While [36] aimed at predefined-time control of actuator faults, [37] introduced adaptive event-triggered control for stability under uncertainties, and [38] investigated the fixed-time consensus for state constraints. However, there is a need for further research to integrate these strategies into a single framework for robust multi-agent formation control. The proposed controller is designed to mitigate the effects of time delays and Byzantine attacks, enabling the followers to effectively track the virtual leader's behavior.

This study presents a novel adaptive formation control technique that combines targeted methods with neural network-based approximation to handle temporal delays and Byzantine attacks. The approach's efficacy in accomplishing the intended formation objectives despite these obstacles is demonstrated through numerical simulations. This study's main contributions are as follows:

- A design of an adaptive leader-follower formation control strategy for nonlinear multi-agent systems with unknown dynamics.
- The use of neural networks for modeling unknown system dynamics in real-time.
- A resilience mechanism to reduce the effects of Byzantine attacks on agent communication.
- A compensation technique for the time delay to maintain stability when performing formation

control tasks.

- A rigorous Lyapunov-based stability analysis to validate the proposed approach.
- Numerous simulations have been performed to demonstrate the effectiveness of our method in the worst adversarial conditions.

All procedural steps and the notation list in the proposed study are described in Figures 1 and 2, respectively.

The content is structured as follows:

(1) Section 1 presents the research background and key challenges tackled in this work.

(2) Section 2 outlines fundamental concepts, covering neural networks, graph theory, and essential lemmas.

(3) Section 3 describes the system model, the design of the control protocol, and supporting theoretical proofs.

(4) Section 4 offers a simulation example to demonstrate the effectiveness of the proposed approach.

(5) Section 5 offers a concise overview of the key findings and proposes potential avenues for future exploration.

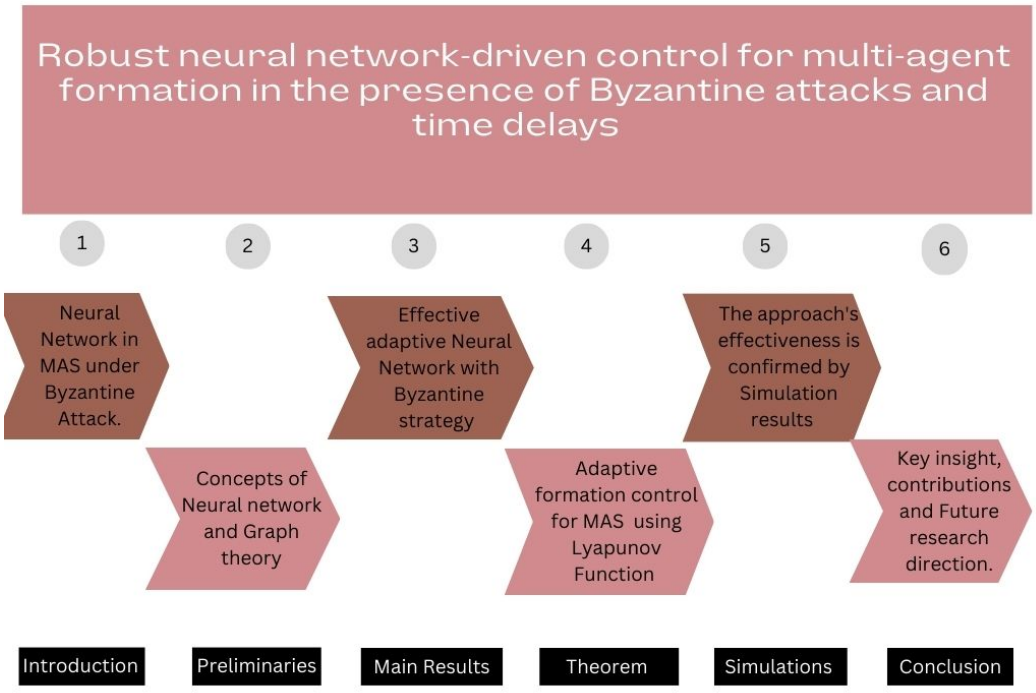

Figure 1. Procedural steps and workflow diagram.

Notation	Meaning
$H(t)$	A continuous Lyapunov function, utilized to evaluate the stability of the system.
$\theta_k(t)$	The position state vector of agent k
$v_k(t)$	The velocity state vector of agent k
$C_k(t-\tau)$	Control input of agent k subject to a time delay
$\Phi_k(\theta_k,v_k)$	Unknown dynamic nonlinear function of agent k
$b_k(t)$	The state and control input of agent k are impacted by the Byzantine attack factor.
$\bar{\theta}(t)$	State of reference position.
$\nabla(t)$	State of reference velocity.
$\mu(t)$	Reference acceleration function with smooth bounds.
$S_{\theta k}(t-\tau)$	Error of position with respect to the leader.
$S_{vk}(t-\tau)$	Error of velocity with respect to the leader.
ω_k	A constant vector that shows the desired relative location between the reference leader and the agent.
$E_{\theta k}(t-\tau)$	Position-based formation error that takes into consideration delays and neighborhood interactions.
$E_{vk}(t-\tau)$	Velocity-based formation error that takes into consideration delays and neighborhood interactions.
V^*_k	Optimal weight matrix for neural networks.
$\hat{V}_k(t)$	Adaptive control weight matrix estimate.
$Q_K(\theta_k,v_k)$	Basis function vector is employed in the approximation of neural networks.
$\epsilon_K(\theta_k,v_k)$	Neural network model approximation error.
α_K	Weight update law design constant.
Υ_K	A matrix with a positive definite constant.
Δ	A diagonal matrix showing ways of communication between the leader and the agents.
O	Adjacency matrix showing agent-to-agent interaction linkages.

Figure 2. List of notations.

2. Preliminaries

2.1. Neural network

It has been shown that neural networks (NNs) can estimate universal functions. Provide a continuous function $\phi(y) : \mathbb{R}^a \times \mathbb{R}^b$, the function over a compact set Θ can be approximated by NN in the following form:

$$\hat{\phi}(\theta) = \mathbf{V}^T Q(\theta), \tag{2.1}$$

where the weight matrix with neuron number c is $\mathbf{V} \in \mathbb{R}^{c\times n}$ and $Q(\theta) = \left[q_1(\theta), \cdots, q_c(\theta)\right]^T$, T is the vector of basis function $q_{k=1}, \ldots, c^{(\theta)} = E^{-\frac{(\theta-\mu_k)^T(\theta-\mu_k)}{2}}$, and $\mu_k = \left[\mu_{k1}, \cdots, \mu_{km}\right]^T$ is the center of receptive field T. The ideal neural weight $\mathbf{V}^* \in \mathbb{R}^{c\times n}$ for the continuous function $\phi(y)$ is defined as

$$V^* := \arg\min_{V\in\mathbb{R}^{c\times n}} \left\{ \sup_{\theta\in\Theta} \|\phi(\theta) - V^T Q(\theta)\| \right\}, \tag{2.2}$$

in order to rewrite $\phi(\theta)$ as

$$\phi(\theta) = V^{*T} Q(\theta) + \epsilon(\theta), \tag{2.3}$$

where the approximation error is represented by $\epsilon(\theta) \in \mathbb{R}^n$ and there exists a constant γ that is positive so that $\|\epsilon(\theta)\| \leq \gamma$.

The optimal NN weight V^* aims to guarantee the smallest possible difference between $V^T Q(\theta)$ and $\phi(\theta)$. However, it is merely an "artificial" quantity for a survey, and it is not feasible to utilize it as a basis for developing the control scheme directly. Instead, the actual control is generally formulated using estimates obtained through adaptive tuning.

2.2. Graph theory

The interconnected graph considered in this research pertaining to the studied multi-agent framework is an undirected connected graph $Z = (O, N, \zeta)$, where $N = \{1, 2, \ldots, m\}$ is the label set of all nodes, $\zeta \in \mathbb{N}\times\mathbb{N}$ is the edge set, and $\mathbf{O} = [o_{kl}] \in \mathbb{R}^{m\times m}$ is the adjacency matrix, with an entry $o_{kl} \geq 0$ indicating the interaction weight shared between agents k and l. The neighbor of node k is considered to be node l if the edge $\aleph_{kl}$ holds $\aleph_{kl} = (k, l) \in \zeta$ the adjacency element $o_{kl} = 1$ and $\lambda k = \{l \mid (k, l) \in \zeta\}$ indicates the neighbor label set. Assuming $\aleph_{kl} \notin \zeta$, then $o_{kl} = 0$, and the graph Z can be referred as an undirected graph whether matrix B adjacency elements meet the requirement $o_{kl} = o_{lk}$, $k, k, l = 1, \ldots, m$ implying that $\aleph_{kl} \in \zeta \iff \aleph_{lk} \in \zeta$. When there is an undirected path $(k, k_1), \ldots, (k_k, l)$, for any two distinguishable nodes k and l, the graph without a direction Z is regarded as linked. The Laplacian matrix by which graph Z is connected is

$$\mathcal{L} = \mathrm{diag}\left(\sum_{l=1}^{m} o_{1l}, \cdots, \sum_{l=1}^{m} o_{nl} \right) - O. \tag{2.4}$$

$\Delta = \mathrm{diag}\{\delta_1, \ldots, \delta_m\}$ is the matrix that describes the communication weights across agents and the leader. $\delta_k = 1$ if the agent k is able to link with the leader, and $\delta_k = 0$ otherwise. While $\delta_k, \ldots, \delta_m \geq 1$, the leader must be associated with at least one agent.

