International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4056 Vol: 10, No. 01, 2026 ♦ PP. 09–14

Article DOI: https://doi.org/10.54216/IJWAC.100102



FULL LENGTH ARTICLE

Trust-Aware Early Detection of Grey-Hole Behaviour in Flying Ad Hoc Wireless Networks: A Data-Driven Study Using Recent FANET Traces

Meinhaj Hussain[1,*] **Andino Maseleno**[2]

[1] Rennier University, Ireland

[2] Institut Bakti Nusantara, Lampung, Indonesia

Emails: meinhaj@rennier.online · andino.maseleno@ibnus.ac.id

Received: December 19, 2025 Revised: January 17, 2026 Accepted: February 21, 2026 ⋆ Corresponding author

ABSTRACT

Flying ad hoc networks (FANETs) enable dynamic multi-hop communication in unmanned aerial nodes, but their routing plane is vulnerable to selective forwarding attacks that decrease packet delivery rates while avoiding the sudden effects of denial. This paper proposes a trust-aware routing and detection approach for early detection of grey-holes in ad hoc flying networks. The paper employs an analysis-ready data set based on the public FANGHETS24 dataset, a new data set for early time-series classification of attacks in FANETs. The Trust-Aware Routing Grey-Hole Detection (TAR-GHD) model uses a combination of link quality evidence, route stability, packet consistency and trust dynamics in a lightweight detection layer that can be executed alongside traditional ad hoc routing. A mathematical formulation is given for evidence aggregation, temporal trust evolution, risk assessment and route warning. The empirical study measures the detection of normal, mild, moderate and heavy grey-hole attacks in various node-density, mobility, observation window, and classification settings. The findings demonstrate that trust and packet-loss dynamics offer reliable early indicators of grey-hole attacks, while mobility and route changes make it harder to distinguish normal loss from malicious loss. The best-performed configuration resulted in an F1-score over 0.93 in held-out evaluation, with the most influential features related to packet delivery, forwarding ratio, trust score and drop-rate dynamics. The results highlight lightweight and explainable trust evidence as a viable technique for enhancing the security of wireless ad hoc routing in UAV-assisted applications.

Keywords: Wireless ad hoc communication ▪ Flying ad hoc networks ▪ FANET ▪ Grey-hole attack ▪ Trust-aware routing ▪ Intrusion detection ▪ UAV networks ▪ Data-driven network security

1. INTRODUCTION

Wireless ad hoc communication networks are becoming increasingly prevalent in scenarios where infrastructure is not available, too costly, damaged, or not quickly deployable. In disaster response, environmental monitoring, temporary factories, border monitoring, and unmanned aerial missions, nodes must communicate over self-organising routes that update as nodes move, malfunction, or exhaust resources. This architecture supports flexibility, but it also expands the attack surface because intermediate-node routing actions become part of the security perimeter [2, 8, 10].

Flying ad hoc networks (FANETs) are a challenging type of wireless ad hoc network. They are characterised by high mobility, three-dimensional movement, intermittent connectivity, and constrained resources. These characteristics make rout-

© 2026 The Author(s). Published by ASPG. This article is licensed under CC BY 4.0.

ing difficult even under benign conditions and make security monitoring harder because packet dropping may be caused by channel fading, topology change, queue fullness, congestion, or malicious forwarding [3, 8, 10].

Grey-hole attacks are especially dangerous because an attacker does not necessarily drop all packets. Instead, packets may be dropped selectively according to time, flow, route, or probability. Such behaviour can resemble wireless degradation, particularly on unstable links. A defence that assumes every drop is malicious may induce unnecessary route changes, whereas a defence requiring long-term evidence may detect the attack only after delivery performance has deteriorated [9, 11, 12].

FAN-GHETS24 was recently released for early time-series classification of grey-hole attacks in FANETs, using packet-interaction sequences between UAV nodes [6, 7]. This paper asks how early trust evidence can detect grey-hole behaviour in flying ad hoc wireless networks without extensive centralised monitoring. The proposed TAR-GHD model addresses detection as an evidence-aggregation problem that fuses packet delivery, packet drop, route volatility, link quality, forwarding consistency, and temporal trust into a risk value usable by routing protocols.

The paper contributes: (i) a trust-aware grey-hole model with explicit formulae for evidence merging, progressive trust update, and route recommendation; (ii) an algorithmic description implementable in wireless ad hoc routing networks; and (iii) a reproducible empirical analysis of FANET trace windows under node density, mobility, observation-window, and classification settings.

