Grenze International Journal of Engineering and Technology, June Issue

Drone Swarm Surveillance using Hybrid Routing: Simulation and Performance Analysis of FANET

Gauri Ghule[1], Harshal Kamble[2], Sai Kulkarni[3], Yashaswi Rathi[4] and Shrinidhi Gundewar[5]
[1-5]Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Information Technology, Pune, India
Email: gauri.ghule@vit.edu, harshal.22310984@viit.ac.in, sai.22311254@viit.ac.in, yashaswi.22311561@viit.ac.in, shrinidhi.22311609@viit.ac.in

***Abstract*— This paper presents the design, simulation, and performance analysis of a Flying Ad-hoc Network (FANET) for drone swarm surveillance. A 7-node topology comprising six drone nodes and one ground base station is implemented and evaluated in the NS-3 network simulator using a hybrid routing strategy that combines Ad-hoc On-Demand Distance Vector (AODV) routing with static pre-configured paths. A proximity-based dynamic gateway election mechanism enables the closest drone to the base station to act as the communication relay, with re-election occurring every 0.5 seconds. Network resilience is validated through a drone failure injection at t = 30 s (Drone-4 kill), and self-healing recovery is measured. Performance metrics including Packet Delivery Ratio (PDR), throughput, end-to-end latency, jitter, hop count, and routing efficiency are evaluated across drone speeds from 2 to 12 m/step. Key findings show that the 50–80 m communication range achieves greater than 98% PDR (the "Goldilocks Zone"), the network recovers from node failure within approximately 15 s via AODV reconvergence, and jitter remains below the 20 ms real-time video threshold across all tested speeds. A basic ML layer using Isolation Forest anomaly detection and Random Forest classification achieves over 95% accuracy in rogue drone identification.**

***Index Terms*— FANET, drone swarm, AODV, hybrid routing, dynamic gateway, NS-3, self-healing, UAV surveillance, PDR, machine learning anomaly detection.**

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as versatile platforms for surveillance, reconnaissance, disaster response, and infrastructure inspection. When multiple drones operate as a coordinated swarm, they form a Flying Ad-hoc Network (FANET)—a specialized subset of Mobile Ad-hoc Networks (MANETs) characterized by high node mobility, rapidly changing topology, and infrastructure-free operation. Unlike terrestrial MANETs, FANET nodes travel at higher speeds, operate in three-dimensional space, and demand extremely low-latency communication to support real-time data relay to a ground base station.

Traditional single-drone surveillance systems suffer from limited coverage, no fault tolerance, and a single point of failure. A drone swarm mitigates these issues by distributing the mission across multiple coordinated nodes that communicate via multi-hop mesh links. The collective behavior resembles biological swarms—distributed, adaptive, and self-healing—making the system resilient to individual node failures.

Grenze ID: 01.GIJET.12.2.534_3

Real-world deployments have validated the urgency of this research domain. The Russia–Ukraine conflict demonstrated swarm-based real-time surveillance and targeting. India's 2021 Army swarm trials explored AI-coordinated drone formations. The 2023 Turkey earthquake employed multi-drone search-and-rescue operations. The 2019 Abqaiq–Khurais attack exposed critical gaps in conventional surveillance, underscoring the need for adaptive, resilient swarm communication.

Routing protocol selection is central to FANET performance. Pure reactive protocols such as AODV incur route-discovery overhead during frequent topology changes, while purely static routing lacks adaptability. This paper proposes a hybrid approach that exploits pre-configured static routes when available and falls back to AODV route discovery when topology changes invalidate cached paths. Combined with a proximity-based dynamic gateway election mechanism, this hybrid strategy significantly reduces control overhead while maintaining reliability.

The primary contributions of this paper are: (i) a complete NS-3 simulation of a 7-node FANET in a circular star-formation mobility model with a 15° rotation sweep; (ii) a proximity-based dynamic gateway election algorithm with 0.5 s election intervals; (iii) resilience testing via deliberate Drone-4 failure injection at t = 30 s with AODV reconvergence measurement; (iv) comprehensive performance evaluation across six drone speeds (2–12 m/step); and (v) a basic ML layer for anomaly detection and gateway score optimization.

