INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 12, Issue 5 - V12I5-1226)
Available online at: https://www.ijariit.com

AI-Driven Anomaly Detection, Identification and Countermeasures for Unmanned Aerial Vehicles: A Review of Sensor-, Flight-Data- and Counter-UAV-Based Approaches

Tuba Reyaz
tubareyaz04@gmail.com
Integral University, Lucknow, India

Mr. Aftab Alam
er.aaftab@gmail.com
Integral University Lucknow

Dr. Faiyaz Ahmad
faiyaz@iul.ac.in
Integral University Lucknow

ABSTRACT

Unmanned aerial vehicles (UAVs) are now used in logistics, agriculture, surveillance and the low-altitude economy, but their growth has created two linked problems: keeping UAVs themselves safe from faults and attacks, and protecting airspace from unauthorized UAVs. This paper reviews 111 studies compiled from seven source papers published between 2019 and 2026 (two comprehensive surveys on counter-UAV sensing and flight-data anomaly detection, one survey on machine learning and large language models (LLMs) for UAV safety and security, and four technical studies). The studies are organized into five areas: (i) multi-sensor detection, identification and localization of hostile UAVs; (ii) physical and cyber countermeasures; (iii) flight-data anomaly detection and recovery; (iv) sensor-malfunction and GNSS-spoofing detection; and (v) vibration-based fault detection and AI-driven safety and security, including LLMs. For each area we summarize the methods, reported accuracy and stated limitations, and compare them in tables. The review shows that deep learning with sensor fusion consistently outperforms single-sensor and classical methods, but that results are hard to compare because datasets differ, anomalies are usually injected artificially, and real-flight validation is rare. We close with a set of research gaps and future directions: public benchmarks, real-flight testing, onboard-efficient models, federated and LLM-based approaches, and joint safety-security frameworks.

Keywords: *UAV, Drone, Anomaly Detection, Counter-UAV, Multi-Sensor Fusion, Deep Learning, Reinforcement Learning, GNSS Spoofing, Large Language Models, Flight Data*

1. INTRODUCTION

UAVs have moved from military use into everyday civil applications. This growth brings two kinds of risk. The first is internal: sensor faults, actuator failures, software errors and cyber attacks such as GPS spoofing can cause a UAV to crash or be hijacked. A review of US Federal Aviation Administration (FAA) data cited in the flight-data survey of Yang et al. found that 90 of 104 UAV accidents (86.54%) were caused by system faults [54]. The second risk is external: small, cheap and low-flying UAVs can be misused near airports, public events and critical infrastructure, and are hard to detect because of their small radar cross-section, low speed and low altitude [1], [3].

These two problems have been studied by largely separate communities. Counter-UAV research focuses on detecting, identifying, localizing and neutralizing unauthorized UAVs using radar, radio-frequency (RF), optical, thermal and acoustic sensors [1], [35]. Flight-data research focuses on finding abnormal behaviour inside a UAV's own telemetry and sensors, using model-based, data-driven and deep-learning methods [24], [54]. A third, newer line of work applies machine learning, deep learning and LLMs to a wide range of safety and security tasks [91]. This review brings the three lines together.

The contributions of this paper are:

- a unified classification of 111 studies drawn from seven source papers;
- comparative tables of detection accuracy, countermeasure range and limits, and anomaly-detection performance;
- a critical discussion of why reported results are not directly comparable; and
- a list of open research gaps and future directions.

© 2026, IJARIIT - All rights reserved.

The rest of the paper is organized as follows. Section 2 describes the scope and method of the review. Section 3 gives a taxonomy. Sections 4 to 9 review each area. Section 10 discusses cross-cutting findings and gaps, Section 11 gives future directions, and Section 12 concludes.

2. REVIEW SCOPE AND METHOD

This review is built from seven source papers. The first row of each source in the compiled tables is the paper itself; the remaining rows are works that paper reviews, compares against or cites. In total the tables contain 111 numbered entries, and we use these numbers as citation keys in square brackets (for example [24]); the full list is given in the References section.

Table -1: Source papers used in this review.

Source	Reference	Focus	Entries
S1	Tao et al. (2026), arXiv:2510.22947v2	Multimodal multi-sensor fusion for UAV identification, localization and countermeasures in the low-altitude economy	[1]–[14]
S2	Battersby (2026), MS thesis, UMass Dartmouth	Reinforcement learning for sensor malfunction detection; sensor fusion vs raw data	[15]–[23]
S3	Yang, Li and Zhu (2024), J. Comput. Des. Eng. 11(2), 176–193	Multivariate regression-based anomaly detection and recovery of UAV flight data	[24]–[34]
S4	Samaras et al. (2019), Sensors 19, 4837	Systematic review of deep learning on multi-sensor data for counter-UAV	[35]–[53]
S5	Yang, Li, Li, Zhang and Zhang (2023), Sci. China Technol. Sci. 66(4), 901–919	Survey of UAV flight data anomaly detection	[54]–[80]
S6	Yilmaz, Ozkat and Gul (2026), Drones 10, 321	Vibration-driven deep learning for rotary-wing UAV anomaly detection	[81]–[90]
S7	Yang, Zhang, Zeng et al. (2025), Drones 9, 392	AI-driven UAV safety and security, from machine learning to LLMs	[91]–[111]

Two cautions apply throughout. First, most accuracy figures come from the studies cited by each source, not from the source papers themselves, and are reported on different datasets, so they cannot be ranked directly. Second, where a source gives no figure we write "not reported" and do not estimate one. Entries marked as baselines or ablations in the compiled tables (for example [25]–[30] and [82]–[85]) are results from a single experimental study, and are comparable with each other only within that study.

