eng

MDPI

Article

Detection-Guided Resilient Consensus Control for UAV Swarms Under Random Denial-of-Service Attacks

Yue Han [1,2], Meini Yuan [1,2], Zhiru Li [2], Jian Shen [1] and Pengyun Chen [1,2,*]

[1] School of Mechanical and Electrical Engineering, North University of China, Taiyuan 030051, China
[2] School of Aerospace Engineering, North University of China, Taiyuan 030051, China
* Correspondence: chenpengyun@nuc.edu.cn

Abstract

Reliable coordination of unmanned aerial vehicle (UAV) swarms is significantly challenged by random denial-of-service (R-DoS) attacks, which introduce stochastic packet loss, time-varying communication interruptions, and strong concealment. Existing fault-tolerant consensus approaches typically assume known attack information or treat attack detection, topology recovery, and control design as separate processes, resulting in limited resilience under dynamically evolving attack conditions. To address this issue, this paper proposes a detection-guided resilient consensus control framework for UAV swarms under R-DoS attacks. A dual-dimensional statistical detection method is developed by jointly modeling packet reception rate (PRR) and inter-arrival time (IAT), enabling real-time identification of attack-induced anomalies through spatio-temporal feature fusion. Based on the detection results, a distributed topology reconstruction strategy is designed, incorporating redundant node identification and cluster-based dynamic communication reconfiguration. The communication graph is adaptively updated via online adjustment of adjacency and Laplacian matrices, and robustness guarantees for the resulting consensus process are analytically established. Hardware-in-the-loop simulation experiments under both single-leader and multi-leader architectures demonstrate that the proposed method can accurately detect attacked nodes, effectively reconstruct the communication topology, and maintain stable formation coordination under severe R-DoS attacks. The position tracking error is constrained within 0.4 m, validating the effectiveness and robustness of the proposed framework. This study is limited to defensive cyber-resilience in a closed hardware-in-the-loop simulation environment and does not address reconnaissance payloads, weaponization, target selection, or operational attack execution. Unlike methods that assume known attack schedules or treat detection, topology recovery, and control separately, this study focuses on their online coupling under unknown random packet loss; its validation is limited to the stated closed HIL impairment model.

Keywords: UAV swarm; Random DoS attack; dual-dimensional joint detection; hierarchical tree topology; fault-tolerant control

Check for updates

Academic Editor: Antonio Gil Bravo

Received: 16 July 2026
Revised: 22 August 2026
Accepted: 28 August 2026
Published: 3 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Unmanned aerial vehicles (UAVs) have been widely deployed in disaster search and rescue, environmental monitoring, precision agriculture, and industrial inspection due to their high maneuverability, environmental adaptability, and flexible task execution capabilities. The effectiveness of UAV swarm cooperative control critically depends on the reliability and continuity of inter-agent communication networks. However, such

networked control systems are highly vulnerable to cyberattacks, among which denial-of-service (DoS) attacks—especially Random DoS (R-DoS) attacks characterized by strong randomness and concealment—pose significant threats. By randomly varying attack pulse intensity, duration, and intervals, R-DoS attacks introduce packet loss, communication delays, and transmission anomalies, which can severely degrade consensus performance and even lead to formation collapse and mission failure.

As UAV swarms are increasingly deployed in safety-critical civilian applications such as emergency response, wildfire monitoring, environmental surveying, and infrastructure inspection, their cybersecurity issues have attracted extensive attention [1–3]. Existing studies have investigated multiple types of attacks, including deceptive attacks [4–6], DoS attacks [7,8], and physical-layer interference [9,10]. Among these, DoS attacks, particularly R-DoS attacks with stochastic and covert characteristics, have become a major threat to the communication reliability of UAV swarm systems [11–13], potentially resulting in formation instability and mission failure [14,15].

In terms of theoretical modeling and analysis of DoS attacks, Amin et al. [16] systematically studied their impact on networked control systems within a secure control framework. De Persis et al. [17] further investigated input-to-state stability under DoS attacks and derived constraints on attack frequency and duration to guarantee system stability. Feng et al. [18] extended these studies to stochastic DoS scenarios. However, most existing work focuses on periodic or deterministic attack patterns and lacks effective mechanisms to capture the stochastic, time-varying, and highly concealed characteristics of R-DoS attacks.

From the perspective of attack detection, current methods mainly rely on single-dimensional indicators such as packet loss rate or communication interruption duration [19–21]. These approaches often fail to accurately characterize R-DoS attacks with random, intermittent, and multi-link coupling features, resulting in missed detections and false alarms. From the perspective of fault-tolerant control, existing methods can be broadly categorized into robust control approaches [22,23] and topology reconstruction approaches [24,25]. Robust control methods enhance system tolerance without requiring explicit attack detection but may sacrifice nominal performance, whereas topology reconstruction approaches dynamically adjust the communication structure based on detection results but often assume accurate attack information.

As a result, most existing studies treat attack detection, node isolation, topology reconstruction, and control design as separate processes. This separation leads to a critical limitation: the lack of an integrated closed-loop mechanism capable of rapidly identifying attacks, isolating compromised nodes, reconstructing communication topology, and updating control strategies in real time. This challenge becomes more prominent in multi-leader UAV swarm scenarios, where maintaining leader information reachability and ensuring hierarchical coordination under partial communication failures remain open problems.

Recent complementary studies address cooperative multi-AAV planning, multirate observation with multiple delays, swarm perception, cooperative localization, and trajectory tracking [26–30]. These developments improve planning and state/trajectory information, but they do not by themselves close the detection–reconfiguration–control loop considered here. Table 1 summarizes the distinction.

Table 1. Representative techniques and limitations relevant to the problem addressed here.

Category	Capability	Remaining Limitation	Refs.
DoS-resilient control	Maintains stability under specified attack/loss bounds	Often assumes attack bounds or separates detection and recovery	[16–18]
Detection/topology recovery	Identifies anomalies or restores connectivity	Single indicators and candidate-link selection may be insufficient	[19–25,31]
Planning, observers, localization, tracking	Improves task planning and state/trajectory quality	Does not directly provide R-DoS detection and graph repair	[26–30]
This work	Couples PRR–IAT detection, reconstruction, and consensus control	Limited to stated graph, calibration, delay, and HIL assumptions	Proposed

To address the above issues, this paper proposes a detection-guided resilient consensus control framework for UAV swarms based on Packet Reception Rate (PRR) [32] and Inter-Arrival Time (IAT) [33] dual-dimensional joint detection. The main contributions are summarized as follows:

(1) A PRR–IAT joint detector is developed with a dimensionless PRR threshold and an aggregate-stream IAT model, allowing online R-DoS indication without requiring a detailed UAV dynamic model.
(2) A multi-leader hierarchical communication topology and distributed redundant node identification algorithm are developed, including explicit link-quality and geometric screening criteria.
(3) A hierarchical cluster-based reconstruction strategy updates the adjacency/Laplacian matrices online and coordinates the consensus controller with node isolation, recovery verification, and optional re-entry.

2. Preliminaries

The communication topology of a UAV swarm with N nodes is modeled as a weighted directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \boldsymbol{A})$ [34–36], where $\mathcal{V} = \{1, 2, \ldots, N\}$ is the node set, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the edge set representing communication links, and $\boldsymbol{A} = [A_{ij}] \in \mathbb{R}^{N \times N}$ is the adjacency matrix. An edge $(j, i) \in \mathcal{E}$ indicates that node i can receive information from node j. The adjacency matrix element satisfies $A_{ij} = 1$ if $(j, i) \in \mathcal{E}$, $A_{ij} = 0$ otherwise, and self-loops are excluded, i.e., $A_{ii} = 0$. The neighbor set of node i is defined as $\mathcal{N}_i = \{j \in \mathcal{V} | (j, i) \in \mathcal{E}\}$. The in-degree of node i is defined as:

Clarification for the spectral analysis: the routing relation may be directed, whereas a control edge is admitted only after the bidirectional verification in Algorithm 1. The effective control adjacency is therefore symmetrized ($a_{ij} = a_{ji}$), and all positive-semidefinite, square-root, and ordered-eigenvalue statements below refer to this effective undirected graph.

$$d_i = \sum_{j=1}^{N} A_{ij} \tag{1}$$

The degree matrix is $\boldsymbol{D} = \mathrm{diag}(d_1, d_2, \ldots, d_N)$. The Laplacian matrix of the graph $\mathcal{G}$ is defined as:

$$\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{A} \tag{2}$$

For the bidirectionally verified effective graph, $\boldsymbol{A} = \boldsymbol{A}^{\mathrm{T}}$ and $\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{A}$ are positive-semidefinite. Its eigenvalues are real and nonnegative; for a connected effective graph, the zero eigenvalue is simple and $\lambda_2(L) > 0$ is the algebraic connectivity. These properties are not asserted for a general nonsymmetric directed Laplacian.

Algorithm 1: Neighbor Node Identification Algorithm

```
// Input: Node i info (ID_i, cluster ID_cluster, level level_i, link threshold Q_th, wait time t0)
// Output: Local neighbor table neighbor_table_i of node i
    Function AdjacentNodeRecognition(ID_i, ID_cluster, level_i, Q_th, t0):
    neighbor_table_i = []
    response_packets = []
    start_time = GetCurrentTime()
// 1. Broadcast neighbor discovery request to assigned cluster
    BroadcastToCluster(ID_cluster, {node_id:ID_i, cluster_id:ID_cluster, level:level_i, Q_th:Q_th})
// 2. Receive and filter response packets meeting link threshold within timeout
    While GetCurrentTime()-start_time < t0 and HasNewPacket():
    pkt = ReceivePacket()
    if pkt[link_quality] >= Q_th: response_packets.append(pkt)
// 3. Hash deduplication + bidirectional verification + build neighbor table
    unique_pkts = RemoveDuplicates(response_packets, Hash)
    for pkt in unique_pkts:
    if SendVerifyAndWaitAck(pkt[node_id], ID_i):
    neighbor_table_i.append({node_id:pkt[node_id], cluster_id:pkt[cluster_id],
    level:pkt[level], link_quality:pkt[link_quality]})
// 4. Synchronize neighbor table to cluster shared data area
    SyncToClusterDataArea(ID_cluster, neighbor_table, ID_i, neighbor_table_i)
Return neighbor_table_i
```

Definition 1 (Spanning Tree). *A directed graph $\mathcal{G}$ contains a spanning tree if there exists a root node $r \in \mathcal{V}$ such that every other node in $\mathcal{V}$ has a directed path from r. For leader–follower consensus, the existence of a spanning tree rooted at the leader node is a necessary condition for consensus convergence.*

Definition 2 (Strong Connectivity). *A directed graph $\mathcal{G}$ is strongly connected if for every pair of nodes $i, j \in \mathcal{V}$, there exists a directed path from i to j and a directed path from j to i. In the multi-leader hierarchical tree topology, each cluster sub-topology is required to maintain connectivity of its effective control graph to guarantee state information reachability.*

3. R-DoS Attack Joint Detection Mechanism Based on PRR–IAT Dual Dimensions

For leader–follower UAV swarms, all nodes periodically transmit data over the same wireless communication channel, while communication and computing resources are limited. In this study, R-DoS is represented only by its observable network effects—stochastic packet loss, intermittent communication interruption, and abnormal packet timing—rather than by a real-world attack implementation. Such effects may arise from generic traffic flooding, selective link disruption, or packet filtering; however, no intrusion procedure, exploit code, access method, radio-frequency interference configuration, or mission-specific operational detail is developed or disclosed. The resulting anomalies are summarized by a sudden decrease in PRR and abnormal IAT fluctuation [34], which are used solely as defensive detection indicators.

3.1. PRR Detection Model

As one of the quantitative indicators of inter-node communication link transmission quality, abnormal fluctuations in PRR can directly reflect data transmission anomalies caused by R-DoS attacks. Within time window T_w, the mathematical expression for PRR is given by Equation (3)

$$PRR = N/N_{total} \tag{3}$$

where N is the total number of packets successfully received by the receiving node within time window T_w, and N_{total} is the total number of packets sent by the corresponding sending node within T_w.

When the UAV swarm is in normal communication state, PRR remains stable and above the preset threshold. When a node in the swarm is under R-DoS attack, the packet loss rate of that node increases sharply, causing N to decrease significantly, leading to the PRR value falling markedly below the preset threshold. To avoid false alarms caused by inherent network fluctuations, a statistical model for PRR needs to be constructed, and the normal fluctuation range of PRR determined through a confidence interval. When the PRR value falls below the lower bound of the confidence interval, it can be determined as a communication anomaly caused by R-DoS attacks; when the PRR value exceeds the upper bound of the confidence interval, potential deceptive attack behavior should be suspected.

Assuming that the UAV swarm network is not subject to DoS attacks, strong electromagnetic interference, extreme weather, or other sudden environmental disasters, and that the UAV swarm hardware is intact and fault-free, then the packet transmission success events of each node are mutually independent. Based on the above assumptions, within a fixed time window T_w, the number of packet transmission failures K of a single node follows a binomial distribution $K = B(n,\ p)$, where n is the total number of packet transmissions initiated by the node within T_w, and p is the probability of a single transmission failure. Since the computational complexity of the binomial distribution is high, it can be approximated as follows according to the approximation principle of probability statistics:

(1) When $p \to 0$ and $n \to \infty$, the binomial distribution can be approximated as a Poisson distribution $P(\lambda) = np$, applicable to scenarios with normal UAV swarm communication and low packet loss rates.
(2) When $np > 10$, the binomial distribution can be approximated as a normal distribution $N(\mu, \sigma^2)$, applicable to scenarios with a high UAV swarm communication load and relatively high packet loss rates.