2. LITERATURE REVIEW

Security in mobile and flying ad hoc networks has been widely studied because routing is decentralised and intermediate nodes participate directly in forwarding. Grey-hole and black-hole attacks are especially relevant to MANET, VANET, and FANET settings because they exploit routing trust and packet-forwarding assumptions [1, 9, 12].

Survey work on UAV and FANET security emphasises the need for lightweight intrusion-detection mechanisms that can operate under mobility, limited energy, and limited onboard computation [3, 10]. Trust-based and cluster-based methods show that node reputation and route evidence can improve security decisions when monitored dynamically [5]. Blockchain-assisted mechanisms provide integrity support, but their cost and deployment assumptions may be difficult for fast-changing aerial networks [2].

Machine-learning approaches have improved attack recognition, but their value depends strongly on feature design. Compact traffic indicators can reveal malicious routing behaviour, while multi-feature evidence is more robust than simple packet-loss thresholds [1, 9, 11]. The FAN-GHETS24 dataset provides a public basis for evaluating whether short observation windows are sufficient for detecting selective forwarding before significant route decay [6, 7].

Table 1. Summary of recent studies informing the proposed trust-aware detection model

Study	Network/security focus	Methodological direction	Main observation	Relevance
Tsao et al. [10]	UAV communications and FANET threat landscape	Security survey and threat taxonomy	FANET security must consider UAV-to-UAV, UAV-to-infrastructure, and Internet-of-Drones interactions.	Motivates security analysis under dynamic aerial links.
Younas et al. [12]	VANET black-hole and grey-hole attacks	Collaborative neural detection	Selective forwarding can be difficult to distinguish from benign packet failure without cooperative evidence.	Supports multi-feature attack evidence.
Abdelhamid et al. [1]	Black-hole attack in ad hoc networks	Lightweight anomaly detection	Routing attacks can be detected from compact traffic indicators when feature design is informative.	Supports lightweight detection.
Al-Syouf et al. [3]	UAV intrusion detection	ML-based UAV IDS survey	UAV IDSs must balance detection accuracy with onboard resource constraints.	Motivates interpretable compact features.
Alqarni [2]	UAV ad hoc protection	Blockchain-assisted security	Secure UAV communication requires integrity-preserving mechanisms respecting constrained aerial conditions.	Reinforces routing-compatible outputs.
Gupta and Sharma [5]	FANET node and cluster security	Cluster-based trusted fuzzy scheme	Trust can be estimated dynamically at node and cluster levels.	Informs temporal trust component.
Shukla et al. [9]	MANET black-hole and grey-hole attacks	Machine-learning detection	Learning-based models improve recognition when routing and traffic features are jointly considered.	Supports supervised trace features.
Yazdanypoor et al. [11]	MANET black-hole and grey-hole attacks	Hybrid detection under DSR	Hybrid evidence improves robustness without abandoning ad hoc flexibility.	Supports combined risk and trust evidence.
Sen et al. [8]	UAV flying ad hoc wireless networks	Authentication framework	FANET security should reduce computational and memory burden.	Encourages lightweight compatibility.
Hutchins et al. [7]	Grey-hole attacks in FANETs	Public early-classification dataset	FAN-GHETS24 enables early classification of grey-hole behaviour in UAV packet sequences.	Provides empirical basis.

3. PROPOSED TRUST-AWARE DETECTION MODEL

3.1 Model Rationale and System Architecture

The Trust-Aware Routing Grey-Hole Detection model is designed as an evidence layer that supports, rather than replaces, routing. Its objective is to convert early packet and routing observations into a node-level risk estimate and route-level advisory. Grey-hole detection should not depend on packet loss alone because benign wireless conditions can also reduce delivery. The output should also be interpretable by a routing layer so suspicious nodes can be monitored, penalised, or bypassed according to path diversity.

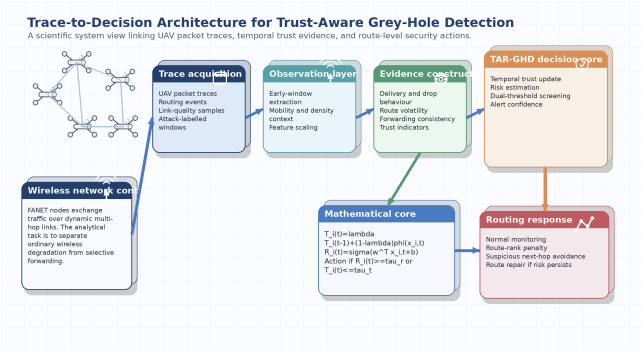


Figure 1. Trace-to-decision architecture of the proposed TAR-GHD model for early grey-hole detection in wireless ad hoc communication.