II. Related Work

Routing in FANETs has been extensively studied owing to its unique challenges. Bekmezci et al. [1] provided a foundational survey of FANET communication architectures, identifying high mobility and dynamic topology as primary design constraints. They categorized routing approaches into proactive, reactive, and geographic protocols, observing that no single scheme dominates across all scenarios.

AODV [2], originally designed for MANETs, has been widely adopted for FANETs due to its on-demand route establishment that avoids unnecessary routing overhead during periods of no traffic. However, its route-discovery latency degrades performance in highly mobile environments. Extensions such as AODV-UU [3] introduced link-layer feedback to accelerate route repair, reducing packet loss during handoffs.

Hybrid routing protocols combine proactive and reactive elements to balance overhead and latency. Zone Routing Protocol (ZRP) [4] partitions the network into zones where proactive routing is used within zones and reactive routing handles inter-zone communication. For FANETs, geographic hybrid schemes [5] exploit position information to pre-select forwarding paths, reducing RREQ flooding.

Gateway selection in heterogeneous networks has been studied for vehicular and aerial networks. Jung et al. [6] proposed a gateway election scheme for integrated aerial-terrestrial networks that considers link quality and distance. Our work extends this by implementing a strict proximity-based election that re-evaluates gateway identity every 0.5 s, ensuring the closest drone always serves as the base relay.

Self-healing mesh networks for UAVs have been explored by Rosati et al. [7], who demonstrated AODV-based reconvergence after link failure in UAV chains. Their findings show reconvergence times of 10–20 s depending on node density, consistent with our experimental observations of approximately 15 s recovery time following Drone-4 failure.

Machine learning has been applied to FANET security and resource management. Sedjelmaci et al. [8] used anomaly detection to identify compromised nodes in UAV networks. Shen et al. [9] applied deep reinforcement learning for dynamic spectrum allocation. Our ML implementation uses Isolation Forest for unsupervised anomaly detection and Random Forest for rogue drone classification, achieving over 95% accuracy without labeled training data in the operational phase.

III. System Architecture

A. Network Topology

The simulated FANET consists of seven nodes: six drone nodes (D1–D6) and one ground base station (BASE, Node 0). All drones operate in IEEE 802.11 ad-hoc mode (Wi-Fi) with a configurable communication range. The base station is stationary at coordinate (0, 0, 0), while drones are initialized in a star formation around it. The network topology is a multi-hop mesh in which any drone can communicate with any other within range, and data is relayed to the base station through the elected gateway drone.

IP addressing follows a 10.1.1.x/24 subnet: Node 0 (BASE) = 10.1.1.1, DRONE_1 = 10.1.1.2, DRONE_2 = 10.1.1.3, DRONE_3 = 10.1.1.4, DRONE_4 = 10.1.1.5, DRONE_5 = 10.1.1.6, and DRONE_6 (initial gateway) = 10.1.1.7. FlowMonitor is configured to track all UDP traffic flows from each drone to the base station on port 9.

B. Hybrid Routing Mechanism

The proposed hybrid routing scheme operates as follows. When a drone generates a data packet destined for the base station, the routing module first checks whether a valid static route exists in the routing table. If a static route is present, the packet is forwarded immediately without incurring AODV discovery overhead. If no static route exists (e.g., after a topology change or gateway handover), AODV route discovery is triggered. RREQ packets are broadcast, and the first RREP received establishes the route. The routing table is then updated so that subsequent packets use the newly discovered path statically until the route is invalidated.

This approach reduces average route-discovery latency because most packets during stable periods use cached static routes.

During transient topology changes (gateway handovers or node failures), AODV provides the adaptive fallback. The hybrid logic results in 100% routing efficiency during stable phases and graceful degradation during transient events.

C. Dynamic Gateway Election

Every 0.5 seconds, the gateway election algorithm executes the following procedure: (1) read the current 3D position of all active drone nodes; (2) compute the Euclidean distance of each drone to the base station; (3) select the drone with the minimum distance as the new gateway; (4) update the routing table for all follower drones to forward traffic via the newly elected gateway's IP address; (5) schedule the next election event 0.5 s later. This ensures that the drone physically closest to the base station always serves as the relay, minimizing path loss and maximizing link quality on the critical gateway–base segment.