For the actual communication scenario of UAV swarms, a normal distribution is used to statistically model PRR. The specific steps are as follows:

(1) Use m trusted initialization windows ($m > 30$ when the normal approximation is used). If an attack is suspected during startup, adaptation is frozen and a stored commissioning threshold or conservative design threshold is used; without either baseline, the detector remains UNCALIBRATED and does not declare a healthy adaptive threshold.
(2) Based on the sampled data, calculate the mean $\overline{N}$, sample mean μ, and sample standard deviation S of the successfully received packet counts as follows:

$$\mu = \frac{1}{m}\sum_{i=1}^{m} N_i,\ S = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}\left(N_i - \overline{N}\right)^2} \tag{4}$$

(3) Calculate the mean reception ratio $\overline{PRR} = \overline{N}/n_w$, where n_w is the fixed number of scheduled packets per window. Dividing the count dispersion S by n_w gives dimensionless $3S/n_w$ and $6S/n_w$ PRR intervals:

$$\overline{PRR} = \frac{\overline{N}}{n_w}, \quad \overline{PRR} - \frac{3S}{n_w} < PRR < \overline{PRR} + \frac{3S}{n_w}, \quad \overline{PRR} - \frac{6S}{n_w} < PRR < \overline{PRR} + \frac{6S}{n_w} \tag{5}$$

During initialization or low-loss operation, the count model is supplemented by a one-sided upper confidence bound on the normal packet-failure probability. This correction is used only to obtain a dimensionless lower PRR threshold; it is not interpreted as a confidence interval for successful-packet counts.

(1) If inter-loss times are approximated as exponential, $\hat{\lambda} = k_f / \sum_i t_i$ estimates the loss-event rate from k_f failures, so $\hat{\lambda} T_w$ is the expected number of loss events in a window, not the number of successfully received packets.

(2) Combining the approximation relationship between the binomial distribution and the Poisson distribution:

$$P(K \le k) \approx \sum_{i=0}^{k} \frac{(\lambda)^i e^{-\lambda}}{i!} \tag{6}$$

(3) Using k_f observed failures among n scheduled transmissions, define the exact one-sided $(1-\alpha)$ Clopper–Pearson upper bound p_U on the normal failure probability. Here, I^{-1} denotes the inverse regularized incomplete beta function:

$$p_U = \begin{cases} I^{-1}_{1-\alpha}(k_f + 1, n - k_f), & k_f < n, \\ 1, & k_f = n. \end{cases} \tag{7}$$

(4) The corrected attack threshold is the corresponding lower bound on packet reception probability:

$$\mu_\alpha = 1 - p_U \tag{8}$$

If the dimensionless monitored PRR falls below the dimensionless threshold μ_α, the PRR channel is declared abnormal.

3.2. IAT Detection Model

Each individual node transmits periodically. The IAT detector is applied to the aggregate authenticated arrival stream formed by many nodes with independent clock phases, access delays, and jitter; for this aggregate stream, an exponential IAT model is used as a calibrated engineering approximation rather than as an exact per-node periodic-arrival law. The approximation and its prediction limits are checked during initialization.

$$P(T < t) = \begin{cases} 1 - e^{-\lambda t}, & t \ge 0 \\ 0, & t < 0 \end{cases} \tag{9}$$

where λ is the rate parameter reflecting the packet arrival rate. A larger λ indicates more frequent packet arrivals and smaller IAT values, and λ is positively correlated with the communication frequency of the UAV swarm. When under R-DoS attack, the attacker injects large numbers of meaningless attack packets into the communication channel, disrupting the arrival rhythm of legitimate packets. This mainly manifests as two types of IAT anomalies: (1) high-frequency injection of attack packets significantly shortens the arrival intervals of some legitimate packets, with IAT values far below the normal level; and (2) attack packets blocking the channel cause legitimate packet transmission delays,

with IAT values far above the normal level. Both types of anomalies cause the distribution characteristics of IAT to deviate from the exponential distribution. By monitoring the deviation of IAT values from the exponential distribution model, R-DoS attacks can be identified. Based on the exponential distribution model of IAT, the normal fluctuation interval of IAT is determined according to significance level α. When the monitored *IAT* value exceeds this interval, communication anomaly is determined. The specific threshold calculation process is as follows:

(1) From aggregate IAT samples $t_1, t_2, \ldots, t_n$, estimate λ by $\hat{\lambda} = n/\sum_{i=1}^{n} t_i$. The exponential approximation is retained only when a goodness-of-fit check on the trusted initialization data is passed.

(2) For a plug-in rate $\hat{\lambda}$ and a central prediction probability $1 - \alpha$, the exponential CDF and survival function give:

$$t_{\text{low}} = -\frac{\ln(1-\alpha/2)}{\hat{\lambda}}, \quad t_{\text{high}} = -\frac{\ln(\alpha/2)}{\hat{\lambda}} \tag{10}$$

(3) Parameter uncertainty is handled separately. Let λ_L and λ_U be the chi-squared confidence limits for the rate; substituting the conservative endpoints into the prediction limits gives:

$$\lambda_L = \frac{\chi^2_{2n,\alpha/2}}{2\sum_{i=1}^{n} t_i}, \quad \lambda_U = \frac{\chi^2_{2n,1-\alpha/2}}{2\sum_{i=1}^{n} t_i}, \quad t'_{\text{low}} = -\frac{\ln(1-\alpha/2)}{\lambda_U}, \quad t'_{\text{high}} = -\frac{\ln(\alpha/2)}{\lambda_L} \tag{11}$$

The interval $[t'_{\text{low}}, t'_{\text{high}}]$ is a conservative prediction interval for an individual aggregate-stream IAT after accounting for rate-estimation uncertainty; it is not described as a confidence interval for an observation.

3.3. PRR–IAT Dual-Dimensional Joint Detection Strategy

PRR detection is based on the statistical features of packet quantity, with a low false alarm rate but limited feature capture ability for attacks, unable to identify *IAT* anomalies caused by some low-intensity R-DoS attacks. IAT detection is based on the distribution features of packet inter-arrival times, with high sensitivity to attacks but susceptibility to inherent network fluctuations, resulting in a higher false alarm rate. To compensate for the limitations of single-dimensional detection, this section proposes a PRR–IAT dual-dimensional joint detection strategy with spatio-temporal feature fusion, integrating the spatial features of PRR with the temporal features of IAT, formulating a multi-rule joint decision mechanism to achieve accurate, real-time identification of R-DoS attacks. The core advantage of this strategy is that it does not rely on precise UAV swarm system models, adapts to dynamic changes in attack features through dynamic threshold adjustment, and can flexibly adjust threshold parameters to meet the detection accuracy requirements of different swarm systems.

The basic principle of PRR–IAT dual-dimensional joint detection is embodied in three aspects of collaborative design, with the two exhibiting strong feature complementarity. PRR is the dimensionless fraction of scheduled packets successfully received within a detection window and mainly captures the surge in packet loss caused by R-DoS attacks; IAT reflects the arrival interval of adjacent packets and mainly captures the traffic burst features caused by R-DoS attacks. Therefore, PRR–IAT dual-dimensional joint detection can comprehensively characterize the communication anomaly features of R-DoS attacks from both temporal and spatial dimensions. Meanwhile, the detection thresholds of both PRR and IAT are dynamically adjusted based on real-time monitored sample data, and keeping their time windows T_w consistent ensures temporal consistency of detection

results. In addition, the PRR–IAT dual-dimensional joint detection adopts a logic of PRR primary decision + IAT auxiliary verification, combined with historical detection data for comprehensive determination, which can effectively reduce missed detection and false alarm probabilities.

Let $A_P(t) = \mathbf{1}\{PRR(t) < \mu_\alpha\}$ and $A_I(t) = \mathbf{1}\left\{IAT(t) \notin [t'_{\text{low}}, t'_{\text{high}}]\right\}$. With window T_w and k required consecutive PRR violations, the joint decision is:

$$D(t) = \mathbf{1}\left\{A_P(t)A_I(t) = 1 \ \vee \ \prod_{r=0}^{k-1} A_P(t - rT_w) = 1\right\} \tag{12}$$

where $D(t) = 1$ indicates that an R-DoS attack is detected at time t, and $D(t) = 0$ indicates normal communication. The specific joint detection rules are:

(1) Rule 1: If $PRR < \mu_\alpha$ and $IAT \notin [t'_{low}, t'_{high}]$ are monitored in the current time window, then $D(t) = 1$, determining that the swarm is under R-DoS attack, immediately triggering attack warning and fault-tolerant control commands.

(2) Rule 2: If $PRR < \mu_\alpha$ but $IAT \in [t'_{low}, t'_{high}]$ is monitored in the current time window, continuous monitoring is initiated. If $PRR < \mu_\alpha$ is satisfied for k consecutive time windows, then $D(t) = 1$, determining that the swarm is under R-DoS attack, triggering a warning. If PRR recovers to normal levels during continuous monitoring, then $D(t) = 0$, determined as a transient network fluctuation, and no warning is triggered.

(3) Rule 3: An IAT-only anomaly with $PRR > \mu_\alpha$ does not cause immediate isolation. It is recorded in a rolling K-window suspicion counter; h or more timing anomalies in that horizon trigger enhanced monitoring and an alarm. This cumulative branch reduces the risk that an ultra-low-frequency, high-variance attack repeatedly passes as isolated jitter.

(4) Rule 4: If $PRR > \mu_\alpha$ and $IAT \in [t'_{low}, t'_{high}]$ are monitored in the current time window, then $D(t) = 0$, determining that the swarm is in normal communication state.

In the above rules, the number of consecutive anomaly determinations k can be flexibly adjusted according to the actual application scenario of the UAV swarm. A larger k leads to higher detection accuracy but reduced real-time performance.

4. Dynamic Fault-Tolerant Control of UAV Swarms Based on Hierarchical Tree Topology

When the PRR–IAT dual-dimensional joint detection mechanism determines that the UAV swarm is under R-DoS attack, some nodes' communication links will fail due to packet loss and transmission delays. Traditional UAV swarm consensus control uses static communication topology with fixed adjacency matrices and Laplacian matrices. Communication link failures cause interruption of inter-node state information exchange, destroying the convergence of consensus control protocols, which in turn leads to formation control deviations.

To address the above problems, this section constructs a consensus fault-tolerant control system for UAV swarms under R-DoS attacks and proposes a dynamic fault-tolerant control method based on hierarchical tree topology. This method, based on consensus control, achieves adaptive repair of the communication network after attacks through hierarchical tree topology design, distributed redundant node identification, and hierarchical dynamic topology reconstruction, enabling online updates of the adjacency matrix and Laplacian matrix based on communication link status, thereby online adjusting the consensus control law. This ensures that UAV swarms, even under R-DoS attacks, can maintain consensus control accuracy of position, velocity, and acceleration, and guarantee the integrity of formation configuration and continuity of task execution.

4.1. UAV Swarm Consensus Control Model

To adapt to the design requirements of distributed consensus control, the UAV dynamics model is reasonably simplified by taking position, velocity, and acceleration as state variables, constructing a simplified third-order dynamics model [37] for the UAV swarm:

$$\begin{cases} \dot{\boldsymbol{x}}_i = \boldsymbol{v}_i \\ \dot{\boldsymbol{v}}_i = \boldsymbol{a}_i \\ \dot{\boldsymbol{a}}_i = \boldsymbol{u}_i \end{cases} \tag{13}$$

where $\boldsymbol{x}_i = [x_i, y_i, z_i]^\top$, $\boldsymbol{v}_i = [\dot{x}_i, \dot{y}_i, \dot{z}_i]^\top$, $\boldsymbol{a}_i = [\ddot{x}_i, \ddot{y}_i, \ddot{z}_i]^\top$ are, respectively, the position, velocity vector, and acceleration vector of the i-th UAV in the swarm, and $\boldsymbol{u}_i$ is the control input vector for consensus control. For the above simplified dynamics model, a distributed consensus control protocol based on a leader–follower mode is designed. The core idea of the protocol is that each follower node adjusts its control input based on state deviations between itself and its neighbor nodes through information exchange, driving all the nodes' positions, velocities, and accelerations to converge to the state of the leader node.

