SNPSG Journal of Intelligent Unmanned Systems

2026, Vol. 1, No. 1, Article 112
DOI: https://doi.org/10.65218/jius.2026.112

REVIEW ARTICLE

Detection Techniques and Mitigation of Jamming Attacks in Unmanned Aerial Vehicles: A Review

Oluwadare Michael Ayegun[1]*, Brendan Chijioke Ubochi[1], Kayode Francis Akingbade[2], and Jide Julius Popoola[1]

1 Department of Electrical and Electronics Engineering, School of Electrical Systems Engineering, The Federal University of Technology Akure, Ondo State, Nigeria

2 Department of Information and Communication Technology, School of Electrical Systems Engineering, The Federal University of Technology Akure, Ondo State, Nigeria

* Corresponding author: Oluwadare Michael Ayegun
Email: oluwadaremichaela@futa.edu.ng

Received: 15 May 2026 | Accepted: 22 June 2026 | Published online: 8 July 2026

Abstract: The widespread adoption of Unmanned Aerial Vehicles (UAVs) has been driven by recent technological advancements, enabling their deployment in many diverse operations and missions previously considered infeasible in both military and civilian applications. UAVs communicate with ground stations through wireless systems, which are inherently vulnerable to Jamming Attacks (JAs) threats. This security threat poses a significant challenge as it can block legitimate control signals from reaching the UAV's receiver, potentially leading to a loss of control or even a crash. This paper presents an overview of Jamming Attack Detection (JAD) and mitigation schemes in UAV communication networks. The study reviews and analyzes approaches and results from 82 research papers published between 2008 and 2025 highlighting the state-of-the-art in JAD and mitigation strategies. Based on the identified shortcomings and emerging trends in UAV wireless communication security, the paper proposes key directions for future research.

Keywords: Unmanned Aerial Vehicle, Jamming Attack, Jamming Attack Detection, Jamming Attack Mitigation, Wireless Communication Networks

1. *Introduction*

Owing to their low setup and maintenance costs, wide coverage areas, and relative ease of deployment, Unmanned Aerial Vehicles (UAVs) have become widely popular for use in applications such as in agriculture, law enforcement, entertainment, and disaster management [1 - 2]. Additionally, UAVs have recently been deployed in wildlife conservation, pipeline inspection, surveillance, and in search-and-rescue operations [3 - 9]. According to the Federal Aviation Administration (FAA), the UAV industry is expected to generate more than 82 billion USD in revenue and create over 100,000 new jobs over the next decade, in the United States alone [10]. Furthermore, by 2030, annual global spending on UAVs is projected to approach 102.4 billion USD, representing a Compound Annual Growth Rate (CAGR) of 19.6%, up from 19.7 billion USD in 2020 [11]. The growing global demand for UAVs is expected to continue, especially with their integration into wireless communication systems such as fifth-generation (5G) cellular networks [12]. Although UAVs were originally developed for military purposes, they are now extensively used for an almost limitless range of civilian applications [13].

Military organizations worldwide are increasingly relying on UAVs as a primary means of collecting intelligence, conducting surveillance and reconnaissance missions, and engaging in armed combat operations [13]. Compared with manned aircraft, UAVs offer several advantages for military missions, including lower procurement costs, ease of operation requiring minimal technical skills or training, the ability to sustain long-duration missions without being constrained by the endurance of human aircrews, and the elimination of personnel risk from injury, capture, or death [14, 15]. The major areas of application of UAVs are illustrated in Figure 1.

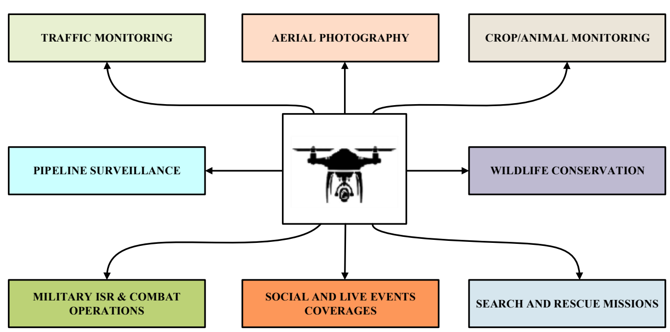

Fig. 1 Major Areas of Application of UAVs

Since UAVs rely on wireless communication systems for remote control operations between the UAV and a ground operator via dedicated Radio Frequency (RF) bands, typically operating at 2.4 GHz and 5.8 GHz [16], they are vulnerable to security threats and data exploitation if there are no measures to adequately secure the communication links. Because UAV control is mediated through the RF channel, an attacker could disrupt operations by jamming the network, transmitting malicious noise signals in order to cause a Denial-of-Service (DoS) condition [17 - 18]. Numerous studies have proposed various Jamming Attack Countermeasure (JAC) schemes to address this challenge [19 - 25]. These schemes range from channel hopping technique, that involves a rapid switching of communication channels, to the more complex game theory-based technique that deploys players (attacker and defender) and reward approach to mitigate attacks. This paper reviews some of the important research findings over the last two

DOI: https://doi.org/10.65218/jius.2026.112

decades, explores the current solutions to the detection and mitigation of jamming signals, identifies existing research gaps, and proposes feasible solutions to the identified gaps. In the remaining part of the paper, Section 2 discusses the UAV's basic wireless communication links and explains jamming techniques and their effects on UAV networks. Section 3 reviews existing Jamming Attack Detection (JAD) methods and JAC schemes. Section 4 outlines key future research directions, and Section 5 presents the study's conclusion

