BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

AI-Based Drone Detection and Threat Mitigation System: A Literature-Based Review of Applications, Challenges and Future Directions

[1]Sarvesh Agrawal

[1]Department of Artificial Intelligence and Data Science,
[1]Ajeenkya DY Patil School of Engineering, Pune, India
Email : sarvesh.agrawal@dypic.in

Abstract

Drones are now used for surveillance, delivery, farming and disaster management. But unauthorized drones can also threaten military bases, airports, borders and key infrastructure. Older detection methods find it hard to spot drones that are small, fast or low-flying. Artificial intelligence (AI) can help to detect, track and classify drones, judge how dangerous they are, and suggest a response. This paper reviews recent studies on AI-based drone detection and threat mitigation. It looks at the main approaches: deep learning on camera images, fusing radar, camera, radio-frequency (RF) and acoustic data, event cameras, UAV cybersecurity and AI-assisted electronic warfare. The paper concludes that future systems should be light, robust, secure and explainable. They should combine several sensors, process data near the source, be tested in real conditions and keep a human in control.

Keywords: Counter-Drone Systems, Drone Detection, Threat Mitigation, Artificial Intelligence, Deep Learning, Multi-Sensor Fusion, UAV Cybersecurity, Edge AI

I. Introduction

A drone, also known as an unmanned aerial vehicle (UAV), is an aircraft that flies without a human pilot on board. Drones are used in surveillance, delivery, farming, disaster management and defense. They are inexpensive, compact and lightweight, and can be flown easily, which makes them useful. It also makes them a security hazard. An unauthorized drone can interfere with an airport, spy on a sensitive site, or cross a border without detection [2], [3].

Older detection systems have poor accuracy for micro-sized drones. A small quadcopter has a weak radar signal, can fly low and slow, and is easy to mistake for a bird. AI is beginning to help. Machine learning and deep learning can learn patterns from images, radio waves, sound and radar data. This enables drones to be identified, monitored and categorised automatically, and helps determine whether action is required [1], [4], [7].

A single warning is not enough. Even when a model generates a score, it does not constitute evidence, and false alarms can have real consequences if one acts on a threat. The AI results of a counter-drone

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

system must be cross-checked against other sensors, tested in realistic conditions and, for serious decisions, examined by a person.

The main objectives of this paper are to:

- Learn how AI is contributing to the counter-drone detection and threat mitigation field.
- Review recent technologies used for AI-based drone detection, tracking and classification.
- Observe and contrast current AI methods and their respective features.
- Delineate the problems and research gaps in existing counter-drone literature.
- Outline the future of AI-powered autonomous technology.

II. Review Methodology

A. Sources and Search

Papers were gathered from IEEE Xplore, SpringerLink, ScienceDirect, the ACM Digital Library, Google Scholar and arXiv. Searches were carried out on drone detection, counter-UAV (counter-unmanned aerial vehicle) systems, multi-sensor fusion, UAV cybersecurity, attacks on detectors, and AI-assisted defense. The field is constantly evolving, so new work from 2025 and 2026 was preferred.

B. Screening and Comparison Framework

All the chosen studies were checked for the following: the AI technique, the application area, the main contribution, the main findings and the limitations. Using the same points for every study simplifies the comparison of studies that use various sensors, models and tests.

C. Scope and Limitations of the Review

This paper only provides a review of the existing literature. It does not train a new model or report new experiments. Some sources are preprints that are not yet peer-reviewed; where they occur, they are identified as such. Readers are advised to consult the original studies before using any result.

III. Background

A. The Drone Threat Landscape

The concern is to keep unauthorized drones out of military bases, transport hubs, borders, mass gatherings and critical facilities such as power plants. Drones are difficult to see. Small drones are slow, can fly low between buildings and trees, and are often constructed from off-the-shelf components. Some fly on their own, so they may not send any control signal for an RF detector to pick up [2], [9].

B. Stages of a Counter-Drone System

Typically, a counter-drone system operates in stages: detect, track, classify, assess the threat and respond. Detection finds that something is in the air. Tracking observes its movement over time. Classification determines whether it is a drone, a bird or something else. Threat assessment considers its type, speed, altitude and path to estimate its severity. Only after that is a response decided. AI can support every stage, but its effectiveness depends on good testing and field trials [3], [4].