2.3. Auxiliary lemmas

Lemma 2.1. *[39] The irreducibility of the Laplacian matrix of an undirected graph Z is an essential and adequate requirement for its connectivity.*

Lemma 2.2. *[39] Consider an irreducible matrix* $\mathcal{L} = [\ell_{kl}] \in \mathbb{R}^{m\times m}$, *whereby* $\ell_{kl} = \ell_{lk} \leq 0$ *and* $\ell_{kk} = -\sum_{l=1}^{m} \ell_{kl}$. *Then, all of the eigenvalues of* $\tilde{\mathcal{L}} = \begin{bmatrix} \ell_{11} + \delta_1 & \cdots & \ell_{1m} \\ \vdots & \ddots & \vdots \\ \ell_{m1} & \cdots & \ell_{mm} + \delta_m \end{bmatrix}$ *are positive, where* $\delta_1, \ldots, \delta_m$ *are non-negative constants stipulating that* $\delta_1 + \cdots + \delta_m > 0$

Lemma 2.3. *[39] When $O_1(\theta) = O_1^T(\theta)$ and $O_2(\theta) = O_2^T(\theta)$, the matrix inequality*

$$\begin{bmatrix} O_1(\theta) & O_3(\theta) \\ O_3^T(\theta) & O_2(\theta) \end{bmatrix} > 0. \tag{2.5}$$

Applies to any of the two inequalities listed below, and at least one of the conditions must be met:
1) $O_1(\theta) > 0,\ O_2(\theta) - O_3^T(\theta)O_1^{-1}(\theta)O_3(\theta) > 0.$
2) $O_2(\theta) > 0,\ O_1(\theta) - O_3(\theta)O_2^{-1}(\theta)O_3^T(\theta) > 0.$

Lemma 2.4. *[39] The initial condition of the continuous function $H(m) \geq 0$ is bounded. The following inequalities can be preserved when this condition occurs $\dot{H}(m) \leq -oH(m) + d$, whereas o and d are two positive constants that are present.*

$$H(m) \leq H(0)E^{-om} + \frac{d}{o}(1 - E^{-om}). \tag{2.6}$$

3. Important results

3.1. Formulation of the problem

An overview of this double integral dynamic model of a nonlinear multi-agent system that includes m agents is as follows

$$\begin{aligned} &\frac{d}{dt}\theta_k(t) = v_k(t-\tau) \\ &\frac{d}{dt}v_k(t) = C_k(t-\tau) + \phi_k(\theta_k, v_k) + b_k(t) \\ &k = 1, \ldots, m. \end{aligned} \tag{3.1}$$

The position state is described as $\theta_k(t) = \left[\theta_{k1}, \cdots, \theta_{kn}\right]^T \in \mathbb{R}^n$, while the velocity state is $v_k(t) = \left[v_{k1}, \cdots, v_{kn}\right]^T \in \mathbb{R}^n$, the control input with time delay is $C_k(t-\tau) \in \mathbb{R}^n$, the undefined nonlinear dynamic function is $\phi(\cdot) \in \mathbb{R}^n$, and b_k is the Byzantine attack of agent k.

The following dynamics, which are seen as independent leader agents, describe the required reference signals as

$$\begin{aligned} &\frac{d}{dt}\bar{\theta}(t) = \bar{v}(t), \\ &\frac{d}{dt}\bar{v}(t) = \mu(t), \end{aligned} \tag{3.2}$$

where the reference position is denoted by $\bar{\theta} \in \mathbb{R}^n$, while the reference velocity is $\bar{v} \in \mathbb{R}^n$, and the smooth bounded function is $\mu(\cdot) \in \mathbb{R}^n$.

3.2. Impacts of Byzantine attacks

The actuator attack against the MAS can be depicted as

$$C_k^c(t) = C_k(t) + \lambda_k C_k^a(t), \tag{3.3}$$

where $C_k(t)$, $C_k^c(t)$, and $C_k^a(t)$ represent the nominal state, corrupted control input, and attack signals; the attack occurs only if λ_k=1; otherwise, λ_k=0.

The actuator attack against the MAS can be depicted as

$$v_k^c(t) = v_k(t) + \mu_k v_k^a(t), \tag{3.4}$$

where $v_k^c(t)$, $v_k(t)$, $v_k^a(t)$ shows the corrupted input, nominal state, and attack signal. Similarly, the attack occurs only when μ_k=1; otherwise, μ_k=0.

By integrating the effects of both assaults, Eqs (3.3) and (3.4) can be written in the following way:

$$b_k(t) = \lambda_k C^a(t) + cV \sum o_{kl}[\mu_l v_l^a(t) - \mu_k v_k^a(t)]. \tag{3.5}$$

Definition 3.1. *In the event that the system's results (3.1) involving multiple agents are determined, the second-order leader-follower formation is accomplished and fulfills the following conditions* $\lim_{t\to\infty} \|\theta_k(t-\tau) - \bar{\theta}_k(t) - \omega_k\| = 0, lim_{t\to\infty}\|v_k(t-\tau) - \bar{v}(t)\| = 0, \quad k = 1, \ldots, m$. *The desired location of the agent k is demonstrated through the constant vector* $\omega_k = \left[\omega_{k1}, \cdots, \omega_{kn}\right]^T \in \mathbb{R}^n$.

Objective of control: The objective is to develop an adaptive control method to facilitate formation in nonlinear multi-agent systems (3.1), ensuring that when the time-delayed and Byzantine attacks alter the states of the agents, all deviation indicators maintain their ultimate boundedness, which is semi-global and uniform. Inspired by the semi-global stabilization techniques for parabolic PDE–ODE systems with input saturation proposed by [40], we aim to design a control strategy that ensures robustness against such adversarial influences. Despite the interfering assaults, the system develops second-order leader-follower relationships.

3.3. Designing the control scheme

Transformations of coordinates should be represented by:

$$\begin{aligned} &S_{\theta k}(t) = \theta_k(t) - \bar{\theta}(t) - \omega_k, \\ &S_{vk}(t) = v_k(t) - \bar{v}(t), \\ &k = 1, \ldots, m. \end{aligned} \tag{3.6}$$

Differentiate the above equation w.r.t time

$$\begin{aligned} \frac{d}{dt}S_{\theta k}(t) &= \frac{d}{dt}\theta_k(t) - \frac{d}{dt}\bar{\theta}(t) - \frac{d}{dt}\omega_k \\ &= v_k(t-\tau) - \bar{v}(t) \\ &= S_{vk}(t-\tau); \\ \frac{d}{dt}S_{vk}(t) &= \frac{d}{dt}v_k(t) - \frac{d}{dt}\bar{v}(t) \\ &= C_k(t-\tau) + \phi_k(\theta_k + v_k) + b_k(t) - \mu(t); \\ k &= 1, \ldots, m. \end{aligned} \tag{3.7}$$

Hence, the error dynamics that follow are generated by (3.1) and (3.2)

$$\frac{d}{dt}S_{\theta k}(t) = S_{vk}(t-\tau),$$

$$\frac{d}{dt}S_{vk}(t) = C_k(t-\tau) + \phi_k(\theta_k + v_k) + b_k(t) - \mu(t),$$
$$k = 1, \ldots, m. \tag{3.8}$$

The following rewriting of error dynamics (3.8) is necessary to simplify

$$\frac{d}{dt}S(t) = \begin{bmatrix} S_V(t-\tau) \\ C(t-\tau) + \Phi(S) + b_k - \mu(t) \otimes 1_m \end{bmatrix}, \tag{3.9}$$

in which $\mathbf{S}(t) = \left[\mathbf{S}_\theta^T(t), \mathbf{S}_v^T(t)\right]^T \in \mathbb{R}^{2mn}$ when $\mathbf{S}_\theta(t) = \left[\mathbf{S}_{\theta 1}^T(t), \cdots, \mathbf{S}_{\theta m}^T(t)\right]^T \in \mathbb{R}^{mn}$ while $\mathbf{S}_v(t) = \left[\mathbf{S}_{v1}^T(t), \cdots, \mathbf{S}_v^T(t)\right]^T \in \mathbb{R}^{mn}$,$\mathbf{C} = \left[\mathbf{C}_1^T, \cdots, \mathbf{C}_m^T\right]^T \in \mathbb{R}^{mn}$, and $\mathbf{\Phi}(\mathbf{S}) = \left[\phi_1^T, \cdots, \phi_m^T\right]^T \in \mathbb{R}^{mn}$ $1_m = \left[1, \cdots, 1\right]^T \in \mathbb{R}^m$, $\otimes$ is the Kronecker product.

