Review

Artificial Intelligence Methods for Unmanned Aerial Vehicles Cybersecurity: A Comprehensive Survey

Thabet Kacem * and Kensley Benjamin

Posted Date: 21 April 2026

doi: 10.20944/preprints202604.1384.v1

Keywords: artificial intelligence; UAV; cybersecurity; machine learning; deep learning; federated learning; reinforcement learning; GNN; generative AI

 doi:10.20944/preprints202604.1384.v1

Review

Artificial Intelligence Methods for Unmanned Aerial Vehicles Cybersecurity: A Comprehensive Survey

Thabet Kacem * and Kensley Benjamin

Department of Computer Science and Information Technology, University of the District of Columbia, USA
* Correspondence: thabet.kacem@udc.edu

Abstract

Unmanned Aerial Vehicles (UAVs) have been widely used in recent years in various applications thanks to advances in communication, Internet of Things and electronics. However, despite the advantages they offer, reports of cybersecurity attacks represent a serious threat to their operation. Classic cryptographic-based solutions and traditional intrusion detection approaches generally struggle to deal with these attacks due to their adaptive and stealthy nature. In this context, Artificial Intelligence (AI) models emerged as potential solutions that hold great promise in addressing this type of attacks. However, most related surveys presented fragmented picture of the state-of-the-art failing to cover all sub-types of AI models, and sometimes not following structured taxonomies or describing popular datasets that were used in the literature. In this paper, we bridge this gap by proposing a novel and comprehensive survey that classifies UAV security research according to the type of AI model, the cyber attacks it thwarts and the related security properties it enforces. This taxonomy does not stop at describing Machine Learning (ML) and Deep Learning (DL) approaches, but it also dives into emerging approaches such as Federated Learning (FL), Reinforcement Learning (RL), Graph Neural Network (GNN) and Generative AI (GAI). We also classify the threat vector according to the layer in the UAV functional stack where the attack takes place. In addition, we describe the datasets, tools and evaluation metrics that were mostly used in the literature. We conclude the survey by summarizing the key insights, discussing the open challenges and enumerating future research directions. We aim that this survey serves as a reference for cyber security researchers and practitioners who tackle UAV security using AI.

Keywords: artificial intelligence; UAV; cybersecurity; machine learning; deep learning; federated learning; reinforcement learning; GNN; generative AI

1. Introduction

In recent years, UAVs [1] have continued to evolve as indispensable assets not only for the military, but across a wide range of civilian, commercial, and industrial applications. With possible usage [2] ranging from aerial surveillance, disaster response, and monitoring to urban mobility, logistics, and agriculture, UAVs are quickly integrating themselves into multiple facets of society. The significance of making sure that they operate securely and reliably is highlighted by their increasing autonomy, communication capabilities, and deployment in crucial operations. However, the widespread adoption of UAVs creates an extensive and expanding attack surface [3]. Since UAVs depend on satellite-based GPS navigation, wireless communication, and frequently centralized or swarm-based communication, they are vulnerable to a variety of cyber-physical threats. Notable examples of cyber attacks include Distributed Denial-of-Service (DDoS) attacks, data injection, GPS spoofing, and manipulation of the Automatic Dependent Surveillance–Broadcast (ADS-B) [4]. Such attacks can have substantial grave consequences for security and privacy.

Traditional cybersecurity measures, while essential, are increasingly unable to deal with the dynamic and adaptive nature of emerging threats. As a result, researchers are employing AI to

 doi:10.20944/preprints202604.1384.v1

complement UAV systems with cybersecurity [5], which would make them more robust and flexible. AI methods, particularly those based on machine learning and deep learning, have the ability to identify abnormalities, categorize threats, forecast hostile behavior, and even react to attacks on their own in real time. Conversely, emerging AI paradigms including RL, FL, GNN, and GAI, have been emerging as solutions that address different and sometimes novel UAV security threats.

Several surveys have examined security, privacy, and operational challenges in UAV systems across civilian, military, and commercial domains as outlined in Table 1. However, these contributions remained fragmented as they did not cover all the spectrum of AI methods. In particular, several surveys focus only on the threats and traditional security measures, without a dedicated AI Model Taxonomy (AIMT) while others stop short at exploring the usage of ML and/or DL in UAV security. However, there is a pressing need of exploring how emerging sub-fields of AI, such as FL, RL, GNN and GAI, relate to UAV security. Also, no survey covered the Tools, Datasets and Metrics (TDM) used as part of the evaluation of AI models used in UAV security.

Table 1. Survey positioning with regards to prior surveys.

Authors	Year	AIMT	ML	DL	FL	RL	GNN	GAI	TDM
Cordill et al. [6]	2025	✓	✓	x	✓	x	x	x	x
Tsao et al. [7]	2022	✓	✓	✓	✓	✓	x	x	x
Bithas et al. [10]	2019	✓	✓	x	✓	x	x	x	x
Sarikaya and Bahtiyar [12]	2024	✓	x	x	x	✓	x	x	x
Wang et al [13]	2024	✓	✓	✓	✓	✓	x	x	x
Adil et al. [14]	2023	x	x	x	x	x	x	x	x
Tlili et al. [15]	2024	x	x	x	x	x	x	x	x
Yang et al. [16]	2025	x	x	x	x	x	x	x	x
Abro et al. [17]	2022	x	x	x	x	x	x	x	x
Pandey et al. [19]	2022	✓	x	x	x	x	x	x	x
Alzubaidi [21]	2025	✓	✓	x	x	x	x	x	✓
Ogab et al. [23]	2023	✓	x	x	x	x	x	x	✓
Our Survey	2026	✓	✓	✓	✓	✓	✓	✓	✓

Cordill et al. [6] provided a systematic analysis of UAV vulnerabilities, classifying them into hardware, software, and communication attacks while emphasizing privacy concerns, including ethical UAV surveillance and compliance with frameworks such as General Data Protection Regulation (GDPR). The authors review state-of-the-art technical solutions such as lightweight encryption, blockchain-based security, and privacy-preserving machine learning, highlighting the integration of both technical and policy perspectives for holistic UAV network security. Tsao et al. [7] focused on security within flying ad-hoc networks (FANETs) and the Internet of Drones (IoD), categorizing threats based on UAV connections with ground control stations and pilot devices. The survey evaluates conventional and novel UAV routing protocols from a cybersecurity perspective and assesses defense mechanisms against key requirements such as availability, authentication, authorization, confidentiality, integrity, privacy, and non-repudiation. Similarly, Rahman et al. [8] and Al-Syouf et al. [9] provided detailed overviews of FANETs and IDS frameworks, emphasizing high-accuracy detection, feature selection methods, datasets, and performance metrics for UAV network security.

Bithas et al. [10] and Syed et al. [11] reviewed the application of ML, blockchain, and digital watermarking for UAV security. ML techniques enhance threat detection and resource management in UAV networks, while blockchain ensures decentralized trust and watermarking secures transmitted media. Sarikaya and Bahtiyar [12] extended this discussion to deep reinforcement learning (DRL),

 doi:10.20944/preprints202604.1384.v1

highlighting adaptive, intelligent countermeasures that complement conventional defense strategies. Wang et al. [13] focused on UAV swarm networks, discussing attacks such as DoS, Man-in-The-Middle (MiTM), and threats against ML models, emphasizing AI-driven and adaptive security mechanisms. Adil et al. [14] examined UAV-assisted IoT applications, categorizing primary threats, reviewing countermeasures, and identifying open research challenges in dynamic, wireless network deployments. Tlili et al. [15] complemented these surveys by presenting a taxonomy of AI-based UAV security approaches, analyzing prevention and detection techniques, and highlighting open research challenges. Yang et al. [16] further explored traditional ML and deep learning (DL) methods for UAV threat mitigation, while introducing large language models (LLMs) as emerging tools for adaptive decision-making.

Abro et al. [17] provided a broader overview of UAV detection, classification, and tracking technologies, identifying vulnerabilities such as control signal jamming, while highlighting relevant legislation and communication standards. Autonomous multi-UAV systems are addressed by work employing the STRIDE model to prioritize cybersecurity threats and propose security design recommendations for safe multi-UAV deployment [18]. Pandey et al. [19] surveyed UAV-assisted networks, detailing intrusion taxonomies, performance metrics, and proactive mitigation strategies integrating mmWave, NOMA, massive MIMO, cognitive radio, software-defined networks, edge/fog computing, blockchain, and ML for secure UAV communications. Similarly, UAV integration into cellular networks is reviewed by [20], highlighting UAV-mounted base stations, interference management, connectivity optimization, regulatory compliance, and cyber-physical security challenges.

Alzubaidi [21] focused on UAV malware detection using ML and DL, providing taxonomies and identifying research gaps and future directions. Mohsan et al. [22] provided a foundational survey on UAV types, swarms, classifications, charging methods, regulations, applications, operational challenges, and security concerns, providing context for the increasing deployment of UAVs across domains. The Internet of Drones (IoD) is highlighted by Ogab et al. [23], emphasizing dynamic UAV networks leveraging IoT for autonomous, collaborative tasks. Despite offering adaptability and scalability, IoD introduces unique security challenges, including resource-constrained IDS deployment, high false positive rates, and limited adaptability to evolving attacks. Systematic reviews consolidate research on ML-based IDSs, datasets, attack classifications, and software environments, providing structured insights into current trends, limitations, and future research directions.

In this survey, we present a thorough analysis of the ways in which artificial intelligence is being used to improve UAV system security. By using a novel taxonomy, we classify and examine the most advanced artificial intelligence techniques available today, encompassing both supervised and unsupervised learning as well as cutting-edge approaches like graph neural networks, reinforcement learning, privacy-preserving federated learning, and generative AI. We also list the commonly used tools and datasets in the research intersecting AI and UAV security. By using this lens, we hope to map the field of AI-driven UAV security research, pinpoint important trends, evaluate present issues, and point out exciting new avenues for future study.

The main contributions of this survey are as follows:

- We developed a novel taxonomy to classify the AI research used for securing UAVs, which goes beyond classical machine learning and deep learning to cover emerging fields such as federated & reinforcement learning along with GNN and generative AI.
- We proposed a refined taxonomy of UAV threats according to its layered stack.
- We described the tools, datasets and evaluation metrics used as part of the AI research for securing UAV operations.
- We highlighted the key insights from our survey by discussing the statistics of coverage of security properties by AI method type versus overall.
- We discussed open challenges and future directions in UAV security using AI.

The remainder of this paper is organized as follows as seen in Figure 1. Section 2 provides a background overview of UAV architecture and threat model. Section 3 describes the proposed

 doi:10.20944/preprints202604.1384.v1

taxonomy. Section 4 describes the machine learning methods while section 5 describes deep learning methods. Section 6 discusses the federated learning methods, section 8 describes GNN methods, and section 9 describes generative AI methods. Section 10 presents the tools, datasets and evaluation metrics. Section 11 summarizes and discusses the findings. Section 12 summarizes the key insights from this survey. Section 13 discusses open challenges while section 14 describes a glimpse on future directions. Finally, section 15 concludes the paper.

Figure 1. Paper outline.

2. UAV Architecture & Threat Model

2.1. UAV Architecture

As illustrated in Figure 2, the architecture of UAV systems is made up of a number of closely related subsystems, particularly those utilized in autonomous or remotely piloted missions. In general, a UAV system consists of the following parts:

- **Airborne Unit:** The physical drone platform includes flight control systems, sensors (GPS, IMU, cameras, and LiDAR), actuators, and mission-specific payloads.
- **Ground Control Station (GCS):** Interfaces that allow human operators to monitor and control UAVs, send commands, and receive telemetry data.
- **Communication Links:** Wireless channels (usually radio frequency) are utilized for control, telemetry, video transmission, and swarm coordination among UAVs.
- **Cloud or Edge Infrastructure:** Some modern unmanned aerial vehicles use cloud-based platforms or adjacent edge servers for computing offloading, data analysis, or fleet coordination.