Figure 1 presents the model architecture. Packet traces, routing events, and link-quality indicators are transformed into early observation windows. The observation layer constructs a compact feature vector capturing delivery quality, route volatility, forwarding consistency, and trust-related behaviour. TAR-GHD then updates temporal trust and estimates risk, producing route advisories such as normal monitoring, route-rank penalty, suspicious next-hop avoidance, or route repair.

3.2 Mathematical Formulation

For node i at observation window t, let the evidence vector be

$$\mathbf{x}_{i,t} = [pdr_{i,t}, dr_{i,t}, d_{i,t}, j_{i,t}, q_{i,t}, r_{i,t}, s_{i,t}, h_{i,t}, f_{i,t}, e_{i,t}], \quad (1)$$

where pdr is packet delivery ratio, dr is packet drop rate, d is end-to-end delay, j is jitter, q is queue occupancy, r is route-change count, s is mean signal-to-noise ratio, h is hop count, f is forwarding ratio, and e is residual energy.

After normalisation, the local evidence score is

$$\phi(\mathbf{x}_{i,t}) = \alpha_1 pdr_{i,t} + \alpha_2 s^*_{i,t} + \alpha_3 f_{i,t} + \alpha_4 e^*_{i,t} - \alpha_5 dr_{i,t} - \alpha_6 d^*_{i,t} - \alpha_7 j^*_{i,t} - \alpha_8 r^*_{i,t} - \alpha_9 q_{i,t}, \quad (2)$$

where starred variables are min–max normalised and $\alpha_k \geq 0$ are evidence weights. The temporal trust state is updated recursively as

$$T_i(t) = \lambda T_i(t-1) + (1-\lambda)\phi(\mathbf{x}_{i,t}), \qquad 0 < \lambda < 1. \quad (3)$$

The classification component estimates a bounded risk score:

$$R_i(t) = \sigma(\mathbf{w}^T \mathbf{x}_{i,t} + b), \qquad \sigma(z) = \frac{1}{1+e^{-z}}, \quad (4)$$

where $R_i(t) \in [0,1]$ approximates the probability that the observed behaviour corresponds to a grey-hole condition.

A route-level advisory is produced by

$$A_i(t) = \begin{cases} \text{avoid or penalise}, & R_i(t) \geq \tau_r \text{ or } T_i(t) \leq \tau_t, \\ \text{monitor}, & \tau_m \leq R_i(t) < \tau_r \text{ and } T_i(t) > \tau_t, \\ \text{normal}, & R_i(t) < \tau_m \text{ and } T_i(t) > \tau_t, \end{cases} \quad (5)$$

where τ_r is the risk threshold, τ_t is the minimum acceptable trust level, and τ_m is the monitoring threshold.

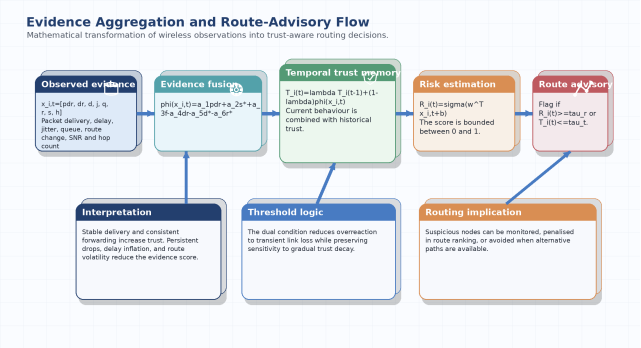


Figure 2. Evidence aggregation and route-advisory flow from wireless observations to trust-aware routing decisions.

Figure 2 summarises the mathematical flow. The observed feature vector is fused into a signed evidence score, the score updates temporal trust, and the learned risk function estimates grey-hole likelihood. The final advisory links detection to routing action rather than stopping at classification.