Define the formation discrepancies in terms of position and velocity as

$$E_{\theta k}(t-\tau) = \sum_{l \in \lambda_k} o_{kl}\left(\theta_k(t-\tau) - \omega_k - \theta_l(t-\tau) + \omega_l\right) + \delta_k\left(\theta_k(t-\tau) - \bar{\theta}(t) - \omega_k\right),$$
$$E_{vk}(t-\tau) = \sum_{l \in \lambda_k} o_{kl}\left(v_k(t-\tau) - v_l(t-\tau)\right) + \delta_k\left(v_k(t-\tau) - \bar{v}(t)\right),$$
$$k = 1, \ldots, m. \tag{3.10}$$

In this context, o_{kl} and δ_k denote elements of O and Δ matrices; the subsection II.B with λ_k represents the neighbor labels for agent k.

Using Eqs (3.6) and (3.10), we can re-express the formation error terms as

$$E_{\theta_K}(t-\tau) = \sum_{l \in \lambda k} o_{kl}(S_{\theta k}(t-\tau) - S_{\theta l}(t-\tau)) + \delta_k S_{\theta k}(t-\tau),$$
$$E_{v_K}(t-\tau) = \sum_{l \in \lambda k} o_{kl}(S_{v_l}(t-\tau) - S_{v_l}(t-\tau)) + \delta_k S_{vk}(t-\tau),$$
$$k = 1, \ldots, m. \tag{3.11}$$

For the unknown nonlinear function $\phi_k(\theta_k, v_k)$ (3.9), consider a compact set $\Theta_k \subset \mathbb{R}^{2n}$, for $\left[\theta_k^T, v_k^T\right]^T \in \Theta_k$. To incorporate the Byzantine attack with a time delay, the expression of $\phi_k(\theta_k, V_k)$ under attack would be modified to include an adversarial impact. $b_k(t-\tau)$ represents the Byzantine attack applied on the function with delay τ. The function can be approximated by an NN model, yielding

$$\phi_k(\theta_k, v_k) = V_k^{*T} Q_k(\theta_k(t-\tau), v_k(t-\tau)) + b_k(t) + \varepsilon_k(\theta_k, v_k). \tag{3.12}$$

Consider the ideal neural weight matrix $V_k^* \in \mathbb{R}^{c_k \times n}$ with neuron number c_k and corresponding basis function vector $Q_k(\theta_k, v_k) \in \mathbb{R}^{c_k}$ with approximation error $\epsilon_k(\theta_k, v_k)$ bounded by $\|\epsilon_k(\theta_k, v_k)\| \leq \gamma_k$, where γ_k is a predetermined constants.

In Eq (3.12), the optimal matrix of weight V_k^* can be expressed as a constant that is not known, making it challenging to implement in practical control designs. To overcome this limitation, we replace the ideal neural network weight V_k^* with the estimated weight $\hat{V}_k(t)$. The formation control is subsequently formulated using the following estimation

$$C_k(t-\tau) = -\beta_\theta E_{\theta k}(t-\tau) - \beta_v E_{v_k}(t-\tau) - \hat{V}_k^T(t-\tau) \times Q_k(\theta_k, v_k) + b_k(t),$$

$$k = 1, \ldots, m. \tag{3.13}$$

In which $V_k^* \in \mathbb{R}^{c_k \times n}$ is the approximate value of V_k^* and $\beta_\theta > 0$, and $\beta_v > 0$ serve as two design constants. And $b_k(t)$ represents a Byzantine attack with a delay of τ. By introducing an adversarial disturbance in the delayed state, it affects the nonlinear dynamics. Even when adversarial interruptions occur, control robustness is maintained by incorporating this change. In order to tune $\hat{V}_k(t)$, the NN updating law is as follows:

$$\begin{aligned} &\frac{d}{dt}\hat{V}_k(t-\tau) = \Upsilon_k \left(Q_k(\theta_k, v_k)(E_{\theta k}(t-\tau) + E_{vk}(t-\tau))^T - \alpha_k \hat{V}_k(t-\tau) \right), \\ &k = 1, \ldots, m, \end{aligned} \tag{3.14}$$

where the design constant is $\alpha_k > 0$ while the positive definite constant matrix is $\Upsilon_k \in \mathbb{R}^{c_k \times c_k}$.

Observation 1: In the control law described in (3.13), the terms related to the position and velocity errors are formulated as specified in (3.10). These error terms are incorporated to ensure effective compensation for deviations in both positional and velocity dynamics, facilitating the system's adherence to the desired formation trajectory. The error terms are expertly designed to enable the agents within the network to successfully achieve their objectives. The neural network expression $\hat{V}_k^T(t-\tau)Q_k(\theta_k, v_k)$ plays a crucial role in compensating for unknown dynamics by dynamically tuning the neural network weight with time delay $\hat{V}_k(t-\tau)$ according to the updating law (3.14). The Byzantine attack factor $b_i(t)$ affects control and system dynamics. This means that an adversary can influence how the system operates. Adding time delays in the agents also makes it harder to keep the formation stable. This unique control strategy addresses formation management in intricate second-rank nonlinear structures. To better address adversarial issues and temporal delays, potential improvements include using the latest strategies like learning via reinforcement or robustness control $\mathbf{H}_0$.

Remark 3.2. *In the design of the proposed robot resilient neural network-driven control the accuracy versus computational cost is a critical issue. The neural network-based approximation enhances the system's adaptability and resistance to Byzantine attacks but implies real-time weight updates and function approximations that increase computational complexity. The accuracy increases with the network complexity and number of computations that are performed, which can increase the time for processing and demand on hardware resources. To this end, we optimize the neural network structure by restricting the number of hidden layers and adjusting adaptation rates, so that the robustness is maintained at the expense of reasonable computational costs. Lightweight neural architectures or distributed processing techniques can also be explored in future research to improve efficiency without compromising accuracy.*

3.4. Proof-based conjecture

Conjecture 1: The nonlinear dynamics of a second-order agent-based system described in (3.1) operates under an undirected connected graph z and maintains bounded initial conditions. By implementing the adaptive formation control law (3.13), the neural network weight updating rule (3.14), and the design constants β_θ and β_v are chosen. Furthermore, incorporating a Byzantine attack function with a time delay into the nonlinear dynamics introduces significant challenges in the delayed

state. This approach enables a robust evaluation of control performance ensuring resilient system operation. The control objectives are achieved for a sufficiently smooth movement trajectory.

$$\beta_\theta > 1, \quad \beta_v > 1\frac{1}{2} + \frac{1}{2(\Psi_{min}^{\tilde{\mathcal{L}}})^2},$$
$$\beta_\theta + \beta_v > \frac{1}{\Psi_{min}^{\tilde{\mathcal{L}}}}. \tag{3.15}$$

Let $\Psi_{min}^{\tilde{\mathcal{L}}}$ denote the smallest matrix's eigenvalue $\tilde{\mathcal{L}}$. This will lead to the achievement of the intended control goals.

(1) Each error will be semi-globally uniformly ultimately bounded, despite the influence of the Byzantine attack factor with time delay $b_k(t)$ affecting agents and control inputs.

(2) Even with temporal delays and Byzantine attacks, the multi-agent creation will be effectively maintained with uniform reference trajectories.

Proof: We select the following Lyapunov function candidate

$$H(t-\tau) = \frac{1}{2}S^T(t-\tau)\left(\begin{bmatrix}(\beta_\theta+\beta_v)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & \tilde{\mathcal{L}} \\ \tilde{\mathcal{L}} & \tilde{\mathcal{L}}\end{bmatrix} \otimes I_m\right) \times S(t-\tau) + \frac{1}{2}\sum_{k=1}^{m} T_r\left\{\tilde{V}_k^T(t-\tau)\Upsilon_k^{-1}\tilde{V}_k(t-\tau)\right\}. \tag{3.16}$$

It is definitely positive. The following outcome is achieved when the design parameters fulfill the condition (3.15).

Where $\tilde{\mathcal{L}} = \mathcal{L} + \Delta$ by Lemma (2.2), positive definiteness of the symmetrical matrix $\tilde{\mathcal{L}}$ is verified. The following result is assured as long as the design parameters meet condition (3.15). $(\beta_\theta + \beta_v)\tilde{\mathcal{L}}\tilde{\mathcal{L}} - \tilde{\mathcal{L}} > 0$. Consequently, the matrix $\begin{bmatrix}(\beta_\theta+\beta_v)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & \tilde{\mathcal{L}} \\ \tilde{\mathcal{L}} & \tilde{\mathcal{L}}\end{bmatrix}$ is also positive definite, as indicated by Lemma 2.3. Therefore, the function $H(\tau)$ can be regarded as a candidate for a Lyapunov function.