Assume the swarm contains N UAV nodes, with the first M ($1 \leq M < N$) nodes as leader nodes forming leader node group $\mathcal{L} = \{1, 2, \ldots, M\}$, and the remaining $N - M$ nodes as follower nodes $\mathcal{F} = \{M+1, M+2, \ldots, N\}$. Leader nodes move cooperatively along preset mission trajectories; their states $\boldsymbol{x}_l, \boldsymbol{v}_l, \boldsymbol{a}_l$ ($l \in \mathcal{L}$) are not affected by follower nodes, and their control inputs are trajectory planning commands. Follower nodes converge toward the state of their assigned leader node by adjusting control inputs based on state deviations through information exchange with neighbor nodes. For the multi-leader architecture, a distributed consensus control protocol is designed. For node i, $i = 1, 2, \ldots, N$, the control protocol is given by Equation (14):

$$u_i = \begin{cases} u_{i,\mathrm{ref}}, & i \in \mathcal{L}, \\ u_{\ell(i),\mathrm{ref}} - \gamma_1 \sum\limits_{j \in \mathcal{N}_i} A_{ij}(\boldsymbol{x}_i - \boldsymbol{x}_j) - \gamma_2 \sum\limits_{j \in \mathcal{N}_i} A_{ij}(\boldsymbol{v}_i - \boldsymbol{v}_j) - \gamma_3 \sum\limits_{j \in \mathcal{N}_i} A_{ij}(\boldsymbol{a}_i - \boldsymbol{a}_j), & i \in \mathcal{F}. \end{cases} \tag{14}$$

where $\boldsymbol{u}_{i,ref}$ is the leader reference input and $u_{\ell(i),\mathrm{ref}}$ is the input of follower i's assigned leader. The added feedforward term cancels $u_{\ell(i),\mathrm{ref}}$ in $\dot{e}_{a,i} = u_i - u_{\ell(i),\mathrm{ref}}$, so the error dynamics remain homogeneous for the nonzero-jerk trajectories used in Section 5. The remaining notation and gains are unchanged.

$$\boldsymbol{e}_i = \begin{bmatrix} \boldsymbol{x}_i - \boldsymbol{x}_l \\ \boldsymbol{v}_i - \boldsymbol{v}_l \\ \boldsymbol{a}_i - \boldsymbol{a}_l \end{bmatrix}, \; i \in \mathcal{F}, l \in \mathcal{L} \tag{15}$$

where $\boldsymbol{e}_i \in \mathbb{R}^9$ is the state error of follower node i relative to its assigned leader node l, and $\boldsymbol{x}$, $\boldsymbol{v}$, $\boldsymbol{a}$ are all three-dimensional vectors. Define the global state error matrix $\boldsymbol{E}$ as:

$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{e}_{M+1}^\top & \boldsymbol{e}_{M+2}^\top & \cdots & \boldsymbol{e}_N^\top \end{bmatrix}^\top \in \mathbb{R}^{9(N-M)} \tag{16}$$

Let L_F be the follower-subgraph Laplacian and B the diagonal leader-pinning matrix. The grounded Laplacian used in the stability analysis is:

$$H = L_F + B = H^T \succ 0 \tag{17}$$

Because H is really symmetric, an orthogonal eigenvector transformation decouples the stacked third-order error dynamics. For every $\lambda \in \sigma(H)$, the modal characteristic polynomial is:

$$p_\lambda(s) = s^3 + \gamma_3\lambda s^2 + \gamma_2\lambda s + \gamma_1\lambda \tag{18}$$

The cubic Routh–Hurwitz criterion gives asymptotic convergence of every mode under the following sufficient conditions:

Delay coupling: the conservative PRR-only detection interval is kT_w and reconstruction takes Δt_{rec}, so $\tau_{\max} = kT_w + \Delta t_{\text{rec}}$. During this finite interval, $\|e(t_a + \tau_{\max})\|$ is bounded by $\exp(\|A_d\|\tau_{\max})\|e(t_a)\| + [\exp(\|A_d\|\tau_{\max}) - 1]\bar{d}/\|A_d\|$ for bounded pre-reconstruction dynamics A_d and disturbance $\bar{d}$. Thus T_w and Δt_{rec} must be selected jointly against the mission error limit.

$$\gamma_1 > 0, \quad \gamma_2 > 0, \quad \gamma_3 > 0, \quad \gamma_2\gamma_3\lambda_{\min}(H) > \gamma_1 \tag{19}$$

4.2. UAV Swarm Hierarchical Tree Communication Topology

The multi-leader hierarchical tree topology takes the leader node group as the top-level core and performs hierarchical division according to the principles of leader clustering, master–slave communication, and local connectivity, constructing an m-layer tree communication network. The specific division rules are as follows: The parent–child hierarchy is a logical routing structure; every edge used by the spectral control analysis is bidirectionally verified and represented symmetrically.

(1) Leader node layer: Contains all leader nodes $\mathcal{L} = \{1, 2, \ldots, M\}$, serving as the top-level core of the entire tree topology. Direct communication links are established between every pair of leader nodes, forming a connected leader node sub-topology responsible for motion control, trajectory planning, and state information distribution of their respective clusters, while achieving cooperative motion of the leader node group. Each leader node serves as the core of a cluster, corresponding to a follower node sub-cluster.

(2) Intermediate node layer: Internal node layer. Nodes at the j-th layer ($2 \leq j < m - 1$) are follower nodes, labeled $u_{j1}, u_{j2}, \ldots, u_{jb_j}$, where $\mathrm{b_j}$ is the number of nodes at the j-th layer. Each intermediate node establishes a direct communication link with only one parent node in the layer above, and simultaneously establishes direct communication links with several child nodes in the layer below, achieving hierarchical transmission of state information.

(3) Leaf node layer: Terminal follower node layer. Nodes are labeled $u_{m1}, u_{m2}, \ldots, u_{mb_m}$. Each node establishes a direct communication link with only one parent node in the layer above, with no child nodes in the layer below. Leaf nodes all belong to a cluster of a certain leader node, obtaining state information of the assigned leader node through hierarchical links. The total number of nodes in the entire multi-leader hierarchical tree topology satisfies the constraint:

$$M + b_2 + b_3 + \ldots + b_m = N \tag{20}$$

Combining the clustering characteristics and hierarchical structure of the multi-leader hierarchical tree topology, three core definitions are clarified that are fully compatible with the single-leader scenario: (1) Internal nodes, referring collectively to leader nodes and follower nodes in the intermediate node layer. Leader nodes handle cluster core control and swarm coordination functions; intermediate layer follower nodes handle information relay within clusters. (2) Communication-redundant nodes, specifically referring to follower nodes in the intermediate node layer that have no child nodes in the next layer

and do not affect the connectivity of the cluster, providing link backups for fault-tolerant control. (3) Cluster sub-topology, the local tree topology rooted at a single leader node. Each cluster is independent and interconnected through the leader node group, enhancing swarm anti-interference capability. The topology communication relationships are quantitatively represented using adjacency matrix $\boldsymbol{A}$ and Laplacian matrix $\boldsymbol{L}$. Core definitions are consistent with the preceding text. The leader node layer achieves full connectivity to ensure swarm coordination. For each connected effective cluster, the Laplacian has one zero eigenvalue, while the corresponding grounded Laplacian is positive definite under leader pinning.

4.3. Distributed Communication-Redundant Node Identification Algorithm

The distributed communication-redundant node identification algorithm adapted for the multi-leader cluster architecture uses a mode of cluster-independent execution and global aggregation synchronization. Each node autonomously completes neighbor node identification and self-state determination without requiring central-node centralized control, and the identification processes of each cluster sub-topology do not interfere with each other. This both ensures identification efficiency and enhances algorithm robustness and scalability, suitable for large-scale multi-leader UAV swarms. The algorithm is divided into two core stages: neighbor node identification and redundant node screening. The pseudocode for its execution process is as follows:

(1) Neighbor Node Identification Algorithm Pseudocode

(2) Redundant Node Screening Algorithm Pseudocode (Algorithm 2)

Algorithm 2: Redundant Node Screening Algorithm

```
// Input: Node i info (ID_i, ID_cluster, level_i, total layers m), local neigh-bor_table_i
// Output: Redundancy status is_redundant of node i
    Function RedundantNodeFiltering(ID_i, ID_cluster, level_i, m, neighbor_table_i):
// 1. Non-redundant determination: leaf node / has child node / critical relay node
    if level_i == m or HasChildNode(neighbor_table_i, level_i, ID_cluster) or
IsCriticalRelay(ID_i, ID_cluster): Return False
// 2. Mark as redundant node, upload info to cluster shared data area
    redundant_info = {node_id:ID_i, cluster_id:ID_cluster, level:level_i, sta-tus:available}
    UploadToClusterDataArea(ID_cluster, redundant_node, redundant_info)
// 3. Cluster master node aggregates deduplication, synchronizes to global data area
    if IsClusterMaster(ID_i):
    cluster_redundant_list = GetUniqueList(GetAllFromClusterDataArea(ID_cluster,
redundant_node))
    SyncToGlobalDataArea(global_redundant_list, cluster_redundant_list)
Return True
```

In the execution process of the above algorithms, candidate links must pass a bidirectional handshake, distance $d_{ir} \le r_c$, delay $\tau_{ir} \le \tau_{\text{link}}$, and PRR/SNR floors. Feasible nodes are ranked by $Q_{ir} = w_1 PRR_{ir} + w_2 SNR_{ir}^n + w_3(1 - d_{ir}/r_c) + w_4(1 - \tau_{ir}/\tau_{\text{link}}) + w_5 E_r^n$, with $\sum_j w_j = 1$; the highest score satisfying $Q_{ir} \ge Q_{\text{th}}$ and the connectivity test is selected.

4.4. Hierarchical Dynamic Topology Reconstruction Rules for R-DoS Attacks in UAV Swarms

When the PRR–IAT dual-dimensional joint detection mechanism determines that a node in the swarm is under R-DoS attack, the system immediately activates the dynamic topology reconstruction mechanism. The core objective is to cut off all communication

links of failed nodes, simultaneously activate the corresponding cluster and global redundant nodes, establish new communication links, update the adjacency matrix and Laplacian matrix, and verify and ensure connectivity of the leader layer and each effective cluster graph.

For the hierarchical features and clustering characteristics of the multi-leader UAV swarm hierarchical tree topology, hierarchical cluster-based dynamic topology reconstruction rules can be formulated. Based on the type and layer of the attacked node, differentiated reconstruction strategies are adopted to verify and ensure that the reconstructed topology still meets the connectivity requirements of multi-leader swarm consensus control, and to ensure that the reconstruction process is simple and efficient. Each cluster sub-topology can independently execute reconstruction operations, triggering global swarm reconstruction only when the leader node layer is under attack, improving system reconstruction efficiency. Before formulating reconstruction rules, the following assumptions are made:

Assumption 1. *There exists a scenario where a single node q in the UAV swarm is under R-DoS attack. The cluster to which q belongs is $\mathcal{L}_q$, and q's layer is l_q. After being attacked by R-DoS, q's PRR value will continuously fall below threshold μ_α, and communication links are completely failed. The number of leader nodes in the swarm $M \geq 2$; when $M = 1$, the framework can degenerate to a single-leader scenario.*

4.4.1. General Procedure for Topology Reconstruction

In the UAV swarm, regardless of whether the attacked node is a leader or follower node, topology reconstruction follows the principles of cluster-independent reconstruction and global coordination guarantee to ensure the standardization of the reconstruction process. To accommodate the independence requirements of the cluster architecture, the general steps for topology reconstruction are designed as follows:

(1) Link severance and cluster localization: The system notifies all nodes via broadcast mechanism to immediately cut off all direct communication links with the attacked node q, and delete q from the local neighbor tables of all nodes. Let the adjacency matrix before topology reconstruction be $\boldsymbol{A}_{\text{old}}$. After cutting off all communication links of q, the adjacency matrix is updated as shown in Equation (21), where $\boldsymbol{e}_q$ is a unit basis vector. Simultaneously, based on q's cluster ID, locate the cluster $\mathcal{L}_q$ to which q belongs and initiate the local reconstruction process of cluster $\mathcal{L}_q$. If the attacked node is a leader node, global reconstruction of the swarm needs to be initiated.

$$\boldsymbol{A}_{\text{del}} = \boldsymbol{A}_{\text{old}} - \boldsymbol{e}_q \boldsymbol{e}_q^\top \boldsymbol{A}_{\text{old}} - \boldsymbol{A}_{\text{old}} \boldsymbol{e}_q \boldsymbol{e}_q^\top \tag{21}$$

(2) Cluster status update: All nodes in the cluster to which the attacked node belongs re-execute the neighbor node identification algorithm, update the local neighbor tables, and synchronize the updated neighbor tables to the cluster shared data area. When the leader node layer is attacked, all leader nodes synchronize updated neighbor tables to the swarm global data area.

(3) Redundant node activation: The master control module selects available redundant nodes in the same cluster, same layer, or adjacent layer as the attacked node q from the cluster-redundant node list (if a follower node is attacked) or the swarm-global redundant node list (if a leader node is attacked), and marks them as reconstruction backup nodes.

(4) Hierarchical cluster reconstruction: Based on the type and layer of the attacked node, execute the corresponding hierarchical cluster reconstruction strategy to re-establish communication links. Let the activated redundant node be r, and establish new links

for child nodes C_q. The link association matrix is $\boldsymbol{B} \in \mathbb{R}^{N\times N}$, where $b_{ir} = 1$ indicates that node $i \in C_q$ has a new link with r, and the rest are 0.