3. TAXONOMY OF THE REVIEWED LITERATURE

The 111 entries fall into five areas, summarized in Table 2.

Table -2: Classification of the reviewed studies.

Area	Goal	Typical sensors / data	Representative methods	Entries
A. Counter-UAV sensing	Detect, classify and localize unauthorized UAVs	Radar, RF, camera, thermal, acoustic	CNN, SVM, YOLO, Faster R-CNN, DBN, MLP, STFT	[1]–[8], [35]–[53]
B. Countermeasures	Neutralize or capture hostile UAVs	Laser, microwave, jamming, spoofing, net capture	GAN, LSTM, DRL, vision-based DL	[9]–[14]
C. Flight-data anomaly detection	Find and recover abnormal onboard data	Telemetry, IMU, navigation sensors	LSTM, 1D CNN, autoencoders, PCA, SVM, Kalman filters	[24]–[34], [54]–[80]
D. Sensor malfunction and GNSS spoofing	Detect faulty sensors and spoofed navigation	GPS/GNSS, IMU, accelerometer	DQN, random forest, SVM, wavelets, LSTM	[15]–[23], [96]–[99]
E. Vibration-based and AI-driven safety/security	Detect structural faults; apply AI and LLMs to safety and security tasks	Vibration, battery data, images, network data	CWT + CNN-BiGRU-SSM-AE, LLMs, RL, multitask learning	[81]–[95], [100]–[111]

4. COUNTER-UAV DETECTION, IDENTIFICATION AND LOCALIZATION

4.1 Overall framework

Tao et al. propose a closed-loop framework in which UAVs are first identified, then localized, then countered, using short-time Fourier transform (STFT) with deep learning, Transformers, digital twins, deep reinforcement learning (DRL), GANs and LSTM [1]. The paper is a survey and conceptual framework with no experiments, and it names data scarcity, adversarial UAVs and weak signals from small UAVs as open problems. Samaras et al. reach a complementary conclusion from a systematic review of deep learning for counter-UAV: micro-Doppler radar is the most promising single sensor, thermal-camera work on UAVs is almost non-existent, and sensor fusion is needed. They recommend a system built from radar, two thermal cameras, a pan-tilt-zoom optical camera and acoustic arrays, fused by deep learning [35].

4.2 RF-based identification

RF fingerprinting identifies a UAV from the signal it transmits. Li et al. used an ASPConv-ResNet34 network and reported an average test accuracy of 99.97%, showing that deep learning beats non-deep-learning RF methods by a wide margin [2]. The limitation of RF methods in general is that a UAV flying without any transmission (a "silent" UAV) cannot be detected [5], [6].

4.3 Radar and micro-Doppler classification

Radar works in any light or weather and gives long range, which is why it dominates the counter-UAV literature [3]. Kang et al. reached at least 85% identification with at most 5% false alarms from Doppler spectrum analysis, but the method is weak on low, slow, small UAVs and cannot separate hovering UAVs from static objects [3]. Harman showed that staring radar can produce 50 detections per second and track irregular paths, though confusion with birds grows as targets shrink [4].

The radar work reviewed by Samaras et al. shows a clear progression from hand-crafted features to deep learning (Table 3). Early work used STFT features with SVM and Naive Bayes and reached 82% on 11 classes at 30 m range [36]. Empirical mode decomposition (EMD) improved accuracy to 89.54% [37] and 92.61% with entropy features [38]. Singular value decomposition (SVD) features at Ka band separated UAVs from artificial birds with 100% accuracy [39]. The first CNN trained directly on micro-Doppler spectrograms reached 99.59% on six classes, though only two drones were used [40]. Using real X-band surveillance radar, a two-stream 1D CNN reached 95% for UAV versus other targets [43]. Several of the highest numbers come from weak test conditions: close range [37], [38], artificial birds [39], or synthetic data where accuracy depends heavily on signal-to-noise ratio [44].

Table -3: Radar- and acoustic-based UAV classification results reported in the reviewed literature.

Entry	Authors (year)	Method	Reported accuracy	Main limitation
[36]	Molchanov et al. (2014)	STFT + SVM / Naive Bayes	82% (11 classes)	30 m range; dwell time under 0.25 s
[37]	Oh et al. (2017)	EMD + nonlinear SVM	89.54%	Close range only
[38]	Ma et al. (2018)	EMD + entropy + SVM	92.61%	Close range only
[39]	Fuhrmann et al. (2017)	SVD + SVM (Ka band)	100% (UAV vs bird); 96.2% (UAV type)	Birds were artificial
[40]	Kim, Kang, Park (2016)	GoogleNet CNN on Doppler images	99.59% (6 classes)	Two drones only
[41]	Mendis et al. (2016)	Spectral correlation + DBN	90% (3 classes)	Only 3 UAV types
[43]	Samaras et al. (2019)	Two-stream 1D CNN	95% (UAV vs other)	Not reported
[44]	Regev et al. (2017)	MLP on complex radar signal	100% (2 classes)	Near-perfect only on synthetic data
[45]	Mohajerin et al. (2014)	MLP on track features	99%	Not reported
[50]	Kim et al. (2017-18)	KNN / ANN on sound (one microphone)	83% to 86%	Single microphone

4.4 Vision, thermal and acoustic detection

For camera-based detection, Faster R-CNN with a VGG-16 backbone gave the best detection, and the authors argue that birds should be treated as a separate class because they raise false positives [46]. YOLO was the fastest detector while Faster R-CNN was the most accurate, and public annotated drone data is scarce, so a synthetic dataset was created by pasting drones onto natural images [47]. For thermal imagery, the only evidence comes from pedestrian detection, where halfway (middle-level) fusion of colour and thermal images worked best [48]; this suggests but does not prove a similar result for UAVs.