The time derivative of $H(t)$ concerning the dynamics described in Eqs (3.9) and (3.14) is given by

$$\begin{aligned}\frac{d}{dt}H(t) =& S^T(t-\tau)\left(\begin{bmatrix}(\beta_\theta+\beta_v)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & \tilde{\mathcal{L}} \\ \tilde{\mathcal{L}} & \tilde{\mathcal{L}}\end{bmatrix} \otimes I_m\right) \times \begin{bmatrix}\mathbf{S}_v(t-\tau) \\ C(t-\tau) + \phi(S) + b_k(t) - \eta(t)\otimes \mathbf{1}_m\end{bmatrix} \\ &+ \sum_{k=1}^{m} T_r\left\{\tilde{V}_k^T(t)\left(Q_k(\theta_k, v_k)\left(E_{\theta k}(t-\tau) + E_{vk}(t-\tau)\right)^T - \beta_k \hat{V}_k(t)\right)\right\}.\end{aligned} \tag{3.17}$$

Given that $E_\theta(t-\tau) = \tilde{\mathcal{L}}\mathbf{S}_\theta(t-\tau)$ and $E_v(t-\tau) = \tilde{\mathcal{L}}\mathbf{S}_v(t-\tau)$, where $E_\theta(t-\tau) = \left[E_{\theta 1}^T(t-\tau), \cdots, E_{\theta m}^T(t-\tau)\right]^T \in \mathbb{R}^{mn}$, $E_v(t-\tau) = \left[E_{V1}^T(t-\tau), \cdots, E_{vm}^T(t)\right]^T \in \mathbb{R}^{mn}$ and $\mathbf{b}(t) = \left[b_1(t)\ b_2(t)\ \cdots\ b_m(t)\right]^T$ represents the Byzantine attack vector applied to each agent so the Eq (3.17) can be reformulated accordingly

$$\begin{aligned}\frac{d}{dt}H(t) =& \left[(\beta_\theta+\beta_v)E_\theta^T(t-\tau)\tilde{\mathcal{L}} + E_v^T(t-\tau), E_\theta^T(t-\tau) + E_v^T(t-\tau)\right]\begin{bmatrix}\mathbf{S}_v(t-\tau) \\ C(t-\tau) + \phi(S) + b_k(t) - \eta(\tau)\otimes \mathbf{1}_m\end{bmatrix} \\ &+ \sum_{k=1}^{m} T_r\left\{\tilde{V}_k^T(t)\left(Q_k(\theta_k, v_k)\left(E_{\theta k}(t-\tau) + E_{vk}(t-\tau)\right)^T - \beta_k \hat{V}_k(t)\right)\right\}.\end{aligned} \tag{3.18}$$

After straightforward steps, the following expression can be derived from Eq (3.18)

$$\begin{aligned}\frac{d}{dt}H(t) = &\sum_{k=1}^{m}\left((\beta_\theta+\beta_v)E_{\theta k}^T(t-\tau)E_{vk}(t-\tau)+E_{vk}^T(t-\tau)\times S_{vk}(t-\tau)\right)\\ &+\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\times(C_k+\phi_k(\theta_k,v_k)+b_k(t)-\eta(t))\\ &+\sum_{k=1}^{m}T_r\left\{\tilde{V}_k^T(t)\left(Q_k(\theta_k,v_k)\left(E_{\theta k}(t-\tau)+E_{vk}(t-\tau)\right)^T-\beta_k\hat{V}_k(t)\right)\right\}.\end{aligned} \tag{3.19}$$

By substituting the neural network approximation from (3.12) and the controller from (3.13) into equation (3.19), we obtain the following result

$$\begin{aligned}\frac{d}{dt}H(t) = &\sum_{k=1}^{m}\left((\beta_\theta+\beta_v)E_{\theta k}^T(t-\tau)E_{vk}(t-\tau)+E_{vk}^T(t-\tau)S_{vk}(t-\tau)\right)\\ &+\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\\ &\left(-\beta_\theta E_{\theta_k}(t-\tau)-\beta_v E_{v_k}(t-\tau)-\hat{V}_k^T(t)Q_k(\theta_k,v_k)+V_k^{*T}Q_k(\theta_k,v_k)+\varepsilon_k(\theta_k,v_k)-\eta(t)+2b_k(t)\right)\\ &+\sum_{k=1}^{m}T_r\{\tilde{V}_k^T(t)Q_k(\theta_k,v_k)\times(E_{\theta k}(t-\tau)+E_{vk}(t-\tau))^T-\beta_k\tilde{V}_k^T(t)\hat{V}_k(t)\}.\end{aligned} \tag{3.20}$$

Considering the equation $\tilde{V}_k(t)=\hat{V}_k(t)-V_k^*$, the following is an alternative expression for Eq (3.20)

$$\begin{aligned}\frac{d}{dt}H(t) = &-\sum_{k=1}^{m}\beta_\theta E_{\theta k}^T(t-\tau)E_{\theta k}(t-\tau)-\sum_{k=1}^{m}\beta_v\times E_{vk}^T(t-\tau)E_{vk}(t-\tau)\\ &+\sum_{k=1}^{m}E_{vk}^T(t-\tau)S_{vk}(t-\tau)-\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\tilde{V}_k^T(t)\times Q_k(\theta_k,v_k)\\ &+\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\times\varepsilon_k(\theta_k,v_k)-\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\times(\eta(t)+2b_k(t))\\ &+\sum_{k=1}^{m}T_r\left\{\tilde{V}_k^T(t)Q_k(\theta_k,v_k)\times\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\right\}-\sum_{k=1}^{m}T_r\left\{\alpha_k\times\tilde{V}_k^T(t)\hat{V}_k(t)\right\}.\end{aligned} \tag{3.21}$$

Based on the properties of the trace operation, we have $g^Tk=T_r(gk^T)=T_r(kg^T)\ \forall g,k\in\mathbb{R}^b$, which leads to the following conclusion:

$$\left(E_{\theta k}(t-\tau)+E_{vk}(t-\tau)\right)^T\tilde{V}_k^T(t)Q_k(\theta_k,v_k)=T_r\left\{\tilde{V}_k^T(t)Q_k(\theta_k,v_k)\left(E_{\theta k}(t-\tau)+E_{vk}(t-\tau)\right)^T\right\}. \tag{3.22}$$

By applying Eq (3.21), the following is a modification of Eq (3.20)

$$\begin{aligned}\frac{d}{dt}H(t) =& -\sum_{k=1}^{m}\beta_\theta E_{\theta k}^T(t-\tau)E_{\theta k}(t-\tau) - \sum_{k=1}^{m}\beta_v \times E_{vk}^T(t-\tau)E_{vk}(t-\tau)\\ &+\sum_{k=1}^{m}E_{vk}^T(t-\tau)S_{vk}(t-\tau) + \sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)\varepsilon_k(\theta_k,v_k)\\ &-\sum_{k=1}^{m}\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)(\eta(t)+2b_k(t))\\ &-\sum_{k=1}^{m}T_r\left\{\alpha_k\tilde{V}_k^T(t)\hat{V}_k(t)\right\}.\end{aligned} \tag{3.23}$$

The following outcomes can be obtained via Young's inequality and the Cauchy-Bunyakovsky-Schwarz inequality

$$\begin{aligned}E_{vk}^T(t)S_{vk}(t) &\le \frac{1}{2}E_{vk}^T(t-\tau)E_{vk}(t-\tau) + \frac{1}{2}S_{vk}^T(t-\tau)S_{vk}(t-\tau), (E_{\theta k}(t-\tau)+E_{vk}(t-\tau))^T\varepsilon_k(\theta_k,v_k)\\ &\le \frac{1}{2}E_{\theta k}^T(t-\tau)E_{\theta k}(t-\tau) + \frac{1}{2}E_{vk}^T(t-\tau)E_{vk}(t-\tau) + \|\varepsilon_k(\theta_k,v_k)\|^2,\\ &\left(E_{\theta k}^T(t-\tau)+E_{vk}^T(t-\tau)\right)(\eta(t)+2b_k(t))\\ &\le \frac{1}{2}E_{\theta k}^T(t-\tau)E_{\theta k}(t-\tau) + \frac{1}{2}\times E_{vk}^T(t-\tau)E_{vk}(t-\tau) + \|\eta(t)+2b_k(t)\|^2\\ &\le \frac{1}{2}E_{\theta k}^T(t-\tau)E_{\theta k}(t-\tau) + \frac{1}{2}\times E_{vk}^T(t-\tau)E_{vk}(t-\tau) + 2\|\eta(t)\|^2 + 8\|b_k(t)\|^2.\end{aligned} \tag{3.24}$$

Each inequality has been adjusted to include the delayed error terms and the impact of the Byzantine attack $b_k(t)$. These changes maintain the structure required for stability analysis while incorporating both time delays and adversarial disturbances, allowing the framework to reflect these influences on system stability more accurately.