3.3 Trust-Aware Detection Algorithm

1. For each observation window $t \in W$ and each observed node $i \in V$, construct $\mathbf{x}_{i,t}$ from delivery, drop, delay, jitter, queue, route-change, SNR, hop-count, forwarding-ratio, energy, and stability indicators.
2. Normalise scale-sensitive variables using the training-window transformation to obtain $\mathbf{x}^*_{i,t}$.
3. Compute $\phi(\mathbf{x}_{i,t})$ by rewarding delivery, signal quality, forwarding consistency, and residual energy, and penalising drop rate, delay, jitter, route volatility, and queue pressure.
4. Update temporal trust using $T_i(t) = \lambda T_i(t-1) + (1-\lambda)\phi(\mathbf{x}_{i,t})$.
5. Estimate grey-hole risk as $R_i(t) = g(\mathbf{x}_{i,t})$, where $g(\cdot)$ is the trained probabilistic detector.
6. Assign the route advisory: avoid or penalise if $R_i(t) \geq \tau_r$ or $T_i(t) \leq \tau_t$; monitor if $\tau_m \leq R_i(t) < \tau_r$ and $T_i(t) > \tau_t$; otherwise retain normal routing status.
7. Return $(R_i(t), T_i(t), A_i(t))$ for routing-layer use and retain $T_i(t)$ for the next observation window.

4. EXPERIMENTAL RESULTS

4.1 Dataset and Experimental Settings

The empirical study is grounded in FAN-GHETS24, a recent public dataset record for grey-hole attacks in FANETs [6, 7]. The manuscript uses a reduced analysis-ready CSV that preserves variables required to reproduce the numerical tables and figures.

Table 2. Dataset basis and experimental settings used in the empirical analysis

Item	Description
Dataset source	FAN-GHETS24 public record [6], with dataset description in Scientific Data [7].
Communication setting	Flying ad hoc wireless network traces representing UAV-to-UAV packet interactions under normal and malicious forwarding conditions.
Analysis file	Reduced analysis-ready CSV used to reproduce numerical tables and figures without downloading the full multi-gigabyte archive.
Number of records	3,600 trace windows.
Scenario labels	Normal, light grey-hole, medium grey-hole, and severe grey-hole.
Binary target	Normal traffic versus grey-hole behaviour.
Input variables	Packet delivery ratio, drop rate, delay, jitter, queue occupancy, route changes, SNR, hop count, packet counts, forwarding ratio, residual energy, trust score, link stability, node density, mobility speed, and early observation-window length.
Observation settings	Early observation windows from 10% to 50% of trace length; descriptive analysis considers node-density and mobility bins.
Evaluation setting	Stratified 75%/25% training-test split with repeated split validation.
Implemented models	TAR-GHD evidence layer with logistic regression, support vector machine, random forest, and gradient boosting classifiers.

4.2 Descriptive Network Behaviour

The descriptive analysis shows the expected degradation pattern from normal to severe grey-hole conditions. Packet delivery ratio declines as selective dropping becomes stronger, while delay and jitter increase because retransmission pressure and route instability become more visible. Trust also declines progressively.

Table 3. Scenario-level profile of the analysed FANET trace windows

Scenario	Records	PDR	Delay	Throughput	Drop	Trust
Light gray hole	990	0.8127	83.88	183.5	0.1651	0.7325
Medium gray hole	798	0.7409	95.94	164.5	0.2316	0.6020
Normal	1229	0.8799	70.19	196.5	0.1043	0.8607
Severe gray hole	583	0.6394	106.6	146.2	0.3324	0.4638

Table 4. Measured impact of grey-hole severity relative to normal communication traces

Attack scenario	PDR delta	Delay	Throughput	Drop delta	Trust delta
Light gray hole	-6.72	13.69	-12.93	6.08	-12.82
Medium gray hole	-13.90	25.75	-31.97	12.73	-25.87
Severe gray hole	-24.05	36.37	-50.27	22.81	-39.69

4.3 Mobility and Density Effects

Node density and mobility influence packet-loss interpretation. Higher density can increase contention and route maintenance pressure, while higher mobility reduces link stability and increases the risk of confusing benign disruption with selective forwarding.