Acoustic detection is cheap but short-ranged. Jeon et al. found that data augmentation improved drone sound detection in real environments, but the system could not detect drones beyond about 150 m [49]. Kim et al. added a background-noise class and improved accuracy from 83% to 86% using one microphone [50].

4.5 Multi-sensor fusion

Fusion is the most consistent recommendation across sources. Park et al. combined a homemade radar with microphones using three voting MLPs; the system had no false negatives and few false positives but only about 50 m range [51]. Hengy et al. and Laurenzis et al. showed that acoustic arrays plus radar cut false alarms and gave localization with bearing errors of 1.5 degrees in azimuth and -2.5 degrees in elevation, about 6 m in position [52]. Diamantidou et al. fused deep features from several sensors in a multimodal network [53], which supports the fused system recommended in [35]. In Battersby's work on onboard sensors, physics-based sensor fusion likewise outperformed raw data (see Section 7) [15].

4.6 Localization and cooperative identification

Time-difference-of-arrival (TDOA) localization needs at least three synchronized stations and angle-of-arrival (AOA) needs at least two; both reach precision within 30 m at ranges of 3 km or more, but neither can find a silent UAV [5], [6]. Remote ID, in which a UAV broadcasts its identity, position and speed, depends on GNSS, has a range of up to 2 km and works only if the UAV cooperates, so it is useful for whitelisting and authentication rather than for finding hostile UAVs [7]. Integrated sensing and communication (ISAC) on 5G-Advanced base stations reuses existing infrastructure and has been deployed at Baoshan Airport and on the Zhoushan

route; it reached at least 95% identification with at most 5% false alarms and localization within 10 m over 1.2 to 1.5 km, although single-station coverage is limited and the technology is at an early commercial stage [8].

5. COUNTERMEASURES AGAINST HOSTILE UAVS

Tao et al. review six countermeasure families and the AI methods that support them [1]. Table 4 compares them. No accuracy figure is reported for any of them; the useful comparison is range, side effects and failure cases.

Table -4: Countermeasures against hostile UAVs.

Entry	Countermeasure	AI method used	Reported range / effect	Limitations
[9]	UAV Hunter net-capture UAV (Zhang, Lu, Yang et al., 2024)	Vision-based DL + DRL path planning	Up to 300 m	Single target; hard to aim
[10]	Laser weapons (Liao et al., 2023)	DL trajectory prediction	Up to 2 km; precise, low cost per shot	Weather sensitive; high system cost
[11]	High-power microwave (Karcz et al., 2024)	DL threat assessment	0.5 to 3 km; about 10 kV/m neutralized test electronics	Large footprint; collateral damage
[12]	RF jamming (Simon and Gotthans, 2022)	GAN shapes jamming signal to spare nearby links	1 to 3 km omnidirectional; 3 to 5 km directional	High electromagnetic interference
[13]	Navigation spoofing (AlAbidy et al., 2024)	Closed-loop DL spoofing	At least 5 km; can redirect or force-land	Ineffective against inertial navigation
[14]	Protocol cracking (Comparetti et al., 2009; Zhang et al., 2022)	LSTM protocol analysis	3 to 5 km; zero collateral interference	Ineffective against DIY UAVs

The table shows a trade-off between range, precision and collateral effects. Kinetic and directed-energy options (net capture, laser) are precise but short-ranged or weather-limited; microwave weapons are area-denial tools with collateral damage; jamming and spoofing have long range but affect other links or fail against UAVs that do not rely on radio or satellite navigation; protocol cracking avoids interference but is defeated by custom-built UAVs. AI mainly contributes at the sensing and planning end (trajectory prediction, threat assessment, signal shaping) rather than as the effector itself.

6. FLIGHT-DATA ANOMALY DETECTION AND RECOVERY

6.1 Survey view

Yang et al. survey flight-data anomaly detection and conclude that data-driven methods dominate, that most work is still theoretical, that real abnormal data is scarce, and that there is no standard flight-data database [54]. They divide methods into knowledge-based, model-based and data-driven groups.

6.2 Knowledge-based and model-based methods

Early approaches use expert knowledge or physical models. An adaptive-threshold neural network for rotorcraft sensor failure adapts to flight conditions and beats fixed thresholds but depends on expert knowledge [55]. A particle filter with fuzzy inference predicts navigation-sensor anomalies early, but particle-filter computation is heavy and unknown anomalies are missed [56]. Kalman-filter variants have been used for sensor and actuator faults: an extended Kalman filter (EKF) is fast but has no fault-tolerant strategy [59]; a dual unscented Kalman filter separates state and parameter estimation on a NASA GTM model [64]; and an EKF with ensemble methods gives more practical airspeed fault detection but at high computation cost [65]. Linear parameter-varying observers [60], least squares with bias compensation for formations [63], sparse optimization for UAV groups [62], and vision-based fault detection, isolation and recovery [61] all share the same weakness: they need accurate physical models or expert knowledge.