(5) Matrix hierarchical update: The global adjacency matrix after reconstruction is:

$$\boldsymbol{A}_{\text{new}} = \boldsymbol{A}_{\text{del}} + \boldsymbol{B} + \boldsymbol{B}^{\top} \tag{22}$$

From the Laplacian matrix definition $\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{A}$, the diagonal elements of the reconstructed degree matrix D_{new} are:

$$d_{ii} = \sum_{j=1}^{N} A_{ij,new} \tag{23}$$

Therefore, the global Laplacian matrix after reconstruction is:

$$\boldsymbol{L}_{\text{new}} = \boldsymbol{D}_{\text{new}} - \boldsymbol{A}_{\text{new}} \tag{24}$$

The updated $\boldsymbol{A}_{\text{new}}$ and $\boldsymbol{L}_{\text{new}}$ are synchronized to the corresponding clusters and all nodes, providing core matrix parameters for online adjustment of the consensus control law.

(6) Adaptive adjustment of control law: Each node online adjusts the consensus control gains γ_1, γ_2, γ_3 based on the updated Laplacian matrix combined with the convergence conditions in Equation (19), and updates the control law. When the leader node layer is attacked, the leader node group synchronously adjusts the cooperative control strategy to achieve fault-tolerant control.

4.4.2. Connectivity Verification for Topology Reconstruction

The core objective of topology reconstruction is to repair communication links damaged by R-DoS attacks and ensure that the reconstructed topology still meets the connectivity requirements of multi-leader swarm consensus control. Therefore, connectivity verification is a key concluding step of the topology reconstruction process and directly determines whether the reconstruction is effective.

After completing the updates of adjacency matrix $\boldsymbol{A}_{\text{new}}$ and Laplacian matrix $\boldsymbol{L}_{\text{new}}$, connectivity verification needs to be conducted from two dimensions. The verification formulas are embedded directly into the verification logic as follows: First, verify the connectivity of the leader node group. The connectivity of the leader node group, as the control core of the swarm, is a prerequisite for overall swarm consistency. The verification standard is that the rank of the leader node group Laplacian matrix $\boldsymbol{L}_{\mathcal{L},new}$ satisfies:

$$rank(\boldsymbol{L}_{\mathcal{L},new}) = M - 1 \tag{25}$$

where M is the number of leader nodes in the swarm. Equation (25) intuitively shows that there are no isolated nodes within the leader node group and effective communication coordination can be achieved between nodes. Second, verify the connectivity of each effective cluster graph. The connectivity of a cluster, as the basic component unit of the swarm, is a guarantee of state information transmission between follower nodes and leader nodes. The verification standard is that the rank of each cluster's Laplacian matrix $\boldsymbol{L}_{k,new}$ satisfies:

$$rank(\boldsymbol{L}_{k,new}) = n_k - 1 \tag{26}$$

where n_k is the total number of nodes in the k-th cluster. Equation (26) ensures that all nodes within the cluster can complete state synchronization through communication links.

If both dimensions of verification pass, the topology reconstruction is considered successful. At this point, the updated $\boldsymbol{L}_{\text{new}}$ is synchronized to the consensus control layer to provide effective topology parameters for control command generation. If either dimension fails verification, the reconstruction is deemed failed, and it is necessary to immediately revert to the adjacency matrix and Laplacian matrix before reconstruction, and re-execute redundant node selection and link reconstruction operations until the connectivity requirements are satisfied.

Optional re-entry is permitted after an isolated node passes h consecutive healthy PRR–IAT windows, authentication and clock checks, and a receive-only probation period. One provisional low-weight link is then restored and monitored; any renewed alarm removes that link and returns the node to ISOLATED.

4.5. Closed-Loop Implementation of Multi-Leader UAV Swarm Consensus Fault-Tolerant Control

The closed loop combines detection, isolation, hierarchical reconstruction, connectivity verification, and controller update. For a fixed reconstructed graph, let each retained control edge e have effective delivery factor $q_e = (1-\rho_e)\left(1-p_{f,e}\right)$, assuming independent attack-induced and residual failures, with $q_e \geq q_{\min} > 0$. If b_e is its grounded incidence vector, then $H_{\text{eff}} = \sum_e q_e b_e b_e^T$ and $H_{\text{new}} = \sum_e b_e b_e^T$, which gives:

$$H_{\text{eff}} - q_{\min} H_{\text{new}} = \sum_e (q_e - q_{\min}) b_e b_e^T \succcurlyeq 0, \quad \lambda_{\min}(H_{\text{eff}}) \geq q_{\min} \lambda_{\min}(H_{\text{new}}) = \underline{\lambda}_{\text{eff}} \tag{27}$$

The positive-semidefinite matrix difference in Equation (27) establishes the eigenvalue lower bound directly. Substituting that bound into the modal polynomial in Equation (18), the Routh array requires $\gamma_2\gamma_3\lambda_{\min}(H_{\text{eff}}) > \gamma_1$, so a worst-case sufficient gain margin is:

$$\gamma_2\gamma_3\underline{\lambda}_{\text{eff}} - \gamma_1 > 0 \tag{28}$$

When Equation (28) holds, the fixed effective weighted graph is asymptotically stable under the stated edge-delivery model. This result is not a sample-path guarantee for arbitrary random link switching; repeated topology changes additionally require a positive dwell time.

Based on the above analysis, the core logic and key formula mapping of the UAV swarm closed-loop consensus fault-tolerant control framework are as follows (Algorithm 3):

Algorithm 3: Multi-Leader Swarm Fault-Tolerant Control Closed-Loop Core Logic

Initialize: $\boldsymbol{N}$ (total nodes), $\boldsymbol{M}$ (leader nodes), control gains γ_1, γ_2, γ_3, attack detection thresholds (μ_α,t'_{low}, t'_{high})
Initialize adjacency matrix $\boldsymbol{A}$, Laplacian matrix $\boldsymbol{L}$
Execute fault-tolerant closed loop:

1. Collect: node states ($\boldsymbol{x}, \boldsymbol{v}, \boldsymbol{a}$) and communication metrics (PRR/IAT)
2. Detect: determine DoS attack per Equation (12), locate attacked nodes and clusters
3. Reconstruct: if attacked, update $\boldsymbol{A}$ and $\boldsymbol{L}$ per Equations (21)–(24); verify connectivity per Equations (25) and (26)
4. Control: generate control commands $\boldsymbol{u}$ per Equation (14) (adapted to reconstructed $\boldsymbol{L}$)
5. Feedback: update node states; verify fault-tolerant robustness per Equations (27) and (28)
6. Loop: feedback states to collection step; iterate

The multi-leader UAV swarm closed-loop consensus fault-tolerant control framework relies on the hierarchical cluster topology architecture, with clusters independently executing attack detection and topology reconstruction to improve fault handling efficiency and reduce global communication overhead. All core steps are quantified through mathematical formulas—from attack detection to topology update and robustness verification—ensuring theoretical rigor and verifiability of the system design. When the number of leader nodes is $M = 1$, the same framework applies with one grounded follower Laplacian; the retained-link lower bound in Equation (27) and gain-margin test in Equation (28) are unchanged. Therefore, the algorithm framework proposed in this paper has good compatibility and extensibility, adaptable to UAV swarm application scenarios of different scales and different leader modes.

An isolated UAV executes the local safe-hold jerk law $u_i^{\mathrm{iso}} = -k_p\left((x_i - x_i^h\right) - k_v v_i - k_a a_i$, where x_i^h is captured at isolation. The gains satisfy $k_p, k_v, k_a > 0$ and $k_a k_v > k_p$, ensuring convergence to the local hold state without neighbor data.

5. Simulation and Results Analysis

5.1. Architecture and Parameter Settings of the HIL Semi-Physical Simulation Platform

A hardware-in-the-loop (HIL) semi-physical simulation platform was constructed for the experiments. Figure 1 presents the software-level detection–reconstruction–control workflow, whereas Figure 2 shows the corresponding hardware architecture and closed-loop data flow.

The platform comprises three interacting layers. First, the upper computer configures the reference trajectories, initial swarm topology, synthetic impairment schedule, and experimental parameters, and records and visualizes the flight states. Second, the real-time emulator executes the UAV dynamics, atmospheric-environment, sensor, and communication-network models. Third, each connected Pixhawk board represents the physical flight controller of one virtual UAV and executes the embedded control program. Accordingly, the UAV plant and environment are simulated by the real-time emulator, whereas flight-control calculations and PWM generation are performed on physical Pixhawk hardware.

During each closed-loop cycle, the real-time emulator transmits simulated GPS and inertial measurements to the corresponding Pixhawk through the Ethernet TCP/IP interface. The Pixhawk calculates the control input and returns PWM commands to the emulator, which advances the UAV dynamic model and generates the measurements for the next cycle. Flight states are also returned to the upper computer for monitoring, visualization, and logging. Connecting multiple Pixhawk boards through the same real-time emulator provides a closed-loop swarm experiment in which the controllers are physical devices and the vehicles, sensors, environment, and communication links are simulated in real time.

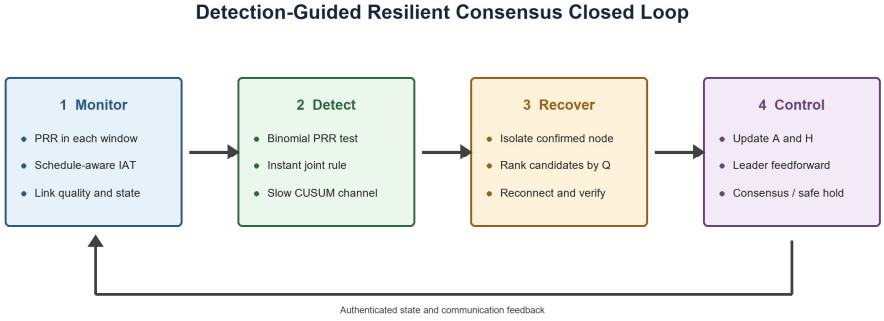


Figure 1. Detection-guided resilient consensus control workflow.

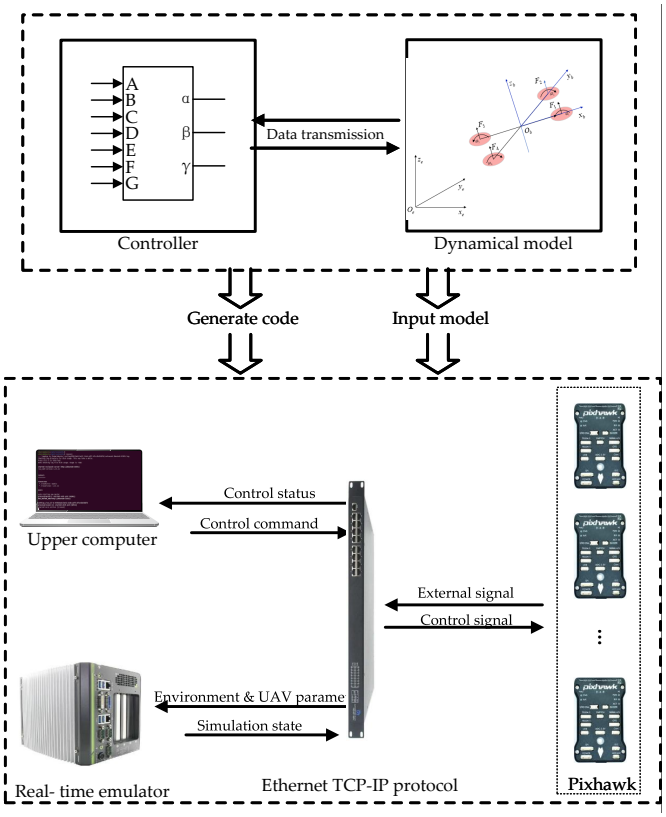


Figure 2. Hardware architecture and closed-loop data flow of the semi-physical simulation platform.

At the communication layer, authenticated inter-UAV state packets pass through the synthetic R-DoS impairment module before being processed by the PRR–IAT detector. The impairment module modifies only packet-delivery and packet-timing variables according to the prescribed schedule. A positive attack decision is passed to the isolation and topology-management logic, which removes the affected node or links, screens redundant candidates, verifies connectivity, updates the adjacency and grounded-Laplacian matrices, and provides the revised neighbor and reference information to the controllers. This functional allocation closes the loop between communication monitoring, topology reconstruction, and embedded control without using an external network or radio-frequency interference.

All experiments reported in this study were conducted in a closed laboratory HIL environment. The R-DoS component was implemented as a synthetic network-impairment model that modifies packet reception and timing variables; it did not involve access to an external network, intrusion into an operational UAV system, radio-frequency jamming, or field deployment. The study evaluates only defensive detection, node isolation, topology reconfiguration, and consensus recovery.

The most recent sensor sample and PWM command are held between the two update rates, forming a multirate closed loop. Inter-UAV communication packets are generated at 50 packets/s. A first-order 10 Hz low-pass filter and the stated sensor-noise model are applied before the feedback measurements are delivered to the controllers. The UAV parameters are listed in Table 2. The Pixhawk control routine operates at 200 Hz with a 5 ms control period, whereas the system-level plant and communication emulation use the 0.01 s step reported in Table 3.

The synthetic R-DoS impairment, PRR–IAT detector, topology manager, and consensus controller are integrated into the HIL platform. The principal settings are listed in Table 3.

Table 2. UAV Parameters Used in Simulation.