By inserting the inequalities from (3.24) into (3.23), the following results are obtained:

$$\begin{aligned}\frac{d}{dt}H(t) \le& -S^T(t-\tau)\left(\begin{bmatrix}(\beta_\theta-1)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & 0\\ 0 & \left(\beta_v-1\frac{1}{2}\right)\tilde{\mathcal{L}}\tilde{\mathcal{L}}-\frac{1}{2}I_n\end{bmatrix}\otimes I_m\right)S(t-\tau)\\ &-\sum_{k=1}^{m}T_r\left\{\alpha_k\tilde{V}_k^T(t)\hat{V}_k(t)\right\} + \sum_{k=1}^{m}\|\varepsilon_k(\theta_k,v_k)\|^2 + 2n\|\eta(t)\|^2 + 8n\|b_k(t)\|^2.\end{aligned} \tag{3.25}$$

By applying the relation $\tilde{V}_k(t) = \hat{V}_k(t) - V_k^*$, the resulting equation can be derived

$$T_r\left\{\alpha_k\tilde{V}_k^T(t)\hat{V}_k(t)\right\} = \frac{\alpha_k}{2}T_r\left\{\tilde{V}_l^T(t)\tilde{V}_k(t)\right\} + \frac{\alpha_k}{2}T_r\left\{\hat{V}_k^T(t)\hat{V}_l(t)\right\} - \frac{\alpha_k}{2}T_r\left\{V_k^{*T}V_k^*\right\}. \tag{3.26}$$

By substituting Eq (3.26) into Eq (3.25), we obtain the following result:

$$\frac{d}{dt}H(t) \le -S^T(t-\tau)\left(\begin{bmatrix}(\beta_\theta-1)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & 0\\ 0 & \left(\beta_v-1\frac{1}{2}\right)\tilde{\mathcal{L}}\tilde{\mathcal{L}}-\frac{1}{2}I_n\end{bmatrix}\otimes I_m\right)S(t-\tau) - \frac{\alpha_k}{2}T_r\left\{\tilde{V}_k^T(t)\tilde{V}_k(t)\right\}$$

$$+ \nabla(t) + 8n\|b_k(t)\|^2. \tag{3.27}$$

Let $\nabla(t)$ be defined as $\nabla(t) = \sum_{l=1}^{a} \frac{\alpha_l}{2} T_r \left\{V_l^{*T} V_l^*\right\} + \sum_{k=1}^{m} \|\varepsilon_k(\theta_k, v_k)\|^2 + n\|\eta(t)\|^2$. Since all components of $\nabla(t)$ are bounded, there exists a constant o such that $\|\nabla(t)\| \leq d_1$. Also, since the Byzantine attack is also bounded, $8n\|b_k(t)\|^2 \leq d_2$.

Let Ψ_{min}^{g} represent the smallest value of the matrix's eigen spectrum $\begin{bmatrix} (\beta_\theta - 1)\tilde{\mathcal{L}}\tilde{\mathcal{L}} & 0 \\ 0 & \left(\beta_v - 1\frac{1}{2}\right)\tilde{\mathcal{L}}\tilde{\mathcal{L}} - \frac{1}{2}I_n \end{bmatrix}$. Additionally, allow for Ψ_{max}^{k} to express the largest value in the matrix's eigen spectrum $\begin{bmatrix} (\beta_\theta + \beta_v)\tilde{\mathcal{L}}^T\tilde{\mathcal{L}} & \tilde{\mathcal{L}} \\ \tilde{\mathcal{L}} & \tilde{\mathcal{L}} \end{bmatrix}$. Additionally, let $\Psi_{\max}^{\Upsilon_k^{-1}}$ be the maximum eigenvalue of Υ_k^{-1}. From Eq (3.24), the following can be derived

$$\frac{d}{dt}H(t) \leq -\frac{\Psi_{\min}^{o}}{\Psi_{\max}^{g}} S^T(t-\tau)\left(\begin{bmatrix} (\beta_\theta + \beta_v)\tilde{\mathcal{L}}^T\tilde{\mathcal{L}} & \tilde{\mathcal{L}} \\ \tilde{\mathcal{L}} & \tilde{\mathcal{L}} \end{bmatrix} \otimes I_m\right) S(t-\tau) - \frac{1}{2}\sum_{k=1}^{m} \frac{\alpha_k}{\Psi_{\max}^{\Upsilon_k^{-1}}} T_r\left\{\tilde{V}_k^T(t)\Upsilon_k^{-1}\tilde{V}_k(t)\right\} + d_1 + d_2. \tag{3.28}$$

Define g as the minimum eigenvalue of $o = \min\left\{2\frac{\Psi_{\min}^{o}}{\Psi_{\max}^{g}}, \frac{\alpha_1}{\Psi_{\max}^{\Upsilon_1^{-1}}} \ldots, \frac{\alpha_m}{\Psi_{\max}^{\Upsilon_m^{-1}}}\right\}$, so the inequality (3.28) becomes

$$\frac{d}{dt}H(t) \leq -oH(t) + d_1 + d_2. \tag{3.29}$$

By applying Lemma (2.4) to Eq (3.29), the following inequality can be obtained

$$H(t) \leq E^{-ot}H(0) + \frac{d_1 + d_2}{o}\left(1 - E^{-ot}\right). \tag{3.30}$$

Based on the inequality provided, the following can be demonstrated

First, the error $S_{\theta k}(t), S_{vk}(t), \tilde{V}_k(t)$ and $k = 1, \ldots, n$ are characterized as semi-globally uniformly ultimately bounded (SGUUB). This is true even in the presence of the Byzantine attack $b_k(t)$ and the time delay $t - \tau$, which impact both the system's dynamics and the control law. Consequently, the system exhibits stability despite adversarial disturbances and time delay effects.

Second, the tracking errors $S_{\theta k}(t)$ and $S_{vk}(t)$ can attain the desired accuracy through the appropriate selection of sufficiently large design parameters. This implies that the multi-agent formation can still be successfully realized in the context of the Byzantine attack and time delay, provided that the design constants are suitably chosen to address these challenges.

Overall, the formation control protocol is resilient to Byzantine attacks and time delays while ensuring the desired tracking performance is achieved. In Figure 3, the working of the proposed study is discussed.

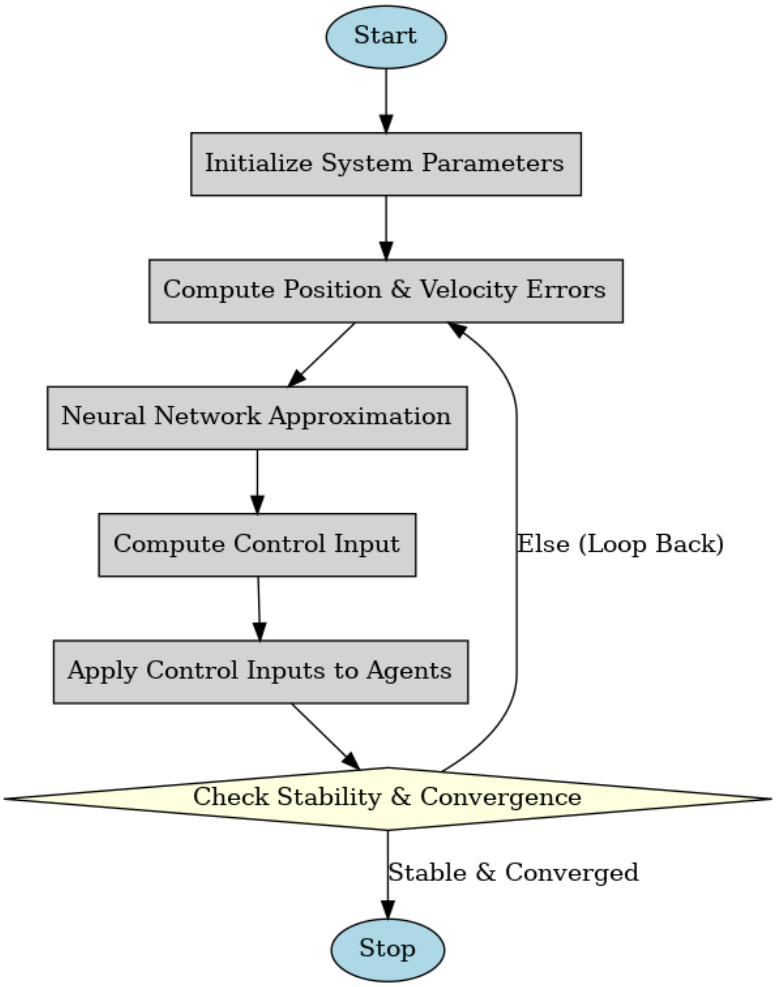

Figure 3. Working of proposed study.

3.5. Simulation

In this simulation, a system composed of four agents functions on a two-dimensional plane. An instance is outlined below:

$$\frac{d}{dt}\theta_k(t) = v_k(t-\tau),$$
$$\frac{d}{dt}v(t) = C_k(t-\tau) + b_k(t) + \begin{bmatrix} \theta_{k1} + \varrho_k \cos^2(\theta_{k1} v_{k1}) \\ v_{k2} + \varphi_k \sin^2(\theta_{k2} v_{k2}) \end{bmatrix},$$
$$k = 1, 2, 3, 4. \tag{3.31}$$

Where $\theta_k(t) = \left[\theta_{k1}, \theta_{k2}\right]$, $v_k(t) = \left[v_{k1}, v_{k2}\right]$, $b_k = \begin{bmatrix} 0.5 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, and $\tau = 0.2$. The values of ϱ_k for $k = 1, 2, 3, 4$ are set to $-0.25, 0.3, -0.2$, and 0.1, respectively, and the values of φ_k for $k = 1, 2, 3, 4$ are $0.3, 0.1, -0.8$, and -0.6, respectively.