6.3 Classical data-driven methods

Data-driven alternatives avoid the need for an accurate model. Principal component analysis (PCA) needs little training data and raised no false alarms on anomaly-free flights, but it overlooks data recovery [31], [66]. Kernel PCA gave satisfactory results on simulated sensor data [32]; hybrid methods (PAA + SVDD + KPCA) lower false positives but were tested only on simulated and Minnesota data [71]. Support vector approaches include a real-time detector for small fixed-wing UAVs that copes with timing deviations but overfits with few samples [75], and active learning with an improved semi-supervised SVM (S3VM), which lowers labelling cost [19], [33], [68]. Other methods include sparse modelling with T-Digest [57], relevance vector machines [73], multivariate Gaussian mixture models [74], clustering of log files [58] and multivariate regression with Pearson correlation for input selection, which captures only linear correlation [72].

6.4 Deep-learning methods

Deep models learn time-series features automatically. LSTM networks are strong at both detection and recovery [67]. Autoencoder variants include LSTM-AE for distributed detection (a single AE can lose too much information) [76], stacked recurrent autoencoders with dynamic thresholding for lower latency [77], and GAN-based trajectory detection that finds contextual anomalies an autoencoder misses [78]. KL divergence with an ANN exploits spatial and temporal correlations online [70], and ANFIS gives fast, robust navigation-sensor fault detection although accuracy and false alarms need work [69].

6.5 A representative comparison: CA-1DCL-EF

Yang, Li, Li and Zhu proposed CA-1DCL-EF, which combines correlation analysis with maximal information coefficient (MIC) for parameter selection, a hybrid 1D CNN-LSTM model and EWMA error filtering [24]. Table 5 compares it with baselines on two flight datasets, T98 and T104. Accuracy is reported for bias and drift anomalies respectively.

Table -5: Detection accuracy (%) on injected bias / drift anomalies and recovery error (Yang et al., 2024 and baselines).

Entry	Method	T98 accuracy (bias / drift)	T104 accuracy (bias / drift)	T98 bias recovery MAE	Notes
[24]	CA-1DCL-EF (proposed)	97.44 / 96.59	91.53 / 94.22	0.04107	Best accuracy and TPR
[25]	LSTM-RF (Wang et al., 2019)	93.34 / 93.72	81.50 / 80.31	0.04744	0% false alarms on T98; TPR as low as 60.63% on T104
[26]	STC-LSTM (Zhong et al., 2022)	84.22 / 89.03	85.41 / 87.34	0.04638	21.44% false alarms on T98 bias
[27]	KNN, k = 50	74.19 / 78.06	64.59 / 69.25	0.09682	Weakest overall; false positives up to 30.94%
[28]	SVR, RBF kernel	81.44 / 81.69	65.09 / 71.31	0.04184	Zero false alarms on T98 but TPR about 63%
[29]	LSTM alone (ablation)	80.22 / 79.72	89.81 / 93.84	0.04096	Misses sharp local changes
[29]	1D CNN alone (ablation)	87.69 / 92.66	67.16 / 68.96	0.07214	Weaker on temporal data

Three observations follow. First, the hybrid model beats all baselines on accuracy, and neither LSTM nor 1D CNN alone performs well on both datasets [29]. Second, in the ablation, removing correlation-based parameter selection hurts most (84.84% / 80.53% on T98 without it), MIC beats Pearson correlation especially on T104, and removing error filtering costs a smaller amount (96.13% / 96.38% on T98) [30]. Third, LSTM alone has a slightly lower recovery error on T98 bias (0.04096 versus 0.04107) than the full model, so the proposed method's advantage lies mainly in detection, not recovery. Limitations are that anomalies were injected by hand (bias and drift only), noise impact was not fully assessed, the threshold is static and baselines are not exhaustive [24].

6.6 Public datasets

The ALFA dataset provides 47 processed flights with 7 fault types, including 23 sudden engine failures, and gives fault ground truth [79]. The University of Minnesota Thor datasets provide public flights with 75 to 95 parameters and are widely used as a benchmark [80]. These two are the main public resources named in the reviewed work, which is one reason many studies fall back on injected anomalies.

7. SENSOR MALFUNCTION AND GNSS SPOOFING DETECTION

7.1 Reinforcement learning with sensor fusion

Battersby applied a deep Q-network (DQN) with a 5-step sliding window to find malfunctions in UAV sensors, comparing three input engines: raw data, physics-based sensor-fused data, and a combination of both [15]. At an attack rate of 0.3, the sensor-fused engine reached 88.06% accuracy on Dataset A and 87.45% on Dataset B, against 67% for raw data, with F1 of 0.81 and 0.79 against 0.12 for raw data and 0.09 for the combination. Training reward was 77,930 for sensor fusion, 24,100 for raw and 28,100 for the combination. Adding raw data to the fused data caused the model to inherit the weaknesses of the raw-data engine. The study is limited by afterwards-injected anomalies, a single drone (DJI Neo), east-coast wooded sites with good weather, no test on drone hardware, and detection delay from the sliding window [15]. This result argues against a competing view that fewer features are better: Yoo et al. proposed a memory-augmented autoencoder with a concise feature set [23], but the thesis argues this leaves the AI to guess the physics.

7.2 Other sensor-data studies

Galvan et al. extracted IMU features and found a CNN-only model best among CNN, LSTM and DNN; it is the only reviewed study that simulated hours of flight [16]. Wei et al. note that few sensor types are used in spoofing studies, so sensor errors can be mistaken for spoofing, and different datasets make accuracy comparison unreliable [22].