Symbol	Parameter Name	Value	Unit
m	UAV mass	1.2	kg
g	Gravitational acceleration	9.8	m/s^2
b	Lift coefficient	5	$N{\cdot}s^2$
d	Torque coefficient	1.239×10^{-5}	$N/(rad/s)^2$
I_x	Moment of inertia about x_b axis	0.0091	$kg{\cdot}m^2$
I_y	Moment of inertia about y_b axis	0.0096	$kg{\cdot}m^2$
I_z	Moment of inertia about z_b axis	0.0189	$kg{\cdot}m^2$
K_1	Air drag coefficient in x_e direction	0.01	N·s/m
K_2	Air drag coefficient in y_e direction	0.012	N·s/m
K_3	Air drag coefficient in z_e direction	0.019	N·s/m
K_4	Air drag moment coefficient about x_e axis	0.0022	N·m·s/rad

Table 3. Main Simulation Parameters.

Parameter Name	Symbol	Value	Unit
Simulation step size	Δt	0.01	s
Total simulation time	T	30	s
Synthetic impairment start	t_{att_sta}	10	s
Synthetic impairment end	t_{att_fin}	25	s
Detection delay	t_{det}	0.5	s
Reconstruction delay	t_{rec}	1.0	s
Detection time window	T_w	1.0	s
Communication frequency	f_{com}	50	pkt/s
Calibration window count	m	30	—
Significance level	α	0.05	—
Consecutive anomaly count	k	3	—
Consensus control gain	γ_1	3	
Consensus control gain	γ_2	8	
Consensus control gain	γ_3	4	
Impairment pulse duration	—	$\exp(1.5)$	
Impairment pulse interval	—	$\exp(2.0)$	
Simulated packet-loss intensity	—	$Beta(2,3)+0.3$	
Impairment random noise	—	$N(0,0.05)$	

The reported HIL results correspond to a 0.5 s detection delay and a 1 s topology-reconstruction delay. Because tracking error at larger delays depends jointly on attack duration, reconstructed topology, controller gains, and UAV dynamics, these results should not be extrapolated beyond this setting. Systematic varied-delay HIL sensitivity testing remains necessary.

5.2. Single-Leader UAV Swarm Fault-Tolerant Control Simulation

The single-leader scenario consists of six UAVs, with the topology structure shown in Figure 3. The leader node moves along a circular trajectory superimposed with sinusoidal altitude changes. The reference trajectory is given by Equation. The initial positions of follower nodes are randomly offset within 2–6 m from the leader node, simulating the initial formation deployment state.

$$\begin{aligned} x(t) &= 10\cos(0.2t) \\ y(t) &= 10\sin(0.2t) \\ z(t) &= 5 + 2\sin(0.3t) \end{aligned} \tag{29}$$

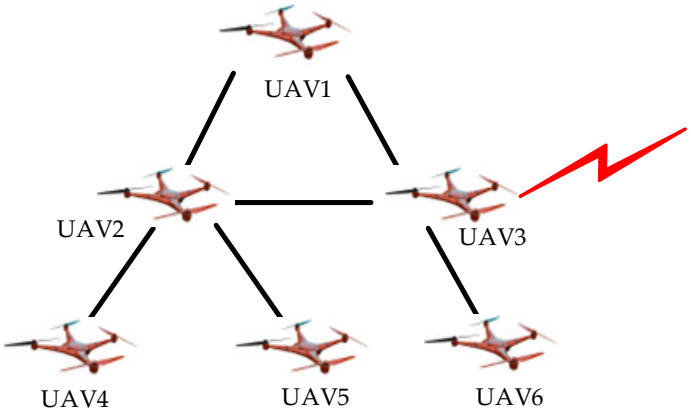


Figure 3. Single-leader UAV swarm topology structure.

In the simulation, the R-DoS attack targets UAV3. After the attack, the state information transmission of its downstream node UAV6 is interrupted. Simulation results are shown in Figures 4–7.

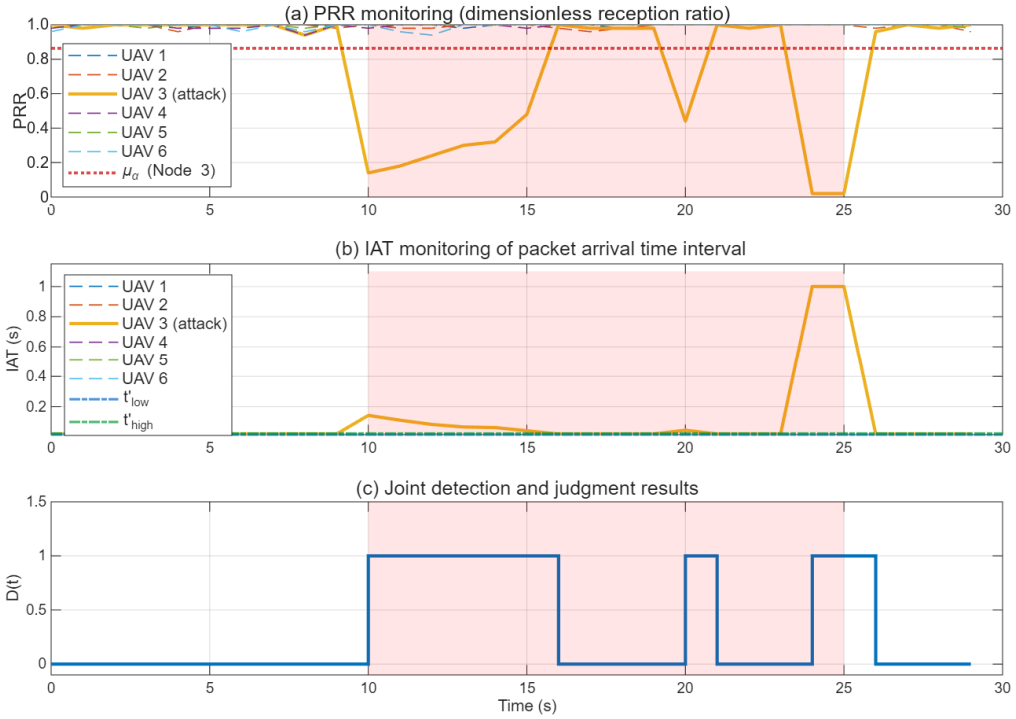


Figure 4. PRR–IAT Dual-Dimensional Joint Detection Results (single-leader scenario).

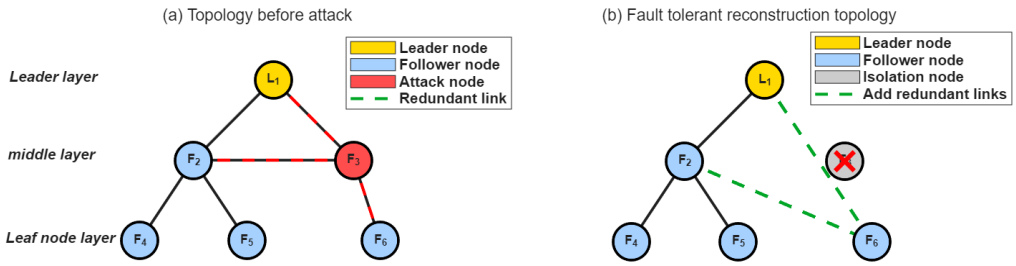


Figure 5. Topology comparison before R-DoS attack and after fault-tolerant reconstruction (single-leader scenario).

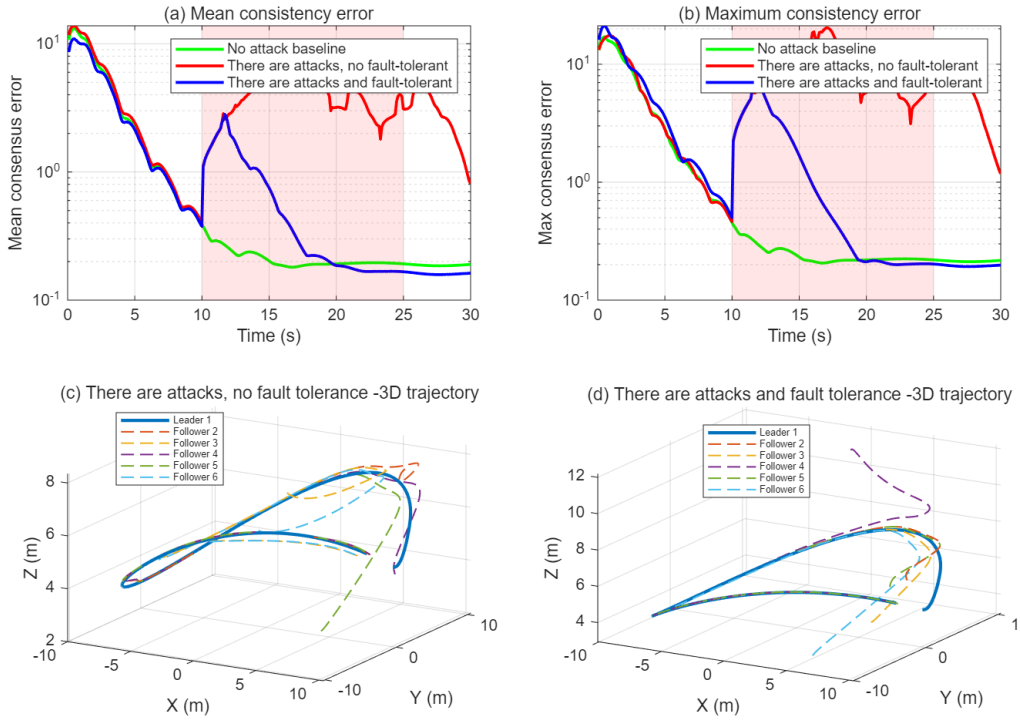


Figure 6. Comparison of Consensus Control Effects (single-leader scenario).

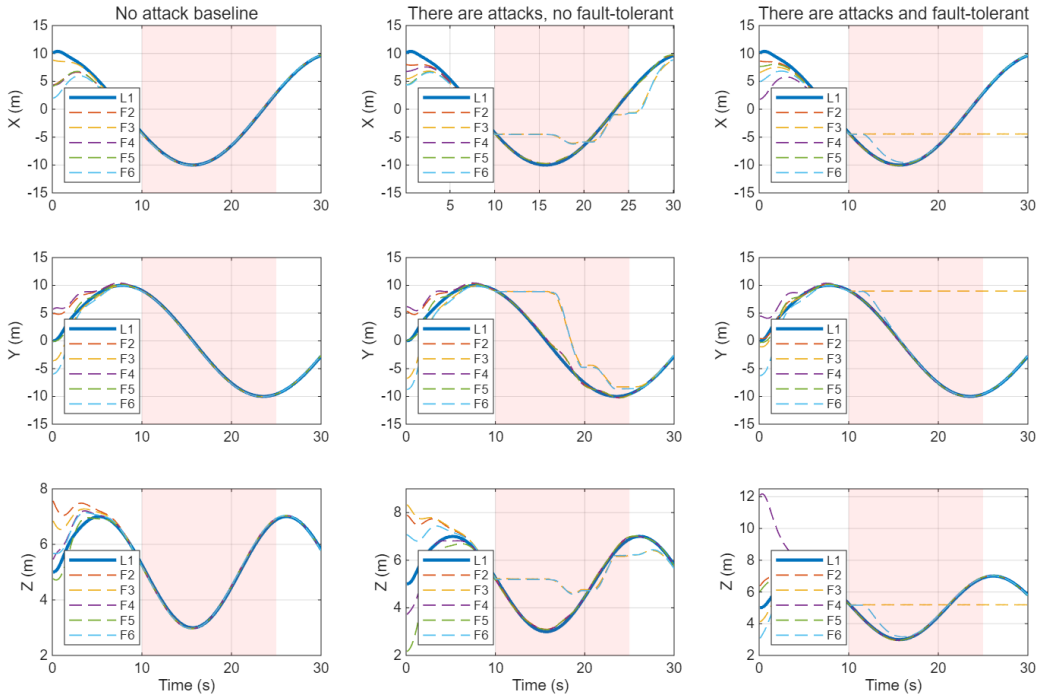


Figure 7. Comparison of x/y/z-axis position tracking (single-leader scenario).

Figure 4 (with its PRR axis normalized to [0, 1]) shows the PRR–IAT dual-dimensional joint detection results after the single-leader UAV swarm receives the R-DoS attack. As can be seen from Figure 4, the PRR–*IAT* dual-dimensional joint detection mechanism can accurately identify the onset of R-DoS attacks. After the attack begins, the PRR value of UAV3 drops sharply, falling clearly below the dimensionless decision threshold μ_α. Meanwhile, the *IAT* value shows large fluctuations, leaving the conservative prediction interval $[t'_{low}, t'_{high}]$. The simultaneous anomalies in both dimensions trigger the attack

determination, verifying the accuracy of the PRR–*IAT* joint detection strategy in a single-leader UAV swarm.

Figure 5 shows the UAV swarm topology before the R-DoS attack and after reconstruction. Before the attack, UAV3 served as an intermediate node to relay state information for UAV6. After the attack, the system identifies UAV4 as an available redundant node through the distributed redundant node identification algorithm, and establishes direct communication links between UAV2 and UAV6, as well as between UAV4 and UAV6, completing the topology reconstruction. The reconstructed Laplacian matrix satisfies the connectivity requirement of Equation (26), ensuring that the remaining effective graph is connected after exclusion of the isolated node.

Figure 6 compares the consensus control effects, and Figure 7 shows the position-tracking results on the x/y/z axes.