The starting positions are as follows: $\theta_{k=1,2,3,4}(0) = \left[2.6, 2.7\right]^T, \left[2.2, -2.1\right]^T, \left[-2.7, 2.2\right]^T, \left[-2.1, -2.7\right]^T$, respectively.

The desired trajectory for the formation movement is defined by the following dynamic function, with starting values $\bar{\theta}(0) = \left[0, 0\right]^T$

$$\frac{d}{dt}\bar{\theta}(t) = \bar{v}(t),$$
$$\frac{d}{dt}\bar{v}(t) = \left[2\cos(0.3t), 2\sin(0.3t)\right]. \tag{3.32}$$

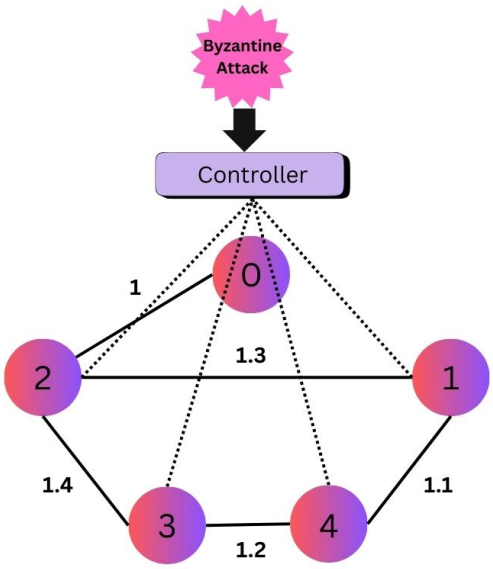

Figure 4. Communication topology.

The following are the reference signals and required relative locations for the agents $\omega_k = 1, 2, 3, 4 = [1.5, 1.5]^T, [1.5, -1.5]^T, [-1.5, 1.5]^T, [-1.5, -1.5]^T$. According to Figure 4, the adjacency matrix describes the connections between agents O given by $O = \begin{bmatrix} 0 & 1.3 & 0 & 1.1 \\ 1.3 & 0 & 1.4 & 0 \\ 0 & 1.4 & 0 & 1.2 \\ 1.1 & 0 & 1.2 & 0 \end{bmatrix}$, while the communication links between the agents and the leader are characterized by the diagonal matrix Δ, defined as $\Delta = \text{diag}(0, 1, 0, 0)$. The formation control approach obtained from (3.13) establishes the design parameters based on the control situations that (3.15) $\beta_\theta = 30$ and $\beta_v = 20$. With 12 neurons in the neural network configuration, the centers are uniformly spaced from -3 and 3. In (3.14), the design parameters are defined by the update rule $\Upsilon_k = 0.8K_{12}$ for $k = 1, 2, 3, 4$ and $\alpha_k = 0.25$ for the same indices, while the initial weights are set as $\hat{V}_{k=1,2,3,4}(0) = [0.4]_{12\times 2}$. The simulation results are further detailed in Figures 5, 6, and 8, which visually depict the various outcomes observed, offering a clear representation of the collected data. Figures 5 and 6 depict the performance metrics related to velocity tracking, clearly showcasing the system's ability to maintain precise velocity control. These figures highlight the system's reliability and efficiency across different operational scenarios. Figure 7 shows the Byzantine attack signal. Moreover, Figure 8 reflects consistent performance by showing

that the neural network weights stay within the defined limits. The simulation results demonstrate that the proposed formation control method is both reliable and effective in meeting the desired control objectives.

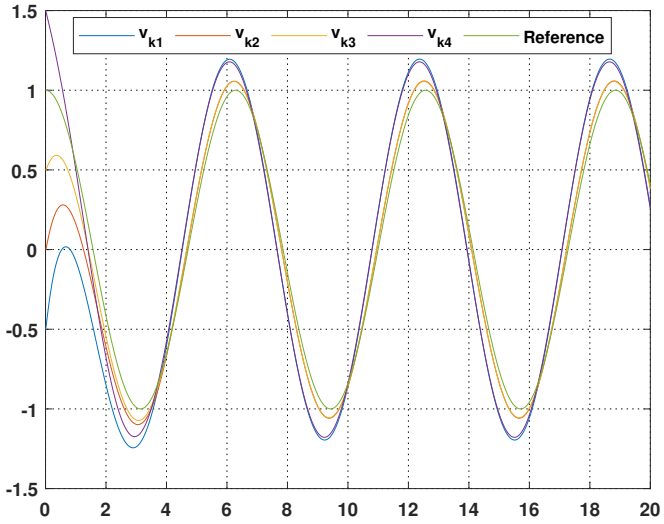

Figure 5. Accurate tracking of velocity for the initial coordinate is essential for achieving precise results.

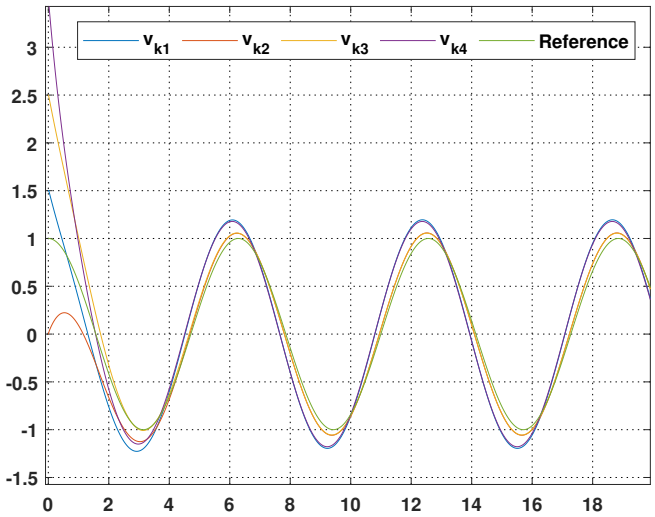

Figure 6. Accurate velocity tracking for the second coordinate is essential for achieving precise results.

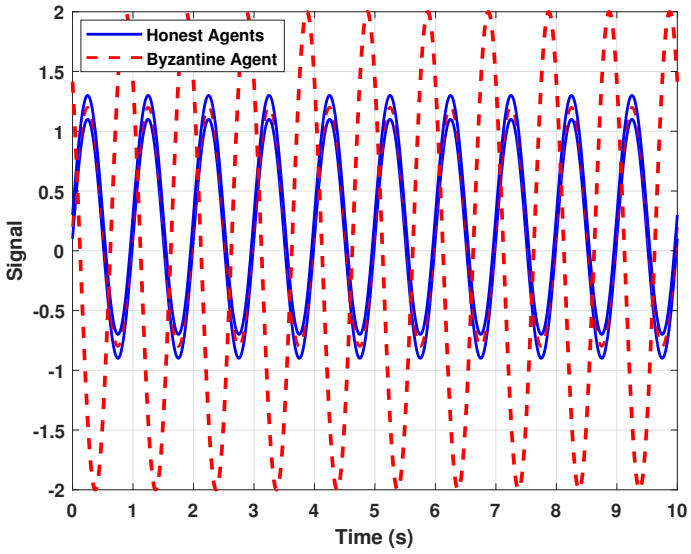

Figure 7. Byzantine attack signal.

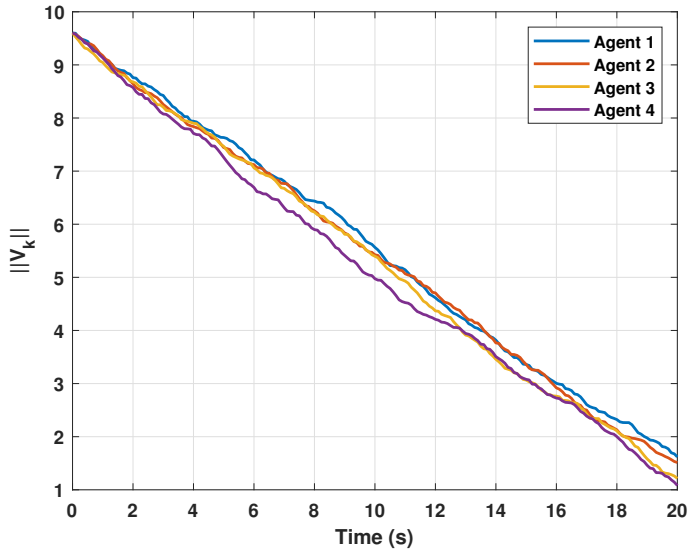

Figure 8. The dimension of the weights in the neural network.