2. *UAV Wireless Communication Links*

The UAV's wireless communication networks offer unparalleled flexibility and convenience but come with challenges related to reliability, security, and performance. The security and reliability of UAV wireless communication links are vital for efficient and safe flight operations [26]. These wireless links are responsible for transmitting RF signals (command, control, telemetry, navigation, and payload signals) between the Ground Control Station (GCS) and the UAV system. The main types of wireless links typically used during UAV operations are: Command and Control (C2) link, telemetry link, payload data or video link, Satellite Communication (SATCOM) link, RF link and cellular network link. The C2 link transmits control and commands signals from the GCS to the UAV and receives flight status from the UAV remotely. The telemetry link sends real-time data about the UAV's flight parameters and system status (e.g., altitude, distance, battery level, flight time) back to the GCS. Payload data link transmits data collected by the UAV's sensors and payloads (e.g., cameras, thermal sensors) to the GCS for further processing and necessary actions depending on potential areas of application. The video link transmits live video feeds from onboard cameras to the GCS for real-time monitoring. The SATCOM link provides the UAV's long-range communication capabilities beyond the line of sight. The RF link provides short to medium-range communication for C2, telemetry, and video. The cellular network link utilizes existing 4G/5G cellular networks to provide UAV's communication links [27]. Despite the importance of these wireless communication links in UAV operations, they are vulnerable to the threats of JA. Figure 2 presents the illustration of UAVs wireless communication links.

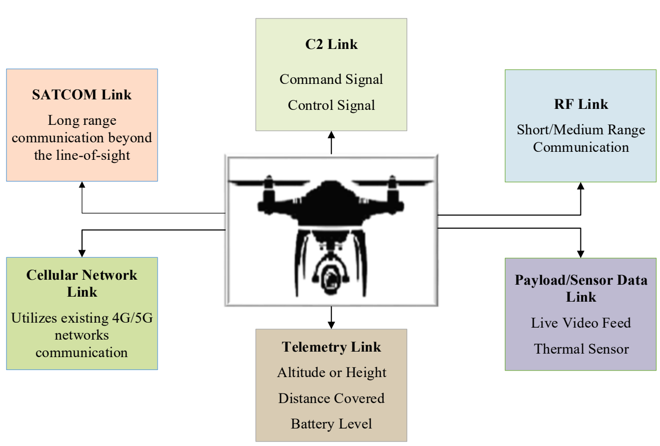

Fig. 2 The Illustration of UAVs Wireless Communication Links

2.1 *Intelligent Jamming Techniques Against UAV Communication Links*

Jamming of wireless communication channels remains one of the most widely employed strategies to disrupt UAV operations across both military and civilian applications [28]. The earlier jamming methods, which depended on accurate signal recognition, parameter extraction, and synthetic generation of jamming signals, faced several obstacles. These obstacles include the difficulty of reliably identifying UAV control signals and the complexity involved in designing and transmitting effective jamming waveforms. To overcome these shortcomings, recent research has shifted toward intelligent jamming approaches supported by advanced signal processing. Such techniques are capable of providing continuous performance evaluation and adaptive feedback, enabling them to respond effectively to the dynamic conditions of UAV communication environments [28].

The growth of modern computational power and the development of Machine Learning (ML) technologies has further accelerated this progress [29 - 32]. In particular, AI-driven methods are now able to autonomously select the most suitable jamming strategy by analyzing available options within waveform libraries. Recent advances also highlight the use of Convolutional Autoencoders (CAEs) [33 - 35], which can generate jamming signals without needing detailed prior knowledge of the target communication link. This capability improves flexibility and effectiveness of jamming signals in hostile environments. Furthermore, combining CAEs with deep residual network modules has been shown to enhance the robustness of jamming signal generation, especially in highly complex and adaptive communication scenarios [28]. Figure 3 presents the system model for generating jamming signal waveforms using the complex convolutional autoencoder.

Another notable threat to the operation of UAVs is the Global Positioning System (GPS) or Global Navigation Satellite System (GNSS) jamming and spoofing attacks. Modern autonomous systems and devices, including the UAV system, rely on GPS/GNSS for positioning, navigation and timing operations. This dependency makes the UAVs susceptible to GPS spoofing and JAs [36]. In order to validate this assertion, the authors in [37] evaluated the vulnerabilities of UAVs to GPS jamming and spoofing attacks. The evaluation was conducted for 2 commercial UAVs: Osman X28 and CSJ S167. The results obtained showed that UAVs are susceptible to GPS jamming and spoofing even at relatively low power levels of interference. Similarly, the study in [38] examined the diverse jamming and spoofing scenarios, evaluating their impacts on the precision and stability of UAV navigation. The results indicate that UAVs experience significant operational interruptions even when subjected to high magnitude pulse waveform jamming and spoofing signals, resulting in loss of location, trajectory errors, and reduced autonomy.

Generally, Jamming Techniques (JTs) in wireless networks can be divided into two broad classes: continuous jammers and intermittent jammers [39]. Continuous jammers emit a persistent, high-power signal or noise on the same channel as

DOI: https://doi.org/10.65218/jius.2026.112

the legitimate communication, thereby overwhelming and degrading all transmissions within that band [40]. Variants of continuous jammers include narrowband, broadband, barrage, single-tone, multi-tone, and frequency-sweeping designs. Intermittent jammers, in contrast, do not transmit continuously but instead disrupt communication links at specific intervals. By alternating between active jamming and silent phases, they are able to conserve energy and reduce the chance of being detected [41]. Common examples of this type include pulse jammers, reactive jammers, and random jammers. Figure 4 illustrates the broad classification of JTs.