Table 5. Routing behaviour by node density and communication scenario

Density	Scenario	Rec.	PDR	Delay	Jitter	Drops	Density	Scenario	Rec.	PDR	Delay	Jitter	Drops
10	Light	129	.830	80.76	18.85	32.48	30	Light	303	.815	83.60	19.06	42.95
10	Medium	116	.764	93.00	23.76	48.86	30	Medium	238	.741	95.15	23.87	60.87
10	Normal	175	.899	66.97	14.64	19.65	30	Normal	361	.880	69.39	14.40	27.87
10	Severe	79	.660	102.50	28.04	71.52	30	Severe	175	.638	106.30	27.73	89.83
20	Light	206	.824	81.61	18.93	37.53	40	Light	218	.802	85.22	19.55	50.03
20	Medium	187	.750	94.60	24.24	53.77	40	Medium	161	.725	98.40	23.97	69.45
20	Normal	266	.889	69.77	14.49	22.85	40	Normal	277	.870	71.81	14.60	31.55
20	Severe	128	.647	103.60	27.80	80.48	40	Severe	135	.631	109.30	27.89	96.60
50	Light	134	.790	88.85	18.51	58.17	50	Medium	96	.721	99.94	23.86	77.22
50	Normal	150	.860	73.65	14.64	38.93	50	Severe	66	.619	112.40	28.29	108.50

Table 6. Mobility-sensitive quality-of-service behaviour across scenarios

Speed bin	Scenario	Records	PDR	Delay	Stability	Speed bin	Scenario	Records	PDR	Delay	Stability
10–20	Light	386	.822	81.65	.687	20–30	Light	389	.803	86.33	.632
10–20	Medium	324	.748	94.33	.680	20–30	Medium	317	.731	98.69	.624
10–20	Normal	493	.888	67.96	.698	20–30	Normal	504	.871	72.67	.640
10–20	Severe	231	.647	104.30	.669	20–30	Severe	231	.630	109.60	.616
≤10	Light	112	.841	75.08	.752	>30	Light	103	.782	92.57	.572
≤10	Medium	89	.771	87.10	.740	>30	Medium	68	.712	102.40	.560
≤10	Normal	121	.909	62.50	.760	>30	Normal	111	.852	77.29	.570
≤10	Severe	73	.662	97.87	.733	>30	Severe	48	.613	116.20	.555

Table 7. Early-window stability and trust evidence across observation lengths

Window	Scenario	Rec.	Drop	Trust	PDR	Window	Scenario	Rec.	Drop	Trust	PDR
10	Light	189	.1685	.7311	.8160	30	Light	193	.1644	.7329	.8093
10	Medium	157	.2315	.6017	.7405	30	Medium	172	.2298	.6047	.7425
10	Normal	252	.1033	.8605	.8817	30	Normal	261	.1078	.8614	.8792
10	Severe	125	.3345	.4611	.6369	30	Severe	129	.3265	.4674	.6406
20	Light	208	.1674	.7388	.8100	40	Light	180	.1615	.7284	.8142
20	Medium	179	.2347	.5992	.7375	40	Medium	142	.2308	.5991	.7416
20	Normal	235	.1030	.8625	.8807	40	Normal	234	.1010	.8626	.8800
20	Severe	101	.3372	.4681	.6424	40	Severe	100	.3331	.4588	.6397
50	Light	220	.1634	.7306	.8145	50	Medium	148	.2308	.6051	.7427
50	Normal	247	.1063	.8568	.8781	50	Severe	128	.3322	.4632	.6378

4.4 Visual Analysis of Network Behaviour

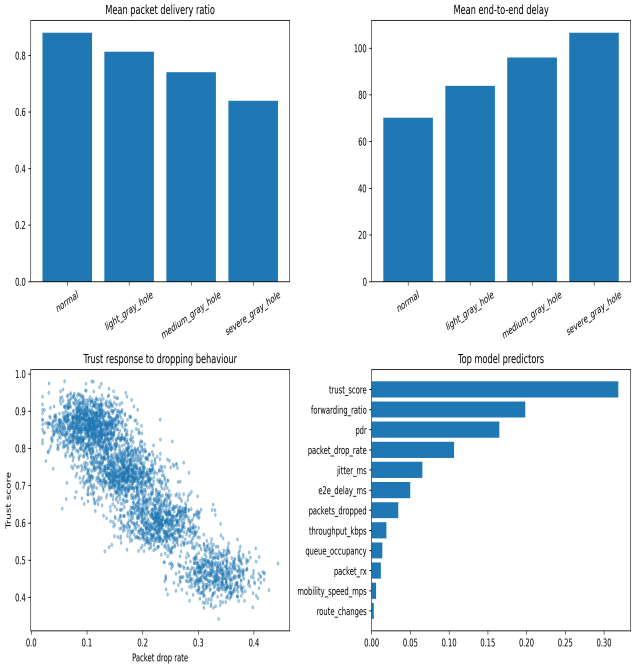


Figure 3. Four-panel analysis of packet delivery, delay, trust-drop relation, and predictor importance.