Additionally, a comparison between our proposed method and existing methods is shown in the Tables 1 and 2.

Table 1. Comparison of our proposed method with existing methods (topology & attack type).

Method	Topology type	Attack type considered
Proposed method	Leader-follower with Byzantine attack	Byzantine attacks
Existing method in [39]	Simple formation control	No attacks
Existing method in [4]	Consensus-based control	Random attack model (stochastic disturbances learning-based adaptation)
Existing method in [16]	Robust control	Static attack model (bounded dropouts disturbances)

Table 2. Comparison of our proposed method with existing methods (performance metrics).

Method	Convergence speed	Robustness to attacks	Handling of time delays
Proposed method	Fast	High	Adaptive delay compensation
Existing method in [39]	Moderate	Low	No compensation
Existing method [4]	Slow	Moderate	Limited compensation
Existing method [16]	Moderate	High	Delay handling

Remark 3.3. *In this study, we focus on fixed time delays* $\tau = 0.2$ *to evaluate the stability and performance of our proposed control strategy. However, in practical scenarios, time delays can vary due to factors like network congestion, changing communication conditions, or environmental influences. Extending our approach to handle time-varying delays is an important direction for future research. This could involve using adaptive delay compensation techniques or Lyapunov-Krasovskii methods to maintain stability despite varying delays. We plan to explore these enhancements in future works to improve the system's robustness.*

3.6. Discussion

Tables 1 and 2 show a comparison between our proposed method and existing methods. Previous methods focused on simple formation control or stochastic disturbance adaptation, while our approach explicitly solves Byzantine attacks in a leader-follower topology. In addition, in terms of performance, the proposed method has faster convergence, and higher robustness against attack, and can perform effective adaptive delay compensation; however, other methods offer limited or no attack resilience and delay handling. Therefore, the results support the effectiveness of the proposed approach for robust and adaptive multi-agent formation control under Byzantine attacks and time delays. While the current study focuses on Byzantine attacks, the proposed neural network-based control framework can be extended to handle more sophisticated adversarial scenarios. Specifically, adaptive mechanisms can be incorporated to counteract dynamic attack intensities by continuously adjusting control gains based on real-time threat assessments. Additionally, collaborative attack mitigation can be addressed by integrating anomaly detection techniques to identify coordinated malicious behaviors among compromised agents. Future work will explore these extensions to further enhance the system's robustness in adversarial environments.

3.7. Advantages and disadvantages of the proposed neural network-based control framework

The advantages of the proposed neural network-based control framework over conventional methods are very significant in handling Byzantine attacks and time delays. Unlike traditional robust control or consensus-based protocols, this approach is dynamic and adapts to adversarial conditions and delayed feedback such that system stability and convergence rate are improved. Its capability to counteract malicious interference and sustain formation control in uncertain environments makes it extremely robust.

However, some potential challenges need further consideration to improve the effectiveness of the model. The delays can cause old feedback to be used, which can result in slow convergence or even system instability. Furthermore, Byzantine attacks that are launched by adversarial agents who may attempt to inject false information or manipulate consensus are a major risk to the system's reliability. Predictive delay compensation mechanisms, improved adversary isolation approaches, and modular and scalable architectures are among the potential countermeasures that can enhance robustness. A more effective mitigation strategy could result from further improvements to attack models, particularly in describing assault plans and objectives. MATLAB simulations can be used to validate the performance and robustness of the proposed framework by modeling delays as $t - \tau$ and adversarial agents that introduce false update values to assess system resilience.

4. Conclusions

This paper describes a new formation control method for second-order multi-agent systems with unknown nonlinear dynamics by using adaptive neural networks in a leader-follower architecture. This method is different from the previous methods because it deals with the issue of unknown dynamic functions in a way that is exclusive to neural network approximation, thus giving a more robust solution for dynamic uncertainty. The proposed framework combines adaptive neural network control with Lyapunv-based stability analysis, all error signals are semi-globally uniformly ultimately bounded (SGUUB), and second-order leader follower formation is achieved regardless of initial conditions. Simulations also show that this approach is effective for real world applications where the dynamics of the systems are complex.

This study presents a significant distinction in that it recognizes the vulnerabilities that can result from Byzantine attacks—data corruption, desynchronization, and delay—something that is not commonly addressed in conventional adaptive formation control techniques. Recognizing these threats, this research stresses the importance of developing robust fault-tolerant strategies to ensure the stability of the system in the presence of hostile actors. This contribution is important because it reveals a major gap in the current literature and at the same time provides a foundation for further developments in resilient multi-agent control.

Future work will aim to improve the proposed approach by integrating fault detection and isolation, and optimal control using reinforcement learning. This will aid the development of a comprehensive framework for resilient control of second-order nonlinear multi-agent systems, an area that has been predominantly focused on first-order systems. Thus, this research opens up new possibilities for the development of intelligent multi-agent systems that are robust and reliable in the context of potential attacks.

Author contributions

Asad Khan: Software, resources, project administration; Azmat Ullah Khan Niazi: Writing-review & editing, supervision; Saadia Rehman: Writing-original draft; Saba Shaheen: Data curation, writing-original draft, writing-review & editing; Taoufik Saidani: Conceptualization; Adnan Burhan Rajab: Formal analysis; Muhammad Awais Javeed: Validation, resources; Yubin Zhong: Supervision, project administration. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgements

This work has been carried out at the University of Lahore, Sargodha Campus. The authors are also grateful for the support from Guangzhou University, China, Northern Border University, Saudi Arabia, Knowledge University and Al-Kitab University Iraq.

The authors extend their appreciation to Northern Border University, Saudi Arabia, for supporting this work through project number (NBU-CRP-2025-2225). This research was also sponsored by the National Natural Science Foundation of China, (grant No. 12250410247), and from the Ministry of Science and Technology of China, (grant No. WGXZ2023054L).

Conflicts of interest

The authors declare they have no conflict of interest.

References

1. D. Maldonado, E. Cruz, J. A. Torres, P. J. Cruz, S. del Pilar, S. Gamboa, Multi-agent Systems: A survey about its components, framework and workflo, *IEEE Access*, **12** (2024), 80950–80975. https://doi.org/10.1109/ACCESS.2024.3409051
2. M. Abbasi, H. J. Marquez, Dynamic event-triggered formation control of multi-agent systems with non-uniform time-varying communication delays, *IEEE T. Autom. Sci. Eng.*, **22** (2025), 8988–9000. https://doi.org/10.1109/TASE.2024.3494658
3. X. L. Quan, R. J. Du, R. C. Wang, Z. S. Bing, Q. Shi, An efficient closed-loop adaptive controller for a small-sized quadruped robotic rat, *Cyborg and Bionic Systems*, **5** (2024), 0096. https://doi.org/10.34133/cbsystems.0096
4. L. H. Ji, Z. Q. Lin, C. J. Zhang, S. S. Yang, J. Li, H. Q. Li, Data-based optimal consensus control for multiagent systems with time delays: using prioritized experience replay, *IEEE T. Syst. Man Cy.*, **54** (2024), 3244–3256. https://doi.org/10.1109/TSMC.2024.3358293
5. Y. H. Sun, Z. N. Peng, J. P. Hu, B. K. Ghosh, Event-triggered critic learning impedance control of lower limb exoskeleton robots in interactive environments, *Neurocomputing*, **564** (2024), 126963. https://doi.org/10.1016/j.neucom.2023.126963