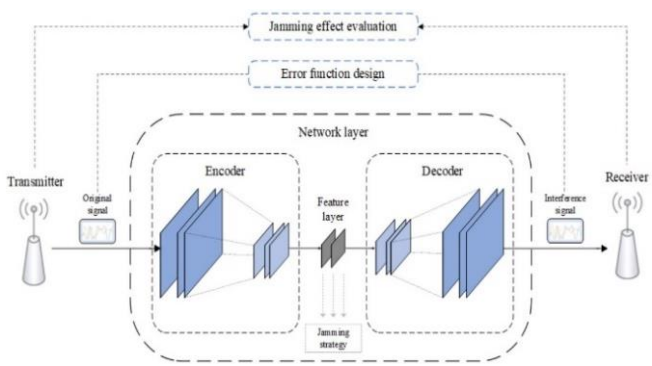

Fig. 3 The Model for Jamming Signal Waveforms Generation by H. Xue *et al.*, 2025 [28]

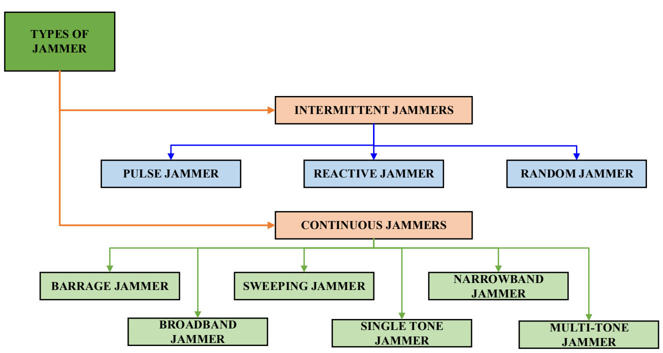

Fig. 4 The Broad Categorization of JTs

2.3 *Effects of Jamming Attacks on UAV Wireless Operations*

The Jamming Attacks (JAs) in UAV's communication network involve deliberately interfering with the radio signals used for wireless communication between the remote GCS and the UAV by the adversary's jammer. By consistently interfering with the communication, an attacker can cause a DoS problem, thus preventing the UAV from receiving commands or sending data, resulting in adverse outcomes such as loss of control, data loss, mission failure, or even a crash [26]. The effects of JAs on UAV wireless networks are summarized under security risk, network reliability, and performance measures and discussed as follows:

a. Security Risk: JA threats introduce profound security risks in UAV's wireless communication networks by undermining the basic functionality of signal transmission and reception. The most immediate risk is signal interference, where adversarial RF signals overlap with legitimate signals, causing distortion and preventing successful demodulation at the receiver. This compromises the confidentiality and integrity of the UAV communication since corrupted signals can result in false data interpretation and hinder secure operations [7]. In addition, JA signals often induce congestion by overwhelming the communication channel with continuous or periodic jamming signals, thereby preventing legitimate users from competing for channel access. This DoS condition disrupts the availability of wireless services, particularly in dense environments where spectrum demand is high [18]. Another serious security risk is signal masking, where a jammer deliberately mimics background noise or overlays malicious transmissions in such a way that legitimate RF signals become indistinguishable from interference. This makes it difficult for UAV receivers to recognize the presence of legitimate communication, thereby providing cover for adversarial actions such as unauthorized access or JAs [9]. Furthermore, the process of JAD itself remains a significant challenge in UAV communication. Advanced JA signals or techniques can emulate environmental noise or apply low-power intermittent emissions, thereby evading conventional intrusion detection systems that rely on energy thresholds or signal anomaly detection [45]. This stealthy nature complicates real-time detection and mitigation, ultimately leaving UAV wireless networks vulnerable to persistent and sophisticated threats.

b. Network Reliability: The reliability of wireless communication networks is highly sensitive to disruptions introduced by JA signals. One of the primary impacts is latency, which increases substantially as communication nodes are forced to perform repeated retransmissions due to corrupted frames and failed acknowledgments. In latency-critical applications such as in UAV operations, vehicular communication systems, and industrial automation, excessive delay can lead to mission failure, loss of synchronization, or even safety hazards [47]. Channel saturation is another key effect, occurring when adversaries deliberately occupy a communication channel with continuous or high-duty-cycle jamming signals. In such scenarios, legitimate users are unable to access the spectrum, resulting in extended queuing delays, inefficient medium utilization, and compromised service quality [26]. This saturation is particularly detrimental in multi-user wireless networks, where fairness and coordinated access mechanisms depend on the availability of idle channels. Additionally, bandwidth degradation arises when a portion of the usable spectrum is rendered inaccessible due to interference from jamming signals. This reduces the effective channel capacity available for legitimate communication, forcing devices such as UAVs to operate under constrained conditions or to switch to less efficient frequency bands [59]. Such limitations not only degrade throughput but also destabilize the continuity of wireless services, leading to unreliable communication performance.

c. Performance Measures: The performance of UAV wireless communication systems deteriorates drastically under the influence of JA signals. A direct consequence is the escalation of the BER, as jamming signals corrupt the modulation process and disrupt synchronization between GCS (transmitters) and UAV (receivers). Higher BER results in frequent frame retransmissions, consuming additional bandwidth and power

DOI: https://doi.org/10.65218/jius.2026.112

resources [56]. This inefficiency is compounded by packet loss, where legitimate data packets fail to reach their intended destinations due to collisions or overwhelming interference. For delay-sensitive applications such as UAV operations, packet loss leads to degraded service quality, communication breakdowns, and operational instability. The reduction in throughput is another critical effect of JAs. Since more bandwidth is consumed by corrupted transmissions and retransmission attempts, the overall data delivery rate declines sharply under jamming. This reduction is particularly damaging in scenarios requiring high data rates, such as multimedia streaming, UAV surveillance, or real-time sensor networks. Furthermore, JA directly threatens network connectivity, as persistent attacks can cause link disruptions, isolate network nodes, or partition communication clusters into disconnected fragments. This not only reduces system availability but may also lead to complete network collapse in mission-critical operations. The cumulative impact of increased BER, packet loss, reduced throughput, and degraded connectivity underscore the vulnerability of UAV wireless systems to performance inefficiencies induced by JA signals [75]. The summary of JTs and their effects on UAVs wireless communication networks are presented in Table 1.