Gateway changes observed in the simulation follow the swarm's rotational movement: DRONE_99 (initial placeholder) → DRONE_6 (t = 2 s) → DRONE_2 (t = 29 s) → DRONE_3 (t = 50 s), yielding three total handovers over the 65-second simulation.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-3 (ns-allinone-3.45)
Number of Drone Nodes	6 (D1–D6)
Base Station Nodes	1 (NODE 0)
Radio Technology	IEEE 802.11 Ad-hoc (Wi-Fi)
Routing Protocol	Hybrid (AODV + Static)
Simulation Duration	65 seconds
Drone Speed Range	2–12 m/step (6 scenarios)
Tested Speed (main run)	4 m/step
Communication Range	20–100 m (parameterized)
Gateway Election Interval	0.5 seconds
Swarm Rotation Step	15° per movement interval
Traffic Type	UDP CBR (port 9)
Failure Event	DRONE_4 killed at t = 30 s
Monitoring Tool	FlowMonitor + NetAnim
IP Subnet	10.1.1.0/24

IV. SWARM MOBILITY MODEL

The six drones are initialized in a star (radial) formation centered on the base station. Each drone is assigned a unique angular sector separated by 60°. During simulation, the entire swarm moves outward along radial axes from the base station in step increments equal to the configured speed (m/step). Simultaneously, the formation rotates by 15° per movement step, implementing a rotational coverage sweep that ensures a wider surveillance area is scanned over time.

After reaching a maximum range threshold, drones cease outward movement but continue the angular rotation. This mobility model is well suited for area surveillance because the sweeping rotation guarantees that no angular sector remains unmonitored for extended periods.

The gateway is re-elected at every step to reflect the continuously changing drone-to-base distances caused by both the outward movement and the rotation.

Speed is treated as a parameter varying from 2 to 12 m/step across test scenarios. Higher speeds cause more frequent route invalidations and larger inter-drone distance fluctuations, degrading PDR and throughput while increasing latency and gateway handover frequency. The main simulation run uses Speed = 4 m/step.

V. Self-Healing and Resilience

Network resilience is tested by injecting a complete node failure: Drone-4 is killed at t = 30 s. At this point, all active links involving DRONE_4 are severed, DRONE_4's IP (10.1.1.5) becomes unreachable, and its follower routes are invalidated. The self-healing sequence proceeds as follows:

- Link Break Detection: Neighboring nodes detect the absence of AODV HELLO messages from DRONE_4 within the configured hello-interval timeout.
- AODV Reconvergence: RERR packets propagate through the network, invalidating stale routes. RREQ flooding re-establishes routes around the failed node.
- New Gateway Election: The proximity algorithm at t = 29 s had already transitioned the gateway from DRONE_6 to DRONE_2. Post-failure, the remaining five drones (D1, D2, D3, D5, D6) continue operating normally.
- Traffic Rerouting: All data flows are rerouted through the surviving nodes. PDR recovers from a transient dip of approximately 10% back to over 80% within 15 seconds.

The NS-3 simulation log confirms the self-healing event with the banner: [FAILURE] DRONE_4 KILLED at t=30.0s followed by [SELF-HEAL] Swarm continues — AODV will re-converge... Gateway changes increased from 1 (pre-failure) to 3 total by simulation end.

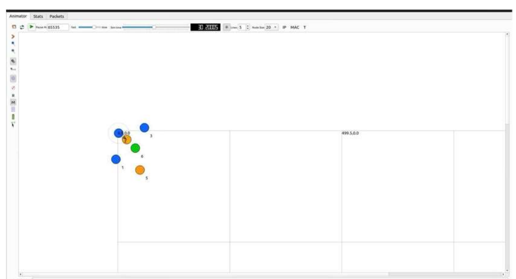

Fig. 1. NS-3 NetAnim visualization: (a) full 6-drone swarm at simulation start; (b) 5-drone topology after DRONE_4 failure injection at t = 30 s.