The UAV system layer stack is rich and diverse, covering a wide range of functions required for remote operations. Actually, there is no widely agreed upon layer stack despite strong contenders such as [24,25]. At the bottom of this system layer stack sits is the physical layer, which collects sensor data along with other functions related to interact with the actuators and radio frequency hardware. The communication layer collects and transmits sensor data, system status updates, and provides command & control links in addition to data links. The navigation layer relies on GPS or GNSS to offer precise localization and route planning. Above this, the control layer transmit flight instructions from the Ground Control Station (GCS) to the UAV via radio frequency (RF) channels, frequently utilizing standardized protocols like MAVLink. Finally, the application layer manages mission-specific functions such as object tracking, delivery scheduling, and environmental monitoring, depending on the UAV's intended use case. These communication channels are vital to mission success, but they are also great targets for cyber-attacks since they are wireless and frequently un-encrypted.

 doi:10.20944/preprints202604.1384.v1

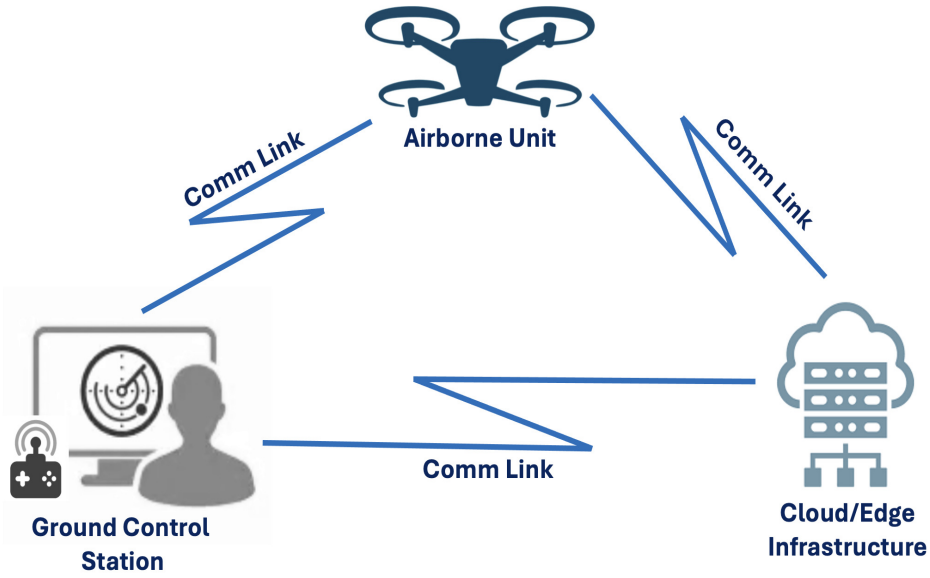

Figure 2. UAV architecture.

2.2. Threat Taxonomy in UAV Systems

UAVs face a distinct and diverse set of cyber-physical threats due to their mobility, reliance on wireless communication, and increasing autonomy. Threats range from attacks on navigation and communication systems to software vulnerabilities and physical tampering. The classification of cyber attacks highlights the most serious attacks clustered according to their respective layers where they take place as follows:

- **Physical Layer:**
  - **RF Jamming:** overwhelms any radio-based communication between the UAV and the GCS by sending high power noise signal on the same frequency.
  - **Sensor Manipulation:** is done by tampering with the inertial and perception sensors used by UAVs to force erroneous state estimations.
  - **Actuator Manipulation:** can be done via various techniques such as signal injection, interference, power disruption and physical tampering.
- **Communication Layer:**
  - **DoS/DDoS:** DoS and DDoS attacks aim to overwhelm the UAV's communication or computing capabilities. This could result in high latency, diminished mission performance, or even a total loss of control.
  - **MiTM:** In MitM scenarios, attackers intercept and manipulate communication between the UAV and the GCS. This facilitate the occurrence of other attacks such as command hijacking, telemetry injection, and illegal access to control channels.
  - **Message Injection:** include leveraging vulnerabilities in widely used protocols in UAV communication to inject malicious data. This includes but is not limited to ADS-B and MAVLink.
- **Navigation Layer**
  - **GPS Spoofing:** GPS spoofing [26] entails sending deceptive signals to confuse the UAV's navigation system, potentially resulting in route diversion or collisions.
  - **Sensor Fusion Attacks:** represents a stealthier version of sensor manipulation as it can evade sensor fusion algorithms such as Kalman Filter.
- **Control Layer:**

 doi:10.20944/preprints202604.1384.v1

- **Command Injection:** leverages vulnerabilities in drone software or communication links in order to take partial or full control of the UAV
- **Command Suppression:** happens when the attacks injects higher priority or conflicting commands thus overriding the legitimate one sent from GCS.

- **Application Layer:**
  - **Malware:** represents any malicious code deployed within the UAV ecosystem to perform malicious actions affecting mostly UAV applications such as mission planning and AI modules.
  - **Data Poisoning:** occurs during training by injecting malicious entries to corrupt the UAV learning mechanism. It occurs during offline or federated training.
  - **Model Evasion:** occurs during runtime inference by injecting adversarial inputs by leveraging lack of robustness that leads to misleading the AI models.
  - **Software Exploitation:** Vulnerabilities in UAV operating systems, firmware, or onboard apps can be used to acquire persistent access, elevate privileges, or disable security features. Once compromised, attackers may maintain covert control over the UAV.

These cyber-attacks can be highly dynamic and context-dependent. As a result, intelligent and adaptive security solutions are becoming increasingly important, driving the adoption of AI-based defenses.

3. Taxonomy of AI Methods for UAV Security

The application of AI into UAV security represents a substantial shift away from conventional, rule-based defenses and toward data-driven and adaptive procedures. Due to their mobility and need for wireless connection, UAVs are vulnerable to both physical and cyber threats. Despite their merits, traditional cybersecurity methods often miss unseen and adaptive attack patterns. AI techniques get beyond these limitations by modeling abnormalities, learning behavioral patterns, and, in some scenarios, adapting on their own to unfavorable circumstances.

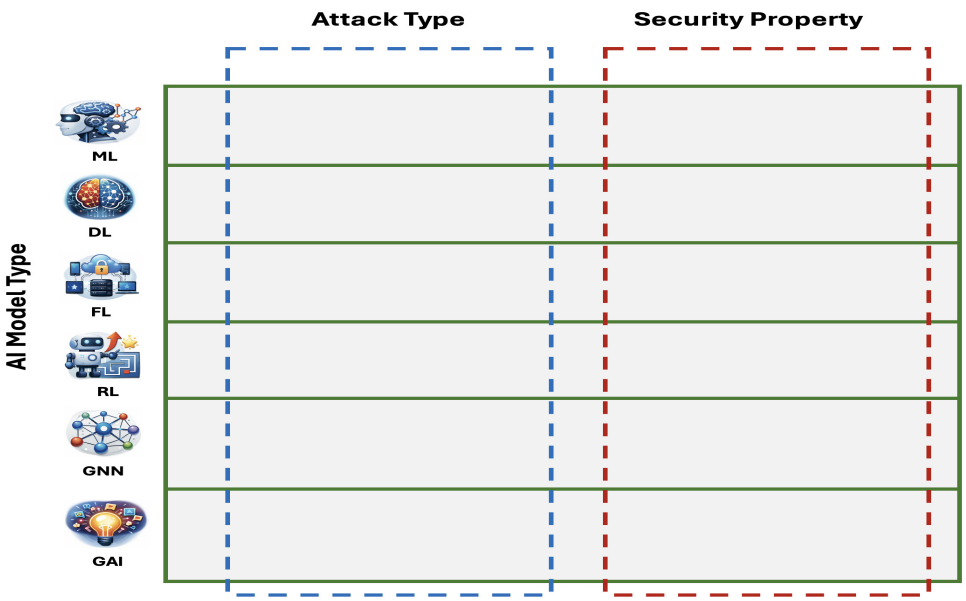

Figure 3. UAV architecture.

This section describes the novel multi-dimensional taxonomy we developed to classify the AI-based research in the context of securing UAV systems. This taxonomy relies on three main dimensions as follows:

- **AI Model Type:** this is the main dimension covering all variety of traditional AI models such as ML and DL, and more advanced ones such as FL, RL, GNN and GAI.

 doi:10.20944/preprints202604.1384.v1

- **Attack Type:** this is the second dimension that covers the cyber attacks thwarted by the AI models in each model type. These attacks are further refined according to the functional UAV layer, i.e. physical layer, communication layer, navigation layer, control layer and application layer.
- **Security Property:** this is the final dimension, which covers the security properties enforced by the proposed works in each AI model category.

Our coverage of security properties goes beyond the classical CIA triad, which represents the foundation of cybersecurity, to include other critical properties in UAV systems such as authenticity and privacy. In fact, authenticity implies verifying the identity of the source of sent data to/from UAVs, while privacy focuses on protecting against sensitive inference that is very important in AI-based systems for UAV security. In addition, such systems can be vulnerable against adversarial inputs thus we consider robustness as part of the security properties due to its role in achieving resilience against such perturbations.

Inclusions criteria of the papers in our survey are described as follows:

- **Publication year:** we considered recent papers published between 2020 and 2025.
- **Reputable publication venue:** IEEE, ACM, Elsevier, Springer, MDPI, or similar journals and/or conferences.
- **Scope:** directly related to AI methods used for UAV security.

4. Machine Learning Methods

Classical and supervised ML techniques [27] have long been used to protect UAV networks by identifying intrusions, spoofing, jamming, and aberrant behaviors via flight data, network traffic, or radio frequency (RF). As seen in Table 2, classical and supervised machine learning algorithms are very popular for UAV security. These algorithms, which use telemetry, network traffic, and RF characteristics, can perform real-time detection under stringent resource limitations, laying the groundwork for more advanced AI-based approaches like deep learning, reinforcement learning, and federated learning.

MAVIDS [28] is an onboard intrusion detection system that uses principal component analysis (PCA) and one-class anomaly detection to detect GPS spoofing and jamming attempts based on UAV flight logs. MAVIDS operates without labeled attack data, under severe onboard resource constraints, and achieves macro-averaged F1 scores of 90.57% and 94.3%, respectively, while retaining real-time detection capabilities even during communication disruptions. Supervised machine learning algorithms have also been used to UAV network traffic.

Moustafa and Jolfaei [29] created a testbed that generated both benign and malicious UAV traffic. They trained classifiers such as Decision Tree, KNN, Naïve Bayes, SVM, and shallow MLP. The Decision Tree achieved the best accuracy (99.99%), followed by KNN and MLP (99.98%). SVM reached competitive accuracy (99%) but had the largest fall-out rate (2.245%). Although rapid to train, Naïve Bayes fared poorly (39.9% accuracy). These findings show that lightweight supervised machine learning models, particularly decision trees, can achieve high accuracy with low computing overhead, enabling real-time intrusion detection for UAV networks.

Shafique et al. [30] employed handcrafted GPS-derived features, such as jitter, shimmer, and frequency modulation, combined with SVM classifiers and a K-fold voting method, to discriminate authentic from counterfeit signals, obtaining 98.7% accuracy and 0.98 F1 score. Agnew et al. [31] investigated predictive modeling of network-level performance statistics, including inter-arrival time, transmission latency, and packet count, for ML-based intrusion detection in SD-UAV networks. Classifiers were able to detect jamming, blackhole, and grayhole attacks even under zero-day settings by simulating normal traffic using queuing theory, enhancing training efficiency and enabling rapid anomaly identification. Lightweight high-precision models, such as Fuzzy Rough Set (FRS) based IDS combined with Shallow Neural Networks (SNN) and Random Forest (RF) [32], maintain 99%

 doi:10.20944/preprints202604.1384.v1

accuracy and low false alarm rates on datasets such as CIC-DDOS2019. This offers interpretable and resource-efficient alternatives to deep learning for constrained UAV hardware.