7.3 GNSS spoofing detection

Table 6 collects spoofing-detection studies. Classical machine learning on multi-channel GPS receivers found random forest best across three missions [17], and wavelet decomposition with SVM was the cheapest and most accurate on GPS and Galileo datasets [18]. Non-AI methods are also represented: Kwon compares GPS acceleration with the onboard accelerometer [20], and Chen's behaviour-rule intrusion detection (BRUIDS) flags an attack when time spent in safe states (165 of 4,608 states) falls below a threshold [21]; both were tested only in simulation. The high accuracy figures in Table 6 come from the AI-safety survey [91]; its common limitation is poor scalability and generalization [96].

Table -6: GNSS-spoofing detection studies.

Entry	Authors (year)	Method	Reported performance	Limitation
[17]	Mouzai et al. (2025)	Decision tree, random forest, XGBoost on multi-channel GPS	Random forest best on 3 missions	Real outdoor attacks are illegal and risky; indoor tests may be biased
[18]	Babic et al. (2025)	Wavelet transform + SVM, KNN, random forest	SVM best on all datasets	Depends on advanced statistics
[20]	Kwon (2020)	GPS vs accelerometer (statistical)	Simulated detection and false-alarm probability	Simulation only
[21]	Chen (2014)	BRUIDS behaviour rules	Attack flagged by time in safe states	Monte Carlo simulation only
[96]	Xidian Univ. (2022)	ML on sensor data	99.69% detection rate	Poor scalability and generalization
[97]	Xidian Univ. (2023)	ML on signal features	94.87% detection; EER about 5%; 0.4 s cycle	Same as above
[98]	King Abdulaziz Univ. (2024)	Adversarial deep learning	98% average	Same as above
[99]	Beirut Arab Univ. (2025)	Genetic-algorithm-tuned LSTM	Accuracy 86.0% to 99.0%; F1 83.0% to 99.0%	Same as above

8. VIBRATION-BASED ANOMALY DETECTION FOR ROTARY-WING UAVS

Yilmaz, Ozkat and Gul propose a model for rotary-wing UAVs that converts vibration signals into continuous wavelet transform (CWT) scalograms and passes them through a CNN-BiGRU-SSM autoencoder (a state-space model autoencoder) [81]. Their main idea is to order recorded fault segments by severity to build a continuous degradation trajectory (about 7.5 hours of data per axis), rather than treating faults as discrete states, which is how earlier vibration studies treat them [86]–[90]. Table 7 compares the model with baselines.

Table -7: Vibration-based anomaly detection on the same data (Yilmaz et al., 2026).

Entry	Model	Precision	Recall	F1	AUROC
[81]	CWT + CNN-BiGRU-SSM-AE (proposed)	0.9959	0.4428	0.6131	0.9284
[82]	Isolation Forest	0.9812	0.1043	0.1886	0.7215
[83]	One-Class SVM	0.9863	0.1307	0.2308	0.7579
[84]	LSTM-AE	0.9921	0.3014	0.4630	0.9027

All models have very high precision but low recall, so the gain comes from catching more anomalies without raising false alarms. Classical models catch only extreme outliers and miss subtle temporal patterns [82], [83]; temporal modelling gives a large gain [84]. In the ablation, test flag rates were 18.84%, 44.20% and 27.54% for CNN-AE, CNN-BiGRU-AE and the full model, which shows that BiGRU raises sensitivity and the state-space module with throttle conditioning balances it [85]. The authors acknowledge that degradation is reconstructed by sorting segments rather than recorded live, that the data come from one indoor laboratory quadrotor, and that few baselines were used [81]. Comparison with other vibration-based or flight-parameter studies [86]–[90] is qualitative only.

9. AI-DRIVEN SAFETY AND SECURITY, INCLUDING LARGE LANGUAGE MODELS

Yang, Zhang, Zeng et al. map machine learning, deep learning and LLMs (including Claude, GPT, Grok, Gemini, LLaMA, DeepSeek, Qwen and Kimi) onto five safety and five security areas, and argue that LLMs can address the data, generalization and interpretability gaps of traditional approaches. They also list the obstacles: LLM latency, limited onboard compute, privacy leakage, poor adaptation to extreme environments, multi-UAV coordination and network quality [91]. Table 8 groups selected studies from that survey by application.

Table -8: AI methods for UAV safety and security (selected studies from Yang et al., 2025).

Entry	Application	Method	Reported result
[92]	Flutter test signal extraction	EMD + CNN	100% on test sets
[93]	Battery management	DNN + LSTM (SOC); random forest (SOH)	SOH 92%; SOC MSE 7.6e-4
[94]	Cross-battery state estimation	LLM framework	2.17% MAE, zero-shot
[95]	Early battery degradation	Transformer-based LLM	0.87% MAE