From Figures 6 and 7, all followers converge in approximately 5 s in the no-attack baseline. During an attack, nodes retained without fault tolerance may drift as their prior acceleration continues to integrate. Under fault tolerance, the attacked node is isolated and executes the local safe-hold law defined in Section 4.5, while healthy nodes reconnect and recover tracking.

The comparison distinguishes short-term natural link recovery from defensive isolation. The plotted fault-tolerant case keeps the attacked node in safe hold; if authenticated communication remains healthy after the attack, the probationary re-entry procedure in Section 4.4.2 may restore it. Permanent exclusion is therefore not required by the framework.

5.3. Multi-Leader UAV Swarm Fault-Tolerant Control Simulation

The multi-leader scenario consists of eight UAVs, with UAV1 and UAV2 as leader UAVs, divided into two independent clusters. The multi-leader hierarchical tree topology is shown in Figure 8. The two leader nodes move along symmetric circular trajectories with a phase difference of π. The reference trajectories are:

$$\begin{aligned} &\text{UAV1} : x(t) = 10 \cdot \cos(0.2t), y(t) = 10 \cdot \sin(0.2t) \\ &\text{UAV2} : x(t) = 10 \cdot \cos(0.2t + \pi), y(t) = 10 \cdot \sin(0.2t + \pi) \end{aligned} \tag{30}$$

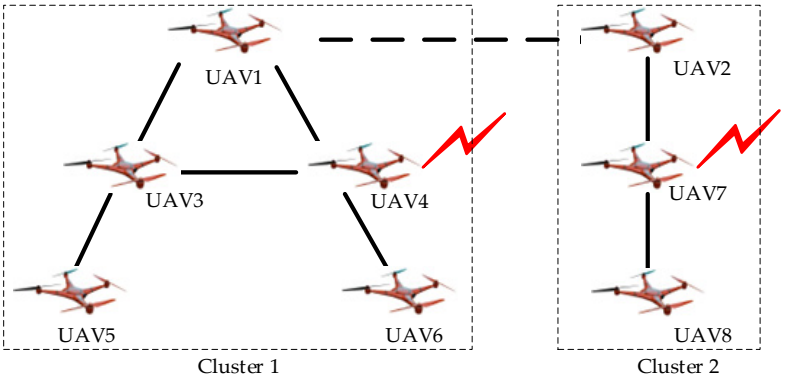


Figure 8. Multi-leader UAV swarm topology structure.

In the simulation, R-DoS simultaneously attacks two targets: UAV4 and UAV7. Simulation results are shown in Figures 9–12.

As can be seen from Figure 9 (with its PRR axis normalized to [0, 1]), in the multi-leader scenario, the PRR–IAT dual-dimensional joint detection mechanism can simultaneously identify attacked nodes in two clusters. After the attack begins, the PRR values of UAV4 (Cluster 1) and UAV7 (Cluster 2) both drop sharply and fall clearly below the dimensionless

decision threshold μ_α. Meanwhile, the IAT values show large fluctuations, leaving the conservative prediction interval $[t'_{low}, t'_{high}]$. The simultaneous anomalies in both dimensions trigger the attack determination. The dual-dimensional joint determination accurately identifies the multi-target characteristics of the R-DoS attack, verifying the adaptability of the detection mechanism to the multi-leader cluster architecture.

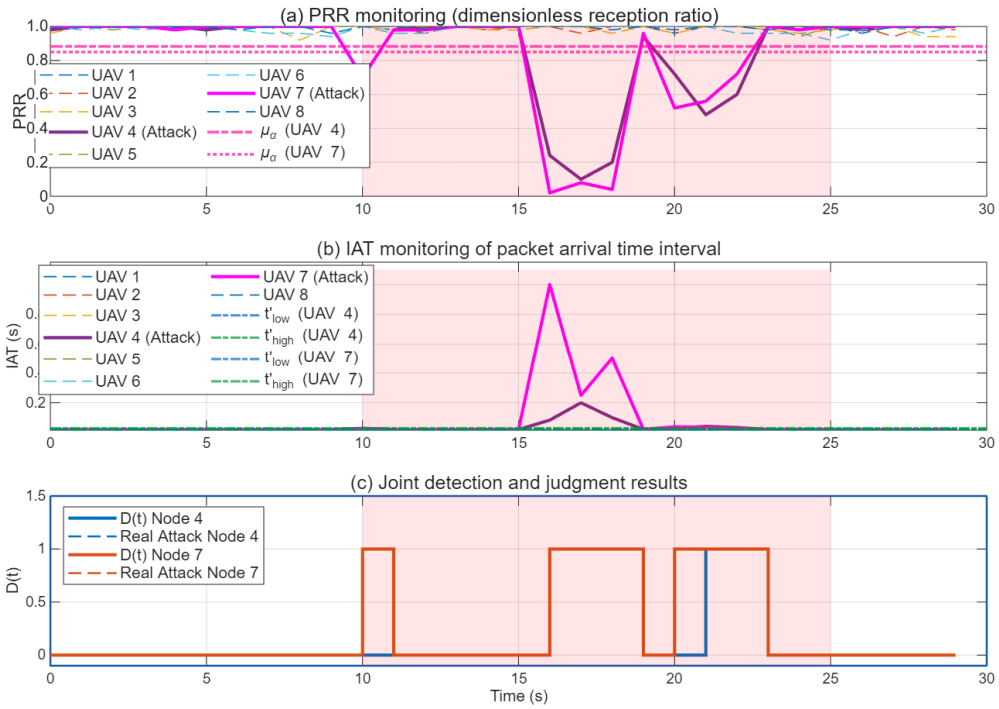


Figure 9. PRR–IAT Dual-Dimensional Joint Detection Results (multi-leader scenario).

Figure 10 shows the UAV swarm topology before and after reconstruction in the multi-leader scenario. After the attack, Cluster 1 activates redundant node UAV3 to establish alternative communication links for UAV5 and UAV6; Cluster 2 activates redundant node UAV8 to establish alternative links for other follower nodes. The two clusters independently execute reconstruction operations without interference. After reconstruction, the Laplacian matrix ranks of each cluster satisfy the connectivity requirement of Equation (26), while the leader node group Laplacian matrix rank satisfies the connectivity requirement of Equation (25), ensuring the overall consensus control foundation of the multi-leader swarm.

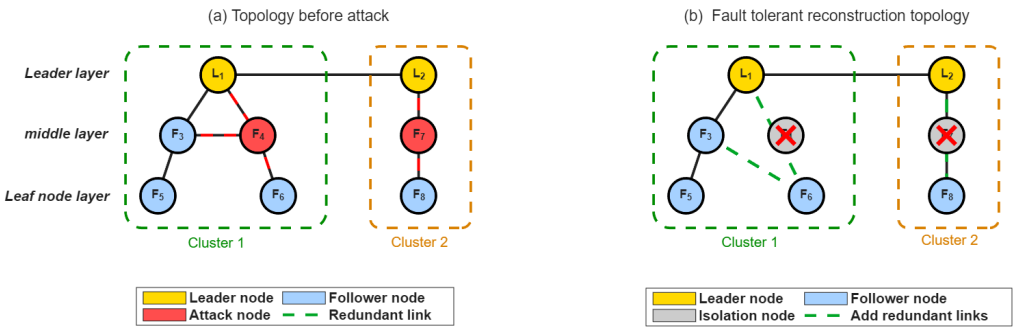


Figure 10. Topology comparison before R-DoS attack and after fault-tolerant reconstruction (multi-leader scenario).

Figure 11 compares the consensus errors of two clusters under three conditions. Similar to the single-leader UAV swarm, in the multi-leader UAV swarm, attacked nodes and their child nodes exhibit position divergence due to control input interruption during the attack.

Under the no-fault-tolerance condition, since the topology matrix remains intact, nodes can naturally converge after the attack ends. Under the fault-tolerant condition, attacked nodes UAV4 and UAV7 remain in safe hold in the plotted scenario and may later enter the probationary re-entry process, but the core subset of the formation maintains stable tracking during the attack period. Compared with the single-leader scenario, the error convergence time in the multi-leader scenario is slightly longer, due to the additional information synchronization overhead required for inter-cluster coordination. However, the advantage of the multi-leader architecture is that the attack impact is confined within a single cluster and will not propagate to the entire swarm through the leader node group, reflecting the natural isolation characteristics of the hierarchical cluster topology.

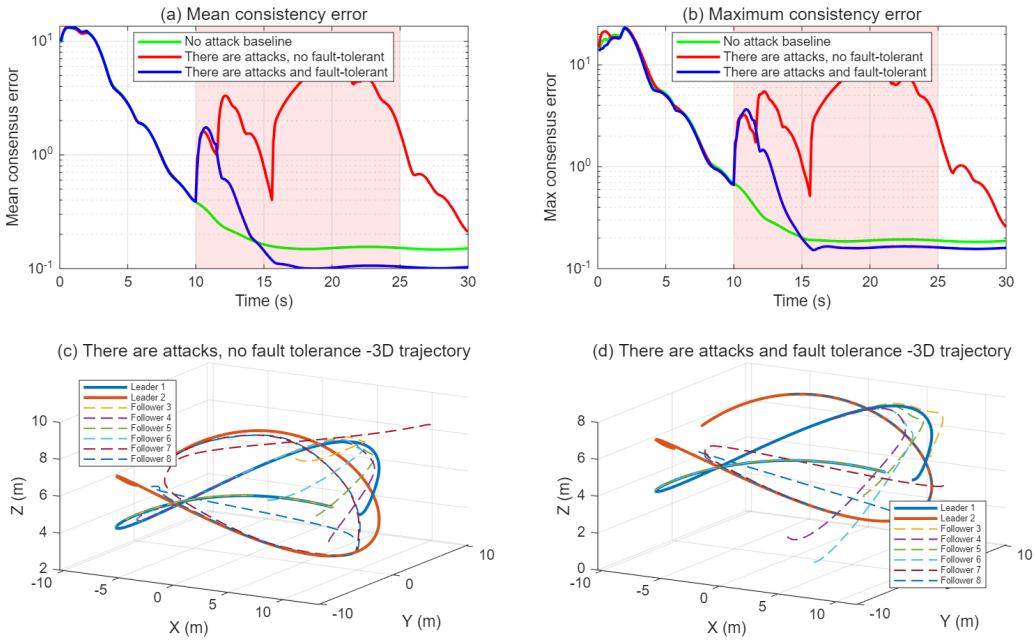


Figure 11. Comparison of Consensus Control Effects (multi-leader scenario).

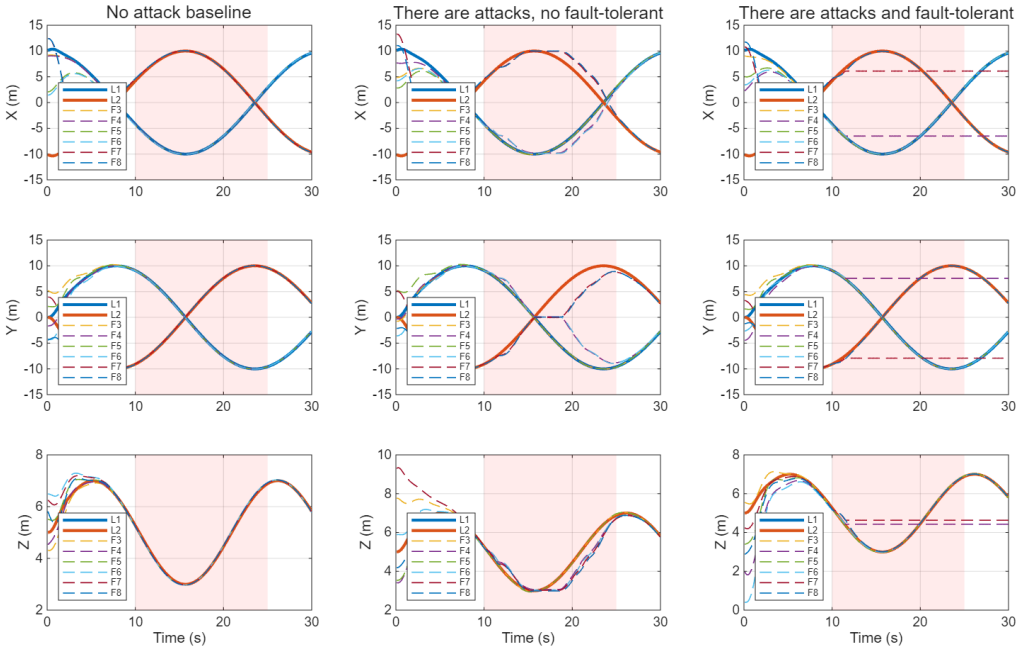


Figure 12. Comparison of x/y/z-axis position tracking (multi-leader scenario).

Figure 12 shows the position tracking effects on the x/y/z axes in the multi-leader scenario. The follower nodes of the two clusters track the symmetric circular trajectories of their respective leader nodes. There is a brief trajectory deviation during the fault-tolerant reconstruction phase after the attack, but trajectory tracking quickly recovers after reconstruction is complete. Consistent with the single-leader scenario analysis, the trajectories of isolated nodes (UAV4, UAV7) show a characteristic of decreasing arc after the peak, reflecting the explicit local safe-hold controller; nodes reconnected through redundant links gradually converge from the offset positions to the desired trajectories. Ultimately, the tracking errors of each axis (excluding isolated nodes) are stabilized within 0.4 m, meeting the accuracy requirements of UAV swarm cooperative tasks.