Table 2. Classification of ML Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Whelan et al [28]	PCA + One Class Classifier	GPS spoofing, Jamming	Physical, Navigation	Availability, Integrity
Moustafa and Jolfaei [29]	Decision Tree, DNN, MLP, SVM	networked UAV attacks	Communication	Confidentiality, Integrity, Availability, Authenticity
Shafique et al. [30]	SVM + K-Fold	GPS spoofing	Navigation	Availability, Integrity
Agnew et al. [31]	Light GBM	DoS (greyhole, blackhole), Jamming	Physical, Communication	Availability
Wu et al. [32]	FRS + SNN + RF	DoS, DDoS	Communication	Availability
Fu et al. [33]	CNN-LSTM	DDoS, Jamming, Command Injection, Malware, Sensor Manipulation	All	Availability, Authenticity, Integrity
Shrestha et al [34]	LR, DT, LDA, KNN, GNB, SGD, K-M	DoS, Botnet, Unauthorized Access	Communication	Availability, Authenticity
Whelan et al. [35]	PCA + One Class Classifier	Sensor Manipulation	Physical	Integrity, Authenticity
Cai et al. [36]	RF Fingerprinting + CNN + DNN	Data Poisoning, Model Evasion	Application	Authenticity, Privacy, Robustness
Mehmood et al. [37]	RF	DoS	Communication	Availability

Identification of UAV operation modes and encrypted communication analysis are examples of resource-efficient detection frameworks. In [38], a method based on packet size and inter-arrival times with re-weighted l1 norm regularization and maximum likelihood estimation achieves 85.7-95.2% detection accuracy within 0.15-0.35 seconds and accurate mode identification (88.5-98.2%), making it suitable for real-time UAV identification in Wi-Fi environments. Hybrid CNN-LSTM architectures [33] used in UAV-assisted agricultural IoT networks detect aberrant behavior with 93.5% accuracy, while reinforcement learning (DDQN) optimizes UAV deployment. Similarly, [34] shows that Decision Trees (DT) trained on CSE-CIC IDS-2018 achieve 99.99% accuracy and zero false negatives in UAV- and satellite-based 5G networks. The authors also tested various other ML algorithms such as Logistic Regression (LR), Linear Discriminant Analysis (LDA), K-nearest Neighbor (KNN), Gaussian Naive Bayes (GNB), Stochastic Gradient Descent (SGD), and K-means (K-M).

A novel technique employing one-class classifiers and PCA for dimensionality reduction [35] detects GPS spoofing with F1 scores of up to 99.73% for malicious readings. RF fingerprinting paired with ML and DL algorithms [36] achieves more than 95% accuracy in UAV recognition with SNR higher than 5dB, even with Gaussian noise. Simulated UAV IDS evaluation [37] shows that Random Forest classifiers reach 95-96% detection accuracy.

 doi:10.20944/preprints202604.1384.v1

5. Deep Learning Methods

DL[39] have become increasingly important for safeguarding UAV systems, allowing strong, real-time detection of both cyber and physical threats. These systems use large-scale network traffic, sensor telemetry, and UAV operational data to detect intrusions, authenticate devices, and assure swarm resilience. The summary of the research work is described in Table 3. Tlili et al. design [40] proposed a model based on LSTM that uses coordinated detection units across UAV platforms, integrating several IDS components to achieve 98.6% global detection accuracy while minimizing onboard computing. UAV-DiPNID [41] uses knowledge distillation via Distilled Pruned Networks (DPN) to create compact deep networks with 99.61% detection accuracy. This reduces inference time by 80.7% and model size by 90%, allowing for real-time deployment on resource-constrained UAV platforms.

Intrusion detection systems (IDS) that use DL models have demonstrated great performance across several UAV datasets. Niyonsaba et al. [42] proposed a hybrid CNN-LSTM method that achieved up to 99.063% accuracy on CICIDS2017, with hybrid models excelling at real-time threat detection. UAV-assisted reconfigurable intelligent surface (RIS) networks use a hybrid method based on LSTM and Deep Deterministic Policy Gradient (DDPG) [43] to improve communication security and achieve 99.10% detection accuracy. UAVs operating as mobile relays can use cooperative jamming tactics optimized using Deep Neural Networks (DNN) and deep Q-networks (DQN) [44] to avoid eavesdropping while responding to channel uncertainty.

Adaptive IDS architectures integrate deep learning and reinforcement learning to provide proactive threat mitigation. Zero Trust Architectures (ZTA) enhance UAV security by continually authenticating network entities and merging RF signals with explainable AI algorithms like SHAP and LIME, achieving 84.59% accuracy [45].

UAV-IDS-ConvNet [46] employs deep CNNs to analyze encrypted Wi-Fi data across multiple UAV platforms, reaching 99.50% two-class accuracy with a prediction time of 2.77 ms and beating existing IDS models by 6-23%. LSTM-RNN architectures [49] provide real-time anomaly detection in FANETs. When combined with big-data stream analytics, they outperform classic systems like Snort by up to 36% in detection accuracy.

Cross-UAV feature fusion in swarm testbeds [50] reveals that integrating cyber and physical telemetry from several UAVs enhances F1 scores, reaching 96.3% when both attacked and benign UAV data are fused, demonstrating the relevance of swarm security. Extensive evaluations of deep learning architectures—including CNN, LSTM, hybrid CNN-LSTM, and ConvLSTM—show that ConvLSTM consistently achieves near-perfect accuracy (99.99%) in UAV network intrusion detection across multiple datasets, emphasizing the importance of modeling spatiotemporal patterns. UAV-CIDS [52], an autonomous collaborative IDS architecture, uses Feed Forward CNN (FFCNN) to identify zero-day and known assaults with 98.23% accuracy and real-time event response. Hybrid techniques, including feature selection, modified deep CNN-BiLSTM architectures, and attention mechanisms such as in [53]. Also, Benjamin and Kacem [54] proposed another hybrid approach based on Transformer and LSTM to detect DoS and DDoS in UAV systems. Kacem and Tossou [55] proposed a transformer-based system to detect replay attacks targeting ADS-B systems.

 doi:10.20944/preprints202604.1384.v1

Table 3. Classification of DL Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Tlili et al. [40]	LSTM	Jamming, MiTM, GPS Spoofing, Malware	All	Availability, Integrity, Confidentiality, Authenticity
Mehdi et al. [41]	DPN	DoS, MiTM	Communication	Availability, Integrity, Authenticity
Niyonsaba [42]	CNN + LSTM	DoS, DDoS, MiTM	Communication	Availability, Authenticity
Mughal et all. [43]	LSTM + DDPG	Jamming	Physical	Availability
Tang et al [44]	DNN + DQN	Jamming	Physical	Availability
Haque et al. [45]	PCA + DNN	MiTM, Command Injection	Communication, Control	Authenticity, Integrity
Abu AL-Haija and Badawi [46]	Deep CNN	DoS, MiTM, Command Injection	Communication, Control	Availability, Integrity, Authenticity
Ramadan et al. [49]	LSTM + RNN	DoS, Malware, Botnet, MiTM	Communication, Application	Availability, Integrity, Authenticity
Mughal et al. [50]	FNN, CNN, RNN	Message Injection, DoS	Communication	Integrity, Availability, Authenticity
Alzahrani [51]	CNN, LSTM, CNN-LSTM, convLSTM	DoS, MiTM, Message Injection	Communication	Availability, Integrity, Authenticity
Jalil Hadi [52]	FFCNN	DoS, Message Injection	Communication	Availability, Integrity, Authenticity
Miao et al. [53]	CNN-biLSTM	DoS, GPS Spoofing, Command Injection	Communication, Navigation, Control	Availability, Integrity, Authenticity
Benjamin and Kacem [54]	Transformer + LSTM	DoS, DDoS	Communication	Availability
Kacem and Tossou [55]	Transformer	ADS-B Message Injection	Communication	Authenticity, Integrity

6. Federated Learning Methods

FL [56] has emerged as a crucial strategy for improving UAV network security, especially in situations where data privacy, distributed computation, and restricted bandwidth are issues. Unlike traditional centralized learning, FL enables UAVs to train models jointly across remote devices without sharing raw data, ensuring privacy while achieving excellent detection accuracy. The summary of research work is Table 4. UAV networks can identify known and undiscovered cyber-attacks, such as blackhole, sinkhole, floods, GPS spoofing, and jamming, by combining FL with machine learning, deep learning, and advanced data augmentation techniques [57–59].

 doi:10.20944/preprints202604.1384.v1

Several frameworks demonstrate the practical application of FL in UAV cybersecurity. Lightweight Spectrogram Network (LSNet) [57] was developed as a zero-trust federated framework for UAV authentication using a spectrogram-based model, achieving over 80% accuracy for recognized UAVs and an AUROC of 0.7 for unknown UAV kinds across five remote clients. FL-IDS [58,60] allows for collaborative intrusion detection in FANETs, identifying high-impact assaults like floods with near-ideal accuracy, even at low attacker ratios, while maintaining privacy and adaptability through weight-sharing. Advanced frameworks use generative models, like CGAN-LSTM architectures and blockchain-based federated aggregation (BFA) [59,68], to improve training data, solve class imbalance, and assure safe, decentralized model updates.

Table 4. Classification of FL Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Zhang et al. [57]	LSNet	Message Injection, Command Injection, Model Poisoning	Communication, Control, Application	Integrity, Authenticity, Privacy, Robustness
Ceviz et al. [58,60]	FedAvg + CNN + DNN	DoS	Communication	Availability, Privacy
He et al. [59]	CGAN-LSTM + BFA	Jamming, DoS, MiTM, Model Poisoning	Communication, Application	Availability, Privacy, Integrity, Robustness
Lu ey al. [61]	L-MDAE	Sensor Manipulation, DoS	Physical, Communication	Availability, Integrity, Authenticity, privacy
Da Silva et al. [62,63]	Light GBM	GPS Spoofing, Jamming	Physical, Navigation	Availability, Integrity, Authenticity, Privacy
Ceviz [64]	Few Shot Learning	DoS	Communication	Availability, Privacy
Mowala et al. [66]	Custom Model	Jamming	Physical	Availability, Privacy
Fahim-Ul-Islam et al. [67]	FedWGCA	Model Poisoning	Application	Robustness, Privacy
Zeng [68]	FL + GAN	Jamming, Message Injection, DoS, GPS Spoofing, Model Evasion	All	Integrity, Authenticity, Availability, Privacy, Robustness
Deng et al. [69]	Custom	DoS, Command Injection, Message Injection	Communication, Control	Availability, Integrity, Authenticity, Privacy
Chai et al. [70]	TCN-Transformer	GPS Spoofing, Jamming	Physical, Navigation	Availability, Integrity, Privacy
Cui et al. [71]	OPFL	DoS, Message Injection, MiTM	Communication	Integrity, Authenticity, Availability, Privacy
Ntizikira et al. [72]	DP + CNN-LSTM	DoS, DDoS, MiTM, Message Injection, Code Injection	Communication, Control	Availability, Integrity, Authenticity, Privacy

 doi:10.20944/preprints202604.1384.v1

FL enables distributed anomaly detection in UAV swarms with excellent accuracy and robustness. Multi-modal denoising autoencoder and federated learning (L-MDAE) [61] uses multi-modal denoising autoencoders trained with FL to detect communication anomalies, with up to 99.19% accuracy across several datasets. Hybrid FL-based IDS frameworks [62,63] combine unsupervised approaches for in-flight anomalies (e.g., GPS spoofing and jamming) with supervised learning for network assaults, resulting in high F1-scores (up to 97.9%) in resource-constrained contexts. Few-shot FL (FSFL-IDS) [64] and continuous learning frameworks (FCL-SBLS) [65] improve flexibility, enabling UAVs to retain detection performance with less computational overhead.