3. *Related Studies on JAD and JAC Strategies in UAV Wireless Network*

Achieving a secure UAV communication against JAs usually requires a two-step process: detection and mitigation. The following sections present a comprehensive review of existing studies on JA detection and the proposed mitigation strategies, highlighting the major research contributions and limitations.

3.1 *JAD Strategies*

In order to mitigate JAs in UAV's wireless networks, several JAD approaches have been suggested [26, 27, 41 - 50]. The majority of the reviewed studies on JAD can be broadly classified into: (i) analytical detection techniques, (ii) ML detection techniques, and (iii) hybrid detection techniques.

a. Analytical Detection Techniques: These techniques involve the monitoring of communication performance metrics such as Signal-to-Noise Ratio (SNR), Received Signal Strength (RSS), Packet Send Ratio (PSR), and Packet Delivery Ratio (PDR) among others, to detect JA signals. For instance, the study in [41] deployed a JAD scheme that leverages network parameters along with additional metrics to distinguish between unintentional interference and JAs, thereby reducing false-positive alarms. Evaluation results demonstrated high accuracy due to an adjustable threshold value. However, the method's performance against sophisticated JAs was not assessed. Similarly, the authors in [42] developed an RSS Index-based Transmission Power Control (RSSITPC) algorithm to classify JAs and legitimate wireless signals based on the voltage levels in received signals. Their results indicated an improved detection accuracy and effectiveness, outperforming other widely used strategies in comparative performance analysis. The approach was not evaluated under scenarios involving multiple or deceptive attackers. Furthermore, the authors in [43] examined the negative influence of JAs on Wi-Fi networks and proposed an instantaneous detection solution capable of monitoring multiple channels simultaneously. Network parameters such as PDR, RSSI, throughput, and latency were tracked. JAs were found to degrade these parameters significantly, corrupting delivered packets and elongated delay times. As a result of these identified anomalies, the proposed JAD method achieved high performance accuracy even against intelligent jammers, while maintaining minimal computational and storage requirements. Although the approach is suitable for deployment on mobile wireless devices such as UAV, the impact of weather conditions or other environmental interference on detection performance was not evaluated.

b. ML Detection Techniques: Using signal quality parameters, a number of studies have demonstrated improved JAD performance by relying on the advanced computational strength of ML and AI technologies. For example, the authors in [44] investigated ML-based JAD using both measured and simulated Radio Signal Strength Information (RSSI) data. The reported results show that when using RSSI alone, the JAD detection accuracy was 98.6% and 89.7% for simulated data and real-world network data, respectively. Also, the multi-path profile information approach for JAD was also evaluated. By including more features in the JAD, the accuracy was improved significantly over the RSSI-based detection. The latter strategy achieved 99.01% accuracy on simulated data with no overhead or communication cost; however, the real-world performance was not assessed. Also, the author in [45] combined ML and time series data for a practical anomaly detection system onboard a UAV to detect unintentional interference, spoofing and JA signals. While the proposed two-level algorithmic approach accurately confirmed the presence of anomaly as either JA or spoofing attack, its practical implementation is hampered by the complexity of the design and the difficulty of deployment. The authors in [46] proposed a ML approach to detect and categorize 4 types of JAs in UAVs communication networks. The B210 Software Defined Radio (SDR) was used to implement each JA type and deployed against Orthogonal Frequency Division Multiplexing (OFDM) used in UAV communication network. The performance evaluation result showed 92.2% confidence in JAs detection and classification. However, sophisticated jammer types such as reactive and deceptive jammers were not considered. The difficulty in addressing the problem of reactive and deceptive jammers is due to the complexity and impracticability of implementation since UAVs are constrained in terms of onboard power, weight, and size. In [26], a lightweight ML approach (LightGBM) was deployed on UAV networks to detect JA signals. The results of the performance evaluation show that although the LightGBM approach uses about half the memory size and is 21 times faster during the prediction than Random Forest and Gradient Boost, it attained a JAD accuracy of 98.4% which is only slightly lower than both Random Forest and Gradient Boost with 98.8% and 99% accuracies, respectively. The authors in [47] proposed a relatively shallow 5-layer CNN-based JAD model for universal jamming signals detection in UAV wireless networks. The study deployed 5 different jammer types acting individually and then together in multiple combinations on legitimate UAV-controller communication signals in a simulation environment.

2026, Vol. 1, No. 1, Article 112
DOI: https://doi.org/10.65218/jius.2026.112

Table 1. Summary of JTs and Effects on UAVs Wireless Network

Effects of Jamming Attack /Jamming Technique	**Narrowband Jamming**	**Broadband Jamming**	**Barrage Jamming**	**Sweeping Jamming**	**Pulse Jamming**	**Single-Tone Jamming**	**Multi-Tone Jamming**	**Random Jamming**	**Reactive Jamming**	**Remark(s)**
Targeted Interference	✓					✓				
Localized Disruption	✓									
Increased Error Rates	✓	✓	✓		✓			✓	✓	
Selective Jamming	✓									
Frequency Congestion	✓									
Widespread Interference		✓								
Severe Connectivity Issues		✓	✓			✓				
Network Congestion		✓					✓			
Decreased Bandwidth		✓	✓							
Signal Interference			✓							
Security Risks			✓							
Intermittent Connectivity				✓						
Inconsistent Performance				✓						
Increased Latency				✓						
Packet Loss				✓						
Network Unreliability				✓						
Intermittent Disruptions					✓					
Variable Latency					✓					
Synchronization Issues					✓					
Reduced Throughput					✓			✓		
Signal Masking						✓				
Channel Saturation						✓				
Poor Network Efficiency						✓			✓	
Broader Disruption							✓			
Increased Complexity							✓			
Unpredictable Disruption								✓		
Broad Spectrum Impact								✓		
Detection Difficulty									✓	