Entry	Application	Method	Reported result
[100]	Dynamic obstacle detection	ML detection + feature tracking (RGB-D)	0.11 m position error; 0.23 m/s velocity error
[101]	Obstacle-avoidance trajectory planning	Gradient-based DL planner	98% success
[102]	LEVIOSA, language to swarm paths	GPT-4o	76.0% success
[103]	Reinforcement-learning flight control	PPO with CRM reward	71% simulated; 52% real flight
[104]	Position and orientation prediction	Multitask CNN	Above 0.91 position accuracy
[105]	Accident detection and advice	YOLOv11s + Moondream2 + GPT-4 Turbo	94.7% accuracy; recall 86.8%; mAP@0.5 92.8%
[106]	UAV detection and identification	Deep learning	100% detection; type 94.6%; state 87.4%
[107]	CNN UAV identification	CNN	94.5% detection rate
[108]	Pilot authentication	DL	95.24%; hijack detection 96.82%
[109]	Pilot identification and operation evaluation (MTL-PIE)	Multitask learning	95.36%; operation 94.47%; 35 ms
[110]	Resilient routing	Adaptive Q-learning	25.23% less overhead; 9.41% higher packet delivery; 5.12% less energy
[111]	Network security with generative AI	Generative AI + diffusion models	25% gain in classification accuracy; over 10% higher communication rates

Two results stand out. The reinforcement-learning flight controller dropped from 71% in simulation to 52% in real flight [103], a concrete example of the simulation-to-real gap. And LLM-based battery estimation reached low error without target-domain training [94], [95], showing early promise for LLMs outside text tasks. Limits reported across this group include unstable battery models across operating conditions and scarce data [93], accuracy loss in changing environments for identification [106], and privacy leakage and sensitive-data dependence in network applications [110].

10. DISCUSSION

10.1 Comparative findings

Several patterns repeat across all five areas.

- **Deep learning beats classical methods when data is available.** RF identification [2], radar CNNs [40], [43], flight-data hybrids [24] and vibration autoencoders [81] all outperform SVM, KNN, Isolation Forest and other classical baselines in their own studies.
- **Fusion helps.** Radar plus acoustic [51], [52], multimodal deep networks [53] and physics-based sensor fusion [15] each outperform single-source inputs. The exception to simple stacking is that combining raw and fused data hurt performance [15].
- **Hybrid architectures balance weaknesses.** Combining a CNN's local-feature strength with an LSTM's temporal strength gave the most balanced results [24], [29]; BiGRU with a state-space module did the same for vibration data [85].
- **Cooperative and non-cooperative methods are complementary.** Remote ID [7] works only with cooperating UAVs; radar, RF, vision and acoustic sensors are needed for the rest [1], [35].

10.2 Why results cannot be ranked

Accuracy figures in this review are not comparable across rows. Datasets differ and some are synthetic or artificial [39], [44]; many spoofing and flight-data studies rely on injected anomalies [15], [24]; ranges and test conditions differ [37], [38], [49], [51]; and the surveys themselves report no accuracy [1], [35], [54], [91]. Several of the strongest numbers (for example 100% accuracy [39], [44], [92], [106]) come from restricted or synthetic settings.

10.3 Research gaps

1. **No standard benchmark.** Only ALFA [79] and the Thor datasets [80] are named public flight-data benchmarks, and there is no standard database for flight anomalies [54]. Public annotated drone images are also scarce [47].
2. **Injected anomalies instead of real ones.** Hand-injected bias and drift [24], afterwards-injected faults [15] and reconstructed degradation [81] limit how far results transfer to real failures.
3. **Little real-flight or hardware validation.** The thesis was not tested on drone hardware [15], several detectors were tested only in simulation [20], [21], and RL control lost almost 20 percentage points in real flight [103].
4. **Narrow test conditions.** One drone model and good weather [15], one indoor quadrotor [81], and two drones [40] are typical.
5. **Thermal and long-range sensing are under-studied.** Thermal UAV work is almost non-existent [35], and acoustic [49], [51] and micro-Doppler [36] results are limited to short range.
6. **Missing recovery in many detectors.** PCA, KPCA, S3VM and LSTM-AE studies overlook data recovery [31]–[34].

7. **Static thresholds and detection delay.** A static threshold [24] and sliding-window delay [15] limit online use.
8. **Deployment limits for LLMs and large models.** Latency, onboard compute and privacy leakage [91], [110].
9. **Adversarial and low-signature UAVs.** Weak signals from small UAVs and adversarial UAVs [1], silent UAVs [5], [6], and countermeasures that fail against inertial navigation [13] or DIY UAVs [14].

11. FUTURE RESEARCH DIRECTIONS

- **Public, real-flight benchmarks** with labelled real anomalies, multiple airframes and weather conditions, covering both flight-data faults and counter-UAV sensing.
- **Hardware-in-the-loop and flight testing** of detectors, with explicit measurement of detection delay and onboard compute cost.
- **Fused, multi-sensor counter-UAV systems** following the radar, thermal, optical and acoustic design recommended in [35], and ISAC-based infrastructure sensing [8].
- **Federated learning, quantum receivers and LLMs,** which Tao et al. name as future work [1], to address data scarcity and privacy.
- **Lightweight LLMs and multimodal models** for onboard or edge use, targeting the latency and compute limits in [91].
- **Continuous degradation modelling and condition-conditioned detectors,** extending the vibration trajectory idea [81] to live data.
- **Adaptive thresholds and online recovery,** so that detection and recovery are handled in one pipeline [24].
- **Joint safety-security frameworks** that separate sensor faults from spoofing attacks, addressing the confusion noted in [22].
- **Robust countermeasures** that combine AI-based sensing with measures effective against silent, inertial-navigation and DIY UAVs [13], [14].

12. CONCLUSION

This review organized 111 studies from seven source papers into counter-UAV sensing, countermeasures, flight-data anomaly detection, sensor-malfunction and spoofing detection, and vibration-based and AI-driven safety and security. Across these areas, deep learning, hybrid architectures and multi-sensor fusion repeatedly outperform single-sensor and classical baselines. The evidence base is, however, uneven: results come from different datasets, many rely on injected or synthetic anomalies, and few have been validated on real hardware or in varied conditions. Progress will depend on shared real-flight benchmarks, deployable lightweight models, and frameworks that treat UAV safety and airspace security together. The tables and entry numbers in this paper are designed to let readers trace each claim back to its source study.