Mowala [66] proposed a FL-based approach for on-device jamming detection based on a custom model where the training depends on both the local and global models along with client group prioritization using Dempster–Shafer theory. Fahim-Ul-Islam [67] proposed FedWGCA frameworks based on weighted Gradient Clipping (GC) aggregation and Attention-based Neural Networks that reduces the impact of malicious updates while preserving accuracy, precision, and recall.

Federated GAN-augmented IDS (FGA-IDS) [68] combines synthetic data generation with FL to enhance detection reliability and reduce bandwidth utilization. Deng et al. [69] proposes a custom model, FIDSUS, that optimizes feature aggregation by collaborative sensing and cross-round feature fusion, resulting in 4-34% greater accuracy compared to conventional FL approaches. Additional research demonstrates FL's potential for UAV navigation and mission-critical operations. TCN-Transformer networks [70] and FL detect GPS spoofing and jamming with greater accuracy. Online personalized FL (OPFL) [71] adjusts models to heterogeneous UAV hardware, attaining 95.88% detection accuracy. SP-IoUAV [72] is a privacy-preserving FL architecture that uses Differential Privacy (DP), secure multi-party computation, and CNN-LSTM models to provide great security (99.98% accuracy) and data confidentiality in real-time threat detection.

7. Reinforcement Learning Methods

RL [47] has emerged as a useful paradigm for improving autonomous UAV security because it allows agents to learn optimal defensive or navigation methods through interaction with dynamic surroundings. In UAV systems, RL techniques such as Deep Q-Networks (DQN), and Policy Gradient approaches are popular since they enable UAVs to deal with threat vectors. Table 5 summarizes the research done in this area.

A lightweight DQN-based Intrusion Detection and Prevention System (IDPS) [48] allowed UAVs to identify harmful actions and respond autonomously under onboard computational constraints. The model achieved 99.70% accuracy, with precision, recall, and F1-scores of 0.95, 0.97, and 0.96, respectively, while using very little energy. A context-adaptive IDS [73] used many independent Deep Reinforcement Learning (DRL) agents to detect and classify complicated attacks. Evaluations on the NSL-KDD, UNSW-NB15, and AWID datasets demonstrate higher accuracy and fewer false positives than conventional approaches. The system remains resistant to adversarial manipulations, and integration with a denoising autoencoder improves resilience and adaptation to changing assault patterns. Similarly, an AI-driven IDS optimized for UAVCAN networks [74] successfully detected developing attack patterns, considerably increasing the cybersecurity and operational resilience of UAV communication systems.

Deep Deterministic Policy Gradient (DDPG) was proposed by Tao et al. [75] to effectively identify intrusions in UAV aerial computing environments, providing advice for future security advancements in these networks. In defense and rescue scenarios, fully autonomous UAVs [76] integrated clever onboard security systems capable of discriminating between normal and faked signals, evading threats, and assuring safe return home under cyber-attack conditions. The approach is based on Self Taught Learning (STL) used with multiclass SVM and DQN. Federated Deep Learning (FDL) techniques have been combined with RL to improve UAV network security. A drone client selection algorithm [77] optimized participation in federated deep learning, resulting in FLID, a federated IDS, combining MLPs, CNNs, and LSTM-based RNNs to detect variants of DoS attacks such as flooding, blackhole, and

 doi:10.20944/preprints202604.1384.v1

selective forwarding in FANETs while maintaining privacy and minimizing computation. Experiments with the WSN-BFSF dataset yielded high results: 99.38% accuracy, 99% precision, 99% recall, and 99% F1-score.

Table 5. Classification of RL Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Bouhamed et al. [48]	DQN	Command Injection, DoS	Communication	Availability, Authenticity, Integrity
Sethi et al. [73]	DQN	DoS, MiTM, Message Injection, Data Poisoning, Model Evasion	Communication, Application	Availability, Integrity, Authenticity, Robustness
Islam et al. [74]	DQN	DoS, Message Injection	Communication	Availability, Integrity, Authenticity
Tao et al. [75]	DDPG	GPS Spoofing, Jamming	Physical, Navigation	Availability, Authenticity, Integrity
Arthur et a. [76]	STL + SVM + DQN	Jamming, Message Injection	Physical, Communication	Availability, Authenticity, Integrity
Benfriha et al. [77]	RL + FDL	DoS	Communication	Availability
Hickling et al. [78]	DDPG + PER + APF	Data Poisoning, Model Evasion	Application	Robustness

Adversarial attack detection framework [78] used explainable DRL with Deep Deterministic Policy Gradient (DDPG), Prioritized Experience Replay (PER), and Artificial Potential Fields (APF) to efficiently avoid obstacles and detect attacks. Experiments with Basic Iterative Method (BIM) adversarial attacks reveal that a CNN-based detector gets 80% accuracy, whereas an LSTM-based detector achieves 91% accuracy with faster processing, allowing for real-time adversary identification. Reinforcement learning equips UAVs with adaptive, proactive, and resilient security capabilities, allowing for autonomous threat detection, optimal navigation, and real-time reaction even in complex situations.

8. Graph Neural Network Methods

GNNs [79] are popular in modeling complex relational data in UAV networks, particularly for applications in swarm coordination, communication, and security. By representing UAVs as nodes and their interactions or communication links as edges, GNNs capture spatial, temporal, and topological dependencies that traditional machine learning models often overlook. The summary of the research works is provided Table 6.

Wang et al. [80] proposed an anomaly detection model for multivariate UAV sequences that integrates GNNs with transformers and a graph attention mechanism. Using a multi-channel transformer for intrinsic pattern extraction, a Graph Attention Network (GAT) for temporal-spatial dependencies, and a multi-channel fusion module using Bi-LSTM with channel attention, their proposed approach achieved accuracies of 92.83% and 96.59% on two UAV datasets while maintaining computational efficiency, outperforming existing anomaly detection methods. Swamy and Sophia [81] proposed a

 doi:10.20944/preprints202604.1384.v1

Spatial-Temporal Fusion GNN enhanced with the Walrus Optimizer. The purpose was to detect data poisoning attacks using visual inputs and control signals from the Udacity and custom GoPro datasets.

Table 6. Classification of GNN Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Wang et al. [80]	GAT + Bi-LSTM	Anomaly Detection	Physical	N/A
Swamy and Sophia [81]	STFGNNet-WO + PPFL	Data Poisoning	Application	Privacy, Robustness
El Rai and Darseesh [82]	Dual-GAT	DoS, Message Injection	Communication	Availability, Authenticity, Integrity
Sun et al. [83]	GAT, GCN, GCN-EW	DoS	Communication	Availability
Mustafa Abro and Abdallah [84]	GAT	Anomaly Detection	Physical	N/A
Mughal et al. [85]	ChebNet	DoS, Message Injection	Communication	Availability, Integrity, Authenticity
Majumder et al.[86]	GCNNs, GATs, GraphSAGE, GT	DoS, Message Injection	Communication	Availability, Integrity, Authenticity
Du et al. [87]	GCN + LSTM	DoS, Message Injection	Communication	Availability, Integrity, Authenticity

By extracting spatial-temporal features through fused adjacency matrices and gated CNN outputs and using a Privacy-Preserving Federated Learning (PPFL) framework, their proposed approach reached 99.2% accuracy, 99% sensitivity, specificity, and precision, and an RMSE of 0.105, surpassing baseline methods in both robustness and predictive performance. Dual-GAT [82], a Dual-Branch GAT architecture for UAV intrusion detection, modeled cyber and physical telemetry data as asynchronous graphs and fused modality-specific representations at the decision level. Evaluated on a public UAV cyber-physical dataset, Dual-GAT outperforms cyber-only, physical-only, and early-fusion approaches, particularly excelling in detecting message injection and DoS attacks requiring domain context. Sun et al. [83] leveraged attack graphs and real-time network measurements to model both static and dynamic network attributes, achieving high precision, recall, F1-score, and AUC while providing insights into uncertainty, explainability, and robustness. A GAT-based approach using Received Signal Strength Indicator (RSSI) data [84] constructed a radius graph representing drone-to-drone communications, incorporating RSSI deviations as node features.

Mughal et al. [85] proposed a model entitled Chebyshev Graph Neural Network (ChebNet) for UAV swarm security. The authors setup a hexagonal UAV swarm testbed study showing that leveraging spatial relationships alongside temporal patterns significantly improves intrusion detection performance under false data injection, evil twin, replay, and DoS attacks compared to traditional deep neural networks. Majumder et al. [86] transformed tabular UAVCAN messages into graph structures then employed GCNNs, GATs, GraphSAGE, and Graph-based Transformers (GT) for intrusion of message injection and variants of DoS such as fuzzing and flooding. Inductive models such as GraphSAGE, GAT, and GT generalize effectively to unseen nodes and achieve high accuracy—for instance, 99.45% compared to 69.81% for baseline LSTM, consistently outperforming traditional

 doi:10.20944/preprints202604.1384.v1

models across complex attack scenarios. For UAV networks with sparse ECU nodes, UAV-GCN-LSTM (UGL) [87] combined GCNs for network topology modeling with LSTMs for sequential behavior, achieving 100% accuracy for flooding, 98.54% for Fuzzing, and 96.35% for Replay attacks, significantly outperforming baseline approaches.

Collectively, these studies underscore the strengths of GNN-based approaches in capturing complex spatiotemporal and relational patterns within UAV networks. By consistently achieving high accuracy, low false positive rates, and robust generalization to unseen scenarios, GNNs provide a reliable, scalable, and efficient solution for UAV security, anomaly detection, and cooperative swarm operations.

9. Generative AI Methods

GAI [88] has emerged as an effective technique for improving UAV cybersecurity by tackling crucial issues such as data scarcity, class imbalance, and the necessity for realistic attack simulation. Generative Adversarial Networks (GANs) are increasingly being used in UAV intrusion detection systems (IDS) to generate synthetic data that mimics actual network traffic or sensor behavior. Generative AI also augments local UAV datasets, decreasing reliance on centralized data gathering and strengthening IDS resilience in dynamic or data-constrained contexts. Summary of the research work done in this category is summarized in Table 7.

Table 7. Classification of GAI Methods.

Authors	Model	Attack Type	UAV Layer	Security Property
Asif et al. [89]	GAN	Jamming, GPS Spoofing, Model Evasion	Physical, Communication, Application	Availability, Integrity, Authenticity, Robustness
El Alami and Rawat[90]	GAN + Transformers	Actuator Manipulation, Jamming, GPS Spoofing	Physical, Navigation	Availability, Integrity, Authenticity
Zhao et al. [91]	MoE-enabled GAI	Jamming, MiTM, Message Injection	Physical, Communication	Availability, Authenticity, Integrity
Panda and Guo [92]	CGAN + CVAE	DoS, Message Injection, MiTM, Model Evasion	Communication, Application	Availability, Integrity, Authenticity, Robustness
Sarrikaya and Bahtiyar [93]	CTGAN + GC + VAE	Jamming	Physical	Availability
Nagendra Kumar et al. [94]	GAN + zk-SNARK + PBFT	Message Injection, MiTM	Communication	Integrity, Authenticity
Zeng and Nait-Abdesselam [95]	HITL-ML + GAN	Model Evasion	Application	Robustness
Gaber et al. [96]	GAN + ML classifiers	Model Evasion	Application	Robustness

A GAN-enhanced IDS [89] generated adversarial samples targeting the IDS's vulnerabilities, which were then used in training to improve robustness. This method outperformed traditional intrusion detection systems in terms of detecting evasion attacks while retaining a low false-positive rate. DroneDefGANt [90] used GAN-based data creation and transformer-based feature extraction to

 doi:10.20944/preprints202604.1384.v1

detect both external threats like GPS spoofing and jamming, as well as internal defects like actuator failures. Synthetic dataset evaluations reveal 97.43% for spoofing and 98.96% for jamming, indicating robustness against Gaussian noise.