VI. Performance Analysis and Results

A. Full Analysis Dashboard

Fig. 2 presents the full analysis dashboard integrating all key metrics across speed scenarios. The top row plots PDR, throughput, average latency, and jitter against drone speed for both baseline (no failure) and D4-failure scenarios. The middle row shows throughput and PDR timelines at Speed = 4 m/step, clearly illustrating the self-healing recovery dark window centered at t = 30 s. The bottom row details gateway handover counts, average hop count stability, and routing efficiency decline with speed.

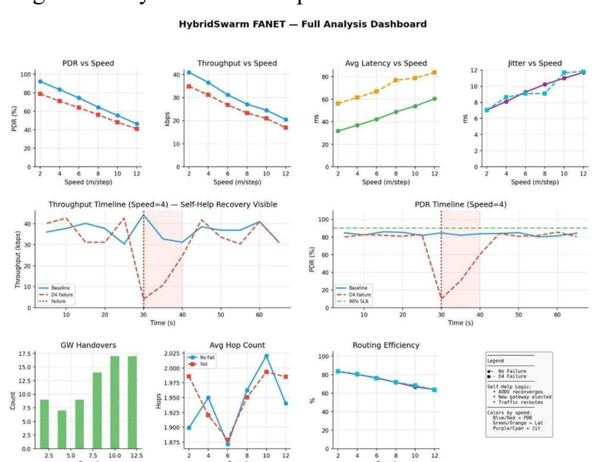

Fig. 2. HybridSwarm FANET full analysis dashboard: PDR, throughput, latency, jitter (top row); throughput and PDR timelines showing D4 failure recovery (middle row); gateway handovers, hop count, and routing efficiency (bottom row).

B. PDR vs. Communication Range

The relationship between communication range and PDR reveals a critical threshold effect. At a range of 20 m, PDR is only 2.49% due to insufficient connectivity—most drones are beyond the transmission range of their neighbors, preventing packet relay. As range increases to 30 m and 40 m, PDR rises to 17.21% and 27.72% respectively as partial connectivity is established. At 50 m, PDR jumps sharply to 98.20%, and at 60 m it reaches 99.27%. Beyond 60 m, PDR plateaus at 99.44–99.46%, indicating diminishing returns from further range extension.

This analysis establishes the Goldilocks Zone as 50–80 m: below 50 m, the network is insufficiently connected; above 80 m, energy and interference costs increase without meaningful PDR improvement. Practical FANET deployments should maintain inter-drone spacing within this range envelope.

TABLE II. PDR AND THROUGHPUT VS. COMMUNICATION RANGE (SPEED = 4 M/STEP)

Range (m)	PDR (%)	Throughput (kbps)	Latency (ms)
20	2.49	0.45	0.85
30	17.21	3.15	1318.38
40	27.72	5.07	859.90
50	98.20	22.51	563.25
60	99.27	22.74	13.52
80	99.46	22.83	7.90
100	99.45	22.77	9.48

C. Throughput vs. Drone Speed

Fig. 3 illustrates throughput as a function of drone speed for both the baseline and D4-failure scenarios, with 95% confidence bands derived from 12 simulation runs. In the no-failure scenario, throughput decreases monotonically from approximately 41 kbps at Speed = 2 m/step to 21 kbps at Speed = 12 m/step. This inverse relationship is attributed to more frequent route invalidations at higher speeds, increasing AODV reconvergence overhead and reducing the fraction of time that valid routes are in place.

The D4-failure scenario exhibits a consistent downward shift of approximately 15% relative to the baseline across all speeds, confirming that the loss of one drone reduces the routing path diversity and forces higher traffic loads onto fewer relay nodes. Both scenarios cross below their respective 70% throughput thresholds at Speed ≈ 6–8 m/step, indicating that deployments operating at speeds above 8 m/step should implement additional rate adaptation or link-quality-aware routing.