The results of the performance evaluation demonstrated that the CNN-based model attained 98% JAD accuracy with a detection latency of 5 ms, which is superior to some selected pre-trained ML algorithms. In addition, the results from an ablation study show that the convolutional layer is the most relevant component of the JAD model as the performance degraded from the baseline value of 98% to 65.3%, when removed. Also, the results revealed that the model relies on signal-relevant features in order to make a detection decision. However, real-world performance of the JAD model was not assessed, but the model's reduced computational cost and fast detection time make it a potentially viable solution to the challenges of JA threats in UAV systems.

c. Hybrid Detection Techniques: The deployment of multiple JAD strategies known as ensemble, combined or hybrid techniques have been explored aiming to improve the detection accuracy. The authors in [48] presented an ensemble of ML and deep learning (DL) models (SVM-CNN) to detect JA signals in wireless network communication. While the results of experimental evaluation demonstrate the efficiency of the ensemble JAD model with 99.74% detection accuracy, the complexity and computational cost signified serious challenges. Similarly, the authors in [49] presented 2 combined strategies to detect JAs in UAV networks: time series and DL strategies. The time series-based approach for jamming signal detection employed the signal trend, seasonality, and residues, while the DL strategy used a computer vision scheme to detect anomaly in the networks. The combined method is appropriate and effective for UAVs since the model implementation does not need extensive computing resources. However, the time series approach struggles in its ability to detect all JA signal variants, while the DL network scheme achieves universal jamming signal detection but requires high resource overhead. The authors in [50] focused on ensemble ML techniques to detect JA signals in wireless communication networks. The effectiveness of Ensemble Learning and the XGBOOST-Ensemble Learning combination at jamming signals detection was determined from a comparison with existing JAD approaches. The study approach deployed a widely used jamming signal detection database: Wireless Sensor Network Dataset (WSN-DS). The obtained results demonstrate that the ensemble method, XGBOOST-Ensemble Learning, is superior in performance to other tested approaches. However, the detection technique was not implemented in real-time to assess a proactive and rapid detection of potential JA signals. Similar

DOI: https://doi.org/10.65218/jius.2026.112

bottle-necks were revealed by the authors in [27], where hybrid-distributed technique was deployed to trail and identify jammer attacks. The JAD method employed an observation approach that uses a single border node for 3D UAV JA localization scheme. The evaluation results show that the accuracy of the localization scheme was highest when compared with other conventional strategies, which makes it a preferred choice for JAD task. However, the challenges of high technical requirement and overhead cost pose threat to its potential real-world deployment.

3.2 *JAC Strategies*

An effective JAC strategy is essential for the protection of UAV's communication networks from JAs signals, particularly in military operations and other critical logistics and delivery services in civil applications [51 - 52]. Some of the earlier JACs techniques include: spread spectrum techniques, encryption, redundant communication channels, anti-jamming antennas, and autonomous operation [52]. The new JAC strategies involve both hardware and software solutions, which include: physical layer-based JAC, deception-based, backscatter-based, ML-based, game theory-based, and Intelligent Reflective Surfaces (IRS) techniques. These approaches are discussed as follows:

a. Physical Layer-Based JAC Techniques: The physical layer-based JAC techniques such as advanced spread spectrum, adaptive beamforming, channel hopping, and MIMO antenna system mitigate jamming signals by manipulating the characteristics/features of the desired signal during transmission and reception. These techniques improve communication resilience and spatial diversity to interference and JA effects [53 - 60]. For instance, the authors in [53] proposed an uncoordinated spread spectrum technique that enables jamming-resistant broadcast communication without shared secret keys between the transmitter and the receiver. Although uncoordinated spread spectrum can handle an unlimited amount of JA signals, the implementation is very expensive. In [54], the authors explored the optimization of Direct Sequence Spread Spectrum (DSSS) to mitigate JA and prevent severe signal degradation. The study examined how the DSSS employs strategies to improve signal quality in difficult channel conditions. However, the study was not extended to the highly sensitive communication channels of UAVs. The authors in [55] developed an intelligent transmitter that performs pulse-shaping to mitigate single tone JA signals in time-hopping spread spectrum systems. The results show that the proposed design performs better than other conventional waveforms but is unsuitable for mitigating sophisticated or multiple JA signals. Similarly, the study in [56] proposed an adaptive channel hopping algorithm for multi-radio communication to evade JAs using only one-hop neighbourhood coordination. Although the implementation cost is very high, the method achieved a significant communication throughput with low latency and reduced control overhead. The study in [57] proposed an evolvable hardware application in which an evolutionary algorithm is used to configure an adaptive beamformer to achieve 2 goals: steering nulls toward JA signals and directing gain toward the desired legitimate signals. Simulation results show that evolutionary algorithm is able to mitigate up to 3 simultaneous JA signals. Although the findings suggest a promising approach for enhancing wireless network security, real-world performance was not evaluated. In [58], the authors evaluated 3 beamforming algorithms: Least Mean Square (LMS), Optimized LMS, and Recursive Least Square (RLS) algorithms. The ability of these algorithms to form a beam in the direction of a desired signal and place a null in the direction of a JA signal was compared through simulation. The results indicated that the RLS algorithm performed best and is suitable for JAC strategy, although practical validation was not conducted. The study in [59] examined unimodular MIMO waveform design for JA mitigation. To reduce the impact of JA, the approach optimizes the MIMO waveform set to minimize the correlation and sidelobe energy between the desired and the JA signals. However, the complexity of the approach makes it undesirable for UAV applications. The authors in [60] proposed a minimum mean square error algorithm combined with Adaptive Side Lobe Cancellation (ASLC) and Frequency Diverse Array (FDA) MIMO to achieve a superior JAC strategy. Simulation results verified the effectiveness of FDA-MIMO, but without a practical assessment. To enhance the reliability of wireless communication systems under JA threats, the authors in [61] introduced a power-control algorithm based on Model Predictive Control (MPC) principles. The approach models the communication system as a linear control system, using the current Signal-to-Jamming-and-Noise-Ratio (SJNR) to predict future system states and transmission power over a defined horizon. Simulation results indicate that the MPC-based algorithm outperformed traditional adaptive power-control schemes, offering faster response times to JA variations and improved communication reliability. However, the study does not evaluate whether this response speed is adequate for UAV applications. The authors in [62] formulated an Interactive Reward Region (IRR) characterization problem in which a UAV and a jammer competitively adjust their transmit power and mobility to maximize individual rewards. Simulation results reveal that jointly optimizing the UAV's transmit power and trajectory optimization enlarges the IRR, while increased mobility and longer flight time further improve the UAV's reward. Nonetheless, the study lacks real-world or field validation.