Zhao et al. [91] relied on a Mixture of Experts (MoE) based GAI model that included GAN, Auto Encoders (AE) and Variational Auto Encoders (VAE) to guide learning and generate high-quality synthetic samples. This approach achieved 99% intrusion detection accuracy while decreasing labeled data requirements by 98%. A Conditional GAN (CGAN) based framework [92] generated stealthy adversarial perturbations that evade traditional IDSs. Detection via a conditional variational autoencoder (CVAE) negative log-likelihood achieves very hight AUC, 99%, demonstrating a reliable defense against stealth attacks. Synthetic data generation with CTGAN, Gaussian Copulas (GC), and VAEs [93] improved IDS performance, with CTGAN providing more realistic distributions and VAE-generated data sustaining IDS accuracy with only a 1% loss.

Generative AI has also been used in more complicated UAV security designs. Nagendra Kumar et al. [94] proposed a solution to deal with message injection and MiTM by leveraging GANs for anomaly detection, zk-SNARK for privacy-preserving identity verification, and PBFT consensus for secure transactions. Their solution achieved 98.4% accuracy, 98.7% precision, 97.9% recall, 98.3% F1-score, and 98.7% AUC while maintaining low latency and reduced computation and communication overhead. Real-time intrusion detection frameworks that combine Human-in-the-Loop Machine Learning (HITL-ML) and GANs [95] to improve adaptability to evolving threats and outperform standard IDSs.

Gaber [96] used GANs to create hybrid datasets of real IoFT traffic and synthetic adversarial attacks. Adversarial training was performed to protect against FGSM, BIM, and C&W attacks. Experimental evaluation tested the effectiveness of ML classifiers such as RF, DT, SVM, and LR reveals that RF achieves up to 96.5% accuracy, demonstrating strong performance in both real and synthetic data.

10. Tools, Datasets & Metrics

There ahs been a great deal of variation in experimental design, datasets, and evaluation metrics across the surveyed literature on UAV and IoT intrusion detection, from classical machine learning to deep learning, generative models, graph neural networks, reinforcement learning, and multitask learning. What is noticed is that there are two main types of datasets: generic cyber security and specialized UAV captures. While the former leverages the similarities between classic cyber attacks in networked environments due to the lack of specialized datasets that capture a wide variety of attacks, the latter dives into more specialized case studies using captures from specific UAV makers or generic protocols used in AUV communication such as MAVLink or ADS-B. Classical machine learning approaches frequently use structured or telemetry-based data, such as GPS logs, handcrafted signal features, or SDN statistical traces, and are frequently evaluated on datasets such as NSL-KDD, UNSW-NB15, KDD-CUP99, WSN-BFSF, and custom UAV-specific datasets such as UAV-IDS 2020. Deep learning and hybrid models rely increasingly heavily on high-dimensional traffic datasets such as CIC-IDS2017, CSE-CIC IDS2018, CIC-DDOS2019, and proprietary UAVCAN or Wi-Fi traffic captures, which provide richer temporal and semantic data. Although promising, GNN and transformer-based solutions often rely on domain-specific graph structures or manually built multi-view packet representations, which limits consistency between research. Reinforcement learning works mostly on simulated environments rather than standardized datasets, making cross-paper comparisons more difficult. Meanwhile, multitask learning research uses multi-view IoT traffic datasets or integrated UAV communication datasets to learn categorization, detection, and device-level tasks. While this diversity shows the UAV security research adaptability, it also highlights a significant reproducibility gap where researchers frequently use alternative datasets, unique pre-processing methods, and non-public traffic captures.

There are three categories of tools used in UAV security: network simulators, navigation simulators and attack generators. For network simulators, prominent tools include Omnet++ and NS3

 doi:10.20944/preprints202604.1384.v1

that are widely used for simulating network communication including some networked-based attacks. Tools such as ArduSIM can also be used in conjunction with them to connect with drone navigation simulators. Tools such as Gazebo and AirSim are widely used in navigation simulations as it allows researchers to simulate 3D physics with great fidelity which allows testing navigation based attacks such as GPS spoofing. Other tools that may be used in this context include Matlab, Simulink and Pixhwak. Finally for attack generation there are a variety of available tools , starting with Aircrack-NG used for launching network-based attacks, Software Defined Radio (SDR) tools such as GNU Radio and HackRF can generate physical or communication based attacks. Tool such as DroneSploit and Nmap are popular for discovering vulnerabilities in networked-based UAVs and are used mostly in conjunction with Kali Linux or Parrot OS.

Evaluation criteria differ greatly among systems, although accuracy, F1-score, precision, recall, false-positive rate (FPR), and false-negative rate (FNR) remain the most used benchmarks. Classical ML systems report good performance. Deep learning models typically outperform ML in term of accuracy, with certain hybrid systems (e.g., CNN-LSTM or distilled models like UAV-DiPNID) reaching up to 99.61% accuracy while drastically lowering model size. GNN and transformer-based models frequently stress enhanced categorization of complex, multi-stage, or hybrid attacks, although their metrics differ greatly because to conflicting job descriptions. Reinforcement learning methods primarily measure reward convergence, attack mitigation success rates, or decision performance under adversarial manipulation, rather than traditional measures such as accuracy or F1, making direct comparisons to supervised learning models problematic. On three separate datasets, MTL systems consistently outperformed single-task designs in terms of multi-task accuracy when compared to specialized models, such as simultaneous anomaly detection, attack identification, and device recognition. Overall, while high accuracy figures are routinely claimed, often exceeding 95-99%, the absence of uniform evaluation settings and agreed benchmarks restricts the legitimacy and reproducibility of many stated metrics.

11. Comparative Analysis

Despite major gains, the literature still has severe methodological limitations that are summarized as follows:

- **Cross-dataset evaluation:** almost every work presents findings from a single dataset or simulation environment, raising worries about overfitting and domain specificity. Few studies examined their models across heterogeneous UAV traffic datasets or test applicability to unknown environments—an critical prerequisite for real-world UAV deployments in which operational conditions vary greatly.
- **Explainability:** while some research use attention processes or feature selection strategies, very few provide interpretable explanations for why a model flags specific telemetry patterns or communication anomalies. This disparity is especially concerning for safety-critical systems like as UAVs, where trust and openness are required.
- **Adversarial perturbations:** denoising autoencoders, and robustness to faked signals, most studies do not systematically assess resilience to adaptive attacks, data poisoning, physical-layer manipulations, or packet-loss situations. RL studies frequently examine robustness through simulation, however these scenarios seldom mimic the complexities of real wireless environments. Similarly, DL and MTL techniques generally presuppose clean, completely labeled datasets, which are rarely met in practice.
- **Reproducibility:** most research lack publicly available code, rely on proprietary UAV datasets, or leave out critical information regarding pre-processing, feature extraction, or hyperparameter tweaking. RL-based works rely on proprietary simulation setups, whereas many transformer/GNN-driven frameworks require domain-specific graph structures or non-standardized multi-view input formats. Even when datasets are made public, preparation procedures vary so greatly that identical models may give different findings across research. These constraints

 doi:10.20944/preprints202604.1384.v1

highlight the urgent need for consistent datasets, uniform evaluation methodologies, explainable intrusion detection algorithms, and robustness tests that are representative of real-world UAV communication scenarios. Without these enhancements, claimed performance measurements, no matter how good, will be difficult to compare, confirm, or trust in mission-critical UAV security deployments.

12. Key Insights

In this section, we summarize the key insight that can be taken from this paper. First, we investigate the mapping between each AI model and every considered security property along with the number of covered papers. In Table 8, we provide these statistics. We refer to security properties as follows: confidentiality (C), integrity (I), availability (Av), authenticity (Au), privacy (P), robustness (R). The first remark is that there are more papers focusing on classical AI models such as ML, DL and FL, when compared to newer and emerging ones such as RL, GNN and GAI. Also, we noticed that availability maintained the highest consistent coverage, which can be explained by the high risk of access to key UAV services such as connectivity or localization. Confidentiality was only lightly covered by ML and DL, which can be explained by the non-secret nature of UAV systems that often use broadcast of location or control messages.

Table 8. Statistic of Security Properties Coverage per AI Methods.

AI Model	C (%)	I (%)	Av (%)	Au (%)	P (%)	R (%)	# Papers
ML	10	50	80	40	0	0	10
DL	7	71	85	78	0	0	14
FL	0	60	73	46	100	20	15
RL	0	71	85	71	0	28	7
GNN	0	50	62	50	12	12	8
GAI	0	62	62	62	0	50	8

The detailed coverage of security properties per AI method is provided in Figure 4 that shows this coverage in a bar chart clustered by each considered AI method. ML methods focus on availability, with 80% of the papers, followed by integrity at 50% then authenticity at 40% and confidentiality at 10%. It is noticed that privacy and robustness are not covered at all, which can be understandable since these security properties are merging ones that cannot be handled by traditional ML models. Statistics for DL methods is quite similar with availability covered at 85%, authenticity at 78%, integrity at 71% and availability at 7%. This can be completely understood since both fall under the traditional AI models.

FL methods covered privacy at 100%, which can be understood since it is the purpose it was designed for. As far as the availability at 73%, integrity at 60%, authenticity at 46% and robustness at 20%. The other key difference, when compared with ML and DL, is the coverage of robustness which is explained by the hybrid nature of some research work conducted in this area that combines FL and GAN. For the remaining advanced AI models, including RL, GNN and GAI, it is noticed that they have common focus on integrity, availability and authenticity with similar ratios, in addition to robustness at a slightly lower rate. RL methods covered availability at 85%, integrity and authenticity at 71% each, and robustness at 28%. GNN has similar statistics by covering integrity and authenticity at 50%, availability at 62%, and both privacy and robustness at 12% each. GAI exhibited equal coverage for integrity, availability and authenticity at 62% each, in addition to robustness at 50%. It is noticed that robustness coverage increased in the emerging AI methods due to the fact that these models appeared in part as a response to the need for these models to address privacy and robustness.

 doi:10.20944/preprints202604.1384.v1

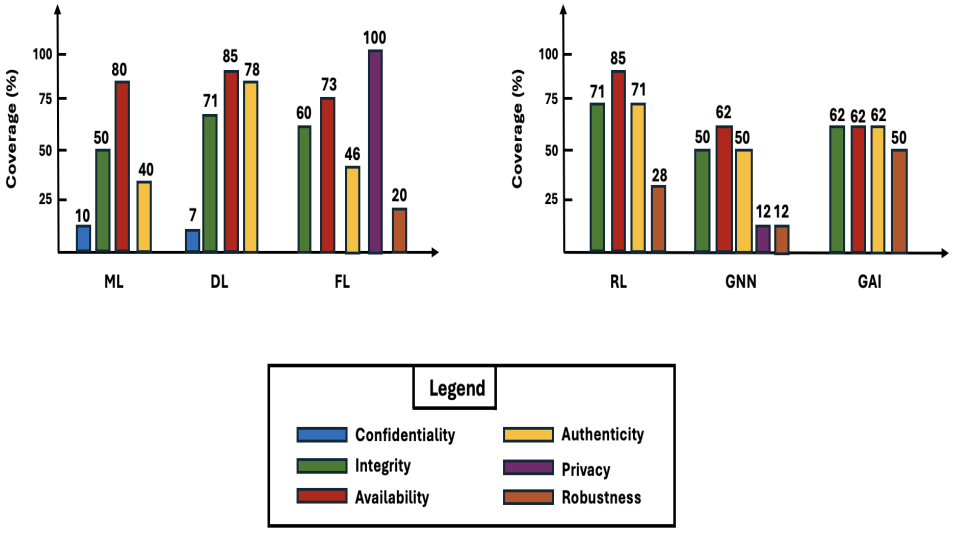

Figure 4. Security Properties Coverage per AI Model Plot.