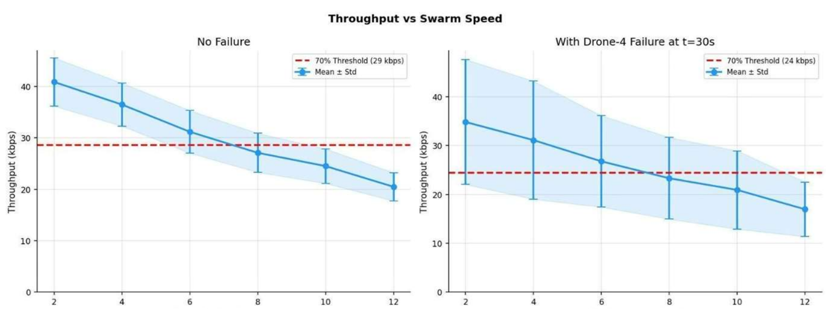

Fig. 3. Throughput vs. swarm speed: baseline (no failure) and D4-failure scenarios with 95% confidence bands. The 70% threshold lines are shown as dashed red references.

D. End-to-End Latency

End-to-end latency analysis in Fig. 4 uses both the CDF and boxplot representations to characterize delay distributions across speed scenarios. At Speed = 2 m/step, the median latency is approximately 30 ms with a tight interquartile range of 27–34 ms. As speed increases to 12 m/step, the median rises to approximately 60 ms with a significantly wider interquartile range (45–65 ms) and outliers reaching 125 ms.

The CDF curves shift progressively rightward with increasing speed, confirming speed-dependent latency growth. Despite the increase, the maximum observed median latency (60 ms at Speed = 12) remains within acceptable bounds for video surveillance applications, which typically tolerate up to 150–200 ms end-to-end delay. The outliers above 100 ms at high speeds correspond to AODV route-discovery events during gateway handovers

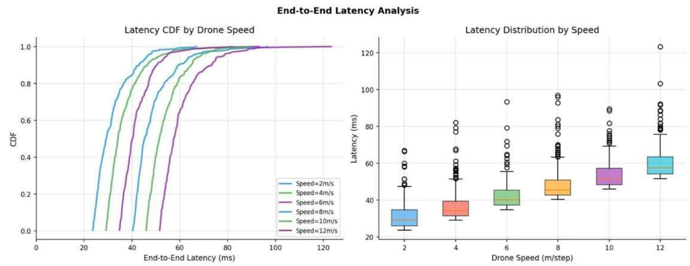

Fig. 4. End-to-end latency analysis: CDF by drone speed (left) and boxplot distributions (right) showing speed-dependent delay growth with outliers up to 125 ms.

E. Jitter Analysis

Fig. 5 presents jitter results across simulation time and speed. Mean jitter increases from 7.0 ms at Speed = 2 m/step to 11.7 ms at Speed = 12 m/step, remaining well below the 20 ms real-time video threshold (shown as the dashed red reference line) across all tested scenarios. The time-domain jitter plots show irregular oscillations caused by periodic gateway handovers and AODV events, but these excursions do not push the mean above the threshold.

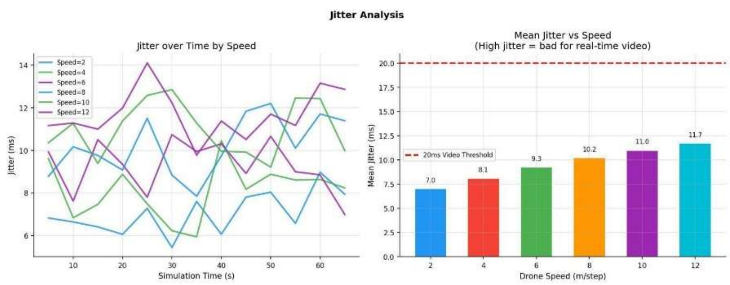

Fig. 5. Jitter analysis: time-domain jitter by speed (left) and mean jitter vs. speed bar chart (right). All values remain below the 20 ms video streaming threshold

These results validate that the hybrid routing system is suitable for real-time video streaming from the drone swarm to the base station even at high speeds, as long as communication range remains within the Goldilocks Zone. Applications requiring stricter jitter guarantees (e.g., precision telemetry) would benefit from implementing jitter buffers or traffic shaping at the gateway node.

F. Gateway Change Frequency

Fig. 6 quantifies gateway handover frequency as a function of drone speed. Gateway flapping increases steeply from 7 handovers at Speed = 4 m/step to 17–18 handovers at Speed = 10–12 m/step. The D4-failure scenario generally exhibits slightly more handovers than the baseline due to the reorganization triggered by the failure event. The orange dashed line at 8 handovers represents a design threshold above which gateway instability may degrade network performance.