REFERENCES

Source papers

S1. Tao, Gao, Ye, Xu et al. (2026). Intelligent Multimodal Multi-Sensor Fusion-Based UAV Identification, Localization, and Countermeasures for Safeguarding Low-Altitude Economy. arXiv:2510.22947v2.

S2. Battersby, M. M. (2026). Finding Malfunctions in UAV Physical Sensors using Reinforcement Learning; Sensor Fusion versus Raw Data. MS thesis, UMass Dartmouth.

S3. Yang, Li, Li and Zhu (2024). Data-driven multivariate regression-based anomaly detection and recovery of UAV flight data. J. Comput. Des. Eng., 11(2), 176-193.

S4. Samaras et al. (2019). Deep Learning on Multi Sensor Data for Counter UAV Applications: A Systematic Review. Sensors, 19, 4837.

S5. Yang, Li, Li, Zhang and Zhang (2023). A survey of UAV flight data anomaly detection: Technologies, applications, and future directions. Sci. China Technol. Sci., 66(4), 901-919.

S6. Yilmaz, Ozkat and Gul (2026). Signal Intelligence: Vibration-Driven Deep Learning for Anomaly Detection of Rotary-Wing UAVs. Drones, 10, 321.

S7. Yang, Zhang, Zeng et al. (2025). AI-Driven Safety and Security for UAVs: From Machine Learning to Large Language Models. Drones, 9, 392.

[1] Tao, Gao, Ye, Xu et al. (2026). Multimodal multi-sensor fusion for UAV identification, localization and countermeasures.

[2] Li et al. (2024). RF-fingerprint UAV identification with ASPConv-ResNet34.

[3] Kang et al. (2021). Radar micro-Doppler of small UAVs.

[4] Harman (2015). Staring vs scanning radar (Alarm).

[5] Sinha and Guvenc (2022). TDOA localization.

[6] Jiang et al. (2020). AOA localization.

[7] Belwafi et al. (2022). Remote ID.

[8] Gao et al. (2015-2023). 5G-A ISAC low-altitude sensing.

[9] Zhang, Lu, Yang et al. (2024). UAV Hunter net-capture UAV.

[10] Liao et al. (2023). Laser anti-drone weapons.

[11] Karcz et al. (2024). High-power microwave.
[12] Simon and Gotthans (2022). Deep learning for RF jamming.
[13] AlAbidy et al. (2024). Navigation spoofing.
[14] Comparetti et al. (2009); Zhang et al. (2022). Protocol cracking.
[15] Battersby, M. M. (2026). Finding malfunctions in UAV physical sensors using reinforcement learning.
[16] Galvan et al. (2021). Sensor data-driven UAV anomaly detection using deep learning.
[17] Mouzai et al. (2025). Multi-channel GPS receivers for detecting spoofing on UAVs.
[18] Babic et al. (2025). GNSS spoofing detection with wavelets and machine learning.
[19] Pan et al. (2020). UAV anomaly detection with active learning and improved S3VM.
[20] Kwon (2020). Direct GPS spoofing detection with AHRS/accelerometer.
[21] Chen (2014). BRUIDS, behavior-rule intrusion detection for malicious UAVs.
[22] Wei et al. (2022). Machine learning spoofing detection.
[23] Yoo et al. (2025). MemAE with a concise feature set.
[24] Yang, Li, Li and Zhu (2024). Multivariate regression-based anomaly detection and recovery of UAV flight data (CA-1DCL-EF).
[25] Wang et al. (2019). LSTM-RF, LSTM with residual filtering.
[26] Zhong et al. (2022). STC-LSTM, spatio-temporal correlation LSTM.
[27] Liu and Ding (2015); Alos and Dahrouj (2020). KNN-based anomaly detection.
[28] Bronz et al. (2020). SVM/SVR regression.
[29] Yang et al. (2024). Ablation: LSTM alone vs 1D CNN alone.
[30] Yang et al. (2024). Ablation: parameter selection, error filtering, PCC vs MIC.
[31] Alos et al. (2020). PCA-based UAV behavior assessment.
[32] Duan et al. (2017). UAV sensor anomaly detection with KPCA.
[33] Pan et al. (2020). UAV anomaly detection with active learning and improved S3VM.
[34] Yang et al. (2023). Unsupervised LSTM-AE for UAV height anomalies.
[35] Samaras et al. (2019). Deep learning on multi-sensor data for counter-UAV: systematic review.
[36] Molchanov et al. (2014). UAV vs bird classification from micro-Doppler.
[37] Oh et al. (2017). Mini-UAV classification with empirical mode decomposition.
[38] Ma et al. (2018). EMD entropy features for mini-UAVs.
[39] Fuhrmann et al. (2017). Micro-Doppler classification at Ka band.
[40] Kim, Kang and Park (2016). Drone classification with CNN on merged Doppler images.
[41] Mendis et al. (2016). Deep learning Doppler radar for micro-UAS.
[42] Wang et al. (2019). CNN radar target detection.
[43] Samaras et al. (2019). UAV classification from surveillance radar.
[44] Regev et al. (2017). Counting propellers and blades with an MLP.
[45] Mohajerin et al. (2014). UAV vs bird track classification.
[46] Saqib et al. (2017). Drone detection with Faster R-CNN.
[47] Aker and Kalkan (2017). Drone detection with YOLO.
[48] Liu et al. (2016). Multispectral (colour + thermal) pedestrian detection.
[49] Jeon et al. (2017). Drone sound detection in real environments.
[50] Kim et al. (2017-18). Real-time UAV sound detection with one microphone.
[51] Park et al. (2015). Radar plus acoustic detection.
[52] Hengy et al.; Laurenzis et al. (2017-18). Multimodal UAV detection (optical, acoustic, radar).
[53] Diamantidou et al. (2019). Multimodal deep learning for UAV detection.
[54] Yang, Li, Li, Zhang and Zhang (2023). Survey of UAV flight data anomaly detection.
[55] Qi et al. (2007). Rotorcraft UAV sensor failure diagnosis.
[56] Bu et al. (2017). UAV navigation sensor anomaly detection.
[57] Radke et al. (2018). "Small data" anomaly detection.
[58] Schmidt et al. (2020). Anomaly detection in CPS log files.
[59] Abbaspour et al. (2017). Sensor/actuator fault detection.
[60] Lopez-Estrada et al. (2016). Quadrotor sensor fault diagnosis.
[61] Suarez et al. (2016). Cooperative sensor fault recovery.
[62] Wang et al. (2015). Anomaly detection in a group of UAVs.