Figure 5 shows the overall coverage of security properties across all AI methods. It is noticed that authenticity, availability and authenticity are starting to get saturated with coverage ranging from 58% to 75%. On the other hand, there is a noticeable gap in the coverage of other security properties including confidentiality with 3%, privacy with 25% and robustness with 15%. It can be understood that achieving confidentiality using AI method may not be a main concern for researchers considering the secrecy of messages is generally not required. Thus, there is not much prospect in research in that context. However, research work focusing on achieving privacy and robustness would be considered as a very hot and promising research area thanks to emerging models in RL, GNN and GAI, and also due to the importance of these security properties in AI-enabled security for UAV applications nowadays.

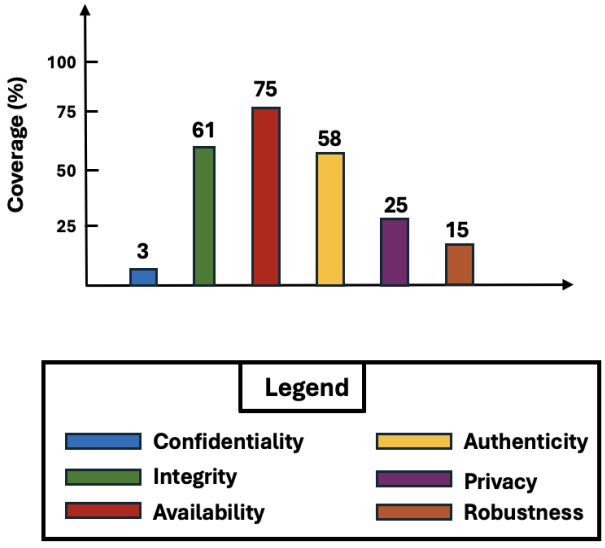

Figure 5. Overall Security Properties Coverage Plot.

13. Open Challenges

Despite significant progress in classical machine learning, deep learning, generative AI, GNNs, reinforcement learning, and, most notably, multitask learning (MTL), a number of persistent challenges

 doi:10.20944/preprints202604.1384.v1

continue to impede the deployment of reliable and generalizable intrusion detection and drone security systems. These challenges are discussed as follows:

- **Data scarcity:** is one of the most fundamental constraints in all techniques. Many UAV-specific datasets, such as GPS spoofing logs, UAVCAN traffic, aerial computing telemetry, or custom RF fingerprints, are extremely small, confidential, or gathered under limited circumstances. Classical machine learning techniques, such as MAVIDS, rely purely on telemetry, whereas many DL- and RL-based algorithms require vast amounts of different training data to avoid overfitting. Even multitask learning frameworks, which normally benefit from shared supervision across tasks, are constrained by the amount and diversity of UAV attack datasets, particularly for hybrid, multi-stage, and zero-day threats. Generative AI has showed promise for developing synthetic attack data, but there are still concerns about distribution fidelity, temporal consistency, and the risk of increasing dataset biases.
- **Real-time Constraints:** present significant deployment issues. UAV platforms have limited onboard computing, memory, and energy resources, but must detect and respond to assaults with millisecond latency. Although many works, such as distributed IDS designs (e.g., E-DIDS), lightweight fuzzy rough set systems, and pruned deep networks (UAV-DiPNID), significantly reduce inference time, more complex methods, such as GNNs, RL agents, and multi-view MTL architectures, continue to struggle to meet hard real-time deadlines in flight. Reinforcement learning and MTL models are more adaptable, but their inference pipelines might be computationally demanding without additional optimization, model reduction, or hardware acceleration.
- **Explainability:** remains weak across nearly all surveyed methodologies. Classical machine learning techniques (e.g., PCA-based anomaly detection, decision trees, and SVMs) allow for partial interpretation, but most deep models including CNN-LSTMs, transformers, GNNs, multi-view architectures, and RL policies—function as black boxes. Only a few efforts explicitly incorporate explainability, such as the explainable DRL adversarial detection framework that employs APF and PER. However, the bulk of cutting-edge systems cannot provide practical explanations for why an assault was identified, what variables influenced the conclusion, or how the UAV should change its behavior. This gap is significant in safety-critical aviation contexts where human operators require transparency and verified logic.
- **Adversarial robustness:** is another big outstanding topic. Deep learning-based IDS models, such as CNNs, LSTMs, transformers, and GNNs, are especially susceptible to evasion attacks, perturbation-based spoofing, and idea drift. While a few studies have examined adversarial settings (e.g., DRL agents tested against adversarial perturbations, denoising autoencoder-enhanced IDSs), the majority of studies continue to assume clean or stationary data distributions. UAV networks are dynamic and vulnerable to hostile actors capable of jamming, replaying, model poisoning, and RF fingerprint obfuscation. Without thorough robustness studies, IDS performance on static datasets may not be consistent with real-world resilience.
- **Absence of set benchmarks:** greatly hinders the comparability and repeatability of investigations. The datasets used in UAV intrusion detection research are inconsistent: NSL-KDD, UNSW-NB15, AWID, WSN-BFSF, KDD-CUP99, CSE-CIC IDS2018, CIC-DDoS2019, UAVCAN logs, RF fingerprint datasets, simulated COOJA traffic, and custom flight logs. Many UAV-focused datasets are private, corporate, or simulator-generated, making it impossible to replicate results. Metrics such as accuracy, F1, recall, fall-out rate, latency, energy consumption, and robustness margins vary greatly, making cross-paper comparisons useless. Multitask learning systems complicate evaluation by introducing many objectives (e.g., anomaly detection, device identification, attack classification) with no consistent reporting requirements.

14. Future Directions

Future directions of UAV security research include the following topics:

 doi:10.20944/preprints202604.1384.v1

- **Federated MTL:** due to the heterogeneous and distributed nature of UAV systems, federated MTL is a promising solution that leverages shared representation with different task-specific heads. This can deal with intermittent client participation that is common in UAV swarms, non-IID data distribution while performing all tasks jointly thus making models less complex and potentially more efficient. Challenges in implementing such solution include dealing with data poisoning, integration with differential privacy and handling communication constraints.
- **Digital Twins:** can be very beneficial in replicating UAV systems thus aiding in simulating attacks and validating defense mechanisms. The benefits include bundling the cyber, physical and AI dimension together facilitating real-time communication between the UAV and its twin while the possibility of being integrated with RL paradigm. Challenges include dealing with the tradeoff between fidelity and computational cost of such solution, and the ability of accurately model the noise.
- **Benchmark Creation:** most existing datasets are fragmented and non-reproducible making the creation of open and curated benchmark a pressing need. Some of the key requirements for such benchmarks is that they have to cover attacks from various layers, multi-modal data and realistic UAV protocols such as ADS-B and MAVLink. Challenges include dealing with distributed and federated environments in addition to including and dealing with adversarial attacks.
- **Trustworthy AI for UAV Security:** the issue with current black-box AI models is that they lack trust in dealing with safety-critical use cases. Some research direction include leveraging explainable AI in making attack detection decisions. Also, another interesting research direction is predicting attacks with high confidence even in the presence of adversarial attacks. In addition, with the rise of popular risk frameworks, such as NIST AI Risk Management Frameworks, it is needed to seamlessly align trustworthy AI solution for UAV security with them. Balancing robustness, explainability and real-time constraints represent the key challenges.

15. Conclusion

UAV ecosystems have been on the rise in recent years, being involved in so many domains and promoting novel services that promote better quality of life and more sophisticated applications. However, due to the rise and widespread of cyber attacks, there has been several approaches to detect and thwart these attacks ranging from classic cryptographic solutions to traditional intrusion based detection. These traditional solutions have been facing challenges in dealing with the sophistication of these attacks though prompting the need of AI-based solutions. On the other hand, most existing surveys present a fragmented view focusing on one type of AI model while neglecting others.

In this paper, we close this gap by proposing a comprehensive survey of AI methods used in UAV security. This covers not only the traditional AI models such as ML and DL but also the emerging ones such as FL, RL, GNN and GAI. We developed an attack taxonomy based on the location of each attack, with regards to the layer in the UAV functional stack. We also proposed a novel taxonomy to classify these AI models based on the type of the model being considered, the attack type and the affected security property.

We complement our survey with a coverage of the datasets, tools and evaluation metrics used in UAV security research in addition of performing a comparative analysis covering the key findings of our classification. We also discuss the open challenges remaining to be solved and the future research directions we think are of high relevance to the research community. We aim that this work will be a reference to be used by UAV security researchers and practitioners who are interested in developing AI-based models to solve the latest UAV security problems.

Author Contributions: Methodology, T.K.; investigation, T.L and K.B; writing—original draft preparation of sections 2, 4-9, 11, 12, K.B.; writing—review and editing of all sections, T.K.; visualization, T.K.; supervision, T.K. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement: There is data to share.

 doi:10.20944/preprints202604.1384.v1

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

References

1. Fahlstrom, P.G., Gleason, T.J. and Sadraey, M.H., 2022. Introduction to UAV systems. John Wiley & Sons.
2. Fan, B., Li, Y., Zhang, R. and Fu, Q., 2020. Review on the technological development and application of UAV systems. Chinese Journal of Electronics, 29(2), pp.199-207.
3. Zhi, Yueyan, Zhangjie Fu, Xingming Sun, and Jingnan Yu. "Security and privacy issues of UAV: A survey." Mobile Networks and Applications 25, no. 1 (2020): 95-101.
4. Kacem, T., Barreto, A., Wijesekera, D. and Costa, P., 2017. ADS-Bsec: A novel framework to secure ADS-B. ICT Express, 3(4), pp.160-163.
5. Sarkar, N.I. and Gul, S., 2023. Artificial intelligence-based autonomous UAV networks: A survey. Drones, 7(5), p.322.
6. Cordill, B.; Fang, D.; Xu, S. A Comprehensive Survey of Security and Privacy in UAV Systems. IEEE Access 2025, 13, 117843–117866. https://doi.org/10.1109/ACCESS.2025.3583985.
7. Tsao, K.-Y.; Girdler, T.; Vassilakis, V. G. A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-Hoc Networks. Ad Hoc Networks 2022, 133, 102894. https://doi.org/10.1016/j.adhoc.2022.102894.
8. Rahman, K.; Aziz, M. A.; Kashif, A. U.; Cheema, T. A. Detection of Security Attacks Using Intrusion Detection System for UAV Networks: A Survey. In Big Data Analytics and Computational Intelligence for Cybersecurity; Ouaissa, M., Boulouard, Z., Ouaissa, M., Khan, I. U., Kaosar, M., Eds.; Springer International Publishing: Cham, 2022; pp 109–123. https://doi.org/10.1007/978-3-031-05752-6_7.
9. AL-Syouf, R. A.; Bani-Hani, R. M.; AL-Jarrah, O. Y. Machine Learning Approaches to Intrusion Detection in Unmanned Aerial Vehicles (UAVs). Neural Comput & Applic 2024, 36 (29), 18009–18041. https://doi.org/10.1007/s00521-024-10306-y.
10. Bithas, P. S.; Michailidis, E. T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A. G. A Survey on Machine-Learning Techniques for UAV-Based Communications. Sensors 2019, 19 (23), 5170. https://doi.org/10.3390/s19235170.
11. Syed, F., Gupta, S.K., Hamood Alsamhi, S., Rashid, M. and Liu, X., 2021. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Transactions on Emerging Telecommunications Technologies, 32(7), p.e4133.
12. Sarıkaya, B. S.; Bahtiyar, Ş. A Survey on Security of UAV and Deep Reinforcement Learning. Ad Hoc Networks 2024, 164, 103642. https://doi.org/10.1016/j.adhoc.2024.103642.
13. Wang, X.; Zhao, Z.; Yi, L.; Ning, Z.; Guo, L.; Yu, F. R.; Guo, S. A Survey on Security of UAV Swarm Networks: Attacks and Countermeasures. ACM Comput. Surv. 2024, 57 (3), 74:1-74:37. https://doi.org/10.1145/3703625.
14. Adil, M.; Jan, M. A.; Liu, Y.; Abulkasim, H.; Farouk, A.; Song, H. A Systematic Survey: Security Threats to UAV-Aided IoT Applications, Taxonomy, Current Challenges and Requirements With Future Research Directions. IEEE Transactions on Intelligent Transportation Systems 2023, 24 (2), 1437–1455. https://doi.org/10.1109/TITS.2022.3220043.
15. Tlili, F., Ayed, S. and Fourati, L.C., 2024. Advancing UAV security with artificial intelligence: A comprehensive survey of techniques and future directions. Internet of Things, 27, p.101281.
16. Yang, Z.; Zhang, Y.; Zeng, J.; Yang, Y.; Jia, Y.; Song, H.; Lv, T.; Sun, Q.; An, J. AI-Driven Safety and Security for UAVs: From Machine Learning to Large Language Models. Drones 2025, 9 (6), 392. https://doi.org/10.3390/drones9060392.
17. Abro, G. E. M.; Zulkifli, S. A. B. M.; Masood, R. J.; Asirvadam, V. S.; Laouiti, A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. Drones 2022, 6 (10), 284. https://doi.org/10.3390/drones6100284.
18. Jacobsen, R. H.; Marandi, A. Security Threats Analysis of the Unmanned Aerial Vehicle System. In IEEE Military Communications Conference (MILCOM); 2021; pp 316–322. https://doi.org/10.1109/MILCOM52596.2021.9652900.
19. Pandey, G. K.; Gurjar, D. S.; Nguyen, H. H.; Yadav, S. Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey. IEEE Access 2022, 10, 112858–112897. https://doi.org/10.1109/ACCESS.2022.3215975.