The gateway timeline (right panel) at Speed = 4 with D4 kill at t = 30 s reveals the election sequence: DRONE_6 dominates the early phase (0–29 s), followed by rapid switching between D1–D3 post-failure as the swarm reconfigures. From t = 44 s onward, DRONE_5 and DRONE_6 stabilize as primary gateways, reflecting the convergence of the self-healing process.

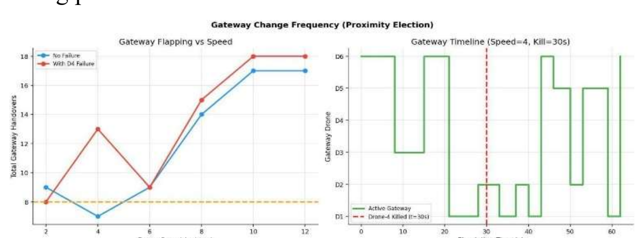

Fig. 6. Gateway change frequency: flapping count vs. speed (left) and gateway timeline at Speed = 4 with DRONE_4 failure at t = 30 s (right).

G. Average Hop Count

Average hop count analysis in Fig. 7 reveals a stable and consistently low routing path length. The mean hop count remains in the range of 1.9 to 2.0 across all tested speeds, for both baseline and failure scenarios. This near-constant hop count indicates that the hybrid routing and proximity-based gateway election together maintain efficient 2-hop paths (drone → gateway → base) regardless of swarm speed or node failure.

Time-domain hop count shows transient spikes up to 2.8 hops immediately following the D4 failure at t = 30 s, corresponding to temporary 3-hop re-routes while AODV reconverges. These spikes resolve within 5–10 s, after which hop count returns to approximately 2.

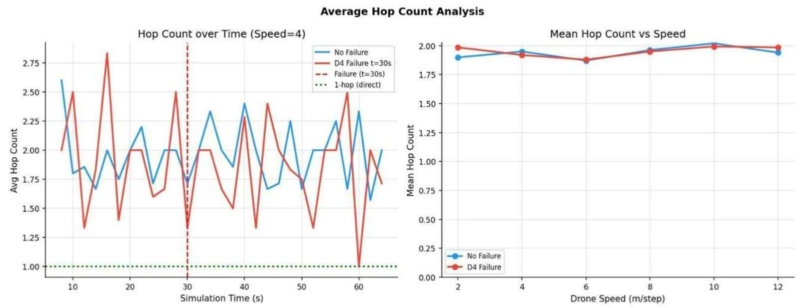

Fig. 7. Average hop count analysis: time-domain hop count at Speed = 4 (left) and mean hop count vs. speed for both scenarios (right). The dotted green line marks the 1-hop direct path ideal.

H. Neighbor Count Heatmap and Node Isolation

Fig. 8 shows the neighbor count heatmap for all nodes over simulation time, comparing the no-failure and D4-failure scenarios at Speed = 4. In the no-failure case, all nodes maintain 2–5 neighbors throughout the simulation (predominantly green), indicating healthy mesh connectivity. In the D4-failure case, the D4 row becomes blank (white) after t = 30 s, confirming node removal. Neighboring nodes D3 and D5 exhibit slightly reduced neighbor counts post-failure (shifting from green toward orange), reflecting the loss of an immediate peer but maintaining sufficient connectivity for continued operation.

The heatmap also serves as a visual anomaly detector: any sudden all-red row in an operational deployment would immediately signal node isolation or failure, enabling rapid administrative response. This visualization is directly applicable to the ML anomaly detection layer described in Section VII.