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

C. Relevance to Current Technology Trends

AI is transforming defense through smart surveillance, automatic detection and quicker decisions. Several trends meet in this topic. These include deep learning models such as convolutional neural networks (CNNs), YOLO and vision transformers; the integration of radar, camera, RF and acoustic data; edge AI for quick local processing; and rising privacy concerns and worries about the security of systems that use AI [1], [4], [7]. Drones are now so common in both civil and military use that the number of drones in research and practice is increasing rapidly.

IV. AI Techniques for Drone Detection and Threat Mitigation

A. Deep Learning on Visual Data

Several models have been developed for object detection, such as CNN-based and YOLO-type networks, and they can find and classify drones in images and video. Vision transformers have also been tried. These models are accurate in complicated scenes. However, they need large and widely varied training datasets, struggle with small or distant drones, and can confuse drones with birds. They are also affected by rain, fog, glare and darkness [4], [7].

B. Multi-Sensor Data Fusion

No single sensor works in all situations. Radar measures range and speed well but struggles with small, slow targets and clutter. Cameras provide detail but need good light and weather conditions. RF sensors see only control and video links, and miss drones that do not use them. Acoustic sensors work only at close range and are affected by noise. Combining these sensors with learned models can make detection more reliable and reduce false alarms. Mapara et al. report that deep learning with multiple sensors improved micro-drone detection [1]. Reviews of AI-based multi-sensor systems also make use of fusion, but note open design questions [3], [7].

C. Event Cameras

An event camera is an imaging system that captures only brightness changes at each pixel, instead of whole frames. It reacts very rapidly and has low delay, which suits small and fast objects. Magrini et al. study the use of event cameras for drone detection [8]. This looks promising for fast targets. Nevertheless, datasets and tools for event cameras are not yet as extensive as those for regular video.

D. Integrated Frameworks and Behavioral Analysis

Some studies do not only examine individual detectors, but also consider complete systems. Kalloniatis et al. give a comprehensive overview of building layered counter-UAV (C-UAV) defenses, called DRONEWALLS, and discuss the technologies and challenges [2]. Li et al. describe an AI-powered air defense system that incorporates multiple sensors against unidentified drones [3]. A recent preprint combines data from non-contact and contact sensors for multi-modal sensor fusion, and uses a knowledge graph to classify intent and reason about the state of the swarm and airspace [9]. Because it is a preprint, its conclusions should be regarded with caution, as preliminary until others reproduce them.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

E. Threat Assessment and Mitigation

Once a drone is detected and classified, the system needs to decide on its severity and the action to take. AI can combine type, speed, altitude, location and behavior into a threat level, and can rank multiple objects at once. The literature groups mitigation techniques into general categories: electronic measures that disrupt or take over the link, physical capture, and directed-energy methods [4], [7]. This review does not concentrate on the hardware. Mitigation also raises legal, safety and ethical issues. Jamming can interfere with legitimate communication and navigation, and in many countries it may only be used by authorized agencies. The literature shows a preference for decision support with a human in the loop for any action that cannot easily be reversed.

F. Cybersecurity and Resilience

A counter-drone system can itself be attacked. Machine learning has been used to detect cyberattacks on unmanned aerial systems, such as intrusions into UAV communication [6]. Xie and Long study fault-tolerant control of UAVs under interference, together with counter-drone strategies [5]. Gazit et al. show that real-world adversarial attacks can fool RF-based drone detectors [10]. This is a useful warning: a detector that scores well on a benchmark may fail when someone deliberately tries to avoid it.

V. Comparative Analysis of the Literature

Table I summarizes the studies reviewed, using the points from Section II. Each entry describes the focus of the work as given in its title and abstract. It is not a ranking, since the studies use different data, sensors and metrics.

There are three salient features. First, deep learning is used together with multi-sensor fusion, since each sensor addresses the weaknesses of the others [1], [3], [7]. Second, even less emphasis is placed on security and robustness than on accuracy, although attacks on detectors have now been demonstrated [6], [10]. Third, many of the works are reviews, frameworks or simulations, so there is little evidence from long-term field use. A combination of several approaches might provide a more complete system, although this benefit remains to be demonstrated in well-designed experiments.