[63] Wang et al. (2016). Bias compensation in multi-UAV formations.
[64] Zhang (2015). Fault detection on NASA GTM UAV.
[65] Guo et al. (2017). Airspeed fault detection via data fusion.
[66] Alos et al. (2020). PCA-based UAV behavior assessment.
[67] Wang et al. (2019). Sensor data anomaly detection with LSTM.
[68] Pan et al. (2020). Active learning + improved S3VM.
[69] Sun et al. (2017). Online navigation sensor fault detection.
[70] Titouna et al. (2020). Online anomaly detection (ALFA data).
[71] Pan (2017). Hybrid data-driven method.
[72] Wang et al. (2019). Multimodal regression detection.
[73] Duan et al. (2017). Sensor data anomaly detection with RVM.
[74] Li et al. (2018). Operational anomaly detection with mGMM.
[75] Bronz et al. (2020). Real-time fault detection, small fixed-wing UAVs.
[76] Bae and Joe (2019). Distributed AI anomaly detection.
[77] Bell et al. (2022). Stacked recurrent autoencoder.
[78] Aksoy et al. (2021). Flight trajectory anomaly detection.
[79] Keipour et al. (2021). ALFA dataset.
[80] Taylor (2012-14). University of Minnesota Thor datasets.
[81] Yilmaz, Ozkat and Gul (2026). Vibration-driven deep learning for anomaly detection of rotary-wing UAVs.
[82] Isolation Forest (generic baseline, Yilmaz et al., 2026).
[83] One-Class SVM (generic baseline, Yilmaz et al., 2026).
[84] LSTM autoencoder (generic baseline, Yilmaz et al., 2026).
[85] Yilmaz et al. (2026). Ablation: CNN-AE vs CNN-BiGRU-AE vs full model.
[86] Chen et al. (2024). UAV anomaly detection from flight parameters (Conv-AE + SVDD).
[87] Jeon et al. (2023). Structural anomalies of quadcopter UAVs (LSTM-AE).
[88] Jung et al. (2024). Anomaly detection from low-sampling-rate vibration data (SR3 + LSTM-AE).
[89] Fang et al. (2025). Cross-system anomaly detection, deep-sea submersibles (DSC-AE).
[90] Jasra et al. (2025). Comparison of unsupervised deep learning on flight data.
[91] Yang, Zhang, Zeng et al. (2025). AI-driven UAV safety and security, from machine learning to LLMs.
[92] Northwestern Polytechnical Univ. (2021). Flutter test signal extraction.
[93] Qatar Univ. (2023). UAV battery management.
[94] Xiamen Univ. (2024). Cross-battery state estimation with an LLM framework.
[95] Purdue Univ. (2025). Early battery degradation detection.
[96] Xidian Univ. (2022). GPS spoofing detection.
[97] Xidian Univ. (2023). GPS spoofing from signal features.
[98] King Abdulaziz Univ. (2024). Adversarial intrusion detection for GPS spoofing.
[99] Beirut Arab Univ. (2025). GPS spoofing detection with tuned LSTM.
[100] Carnegie Mellon Univ. (2024). Dynamic obstacle detection and tracking.
[101] Univ. of Hong Kong (2022). Trajectory planning for obstacle avoidance.
[102] Florida Inst. of Technology (2024). LEVIOSA, natural language to swarm paths.
[103] National Chung Hsing Univ. (2024). Reinforcement learning flight control.
[104] National Defense Academy of Japan (2022). Position/orientation prediction.
[105] Jeonbuk National Univ. (2024). Accident detection and emergency suggestions.
[106] Qatar Univ. (2020). UAV detection and identification.
[107] Kumoh National Inst. of Tech. (2021). CNN UAV identification.
[108] Northwestern Polytechnical Univ. (2023). Pilot authentication.
[109] Northwestern Polytechnical Univ. (2024). MTL-PIE, pilot identification and operation evaluation.
[110] Beijing Univ. of Posts and Telecom. (2022). Resilient routing for UAV networks.
[111] Jilin Univ. (2024). UAV network security with generative AI.