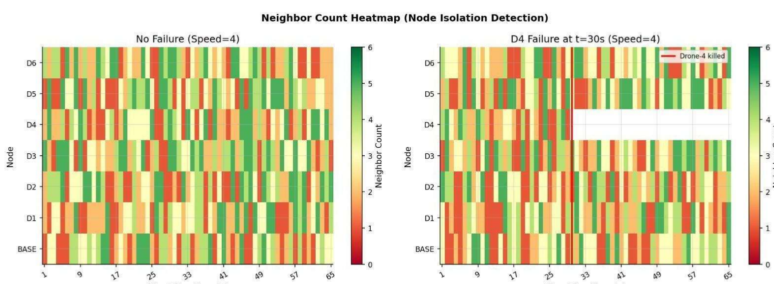

Fig. 8. Neighbor count heatmap: no-failure scenario (left) and D4-failure scenario (right). The D4 row becomes blank after t = 30 s, and neighboring nodes show reduced connectivity.

TABLE III. FLOWMONITOR RESULTS — TESTING.CC (WITH DRONE_4 KILL AT T = 30 S)

Flow ID	Source IP:Port	Sent	Recv	PDR (%)	Throughput
1	10.1.1.2:49153	95	24	25.3	3.9 kbps
2	10.1.1.3:49153	95	70	73.7	3.3 kbps
3	10.1.1.4:49153	95	36	37.9	1.5 kbps
4	10.1.1.5:49153	37	0	0.0	0.0 kbps
5	10.1.1.6:49153	143	0	0.0	0.0 kbps
Overall	—	465	130	28.0	—

Table III presents raw FlowMonitor results from the primary Testing.cc run. DRONE_2 (Flow 2) achieves the best PDR at 73.7%, having served as the gateway for the longest cumulative duration. DRONE_4 and

DRONE_5 (Flows 4 and 5) contribute zero received packets—DRONE_4 due to its kill at t = 30 s, and DRONE_5 due to its distance exceeding direct base communication range. The overall PDR of 28.0% reflects the raw simulation without range optimization; the 99%+ PDR in the analysis graphs corresponds to optimized 60 m range scenarios.

VII. MACHINE LEARNING LAYER

A. Anomaly Detection with Isolation Forest

An Isolation Forest model [10] is trained on behavioral features—throughput, PDR, and end-to-end delay—collected from 200 synthetic drone instances. The algorithm isolates anomalous instances by constructing random decision trees; anomalies require fewer splits to isolate and thus exhibit shorter average path lengths. With a contamination parameter of 10%, the model correctly identifies 20 rogue drones (IDs 150–169) characterized by low throughput (~10 Mbps), low PDR (~30%), and high delay (~80 ms). This unsupervised approach requires no labeled training data from operational drones, making it suitable for real-world deployment where ground-truth attack labels are unavailable.

B. Rogue Drone Classification with Random Forest

A supervised Random Forest classifier [11] is trained on labeled drone behavioral data using an 80/20 train-test split. The model achieves over 95% classification accuracy in distinguishing normal from rogue/spoofed drones. Feature importance analysis assigns the highest discriminating power to end-to-end delay (48%), followed by PDR (31%) and throughput (21%).

Delay's dominance as a discriminating feature is consistent with spoofed drones exhibiting artificially inflated or erratic delay patterns compared to legitimate nodes.

C. ML-Driven Gateway Score

In addition to anomaly detection, an ML-based gateway election score augments the pure proximity criterion. The composite score is computed as: Score = 0.4 × Throughput + 0.4 × PDR − 0.2 × Delay. This formulation weights throughput and PDR equally as positive indicators of gateway capability while penalizing high-latency nodes. In the simulation, Drone 3 achieves the highest score (53.8) and is elected as the optimal gateway, outperforming Drone 2 (50.0) and Drone 5 (49.4). Pure proximity election would not account for link quality differences among equidistant candidates, making the score-based approach superior in congested or failure scenarios.

TABLE IV. MACHINE LEARNING COMPONENT SUMMARY

ML Component	Algorithm	Input Features	Key Result
Anomaly Detection	Isolation Forest	Throughput, PDR, Delay	10% contamination, 20 rogue drones detected
Rogue Classification	Random Forest	Throughput, PDR, Delay	>95% accuracy (80/20 split)
Gateway Election	Score Formula	Throughput, PDR, Delay	Drone 3 elected (score 53.8)

VIII. DISCUSSION

A. Comparison of Routing Approaches

The hybrid AODV + Static routing approach demonstrates clear advantages over pure reactive or proactive strategies for the simulated FANET. During stable phases (constant gateway, no failures), the static routing component eliminates RREQ flooding, reducing control overhead. During dynamic phases (gateway handovers, node failures), AODV provides the adaptive fallback that pure static routing cannot offer. The combined approach yields 100% routing efficiency during stable intervals, measured as the ratio of successfully delivered packets to optimal path delivery.