Table I: Comparison of AI-Based Counter-Drone Studies

Ref.	Technique	Potential Contribution	Limitation
[1] Mapara et al., 2026	Deep learning with multiple sensors	Micro-drone detection for counter-drone systems	Deployment cost and complexity of a multi-sensor setup
[2] Kalloniatis et al., 2026	Layered DRONEWALLS framework	Technologies and challenges for effective counter-UAV defense	Limited real-world validation
[3] Li et al., 2026	Multi-sensor AI	Air threat defense against unidentified drones	Computational load and field testing needed

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

Ref.	Technique	Potential Contribution	Limitation
[4] Jaggupalli et al.	AI, ML and DL review	Overview of integrated detection and autonomous defense	Mostly a review; limited experimental evidence
[5] Xie and Long, 2026	Fault-tolerant control, disturbance estimation	UAV control that tolerates interference and faults, with counter-drone strategies	Focus on control, not detection
[6] Mouatassim et al., 2026	Machine learning for attack detection	Cyberattack detection in unmanned aerial systems	Needs large and diverse datasets
[7] Smailov et al., 2025	AI-augmented multisensor review	Review of architectures for detecting and neutralizing UAVs	Mostly theoretical
[8] Magrini et al., 2025	Event cameras	Fast, low-latency drone detection	Limited datasets and tools
[9] Bayizere, 2026 (preprint)	Multi-modal fusion, intent classification	Framework for threat detection and swarm reasoning	Not peer reviewed; needs independent validation
[10] Gazit et al., 2025 (preprint)	Adversarial attacks on RF detectors	Shows RF detectors can be evaded in the real world	Attack-focused; defenses need further study

VI. Challenges and Ethical Concerns

A. Small and Low-Flying Drones

Small, fast and low-flying drones give weak signals and blend into clutter, so they are hard to detect. Telling them apart from birds and other objects is a steady source of false alarms [4], [7].

B. Weather and Environment

Performance can drop in fog, rain, smoke, darkness and cluttered scenes. Models need to work across many conditions, not just the data they were trained on.

C. Real-Time Processing and Latency

Deep networks need a lot of computing power, but a response must be fast. Light models and edge AI, which process data close to the sensor, reduce delay and bandwidth. They may, however, lose some accuracy.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

D. Sensor Integration

There are relatively few standard methods for combining radar, RF, acoustic, infrared and camera data. These sources vary in speed, format and error type, which makes them hard to fuse. Adaptive methods are still an open problem [3], [7].

E. Security of the AI System

Counter-drone systems are vulnerable to jamming, adversarial inputs and spoofing [6], [10]. A system that can be deliberately deceived creates an illusion of safety.

F. Cost and Real-World Validation

The deployment of multi-sensor systems is expensive [1]. The majority of studies rely on simulation or small field trials, and large data sets are scarce in the real world [2].

G. Legal, Safety and Ethical Concerns

direct beneficiaries of the mitigation.Automated mitigation can impact those who are not the direct beneficiaries of the mitigation. interfere with communication, for example by eye contact, by facial expression, by gestures, by touch, by touch alone, by moving away, or by throwing away a ball or toy. or falling debris. Another consideration is privacy – as sensors may record people. There should be clear rules as to who may: Apply mitigation, human supervision and accountability for Errors or notes of all decisions.

VII. Evaluation of Counter-Drone Systems

There is no single test that's right for all systems, as each part has a different job. The measurement of a detector should be based on the detection rate, False alarm rate, small target range and performance. A classifier needs to be evaluated based on its ability to classify drones from birds and other objects. The judgment of a tracker should be based on:Judging a tracker should be based on: how faithful it is to a target. The entire system should be configured to For end to end delay, behavior in bad weather, and other factors, be tested. Tolerance of challenge to inputs. Results should include Difficult conditions and, if possible, field data. A high The benchmark score does not guarantee for real use. A A model which performs well on a clean test set can perform poorly on an An attack by an unknown drone or malicious drone [10].

VIII. Research Gaps and Future Directions

A. Research Gaps

The review highlights a number of further areas for improvement:

- * * Reliable detection of small, fast and low-flying drones, Using better data and higher resolution sensing.
- An accurate and rapid edge detection in real-time for light models. response.
- Traditional and novel techniques for integrating radar and RF, camera, Acoustic and infrared data.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

- Embed and secure explainable and attack resistant AI models that is resistant to jamming, spoofing and attacks by adversaries.
- Real-world validation, beyond simulation, at large scale.
- Fog, rain, night, smoke and dust will not affect the performance. cluttered scenes. In summary, there is a need to develop an integrated, real-time, robust Delivering an AI-based counter-drone system that is both effective and secure.Providing an effective and secure system of AI-based counter-drone. Effectively in diverse real-life contexts.