5.4. Fault-Tolerant Control Simulation for Leader Node Under Attack

To evaluate the fault-tolerant framework under loss of a reference source, the leader-node attack experiment uses the same eight-UAV, two-cluster topology as Section 5.3. UAV1 and UAV2 initially provide the reference inputs for their respective clusters. The synthetic R-DoS impairment is applied to UAV2 from 10 s to 25 s; therefore, UAV2 is both the attacked communication node and the unavailable reference source for Cluster 2. Simulation results are shown in Figures 13–16.

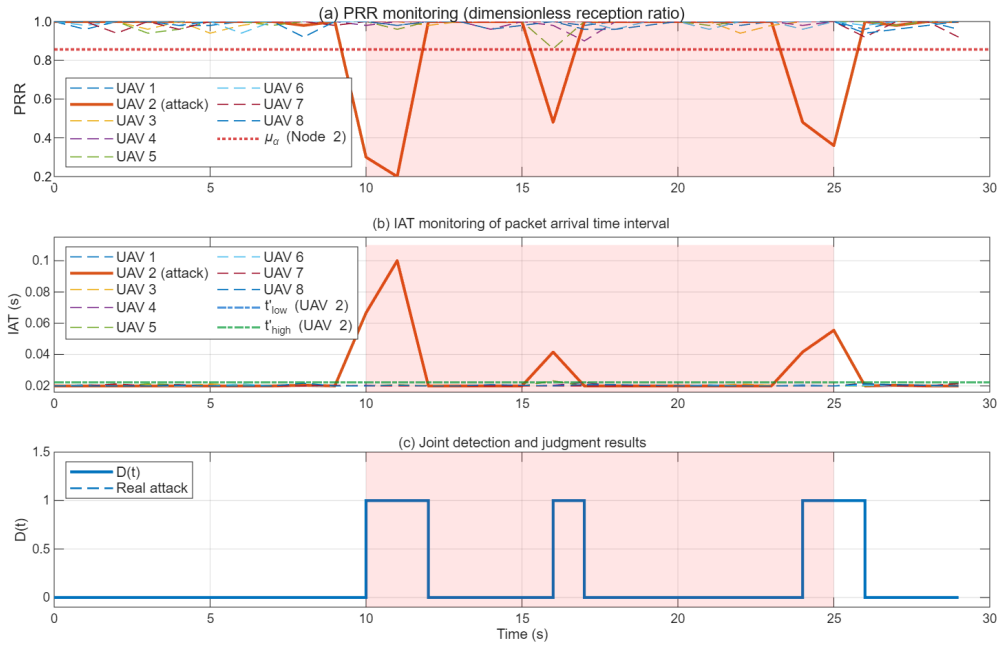


Figure 13. PRR–IAT Dual-Dimensional Joint Detection Results (leader node attack scenario).

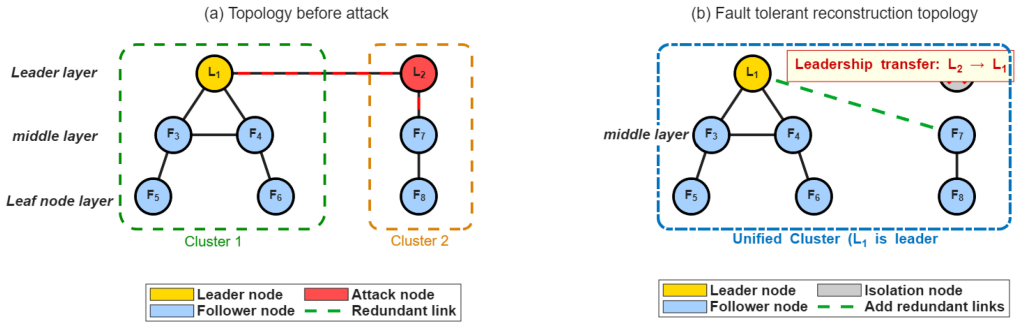


Figure 14. Topology comparison before R-DoS attack and after fault-tolerant reconstruction (leader node attack scenario).

After the PRR–IAT detector declares UAV2 abnormal, UAV2 is removed from the effective leader set and executes the local safe-hold controller. The topology manager then selects the healthy leader UAV1, activates the bidirectionally verified link between UAV1 and UAV7, and recalculates the adjacency and grounded-Laplacian matrices. UAV7 and UAV8 consequently switch from the unavailable UAV2 reference to the surviving UAV1 reference. The original two-cluster topology is thereby converted into a unified single-leader topology after the configured 0.5 s detection delay and 1 s reconstruction delay.

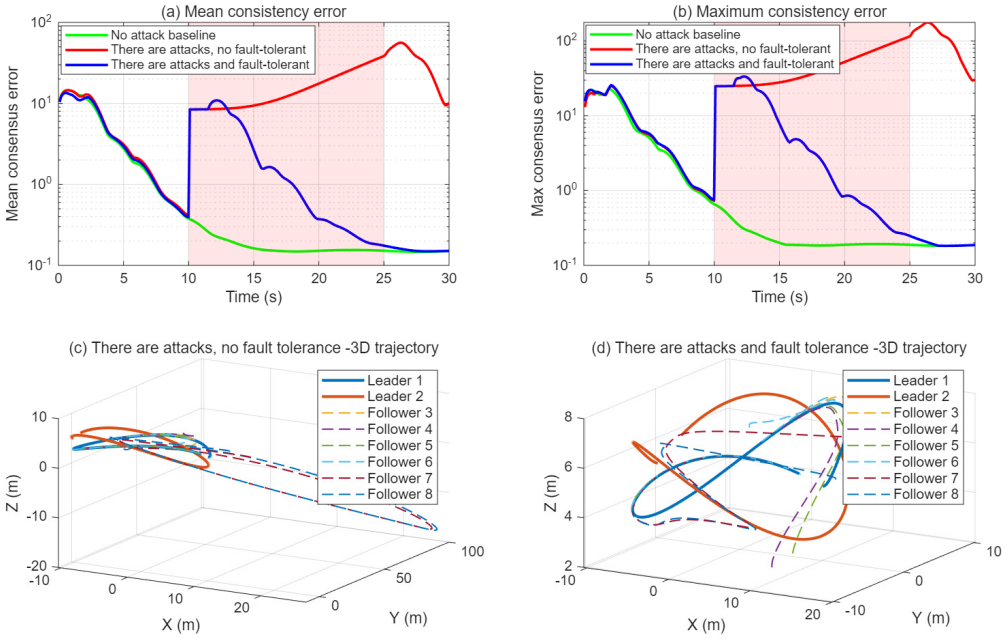


Figure 15. Comparison of Consensus Control Effects (leader node attack scenario).

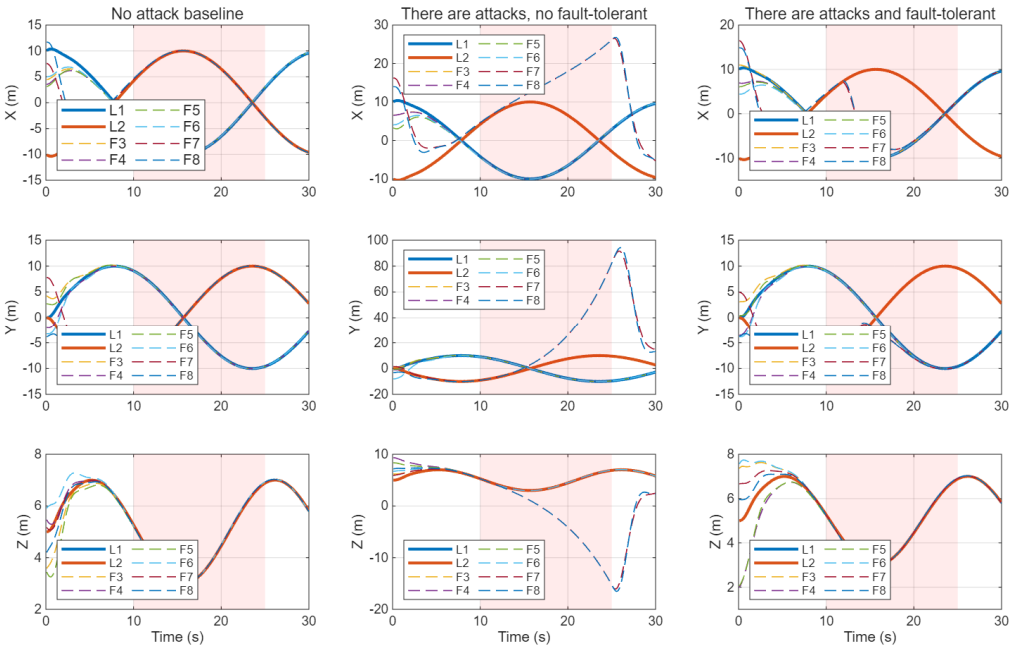


Figure 16. Comparison of x/y/z-axis position tracking (leader node attack scenario).

As can be seen from Figure 13 (with its PRR axis normalized to [0, 1]), in the scenario where a leader node is under attack, the PRR–IAT dual-dimensional joint detection mechanism can also accurately identify the attacked node. The PRR value of UAV2 (leader node 2) drops sharply and falls clearly below the dimensionless decision threshold μ_α. Meanwhile, the *IAT* value shows large fluctuations, leaving the conservative prediction interval $[t'_{low}, t'_{high}]$, triggering the attack determination and verifying the adaptability of the detection mechanism when a leader node is under attack.

Figure 14 shows the UAV swarm topology before and after reconstruction when leader node 2 is under R-DoS attack. After the attack, the system isolates the attacked leader node UAV2 and transfers leader authority to the healthy leader node UAV1, while activating redundant links connecting UAV1 and UAV7. At this point, the dual-cluster structure is reconstructed into a unified single-leader UAV swarm. The Laplacian matrix rank of the reconstructed single-leader UAV swarm satisfies the connectivity requirement of Equation (26), ensuring connectivity of the reconstructed effective graph.

Figure 15 compares the consensus-error evolution in the leader-node attack scenario. This case is more demanding than a follower-node attack because loss of UAV2 simultaneously removes a communication node and the reference input of an entire cluster. Without fault-tolerant reconstruction, the followers of Cluster 2 accumulate tracking error after losing the UAV2 reference. The impairment ends at 25 s, leaving only 5 s in the reported 30 s observation interval; the curves therefore show that the errors do not recover within the remaining experiment rather than proving that recovery is impossible for all later times. With fault tolerance, the errors first increase during detection and reconstruction and then decrease after leader-authority transfer, link activation, and reference switching. The need to perform both topology repair and authority reassignment explains the longer transient relative to the follower-node attack cases.

Figure 16 presents the x/y/z-axis tracking results. In the no-attack baseline, each follower tracks the reference trajectory of its assigned leader. Under attack without fault tolerance, UAV7 and UAV8 lose the UAV2 reference and develop coordinated drift on all three axes. Under fault tolerance, the trajectories of UAV7 and UAV8 leave the drifting state after UAV7 is linked to UAV1 and both followers adopt the surviving leader reference. Cluster 1 remains comparatively continuous because its leader is not attacked. The isolated UAV2 no longer supplies a reference to the swarm and is decoupled from the reconstructed control graph. By the end of the reported interval, the surviving followers recover tracking errors close to the baseline, supporting the effectiveness of the combined isolation, authority-transfer, and topology-reconstruction mechanism under the stated HIL conditions.

5.5. Discussion

The three HIL scenarios reveal different reconstruction requirements. A follower attack in the single-leader swarm requires local link replacement, whereas simultaneous follower attacks in the multi-leader swarm can be handled independently within the affected clusters. In contrast, a leader attack requires both topology reconstruction and reassignment of the reference authority. This structural difference explains the larger transient error and longer recovery process in Section 5.4. Across all three cases, the PRR–IAT detector supplies the same attack decision interface; the subsequent recovery action depends on whether the affected node is a follower, an inter-cluster relay, or a leader.

The results also illustrate a trade-off between detection reliability and recovery speed. Increasing the detection window T_w or the consecutive anomaly number k can reduce sensitivity to short network fluctuations, but it also increases the conservative interval $\tau_{\max} = kT_w + \Delta t_{\text{rec}}$ before the reconstructed controller becomes active. The accumulated error during this interval must therefore be considered together with the modal gain condi-

tion in Equation (19) and the effective-connectivity lower bound in Equations (27) and (28). Similarly, conservative node isolation improves containment but temporarily reduces the available graph, while additional redundant links improve connectivity at the cost of communication and verification overhead.

The HIL platform strengthens the validation by closing the loop through physical flight-control hardware, but it does not constitute field-flight validation. The current evidence is limited to a synthetic communication-impairment model, the stated 0.5 s/1 s delay setting, a limited swarm size, fixed reconstructed graphs over each analysis interval, and the implemented sensor-noise and vehicle models. Wind disturbances, unmodeled dynamics, time-varying sensing delays, arbitrary random graph switching, larger swarms, and radio-channel effects remain outside the validated scope. Future work will therefore require varied-delay HIL sensitivity experiments and field tests under more realistic communication and environmental disturbances.