 doi:10.20944/preprints202604.1384.v1

20. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L. G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. IEEE Communications Surveys & Tutorials 2019, 21 (4), 3417–3442. https://doi.org/10.1109/COMST.2019.2906228.
21. Alzubaidi, A. A. Systematic Literature Review for Detecting Intrusions in Unmanned Aerial Vehicles Using Machine and Deep Learning. IEEE Access 2025, 13, 58576–58599. https://doi.org/10.1109/ACCESS.2025.3552329.
22. Mohsan, S. A. H.; Othman, N. Q. H.; Li, Y.; Alsharif, M. H.; Khan, M. A. Unmanned Aerial Vehicles (UAVs): Practical Aspects, Applications, Open Challenges, Security Issues, and Future Trends. Intel Serv Robotics 2023, 16 (1), 109–137. https://doi.org/10.1007/s11370-022-00452-4.
23. Ogab, M.; Zaidi, S.; Bourouis, A.; Calafate, C. T. Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review. IEEE Access 2025, 13, 96681–96714. https://doi.org/10.1109/ACCESS.2025.3575236.
24. Sharifi, I., Ghazanfari, M., Taye, A., Wei, P., Ahmed, M., Tae Kim, H., Ghasemi, M., Gupta, V., Dahle, N.W., Canady, R. and Diaz-Gonzalez, A., 2026. A Survey of Security Challenges and Solutions for UAS Traffic Management (UTM) and small Unmanned Aerial Systems (sUAS). In AIAA SCITECH 2026 Forum (p. 2892).
25. Umrani, M.I., Butler, B., O'Driscoll, A. and Davy, S., 2026. Toward Secure Complex UAV Cyber-Physical Systems: A Unified Threat Taxonomy and Cross-Layer Survey of Cybersecurity Challenges. Internet of Things, p.101902.
26. Chamola, V.; Kotesh, P.; Agarwal, A.; Naren; Gupta, N.; Guizani, M. A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. Ad Hoc Networks 2021, 111, 102324. https://doi.org/10.1016/j.adhoc.2020.102324.
27. Zhou, Z.H., 2021. Machine learning. Springer nature.
28. Whelan, J.; Almehmadi, A.; El-Khatib, K. Artificial Intelligence for Intrusion Detection Systems in Unmanned Aerial Vehicles. Computers and Electrical Engineering 2022, 99, 107784. https://doi.org/10.1016/j.compeleceng.2022.107784.
29. Moustafa, N.; Jolfaei, A. Autonomous Detection of Malicious Events Using Machine Learning Models in Drone Networks. In Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond; DroneCom '20; Association for Computing Machinery: New York, NY, USA, 2020; pp 61–66. https://doi.org/10.1145/3414045.3415951.
30. A. Shafique; A. Mehmood; M. Elhadef, Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. In IEEE Access, vol. 9, pp. 93803-93815, 2021, doi: 10.1109/ACCESS.2021.3089847
31. D. Agnew; A. D. Aguila; J. Mcnair, Enhanced Network Metric Prediction for Machine Learning-Based Cyber Security of a Software-Defined UAV Relay Network. in IEEE Access, vol. 12, pp. 54202-54219, 2024, doi: 10.1109/ACCESS.2024.3387728.
32. Wu, Y.; Yang, L.; Zhang, L.; Nie, L.; Zheng, L. Intrusion Detection for Unmanned Aerial Vehicles Security: A Tiny Machine Learning Model. IEEE Internet of Things Journal 2024, 11 (12), 20970–20982. https://doi.org/10.1109/JIOT.2024.3360231.
33. Fu, R.; Ren, X.; Li, Y.; Wu, Y.; Sun, H.; Al-Absi, M. A. Machine-Learning-Based UAV-Assisted Agricultural Information Security Architecture and Intrusion Detection. IEEE Internet of Things Journal 2023, 10 (21), 18589–18598. https://doi.org/10.1109/JIOT.2023.3236322.
34. Shrestha, R.; Omidkar, A.; Roudi, S. A.; Abbas, R.; Kim, S. Machine-Learning-Enabled Intrusion Detection System for Cellular Connected UAV Networks. Electronics 2021, 10 (13), 1549. https://doi.org/10.3390/electronics10131549.
35. Whelan, J.; Sangarapillai, T.; Minawi, O.; Almehmadi, A.; El-Khatib, K. Novelty-Based Intrusion Detection of Sensor Attacks on Unmanned Aerial Vehicles. In Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks; Q2SWinet '20; Association for Computing Machinery: New York, NY, USA, 2020; pp 23–28. https://doi.org/10.1145/3416013.3426446.
36. Z. Cai; Z. Liu; L. Kou. Reliable UAV Monitoring System Using Deep Learning Approaches. In IEEE Transactions on Reliability, vol. 71, no. 2, pp. 973-983, June 2022, doi: 10.1109/TR.2021.3119068.
37. Mehmood, R. T.; Ahmed, G.; Siddiqui, S. Simulating ML-Based Intrusion Detection System for Unmanned Aerial Vehicles (UAVs) Using COOJA Simulator. In 2022 16th International Conference on Open Source Systems and Technologies (ICOSST); 2022; pp 1–10. https://doi.org/10.1109/ICOSST57195.2022.10016875.
38. Alipour-Fanid, A.; Dabaghchian, M.; Wang, N.; Wang, P.; Zhao, L.; Zeng, K. Machine Learning-Based Delay-Aware UAV Detection and Operation Mode Identification Over Encrypted Wi-Fi Traffic. IEEE Transactions on Information Forensics and Security 2020, 15, 2346–2360. https://doi.org/10.1109/TIFS.2019.2959899.

 doi:10.20944/preprints202604.1384.v1

39. LeCun, Y., Bengio, Y. and Hinton, G., 2015. Deep learning. nature, 521(7553), pp.436-444.
40. Tlili, F.; Ayed, S.; Chaari Fourati, L. Exhaustive Distributed Intrusion Detection System for UAVs Attacks Detection and Security Enforcement (E-DIDS). Computers & Security 2024, 142, 103878. https://doi.org/10.1016/j.cose.2024.103878.
41. Medhi, J.; Liu, R.; Wang, Q.; Chen, X. A Lightweight and Efficient Intrusion Detection System (IDS) for Unmanned Aerial Vehicles. Neural Computing and Applications 2025, 37 (20), 15819–15836. https://doi.org/10.1007/s00521-025-11276-5.
42. Niyonsaba, S., Konate, K. and Soidridine, M.M., 2024, July. Deep learning based intrusion detection for cybersecurity in unmanned aerial vehicles network. In 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET (pp. 1-6). IEEE.
43. Mughal, U. A.; Alkhrijah, Y.; Almadhor, A.; Yuen, C. Deep Learning for Secure UAV-Assisted RIS Communication Networks. IEEE Internet of Things Magazine 2024, 7 (2), 38–44. https://doi.org/10.1109/IOTM.001.2300132.
44. Tang, X.; Liu, N.; Zhang, R.; Han, Z. Deep Learning-Assisted Secure UAV-Relaying Networks With Channel Uncertainties. IEEE Transactions on Vehicular Technology 2022, 71 (5), 5048–5059. https://doi.org/10.1109/TVT.2022.3151471.
45. Haque, E.; Hasan, K.; Ahmed, I.; Alam, M. S.; Islam, T. Enhancing UAV Security Through Zero Trust Architecture: An Advanced Deep Learning and Explainable AI Analysis. arXiv March 25, 2024. https://doi.org/10.48550/arXiv.2403.17093.
46. Abu Al-Haija, Q.; Al Badawi, A. High-Performance Intrusion Detection System for Networked UAVs via Deep Learning. Neural Comput & Applic 2022, 34 (13), 10885–10900. https://doi.org/10.1007/s00521-022-07015-9.
47. Kaelbling, L.P., Littman, M.L. and Moore, A.W., 1996. Reinforcement learning: A survey. Journal of artificial intelligence research, 4, pp.237-285.
48. Bouhamed, O., Bouachir, O., Aloqaily, M. and Al Ridhawi, I., 2021, May. Lightweight ids for uav networks: A periodic deep reinforcement learning-based approach. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 1032-1037). IEEE.
49. Ramadan, R.A., Emara, A.H., Al-Sarem, M. and Elhamahmy, M., 2021. Internet of drones intrusion detection using deep learning. Electronics, 10(21), p.2633.
50. Mughal, U. A.; Hassler, S. C.; Ismail, M. Machine Learning-Based Intrusion Detection for Swarm of Unmanned Aerial Vehicles. In 2023 IEEE Conference on Communications and Network Security (CNS); 2023; pp 1–9. https://doi.org/10.1109/CNS59707.2023.10288962.
51. Alzahrani, A. Novel Approach for Intrusion Detection Attacks on Small Drones Using ConvLSTM Model. IEEE Access 2024, 12, 149238–149253. https://doi.org/10.1109/ACCESS.2024.3471806.
52. Jalil Hadi, H.; Cao, Y.; Li, S.; Hu, Y.; Wang, J.; Wang, S. Real-Time Collaborative Intrusion Detection System in UAV Networks Using Deep Learning. IEEE Internet of Things Journal 2024, 11 (20), 33371–33391. https://doi.org/10.1109/JIOT.2024.3426511.
53. Miao, S., Pan, Q. and Zheng, D., 2024. Unmanned aerial vehicle intrusion detection: Deep-meta-heuristic system. Vehicular Communications, 46, p.100726.
54. Benjamin, K. and Kacem, T., 2025, May. UAV DoS Attack Detection using a Hybrid Transformer-LSTM Approach. In 2025 International Wireless Communications and Mobile Computing (IWCMC) (pp. 1702-1708). IEEE.
55. Kacem, T. and Tossou, S., 2024, May. ADS-B replay attack detection using transformers. In 2024 International Wireless Communications and Mobile Computing (IWCMC) (pp. 144-149). IEEE.
56. Kairouz, P. and McMahan, H.B., 2021. Advances and open problems in federated learning. Foundations and trends in machine learning, 14(1-2), pp.1-210.
57. Zhang, H.; Zhou, F.; Wang, W.; Wu, Q.; Yuen, C. A Federated Learning-Based Lightweight Network With Zero Trust for UAV Authentication. IEEE Transactions on Information Forensics and Security 2025, 20, 7424–7437. https://doi.org/10.1109/TIFS.2025.3587624.
58. Ceviz, O.; Sadioglu, P.; Sen, S.; Vassilakis, V. G. A Novel Federated Learning-Based IDS for Enhancing UAVs Privacy and Security. Internet of Things 2025, 31, 101592. https://doi.org/10.1016/j.iot.2025.101592.
59. He, X.; Chen, Q.; Tang, L.; Wang, W.; Liu, T. CGAN-Based Collaborative Intrusion Detection for UAV Networks: A Blockchain-Empowered Distributed Federated Learning Approach. IEEE Internet of Things Journal 2023, 10 (1), 120–132.
60. Ceviz, O.; Sadioğlu, P.; Sen, S.; Vassilakis, V. A Novel Federated Learning-Based Intrusion Detection System for Flying Ad Hoc Networks; 2023. https://doi.org/10.48550/arXiv.2312.04135.