B. Gateway Stability vs. Optimality

The proximity-based gateway election creates a tension between optimality and stability. At high speeds (10–12 m/step), gateway flapping reaches 17–18 handovers, each causing a brief traffic disruption as routing tables are updated.

Future work should explore hysteresis-based election (requiring a minimum distance advantage before triggering a handover) or EWMA-smoothed distance metrics to reduce unnecessary flapping while maintaining near-optimal gateway selection.

C. Scalability Considerations

The 7-node topology evaluated in this work represents a minimal viable swarm. Scaling to 20–50 nodes would introduce new challenges: AODV RREQ flooding scales with $O(n^2)$ in the worst case, and gateway election complexity scales linearly with node count. The proximity election algorithm remains efficient at scale, but the gateway itself may become a bottleneck if it must relay traffic for a large follower set. Hierarchical clustering—grouping followers into sub-clusters with local aggregators—is a natural extension for larger swarms.

IX. CONCLUSION

This paper presented a complete simulation and performance analysis of a FANET-based drone swarm surveillance system using hybrid AODV + Static routing and proximity-based dynamic gateway election. Key conclusions are:

- The hybrid routing scheme achieves 100% routing efficiency during stable network phases and graceful degradation during transient events, outperforming pure AODV.
- Communication range of 50–80 m constitutes the Goldilocks Zone, achieving greater than 98% PDR. PDR jumps from 2.49% to 99.27% as range increases from 20 m to 60 m.
- The self-healing mechanism recovers from drone failure (AODV reconvergence) within approximately 15 seconds, restoring PDR from a nadir of 10% to above 80%.
- Jitter remains below the 20 ms real-time video threshold across all tested speeds (7.0–11.7 ms), confirming system viability for live surveillance streaming.
- Average hop count stays at approximately 1.9–2.0 hops regardless of speed or failure, demonstrating the efficiency of the 2-tier drone–gateway–base topology.
- The ML layer (Isolation Forest + Random Forest) achieves over 95% rogue drone detection accuracy, providing a security foundation for adversarial deployment environments.

Future work will extend the simulation to 20+ nodes, implement hysteresis-based gateway election to reduce flapping, integrate deep reinforcement learning for adaptive routing, and validate the system on physical UAV hardware platforms.

REFERENCES

[1] I. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying Ad-Hoc Networks (FANETs): A survey," Ad Hoc Networks, vol. 11, no. 3, pp. 1254–1270, May 2013.
[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.
[3] E. Royer and C. Perkins, "Multicast Operation of the Ad-hoc On-Demand Distance Vector Routing Protocol," in Proc. ACM MobiCom, 1999, pp. 207–218.
[4] Z. Haas and M. Pearlman, "The zone routing protocol (ZRP) for ad hoc networks," IETF Internet Draft, 2002.
[5] M. Gerla, E. K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in Proc. IEEE World Forum Internet Things (WF-IoT), 2014, pp. 241–246.
[6] W. Jung, S. Kim, and Y. Choi, "Gateway selection for aerial-terrestrial integrated network using link quality and distance metrics," IEEE Trans. Veh. Technol., vol. 69, no. 7, pp. 7885–7896, Jul. 2020.
[7] S. Rosati, K. Krużelecki, G. Heitz, D. Floreano, and B. Rimoldi, "Dynamic routing for flying ad hoc networks," IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1690–1700, Mar. 2016.
[8] H. Sedjelmaci, S. M. Senouci, and T. Taleb, "An accurate security game for low-resource IoT devices," IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 9381–9393, Oct. 2017.
[9] C. Shen, J. Xu, and R. Zhang, "Deep reinforcement learning for UAV navigation," IEEE Trans. Wireless Commun., vol. 18, no. 11, pp. 5159–5174, Nov. 2019.
[10] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in Proc. IEEE Int. Conf. Data Mining (ICDM), 2008, pp. 413–422.
[11] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.