6. Conclusions

This paper addresses the security problem of UAV swarm consensus control under R-DoS attacks, and proposes a dynamic fault-tolerant control method based on PRR–IAT dual-dimensional joint detection. The main conclusions are as follows:

(1) The proposed PRR–IAT dual-dimensional joint detection mechanism achieves accurate, real-time identification of R-DoS attacks through spatio-temporal feature fusion and multi-rule joint determination without relying on precise system models. Compared with single-dimensional detection methods, it effectively reduces missed detection and false alarm probabilities.

(2) The dynamic fault-tolerant control method based on hierarchical tree topology achieves adaptive repair of the communication network through online updates of the adjacency matrix and Laplacian matrix. In three typical scenarios—single-leader, multi-leader, and leader node under attack—it can effectively restore swarm consensus control.

(3) Theoretical analysis and simulation experiments verify that, when the effective-weighted-graph lower-bound condition in Equation (28) is satisfied, the reconstructed fixed topology preserves consensus convergence under the stated assumptions; the HIL results show position tracking errors on each axis within 0.4 m.

This HIL model does not include wind gusts, unmodeled vehicle dynamics, or time-varying sensing delays. Integrating disturbance observers and delay-aware consensus mechanisms is therefore left for future work.

Author Contributions: Conceptualization, Y.H.; methodology, J.S. and Z.L.; software, P.C.; validation, Y.H., and M.Y.; formal analysis, J.S.; investigation, M.Y.; resources, P.C.; data curation, J.S.; writing—original draft preparation, Y.H., Z.L. and P.C.; writing—review and editing, P.C.; visualization, M.Y.; supervision, P.C.; project administration, J.S.; funding acquisition, P.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Shanxi Provincial Key Research and Development Project, grant number 202202020101001, National Natural Science Foundation of China, grant number 51909245.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: This research is limited to resilient cooperative control and cybersecurity of networked UAV systems. Its primary intended benefits are improving the safety, continuity, and fault tolerance of civilian UAV swarm operations, including disaster response, environmental monitoring, precision agriculture, and infrastructure inspection. The authors acknowledge that general swarm-control and cyber-resilience methods may have dual-use potential. This study is

defensive in nature and does not address reconnaissance payloads, weaponization, target selection, or operational attack execution. All experiments were performed in a closed HIL simulation environment using synthetic communication impairments. Precautions were taken to avoid disclosing real-world intrusion procedures, access credentials, radio-frequency interference configurations, or mission-specific operational details. The authors will comply with applicable national and international laws, institutional requirements, and guidance concerning dual-use research of concern, and advocate responsible deployment, ethical review, regulatory compliance, and transparent reporting to mitigate misuse risks and promote beneficial outcomes.

Data Availability Statement: The non-sensitive simulation data supporting the conclusions of this article will be made available by the authors upon reasonable request. The study does not provide operational intrusion code, access credentials, radio-frequency jamming configurations, or mission-specific deployment data.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The main symbols used in the manuscript.

Symbol	Description
$G = (V, E)$, $\mathcal{N}_i$	Communication graph and neighbor set of node i
A, D, L	Adjacency, degree, and effective symmetric Laplacian matrices
L_F, B, H	Follower Laplacian, leader-pinning matrix, and grounded Laplacian
T_w, m, n_w	Detection window, trusted calibration window count, and scheduled packets per window
N, N_{total}, S	Received count, scheduled count, and count standard deviation
PRR, μ_α	Packet reception ratio and its dimensionless lower threshold
k_f, p_U	Observed failure count and its one-sided binomial upper probability bound
$\hat{\lambda}$, λ_L, λ_U, α	Estimated IAT rate, its confidence limits, and significance level
IAT, t'_{low}, t'_{high}	Aggregate-stream inter-arrival time and conservative prediction limits
k, K, h	Consecutive PRR count, suspicion horizon, and timing-anomaly count
A_P, A_I, $D(t)$	PRR flag, IAT flag, and joint attack decision
x_i, v_i, a_i, u_i	Position, velocity, acceleration, and jerk input of UAV i
γ_1, γ_2, γ_3	Consensus gains for position, velocity, and acceleration errors
Δt_{rec}, $\tau_{\max}$	Reconstruction delay and conservative detection-plus-reconstruction interval
q_e, $q_{\min}$, ρ_e, $p_{f,e}$	Edge delivery factor, its lower bound, attack loss, and residual failure probability
d_{ir}, r_c, τ_{ir}, τ_{link}	Candidate distance/range and measured/allowable link delay
Q_{ir}, Q_{th}, w_j	Candidate score, admission threshold, and score weights
x_i^h, k_p, k_v, k_a	Isolation hold position and local safe-hold gains

References

1. Umrani, M.I.; Butler, B.; Davy, S. Toward secure complex UAV cyber-physical systems: A unified threat taxonomy and cross-layer survey of cybersecurity challenges. *Internet Things* **2026**, *37*, 101902. [CrossRef]
2. Burbank, J.; Toro, C.; Emmanuela, A.; Naima, K. Detection and Mitigation of Cyber Attacks on UAV Networks. *Electronics* **2026**, *15*, 317. [CrossRef]
3. Yu, Z.Q.; Cui, Y.W.; Yang, H.C.; Li, M.N.; Zhour, R.F. Cooperative Security Control of Swarm Unmanned Aerial Vehicles Under Cyber Attacks. *J. Nav. Aviat. Univ.* **2023**, *38*, 457–465+482.
4. Xu, L.L.; Yu, J.; Hu, C. Finite-Time Synchronization of Fractional-Order Complex-Valued Multi-Layer Network via Adaptive Quantized Control Under Deceptive Attacks. *Fractal Fract.* **2025**, *9*, 47. [CrossRef]
5. Ma, X.M.; Gao, M.G. "Lure the Enemy in Deep": Confronting Rogue UAV Through Diverse Hybrid Jamming. *IEEE Access* **2025**, *13*, 68351–68369. [CrossRef]
6. Slimane, H.O.; Benouadah, S.; Khoei, T.T.; Kaabouch, N. A Light Boosting-based ML Model for Detecting Deceptive Jamming Attacks on UAVs. In *Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*; ELECTR NETWORK; IEEE: New York, NY, USA, 2022; pp. 328–333.

7. Lu, A.Y.; Zhang, J.N.; Wang, Q.J.; Ji, H.K.; Yin, L.B.; Zhu, L.Q.; Sun, B.X. A survey on secure protection of cyber-physical systems under cyber attacks. *Control Decis.* **2026**, *41*, 1–18. [CrossRef]
8. Miao, S.T.; Li, Y.; Pan, Q. Honeypot Game Theory against DoS Attack in UAV Cyber. *Comput. Mater. Contin.* **2023**, *76*, 2745–2762. [CrossRef]
9. Lu, A.Y.; Yang, G.H. Secure state estimation for cyber-physical systems under sparse sensor attacks via a switched Luenberger observer. *Inf. Sci.* **2017**, *417*, 454–464. [CrossRef]
10. Hassler, S.C.; Mughal, U.A.; Ismail, M. Cyber-Physical Intrusion Detection System for Unmanned Aerial Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 6106–6117. [CrossRef]
11. Song, X.L.; Li, Y.Y.; He, D.F. Secure H∞ Platooning Control for Connected Vehicles Subject to External Disturbance and Random DoS Attacks. *ACTA Autom. Sin.* **2024**, *50*, 348–355.
12. Fu, M.R.; Yu, Z.Q. Resilient tracking control of UAV with event-triggered communication against stochastic DoS attacks and faults. *Inf. Sci.* **2026**, *735*, 123074. [CrossRef]
13. Song, X.; Liu, X.; Shan, H.; Lu, R. Time-Delay Robust Safety Control of Connected Vehicles Under Stochastic DoS Attack. *IEEE Internet Things J.* **2025**, *12*, 29485–29494. [CrossRef]
14. Liu, C.; Liu, L.; Cao, J.; Luo, Y. Event-Triggered Secure Formation Tracking of Delayed Multi-UAV Systems Subject to DoS Attacks. *IEEE Trans. Netw. Sci. Eng.* **2026**, *13*, 655–667. [CrossRef]
15. Lu, J.Q.; Xing, M.P.; Zhang, J. A survey on secure and privacy protection of multi-agent systems consensus under cyber attacks. *Control Decis.* **2025**, *40*, 3201–3219.
16. Amin, S.; Litrico, X.; Sastry, S.; Bayen, A.M. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. *IEEE Trans. Control Syst. Technol.* **2013**, *21*, 1963–1970. [CrossRef]
17. De Persis, C.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [CrossRef]
18. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Networked control under random and malicious packet losses. *IEEE Trans. Autom. Control* **2017**, *62*, 2434–2449.
19. Qiu, L.; Lin, S.; Chen, R.; Teng, J.; Wu, Z.; Najariyan, M. Resilient Dual-mode Model Predictive Control for Constrained Linear Networked Control Systems with Random DoS Attacks. *Int. J. Control Autom. Syst.* **2025**, *23*, 105–114. [CrossRef]
20. Wu, J.; Peng, C.; Zhang, J.; Tian, E. A Sampled-Data-Based Secure Control Approach for Networked Control Systems Under Random DoS Attacks. *IEEE Trans. Cybern.* **2024**, *54*, 4841–4851. [CrossRef] [PubMed]
21. Zhang, D.W.; Liu, G.P.; Cao, L. Secure Predictive Coordinated Control of High-Order Fully Actuated Networked Multiagent Systems Under Random DoS Attacks. *IEEE Trans. Cybern.* **2023**, *54*, 2668–2679. [CrossRef] [PubMed]
22. Deng, C.; Che, W.W. Fault-tolerant fuzzy formation control for a class of nonlinear multiagent systems under directed and switching topology. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 5456–5465. [CrossRef]
23. Guo, Y.; Liao, L.; Zhang, X.; Zhang, Y.; Wang, K. Finite-time fault-tolerant control of compound actuator faults for unmanned aerial vehicles. *Acta Aeronaut. Astronaut. Sin.* **2026**, *47*, 332659.
24. Park, T.J.; Ahn, C.S.; Hong, S.K. Self-reconfiguration of a networked multi-agent system for resilient operation under adversarial attacks. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 783–794.
25. Song, Y.C.; Qi, R.Y.; Jiang, B. Distributed topology reconstruction of UAV formation network under communication fault. *Acta Aeronaut. Astronaut. Sin.* **2025**, *46*, 331914.
26. Cui, Y.K.; Chen, J.B.; Lin, H.; Shu, Z.; Huang, T.W. Cooperative Multi-AAV Path Planning for Discovering and Tracking Multiple Radio-Tagged Targets. *IEEE Trans. Syst. Man Cybern. Syst.* **2025**, *55*, 2463–2475. [CrossRef]
27. Galicia-Galicia, L.A.; Hernández-González, O.; Garcia-Beltran, C.D.; Valencia-Palomo, G.; Guerrero-Sánchez, M.E. Distributed Observer for Linear Systems with Multirate Sampled Outputs Involving Multiple Delays. *Mathematics* **2024**, *12*, 2943. [CrossRef]
28. Zhang, T.W.; Gao, G.; Ke, X.; Zhang, X.L. Swarm Learning: Perception–Retrieval–Localization for Ship Detection from Synthetic Aperture Radar Remote Sensing Imagery. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* **2026**, *19*, 12384–12395. [CrossRef]
29. Luo, X.C.; Du, X.Y.; Yue, S.; Lv, Y.X.; Zhang, L.L.; He, X.F.; Wu, W.Q.; Mao, J. DTVIRM-Swarm: A Distributed and Tightly Integrated Visual-Inertial-UWB-Magnetic System for Anchor Free Swarm Cooperative Localization. *Drones* **2026**, *10*, 49. [CrossRef]
30. Abro, G.E.M.; Abdallah, A.M. Swarm Coordination and Trajectory Tracking in Quadrotor UAVs Using Fractional-Order PID Control Strategy. *IEEE Trans. Autom. Sci. Eng.* **2026**, *23*, 2995–3008. [CrossRef]
31. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
32. Xia, Y. Research on Link Quality Estimation of Heterogeneous Wireless Sensor Networks. Master's Thesis, Chongqing University of Technology, Chongqing, China, 2020.
33. Sharma, S. Analysis of Power-Law Queues Using Maximum Entropy Framework: An Application to Performance Evaluation of Network Systems. *Wirel. Pers. Commun.* **2024**, *145*, 679–697. [CrossRef]
34. Wang, Q.L.; Psillakis, H.E.; Sun, C.Y. Adaptive Cooperative Control with Guaranteed Convergence in Time-Varying Networks of Nonlinear Dynamical Systems. *IEEE Trans. Cybern.* **2019**, *50*, 5035–5046. [CrossRef] [PubMed]

35. Horn, E.A.; Johnson, C.R. *Matrix Analysis*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2012.
36. Beard, R.W.; McLain, T.W. *Small Unmanned Aircraft: Theory and Practice*, 2nd ed.; Princeton University Press: Princeton, NJ, USA, 2012.
37. Gou, J.; Liang, T.; Tao, C.; Ma, B.; Wang, H.; Wu, Y. Formation control and aggregation method of UAV based on consensus theory. *J. Beijing Univ. Aeronaut. Astronaut.* **2024**, *50*, 1646–1654.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.