 doi:10.20944/preprints202604.1384.v1

61. Lu, Y.; Yang, T.; Zhao, C.; Chen, W.; Zeng, R. A Swarm Anomaly Detection Model for IoT UAVs Based on a Multi-Modal Denoising Autoencoder and Federated Learning. Computers & Industrial Engineering 2024, 196, 110454. https://doi.org/10.1016/j.cie.2024.110454.
62. da Silva, L.; Ferrao, I.; Dezan, C.; Espes, D.; Castelo Branco, K. Anomaly-Based Intrusion Detection System for In-Flight and Network Security in UAV Swarm; 2023; pp 812–819. https://doi.org/10.1109/ICUAS57906.2023.10155873.
63. da Silva, L. M.; Ferrão, I. G.; Diniz, B. A.; Carciofi, T. P.; Ziliol, V. D.; Dezan, C.; Espes, D.; Branco, K. R. L. J. C. Collaborative Intrusion Detection System for Network and Flight Security in Unmanned Aerial Vehicles Group. In 2025 International Conference on Unmanned Aircraft Systems (ICUAS); 2025; pp 1027–1034.
64. Ceviz, O.; Sen, S.; Sadioglu, P. Distributed Intrusion Detection in Dynamic Networks of UAVs Using Few-Shot Federated Learning. In Security and Privacy in Communication Networks; Alrabaee, S., Choo, K.-K. R., Damiani, E., Deng, R. H., Eds.; Springer Nature Switzerland: Cham, 2026; pp 131–153. https://doi.org/10.1007/978-3-031-94448-2_7.
65. He, X., Chen, Q., Tang, L., Wang, W., Liu, T., Li, L., Liu, Q. and Luo, J., 2023. Federated continuous learning based on stacked broad learning system assisted by digital twin networks: An incremental learning approach for intrusion detection in UAV networks. IEEE Internet of Things Journal, 10(22), pp.19825-19838.
66. N. I. Mowla, N. H. Tran, I. Doh and K. Chae, "Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network," in IEEE Access, vol. 8, pp. 4338-4350, 2020, doi: 10.1109/ACCESS.2019.2962873.
67. Fahim-Ul-Islam, Md.; Chakrabarty, A.; Hakimi, H. S.; Maidin, S. S. FedWGCA: A Federated Learning Based AAV Intrusion Detection With Gradient Clipping and Attention-Based Neural Networks. IEEE Open Journal of the Computer Society 2025, 6, 1799–1809. https://doi.org/10.1109/OJCS.2025.3616394.
68. Zeng, Q.; Olatunde-Salawu, S.; Nait-Abdesselam, F. FGA-IDS: A Federated Learning and GAN-Augmented Intrusion Detection System for UAV Networks. In 2024 IEEE 10th International Conference on Collaboration and Internet Computing (CIC); 2024; pp 50–59. https://doi.org/10.1109/CIC62241.2024.00017.
69. Deng, J., Wang, W., Wang, L., Bashir, A.K., Gadekallu, T.R., Feng, H., Lv, M. and Fang, K., 2025. FIDSUS: Federated intrusion detection for securing UAV swarms in smart aerial computing. IEEE Internet of Things Journal.
70. Chai, Y., Liu, M. and Li, M., 2025. Navigation spoofing and jamming signals identification of UAV based on federated learning. IEEE Internet of Things Journal.
71. Cui, X., Wu, J., Fan, X., Yu, Q., Wang, T., Li, G. and Luo, C., 2025, June. Online personalized federated learning methods for intrusion detection in dynamic UAV networks. In International Conference on Wireless Artificial Intelligent Computing Systems and Applications (pp. 394-405). Singapore: Springer Nature Singapore.
72. Ntizikira, E.; Lei, W.; Alblehai, F.; Saleem, K.; Lodhi, M. A. Secure and Privacy-Preserving Intrusion Detection and Prevention in the Internet of Unmanned Aerial Vehicles. Sensors 2023, 23 (19), 8077. https://doi.org/10.3390/s23198077.
73. Sethi, K.; Sai Rupesh, E.; Kumar, R.; Bera, P.; Venu Madhav, Y. A Context-Aware Robust Intrusion Detection System: A Reinforcement Learning-Based Approach. Int. J. Inf. Secur. 2020, 19 (6), 657–678. https://doi.org/10.1007/s10207-019-00482-7.
74. Islam, M. R.; Yusupov, K.; Muminov, I.; Sahlabadi, M.; Yim, K. Cybersecurity in UAVs: An Intrusion Detection System Using UAVCAN and Deep Reinforcement Learning. In Advances on Broad-Band Wireless Computing, Communication and Applications; Barolli, L., Ed.; Springer Nature Switzerland: Cham, 2025; pp 123–131.
75. Tao, J.; Han, T.; Li, R. Deep-Reinforcement-Learning-Based Intrusion Detection in Aerial Computing Networks. IEEE Network 2021, 35 (4), 66–72. https://doi.org/10.1109/MNET.011.2100068.
76. Arthur, M. P. Detecting Signal Spoofing and Jamming Attacks in UAV Networks Using a Lightweight IDS. In 2019 International Conference on Computer, Information and Telecommunication Systems (CITS); 2019; pp 1–5. https://doi.org/10.1109/CITS.2019.8862148.
77. Benfriha, S.; Labraoui, N.; Bany Salameh, H. A.; Bensaid, R. Reinforcement Learning-Based Drone-Client Selection for Efficient Federated Learning-Based Intrusion Detection in FANETs. Cluster Comput 2025, 28 (8), 549. https://doi.org/10.1007/s10586-025-05188-1.
78. Hickling, T.; Aouf, N.; Spencer, P. Robust Adversarial Attacks Detection Based on Explainable Deep Reinforcement Learning for UAV Guidance and Planning. IEEE Transactions on Intelligent Vehicles 2023, 8 (10), 4381–4394. https://doi.org/10.1109/TIV.2023.3296227.
79. Zhou, J., Cui, G., Hu, S., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C. and Sun, M., 2020. Graph neural networks: A review of methods and applications. AI open, 1, pp.57-81.

 doi:10.20944/preprints202604.1384.v1

80. Wang, G.; Ai, J.; Mo, L.; Yi, X.; Wu, P.; Wu, X.; Kong, L. Anomaly Detection for Data from Unmanned Systems via Improved Graph Neural Networks with Attention Mechanism. Drones 2023, 7 (5), 326. https://doi.org/10.3390/drones7050326.
81. Swamy, K. K.; Sophia, S. Detecting Poisoning Attacks in UAVs via Spatio-Temporal Graph Neural Network and Walrus Optimizer. In 2025 5th International Conference on Soft Computing for Security Applications (ICSCSA); 2025; pp 2004–2011. https://doi.org/10.1109/ICSCSA66339.2025.11170740.
82. El Rai, M. C.; Darseesh, M. Dual-Branch Graph Attention Network for Cyber-Physical Intrusion Detection System for Unmanned Aerial Vehicles. In 2025 International Conference on Communication, Computing, Networking, and Control in Cyber-Physical Systems (CCNCPS); 2025; pp 381–384. https://doi.org/10.1109/CCNCPS66785.2025.11135729.
83. Sun, Z.; Teixeira, A. M. H.; Toor, S. GNN-IDS: Graph Neural Network Based Intrusion Detection System. In Proceedings of the 19th International Conference on Availability, Reliability and Security; ARES '24; Association for Computing Machinery: New York, NY, USA, 2024; pp 1–12. https://doi.org/10.1145/3664476.3664515.
84. Mustafa Abro, G. E.; Abdallah, A. M. Graph Attention Networks For Anomalous Drone Detection: RSSI-Based Approach with Real-World Validation. Expert Systems with Applications 2025, 273, 126913. https://doi.org/10.1016/j.eswa.2025.126913.
85. Mughal, U. A.; Atat, R.; Ismail, M. Graph Neural Network-Based Intrusion Detection System for a Swarm of UAVs. In MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM); 2024; pp 578–583. https://doi.org/10.1109/MILCOM61039.2024.10773671.
86. Majumder, R.; Comert, G.; Werth, D.; Gale, A.; Chowdhury, M.; Salek, M. S. Graph-Powered Defense: Controller Area Network Intrusion Detection for Unmanned Aerial Vehicles. arXiv August 8, 2025. https://doi.org/10.48550/arXiv.2412.02539.
87. Du, Y.; Li, Y.; Cheng, P.; Han, Z.; Wang, Y. UGL: A Comprehensive Hybrid Model Integrating GCN and LSTM for Enhanced Intrusion Detection in UAV Controller Area Networks. Computer Networks 2025, 262, 111157. https://doi.org/10.1016/j.comnet.2025.111157.
88. Feuerriegel, S., Hartmann, J., Janiesch, C. and Zschech, P., 2024. Generative AI: S. Feuerriegel et al. Business & information systems engineering, 66(1), pp.111-126.
89. Asif, M.; Rahman, M. A.; Akkaya, K.; Shahriar, H.; Cuzzocrea, A. Adversarial Data-Augmented Resilient Intrusion Detection System for Unmanned Aerial Vehicles. In 2023 IEEE International Conference on Big Data (BigData); 2023; pp 5428–5437. https://doi.org/10.1109/BigData59044.2023.10386140.
90. El Alami, H.; Rawat, D. B. DroneDefGANt: A Generative AI-Based Approach for Detecting UAS Attacks and Faults. In ICC 2024 - IEEE International Conference on Communications; 2024; pp 1933–1938. https://doi.org/10.1109/ICC51166.2024.10622524.
91. Zhao, C.; Du, H.; Niyato, D.; Kang, J.; Xiong, Z.; Kim, D. I.; Shen, X.; Letaief, K. B. Enhancing Physical Layer Communication Security Through Generative AI with Mixture of Experts. IEEE Wireless Communications 2025, 32 (3), 176–184. https://doi.org/10.1109/MWC.001.2400150.
92. Panda, D. K.; Guo, W. Generative Adversarial Evasion and Out-of-Distribution Detection for UAV Cyber-Attacks. arXiv June 26, 2025. https://doi.org/10.48550/arXiv.2506.21142.
93. Sarikaya, B. S.; Bahtiyar, Ş. Generative Adversarial Networks for Synthetic Jamming Attacks on UAVs. In 2024 9th International Conference on Computer Science and Engineering (UBMK); 2024; pp 760–765. https://doi.org/10.1109/UBMK63289.2024.10773419.
94. Nagendra Kumar, D; Sundarakantham, K.D.; Dharani, J; Singh, K. Generative AI Based Blockchain Framework for Secure and Private Communication in Internet of Drones Systems. Social Science Research Network: Rochester, NY September 1, 2025. https://doi.org/10.2139/ssrn.5428949.
95. Zeng, Q.; Nait-Abdesselam, F. Leveraging Human-In-The-Loop Machine Learning and GAN-Synthesized Data for Intrusion Detection in Unmanned Aerial Vehicle Networks. In ICC 2024 - IEEE International Conference on Communications; 2024; pp 1557–1562. https://doi.org/10.1109/ICC51166.2024.10622433.
96. Gaber, T., Ali, T., Nicho, M. and Torky, M., 2025. Robust attacks detection model for internet of flying things based on generative adversarial network (gan) and adversarial training. IEEE Internet of Things Journal.