b. Deception-Based JAC Techniques: Deception-based techniques are designed to confuse or mislead the jammer, making it difficult for the attacker to effectively disrupt the UAV's operations. This technique involves creating false signals or mimicking legitimate communications to mask the true signal. The authors in [19] approach the JA problem by intentionally modifying the legitimate information, making the network to create irregular ambiguity to mislead the adversary jammer and in this way, prevent network jamming. This strategy improves network security and robustness. However, it is not suitable for non-reactive jammers and cannot overcome sophisticated smart jammers. The study in [63] employed a deception technique that is based on renowned military tactics. The strategy was employed to mitigate reactive JAs operating with a very low power known for its hard-to-detect characteristic. The strategy effectively mitigates reactive JAs, but is however not suitable against non-reactive jammers.

DOI: https://doi.org/10.65218/jius.2026.112

Another deceptive approach used by the authors in [64] deceives the attacker into directing an attack towards a victim channel while simultaneously preserving the legitimate users' communications in another channel. The network attained improved throughput under reactive JAs signals. However, non-reactive jammer types were not assessed. Similarly, the authors in [20] worked on a smart hybrid deception and ambient backscatter communication-based technology. The study through deception, motivates the RF signal jammer to continuously attack a channel which contains fake transmissions. The approach leverages on jamming signals to transmit desired legitimate RF signals safely. The transmitter achieves an effective performance with a lower Bit Error Rate (BER) at high jamming signal power during channel attack. However, the approach cannot deal with multiple malicious attacks. The study in [65] introduced a dual-UAV strategy for securing wireless communication network. In this approach, a UAV sends confidential messages to a legitimate user while another cooperative UAV confuses the attacker by transmitting artificial noise signals. The deception-based technique deals successfully with reactive jammers and enhances the resilience of UAV communication systems by making it significantly more difficult for jammers to interfere with or hijack the UAVs. However, the proposed JA mitigation strategy is not suitable for lone UAV applications.

c. Backscatter-Based JAC Techniques: The backscatter-based techniques leverage on the concept of backscatter communication, where devices reflect existing signals rather than generate new ones. This approach helps UAVs maintain communication, even in the presence of jamming signals, by using passive or semi-passive methods. The study in [66] proposed using transmitter augmentation with an ambient backscatter tag for defeating intelligent and reactive JA signals with high power capability. Precisely, during a communication channel attack by the jammer signals, the transmitter attracts the jammer by deception to continue its data transmission. Consequently, the tag reflects or backscatters data signals based on both the jamming signals and legitimate signals from the jammer and transmitter, respectively, for the purpose of JAC. The performance evaluation results show significant improvement in the system BER and signal throughput. However, backscattering signals from multiple radio sources results in higher BER. Similarly, the authors in [67] introduced a novel idea for JAC in which a transmitter leverages the JA signals to transmit legitimate data when a jammer attacks the channel. The technique known as ambient backscatter technique uses energy harvested from the jamming signals during attacks to support the legitimate communication. In addition, a Reinforcement Learning (RL) algorithm was deployed, and this enabled the transmitter to obtain the optimal operation policy through real-time interaction processes with the attacker in order to effectively deal with the uncertainty posed by a jammer. The results show the effectiveness of the JAC technique in JA mitigation, attaining less packet loss and higher throughput under powerful JA signals. In another study, the authors in [68] deployed an intelligent ambient backscatter communication approach for energy efficiency improvement in a cognitive radio system during jamming signal attacks. The approach achieved efficient energy management. It was found that the efficiency reduces if a burst of packets is exchanged between pairs of nodes. Hence, backscatter-based techniques provide a stealthy and energy-efficient way to maintain communication in the presence of JAs, thus enhancing the robustness of UAV operations in contested environments.