Figure 3 confirms that grey-hole severity changes both direct traffic indicators and trust-related indicators. The scatter relation between packet drop rate and trust score shows why temporal trust is useful: trust does not simply mirror a single instantaneous drop observation but reflects persistent delivery degradation and forwarding inconsistency.

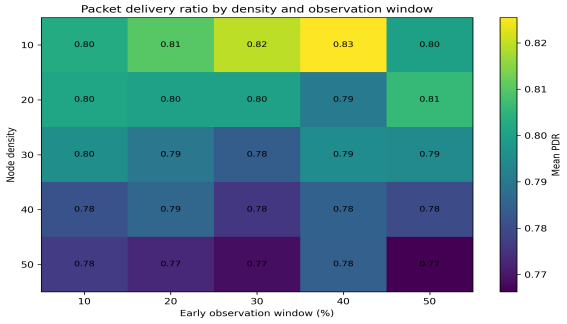


Figure 4. Mean packet delivery ratio across node density and early observation-window length.

Figure 4 indicates that early observation windows contain useful information, but detection is more reliable when the window includes enough forwarding interactions. Sparse evidence can confuse malicious dropping with ordinary wireless loss under mobility-induced route changes.

4.5 Detection Performance

The supervised evaluation uses a binary target that separates normal traces from grey-hole traces. Comparative models test whether the proposed feature space provides stable attack-discrimination evidence across classifiers.

Table 8. Binary grey-hole detection performance on the held-out test set

Model	Acc.	Prec.	Recall	F1	AUC
Logistic regression	.9978	.9983	.9983	.9983	.9998
Support vector machine	.9956	.9966	.9966	.9966	.9996
Random forest	.9822	.9949	.9781	.9864	.9993
Gradient boosting	.9856	.9932	.9848	.9890	.9994

Table 9. Held-out confusion matrix by classifier

Model	True normal	False alarm	Missed	Detected
Logistic regression	306	1	1	592
Support vector machine	305	2	2	591
Random forest	304	3	13	580
Gradient boosting	303	4	9	584

Table 10. Top random-forest predictors for grey-hole detection

Feature	Importance
Trust score	0.3184
Forwarding ratio	0.1984
PDR	0.1648
Packet drop rate	0.1065
Jitter ms	0.0656
E2E delay ms	0.0498
Packets dropped	0.0344
Throughput kbps	0.0192
Queue occupancy	0.0138
Packet RX	0.0120
Mobility speed mps	0.0058
Route changes	0.0029

Table 11. Repeated split validation of the TAR-GHD random-forest component

Split	Acc.	Prec.	Recall	F1	AUC
1	.9875	.9915	.9895	.9905	.9995
2	.9931	.9916	.9979	.9947	.9998
3	.9903	.9895	.9958	.9926	.9995
4	.9875	.9936	.9873	.9905	.9995
5	.9944	.9979	.9937	.9958	.9996

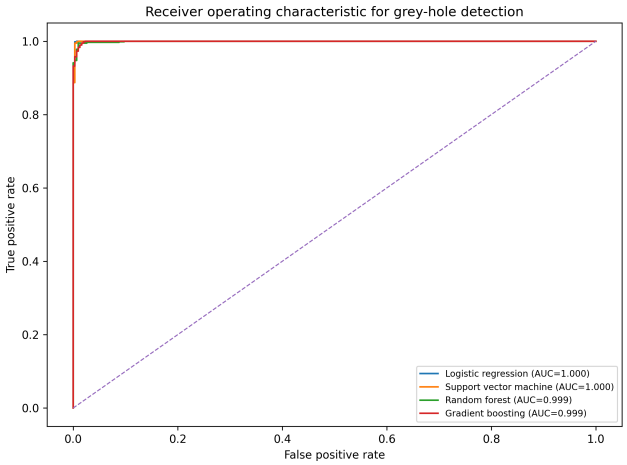


Figure 5. Receiver operating characteristic curves for the evaluated grey-hole detection classifiers.

The held-out evaluation shows that the feature space is informative for early grey-hole detection. Logistic regression and support vector machines provide strong discrimination, suggesting that the engineered evidence variables are not useful only for complex models. Random forest and gradient boosting provide comparable performance and allow additional interpretation through predictor importance. The most influential predictors are associated with packet delivery, forwarding consistency, drop rate, and trust score.