B. Future Directions

Following these opportunities can be opportunities for future work. First, light and Highly efficient small drone detection AI models. Second, adaptive sensor fusion based on the condition and the failure of sensors. Third, closer links between AI and electronic warfare for detection and mitigation, within legal limits. Fourth, built-in Explainability and adversarial testing, and cybersecurity. Fifth, It is important to consider field validation that uses shared benchmarks and reproducible. reporting. All this should be systematically evaluated, and humanized. should be demonstrated in, and be beneficial to, supervision, Studies and field evidence which can be reproduced.

IX. Conclusion

AI can greatly improve drone detection, tracking, An assessment of threat and classification. More recent research has revealed that The most effective way for deep learning to work with multi-sensor fusion is also the most effective approach for deep learning in general. promising direction, while edge processing, event cameras The areas that are expanding are and by electronic warfare with help from AI. Still, minimize the ability to detect small targets, bad weather, delay, cost, There is a lack of field testing and cybersecurity are large issues. obstacles. Whether it is for interception, search and rescue, or other operational missions, counter-drone AI must complement human operators, not replace them. Future research should strive to be reliable, sensible, safe and tested systems that run in the real conditions.

References

[1] T. M. Mapara, S. Sesham, and F. Shafuda, “Deep learning based micro-drone detection for reliable counter-drone systems using multiple sensors,” J. Intell. Robot. Syst., vol. 112, Art. no. 71, 2026, doi: 10.1007/s10846-026-02406-9.

[2] S. Kalloniatis et al., “On the construction of effective DRONEWALLS: Technologies and challenges for counter-UAV systems,” J. Air Transport Research Society, vol. 6, Art. no. 100093, 2026, doi: 10.1016/j.jatrs.2025.100093.

[3] X. Li et al., “Air threat defense system from unidentified drones using multi-sensor AI,” in Proc. 15th Int. Conf. Informatics, Environment, Energy and Applications, ACM, 2026, doi: 10.1145/3803833.3803840.

[4] D. Jaggupalli, A. Tarigoppula, and J. Pujith, “AI, ML and DL-based integrated drone detection and autonomous defence systems: A review,” in Proc. IEEE Int. Conf. Intelligent Systems and Applications (ICISA), 2025/2026.

[5] Z. Xie and Y. Long, “Anti-interference and fault-tolerant control of UAVs integrating residual-based diagnosis, disturbance estimation with counter-drone strategies,” Scientific Reports, vol. 16, 2026, doi: 10.1038/s41598-026-37984-z.

BODHIVRUKSHA JOURNAL OF DIVERSE DISCIPLINE
E-ISSN : 3139-1486
An Open Access, Peer-Reviewed, Multidisciplinary Scholarly Journal
Bi-monthly | Multilingual (English, Hindi, Marathi) | Academic Research
@ Volume 2, Issue 5 (September-October 2026) (Special Issue 1) ISSN: 3139-1486 (Online)

[6] T. Mouatassim, M. Airaj, and E. M. El Guarmah, "Safeguarding the skies: The rise of machine learning approaches for cyberattack detection in unmanned aerial systems," Cybersecurity, vol. 9, 2026.
[7] N. Smailov, N. Kashkimbayeva, N. Kubanova, A. Sabibolda, and Y. Mailybayev, "Review of AI-augmented multisensor architectures for detecting and neutralizing UAV threats," Int. J. Innovative Research and Scientific Studies, vol. 8, no. 5, 2025.
[8] G. Magrini, L. Berlincioni, L. Cultrera, F. Becattini, and P. Pala, "Drone detection with event cameras," in Proc. ICCV Workshops, 2025.
[9] M. Bayizere, "DroneShield-AI: A multi-modal sensor fusion framework for real-time autonomous drone threat detection, behavioral intent classification, and swarm intelligence in contested airspace," arXiv:2606.11687, 2026.
[10] O. Gazit, Y. Itzhakev, Y. Elovici, and A. Shabtai, "Real-world adversarial attacks on RF-based drone detectors," arXiv:2512.20712, 2025.