d. ML-Based JAC Techniques: ML-based JAC strategies rely on advanced algorithms to mitigate JAs in wireless communication networks, particularly UAV networks. For example, the authors in [69] modelled the data transmission problem in a wireless network caused by JA using a Markov Decision Process (MDP). Subsequently, a modified Q-Learning (QL) algorithm was used to improve the transmitted signal's throughput and reduce the packet loss through the implementation of an appropriate mitigation strategy by the adequately trained transmitter. However, the strategy seemed to be inadequate under multiple JAs signals. Similarly, the authors in [70] investigated the JAC performance of a cognitive radar under a partially observable MDP model. The study utilized Deep Q-Network (DQN) and Long Short Term Memory (LSTM) networks under a range of SNR values to compute the optimal policy. Simulation results confirmed the potential and success of the strategies. The LSTM using Mellowmax operator provides strong and robust security system than other networks in simulations. However, a real-world performance evaluation was not conducted. In a similar manner, the study in [21] employed a ML-based JAC strategy for cognitive radio networks to resist aggressive jammers, where both JA signals and JAC approaches are derived using the game theory framework of Markov. The approach outperforms existing strategies used to mitigate JA signals over a wide range of communication scenarios, but was not assessed practically. Also, the authors in [71] proposed a cellular system relay scheme for UAV operation that is based on Deep RL (DRL) to improve smart JA signals mitigation. To achieve effective network protection, this scheme does not require a prior information of the jammer and the communication network models. Instead, it relies on the observed current status of the wireless network and the previous JAC relay experiences. The strategy achieved improved BER and reduced energy consumption for the cellular system compared to the existing scheme. However, it is ineffective whenever the UAV is far from network attack position. By leveraging on ML-based countermeasures, UAVs can maintain reliable communication and navigation, thus ensuring mission success even when attacked by sophisticated jammers.

e. Game Theory-Based JAC Techniques: The game theory-based JAC in UAV networks involve modeling the interface between the jammer (attacker) and the UAV (defender) as a competitive game. This approach helps in understanding and predicting the behaviour of both parties and devising optimal strategies to counteract and minimize the impact of JA signals. In this scheme, the UAV and the jammer are modelled as rational players with conflicting objectives: the UAV aims to maintain a reliable communication while the jammer seeks to disrupt it. The scheme employs various types of game models in achieving its countermeasure strategy. For instance, in [72] a game theory by Markov was proposed to model and investigate the JAC approach, and a collaborative algorithm based on

DOI: https://doi.org/10.65218/jius.2026.112

multi-agent jamming countermeasure was used to attain enhanced JAC strategy. The approach is superior to independent QL method in terms of countermeasure performance. However, the method's drawbacks are increased cost and longer mitigation time. Also, from the perspective of a game, the authors in [73] proposed a multi-user power control problem in a relay-assisted JAC using the Bayesian 3-layer Stackelberg game in which legitimate users, relay users and the jammer act as leaders, vice-leaders, and follower, respectively, to resist JAs in a wireless network. The approach attained effective JAC, but it was found that erroneous allocation of roles/levels could jeopardize performance. In [74], a stochastic game framework was used to design and investigate the multi-user counter-jamming problem in order to obtain an ideal jamming countermeasure using the proposed joint multi-agent JAC algorithm. The method achieved higher average PDR than the tested ML-based and the frequency-hopping methods. However, it is not cost effective as it requires multiple agents for improved efficiency. Also, the study in [22] deployed a game theory-based JAC scheme to identify the best communication channel for jamming-resistant transmission in a cognitive radio network using concepts such as defining states, actions, and players' rewards. The scheme provides an optimal channel for the secondary user to avoid JA signals and improve the security level of the network. Based on the simulation results, the scheme's efficiency in improving the long-term performance of the network was demonstrated. However, the scheme is not suitable for multiple secondary users as it would require larger state and action spaces. Game-theoretic learning JAC pattern strategy was introduced by the authors in [75] using Stackelberg, Markov and hyper graph-based JAC game models. Although, this approach demonstrated a very good performance, it is hard to implement due to compatibility challenges arising from using two different game techniques. Game theory-based strategies are promising and can allow UAVs to systematically analyze and counteract JAs, thus enhancing resilience and reliability of UAVs even in contested environments.

f. Intelligent Reflective Surfaces (IRS) JAC Techniques: An IRS technique is an emerging technology used to optimize wireless communication performance. It is a smart wireless technology that helps to resist interference caused by JA signals by intelligently controlling how signals are reflected or redirected through its surface reflecting elements [76 - 78]. The authors in [76] used an IRS to prevent JA interference by adjusting the surface reflecting elements at the IRS. Also, the power allocation at the receiver base station and reflecting beam-forming at the IRS was formulated as a joint-optimization problem while ensuring that legitimate users have good quality of service. Performance evaluation results show that the technique effectively improves both the transmission protection level and the IRS-assisted JAC system rate compared with existing solutions. However, the performance of the model under low-powered jammers and other traditional JA techniques was not evaluated. Similarly, the authors in [77] investigated UAV communication networks, where an IRS is employed to help in the signal transmission between a Ground Node (GN) and the UAV receiver during JA signals interference. The average rate of the UAV communication was maximized by jointly optimizing the IRS's passive beam-forming, the UAV's trajectory, and the GN's transmit power. Moreover, some challenges encountered were overcome using an alternating optimization-based algorithm which employs the Successive Convex Approximation (SCA) and Semi-Definite Relaxation (SDR) techniques. The results show that although the performance depends on the location of the IRS, the strategy improved the average rate of UAV communication significantly compared to the baseline strategies. The authors in [78] proposed an Aerial Reconfigurable Intelligent Surface (ARIS) for JAC in wireless communications. The ARIS could be flexibly deployed in the air in order to mitigate JA signals and enhance effective legitimate communications. In the study, the location of ARIS is obtained by successive convex approximation and the reflection beamformer is tackled with manifold optimization. Evaluation results confirmed its effectiveness in mitigating JA through an optimized deployment and reflection of the ARIS. The evaluation results reveal that by increasing the number of reflecting elements and with proper deployment, the ARIS can effectively compensate for unfavourable transmission scenarios and improve the system's performance. However, the performance of the strategy using low or wrongly placed reflecting elements were not assessed.