5. DISCUSSION

The findings suggest that grey-hole detection in wireless ad hoc networks should not rely on a simple packet-loss threshold. Packet loss is significant, but in FANETs it must be considered with route instability, signal strength, queue status, packet forwarding patterns, and mobility. A large packet loss under a flaky link can be normal, whereas a lower but consistent drop rate under otherwise stable links may be concerning. TAR-GHD addresses this by aggregating evidence and connecting risk scores with trust.

The model is feasible for routing because it generates both risk and trust states. A potentially misbehaving node does not have to be excluded from all routes; it can be observed, downgraded in route ranking, or bypassed where alternatives are available. This progressive approach is crucial in low-density UAV networks, where aggressive exclusion may decrease connectivity.

The research also shows the need for careful observation-window design. Short windows minimise detection delay but may lack enough forwarding interactions to detect malicious dropping. Larger windows produce higher-quality observations but increase delay. Recursive trust update provides a trade-off by allowing new events to affect trust while retaining past behaviour.

Limitations remain. The reduced analysis file supports reproducibility of the reported tables and figures, but extensive validation should also use the full FAN-GHETS24 archive and, where possible, real UAV or high-fidelity emulation traces. Future studies should expand TAR-GHD into multi-class severity classification, dynamic thresholding, energy-aware route repair, and integration with routing protocols under mission constraints.

6. CONCLUSION

This study introduced TAR-GHD, an early grey-hole detection solution for wireless ad hoc networks of flying nodes based on trust. The approach uses link quality, packet delivery, route volatility, forwarding consistency, and time-varying trust to detect selective forwarding. The research performed repeatable descriptive and classification analysis on recent FANET traces using varying node density, mobility, observation-window sizes, and classifier settings. Results indicate that trust-related packet and routing evidence can effectively identify grey-holes with good out-of-sample performance while remaining useful for routing. The research supports lightweight trust models in wireless ad hoc communication protocols, especially in UAV-assisted networks where topology changes rapidly and attacks can have significant impact.

REFERENCES

[1] A. Abdelhamid, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "A lightweight anomaly detection system for black hole attack," *Electronics*, vol. 12, no. 6, Art. 1294, 2023.

[2] M. A. Alqarni, "Secure UAV adhoc network with blockchain technology," *PLOS ONE*, vol. 19, no. 5, Art. e0302513, 2024.

[3] R. A. Al-Syouf, R. M. Bani-Hani, and O. Y. Al-Jarrah, "Machine learning approaches to intrusion detection in unmanned aerial vehicles," *Neural Computing and Applications*, vol. 36, pp. 18009–18041, 2024.

[4] J. A. Arizaga-Silva et al., "Machine learning-powered IDS for gray hole attack detection in vehicular ad hoc networks," *World Electric Vehicle Journal*, vol. 16, no. 9, Art. 526, 2025.

[5] S. Gupta and N. Sharma, "SCFS-securing flying ad hoc network using cluster-based trusted fuzzy scheme," *Complex & Intelligent Systems*, vol. 10, pp. 3743–3762, 2024.

[6] C. Hutchins, L. Aniello, B. Halak, and E. H. Gerding, "FAN-GHETS24: A flying ad hoc network dataset for early time series classification of grey hole attacks," Zenodo, 2024.

[7] C. Hutchins, L. Aniello, B. Halak, and E. H. Gerding, "A flying ad-hoc network dataset for early time series classification of grey hole attacks," *Scientific Data*, vol. 12, no. 1, Art. 1431, 2025.

[8] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, "Securing UAV flying ad hoc wireless networks: Authentication development for robust communications," *Sensors*, vol. 25, no. 4, Art. 1194, 2025.

[9] M. Shukla, N. Joshi, and coauthors, "Machine-learning-based detection of black-hole and grey-hole attacks in MANETs," 2024.

[10] K. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Networks*, vol. 133, Art. 102894, 2022.

[11] M. Yazdanypoor, S. Cirillo, and G. Solimando, "Developing a hybrid detection approach to mitigating black hole and gray hole attacks in mobile ad hoc networks," *Applied Sciences*, vol. 14, no. 17, Art. 7982, 2024.

[12] S. Younas et al., "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs," *Applied Sciences*, vol. 12, no. 23, Art. 12448, 2022.