6. B. Ibrahim, H. Noura, Formation flight control of multi-UAV system using neighbor-based trajectory generation topology, *Wseas Transactions on Applied and Theoretical Mechanics*, **15** (2020), 173–181. https://doi.org/10.37394/232011.2020.15.20
7. J. P. Hu, B. Chen, B. K. Ghosh, Formation-circumnavigation switching control of multiple ODIN systems via finite-time intermittent control strategies, *IEEE T. Control Netw.*, **11** (2024), 1986–1997. https://doi.org/10.1109/TCNS.2024.3371597
8. A. Khan, A. U. K. Niazi, W. Abbasi, F. Awan, M. M. A. Khan, F. Imtiaz, Cyber secure consensus of fractional order multi-agent systems with distributed delays: Defense strategy against denial-of-service attacks, *Ain Shams Eng. J.*, **15** (2024), 102609. https://doi.org/10.1016/j.asej.2023.102609
9. H. T. Reda, A. Anwar, A. Mahmood, Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts, *Renew. Sust. Energy Rev.*, **163** (2022), 112423. https://doi.org/10.1016/j.rser.2022.112423
10. N. Suryanto, Y. Kim, H. Kang, H. T. Larasati, Y. Yun, T. T. H. Le, et al., DTA: Physical camouflage attacks using differentiable transformation network, In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, 15305–15314. `https://islab-ai.github.io/dta-cvpr2022/`
11. Y. S. Liu, W. X. Li, X. W. Dong, Z. Ren, Resilient formation tracking for networked swarm systems under Malicious data deception attacks, *Int. Jo. Robust Nonlin.*, **35** (2024), 2043–2052. https://doi.org/10.1002/rnc.7777
12. A. Khan, M. A. Javeed, A. U. K. Niazi, S. Rehman, W. U. Hassan, Y. B. Zhong, A robust control framework for multi-agent systems under Byzantine attacks using hybrid event-triggered techniques, *Ain Shams Eng. J.*, **15** (2024), 103149. https://doi.org/10.1016/j.asej.2024.103149
13. F. Ding, R. Wang, T. D. Zhang, G. Zheng, Z. X. Wu, S. Wang, Real-time trajectory planning and tracking control of bionic underwater robot in dynamic environment, *Cyborg and Bionic Systems*, **5** (2024), 0112. https://doi.org/10.34133/cbsystems.0112
14. J. F. Hao, P. Chen, J. Chen, X. Li, Effectively detecting and diagnosing distributed multivariate time series anomalies via Unsupervised Federated Hypernetwork, *Inform. Process. Manag.*, **62** (2025), 104107. https://doi.org/10.1016/j.ipm.2025.104107
15. Z. Wang, M. L. Chen, Y. L. Guo, Z. Li, Q. F. Yu, Bridging the domain gap in satellite pose estimation: A self-training approach based on geometrical constraints, *IEEE T. Aero. Elec. Sys.*, **60** (2023), 2500–2514. https://doi.org/10.1109/TAES.2023.3250385
16. H. B. Zeng, Z. J. Zhu, T. S. Peng, W. Wang, X. M. Zhang, Robust tracking control design for a class of nonlinear networked control systems considering bounded package dropouts and external disturbance, *IEEE T. Fuzzy Syst.*, **32** (2024), 3608–3617. https://doi.org/10.1109/TFUZZ.2024.3377799
17. D. B. Tong, B. Ma, Q. Y. Chen, Y. B. Wei, P. Shi, Finite-time synchronization and energy consumption prediction for multilayer fractional-order networks, *IEEE T. Circuits-II*, **70** (2023), 2176–2180. https://doi.org/10.1109/TCSII.2022.3233420
18. J. L. Guo, Y. K. Li, B. Huang, L. Ding, H. B. Gao, M. Zhong, An online optimization escape entrapment strategy for planetary rovers based on Bayesian optimization, *J. Field Robot.*, **41** (2024), 2518–2529. https://doi.org/10.1002/rob.22361

19. M. Shi, D. B. Tong, Q. Y. Chen, W. N. Zhou, Pth moment exponential synchronization for delayed multi-agent systems with Lévy noise and Markov switching, *IEEE T. Circuits-II*, **71** (2023), 697–701. https://doi.org/10.1109/TCSII.2023.3304635

20. X. Liu, S. C. Lou, W. Dai, Further results on "System identification of nonlinear state-space models", *Automatica*, **148** (2023), 110760. https://doi.org/10.1016/j.automatica.2022.110760

21. W. M. Wang, H. B. Zeng, J. M. Liang, S. P. Xiao, Sampled-data-based load frequency control for power systems considering time delays, *J. Franklin I.*, **362** (2025), 107477. https://doi.org/10.1016/j.jfranklin.2024.107477

22. J. X. Lv, X. Z. Ju, C. H. Wang, Neural network prescribed-time observer-based output-feedback control for uncertain pure-feedback nonlinear systems, *Expert Syst. Appl.*, **264** (2025), 125813. https://doi.org/10.1016/j.eswa.2024.125813

23. Z. S. Zhou, Y. F. Wang, G. F. Zhou, X. L. Liu, M. Y. Wu, K. P. Dai, Vehicle lateral dynamics-inspired hybrid model using neural network for parameter identification and error characterization, *IEEE T. Veh. Technol.*, **73** (2024), 16173–16186. https://doi.org/10.1109/TVT.2024.3416317

24. L. Fu, J. Q. Wang, X. W. Fu, G. L. Zhao, Finite-time Pade-based adaptive FNN controller implementation for microbial fuel cell with delay and multi-disturbance, *Int. J. Hydrogen Energ.*, **98** (2025), 1034–1043. https://doi.org/10.1016/j.ijhydene.2024.10.372

25. F. Z. Song, Y. Liu, Y. Dong, X. K. Chen, J. B. Tan, Motion control of wafer scanners in lithography systems: From setpoint generation to multi-stage coordination, *IEEE T. Instrum. Meas.*, **73** (2024), 7508040. https://doi.org/10.1109/TIM.2024.3413202

26. Y. Y. Liu, Q. L. Hu, G. Feng, Navigation functions on 3-manifold with boundary as a disjoint union of Hopf tori, *IEEE T. Automat. Contr.*, **70** (2025), 219–234. https://doi.org/10.1109/TAC.2024.3419817

27. B. Xu, X. Y. Wang, J. Zhang, Y. Guo, A. A. Razzaqi, A novel adaptive filtering for cooperative localization under compass failure and non-gaussian noise, *IEEE T. Veh. Technol.*, **71** (2022), 3737–3749. https://doi.org/10.1109/TVT.2022.3145095

28. Z. M. Zou, S. M. Yang, L. Zhao, Dual-loop control and state prediction analysis of QUAV trajectory tracking based on biological swarm intelligent optimization algorithm, *Sci. Rep.*, **14** (2024), 19091. https://doi.org/10.1038/s41598-024-69911-5

29. Y. F. Yin, Z. T. Wang, L. L. Zheng, Q. R. Su, Y. Guo, Autonomous UAV navigation with adaptive control based on deep reinforcement learning, *Electronics*, **13** (2024), 2432. https://doi.org/10.3390/electronics13132432

30. G. L. Jing, Y. F. Zou, M. H. Xu, Y. Q. Zhang, D. X. Yu, Z. G. Shan, et al., Nicaea: A Byzantine fault tolerant consensus under unpredictable message delivery failures for parallel and distributed computing, *IEEE T. Comput.*, **74** (2025), 915–928. https://doi.org/10.1109/TC.2024.3506856

31. H. L. Wei, H. Zhang, K. AI-Haddad, Y. Shi, Ensuring secure platooning of constrained intelligent and connected vehicles against Byzantine attacks: A distributed MPC framework, *Engineering*, **33** (2024), 35–46. https://doi.org/10.1016/j.eng.2023.10.007

32. J. A. V. Trejo, M. Adam-Medina, C. D. Garcia-Beltran, G. V. G. Ramírez, B. yolanda lópez Zapata, E. M. Sanchez-Coronado, et al., Robust formation control based on leader-following consensus in multi-agent systems with faults in the information exchange: Application in a fleet of unmanned aerial vehicles, *IEEE Access*, **9** (2021), 104940–104949. https://doi.org/10.1109/ACCESS.2021.3098303

33. S. Manfredi, Robust consensus design of uncertain multiagent systems with bounded gains and incremental nonlinear interactions, *IEEE T. Ind. Inform.*, **20** (2024), 11844–11853. https://doi.org/10.1109/TII.2024.3413319

34. H. Meng, D. H. Pang, J. D. Cao, Y. C. Guo, A. U. K. Niazi, Optimal bipartite consensus control for heterogeneous unknown multi-agent systems via reinforcement learning, *Appl. Math. Comput.*, **476** (2024), 128785. https://doi.org/10.1016/j.amc.2024.128785

35. Y. H. Lan, J. Y. Zhao, Improving track performance by combining padé-approximation-based preview repetitive control and equivalent-input-disturbance, *J. Electr. Eng. Technol.*, **19** (2024), 3781–3794. https://doi.org/10.1007/s42835-024-01830-x

36. X. Z. Ju, Y. S. Jiang, L. Jing, P. Liu, Quantized predefined-time control for heavy-lift launch vehicles under actuator faults and rate gyro malfunctions, *ISA T.*, **138** (2023), 133–150. https://doi.org/10.1016/j.isatra.2023.02.022

37. F. Ding, K. C. Zhu, J. Liu, C. Peng, Y. F. Wang, J. G. Lu, Adaptive memory event triggered output feedback finite-time lane keeping control for autonomous heavy truck with roll prevention, *IEEE T. Fuzzy Syst.*, **32** (2024), 6607–6621. https://doi.org/10.1109/TFUZZ.2024.3454344

38. S. B. Long, W. C. Huang, J. H. Wang, J. R. Liu, Y. X. Gu, Z. A. Wang, A fixed-time consensus control with prescribed performance for multi-agent systems under full-state constraints, *IEEE T. Autom. Sci. Eng.*, **22** (2025), 6398–6407. https://doi.org/10.1109/TASE.2024.3445135

39. G. X. Wen, C. Y. Zhang, P. Hu, Y. Cui, Adaptive neural network leader-follower formation control for a class of second-order nonlinear multi-agent systems with unknown dynamics, *IEEE Access*, **8** (2020), 148149–148156. https://doi.org/10.1109/ACCESS.2020.3015957

40. X. Xu, B. Li, Semi-global stabilization of parabolic PDE–ODE systems with input saturation, *Automatica*, **171** (2025), 111931. https://doi.org/10.1016/j.automatica.2024.111931

AIMS Press