3.3 *Criteria for JAD/JAC Techniques Performance Comparison*

The growing diversity of UAV platforms and the sophistication of modern JA strategies highlight the urgent need for standardized comparison criteria to evaluate the effectiveness of JAD and JAC techniques. Such criteria include detection accuracy and false alarm rate, which ensure reliable identification of JAs without misclassifying background noise as JA; latency and Real-Time Responsiveness (RTR), which are critical for time-sensitive UAV control loops; and robustness to different JA variants, since systems must perform consistently under barrage, reactive, deceptive, or broadband jamming scenarios. In addition, throughput and PDR serve as key indicators of how well communication performance is sustained during jammer attacks, while computational overhead is a vital consideration for UAVs with limited onboard resources and flight endurance. Finally, scalability and generalizability determine whether the proposed solutions can be applied across different UAV platforms, mission types, and operational environments without extensive reconfiguration. By embedding these evaluation benchmarks into this review study, a fair, transparent, and reproducible basis for comparing existing JAD and JAC approaches is achieved. The summary of JAD/JAC techniques average performance analysis is presented in Table 2.

Table 2. Comparison of Average Performance Analysis of JAD/JAC Techniques

JAD/JAC Technique	Detection Accuracy	False Alarm Rate	Latency/ RTR	Robustness to JA Variants	Throughput/ PDR	Computational Overhead	Scalability/ Generalization
Analytical JAD	*Medium*	*High*	*Low*	*Low-Medium*	*Medium*	*High*	*Low*
ML-Based JAD	*Very High*	*Low*	*Very Low*	*High*	*High*	*Medium-Low*	*Medium-High*
Hybrid JAD	*High*	*Low*	*High*	*Very High*	*High*	*Low*	*High*
Deception-Based JAC	*N/A*	*N/A*	*Medium*	*Medium*	*Medium*	*Medium*	*Medium*
Backscatter-Based JAC	*N/A*	*N/A*	*Medium*	*Medium*	*Medium-High*	*High*	*Low*
ML-Based JAC	*N/A*	*N/A*	*Very High*	*Very High*	*High*	*Medium-Low*	*High*
Game Theory-Based JAC	*N/A*	*N/A*	*Medium*	*Medium-High*	*Medium-High*	*Medium*	*High*
IRS-Based JAC	*N/A*	*N/A*	*Medium*	*Medium High*	*High*	*Medium-High*	*Medium*
Physical Layer-Based JAC	*N/A*	*N/A*	*High*	*High*	*High*	*High*	*High*

4. *Future Research Directions*

The development of effective JAD and JAC strategies is important for a secure and reliable operation of UAVs. As UAVs become more ubiquitous across different sectors, the need for a robust JA mitigation solution will continue to grow. The challenge of implementing effective JAD and JAC schemes for efficient UAV's communication is greater compared to executing a JA [79]. Hence, ongoing studies in this field are vital not only for enhancing UAV capabilities but also for ensuring that these systems can operate safely in increasingly contested and complex electromagnetic environments. Some of the explored solutions will require advanced signal processing techniques, ML, multi-antenna systems, cooperative strategies and hardware-based solutions. The future research areas will focus on developing universal lightweight and energy-efficient JAD/JAC that can be easily integrated into existing UAV platforms for the next generation of jamming-resilient UAVs. Figure 5 illustrates the future research directions and the details are contained in subsections 4.1 - 4.5.

4.1 *Datasets Generation*

The unavailability of reliable dataset for effective JAD and countermeasure design undermines research effort, particularly, in the UAV wireless communication network. As a result of dataset scarcity, most of the existing research studies on UAV's JA mitigation approach have focused on specific jammer types. Consequently, this deficiency leads to limitations in the JAC models as some of the approaches remained untested or struggle under unfamiliar single or multiple JA signal types. Hence, future studies could explore other means of generating reliable dataset such as MATLAB and Software Defined Radio (SDR) platforms for modeling and development of efficient JAD and mitigation models [80].

4.2 *Universal and Sophisticated JAD Technique*

The increasing advancement in technology has enabled the production of low-cost and effective network jamming devices [81]. This necessitates the development of efficient, universal and sophisticated UAV's network JAD techniques that will be capable of differentiating between legitimate signals and all types of intentional JA signals. Also, an efficient JAD algorithm should be able to identify and discriminate between temporary network interruption/interference and actual JA signals. This capability is currently absent in the current studies. Future research works need to anticipate and counteract increasingly sophisticated JA strategies.

4.3 *Universal JAC Technique*

The review and analysis of existing wireless network JAC strategies indicate that there is currently no single countermeasure technique that can effectively deal with multiple types of JAs acting alone or together. The existing techniques are strategically employed to deal with a certain type of network jammers. For instance, the authors in [82] focused on reactive jammers and as a result, the developed system is not

DOI: https://doi.org/10.65218/jius.2026.112

effective in dealing with other sophisticated jammers. Hence, a single practical JAC solution can be developed to mitigate all forms of JAs.

4.4 *Real-Time JAC Implementation Technique*

The power resource constraint in the UAV operations is a major challenge, primarily due to the limited onboard battery capacity as well as the high energy demands of various UAV's components (propulsion motors, communication systems, attached sensors and onboard processing units). The power constraints affect the UAV's flight time, range, sensor capability and overall mission performance. In addition to these already established UAV's power-driven components, many existing UAV's JAC techniques require significant processing power, making real-time implementation difficult in resource-constrained UAVs. Hence, future studies on JAC strategy for UAV's wireless network should provide very low processing power for fast-detection and reaction mechanisms that will be capable of detecting and localizing the jammer in real time. Consequently, the future implementation of real-time JAC approach should address power resource constraints that is essential for improving the overall endurance, reliability and versatility of UAVs. This is particularly important in applications requiring extended flight duration, while protecting the UAVs in challenging network environments.

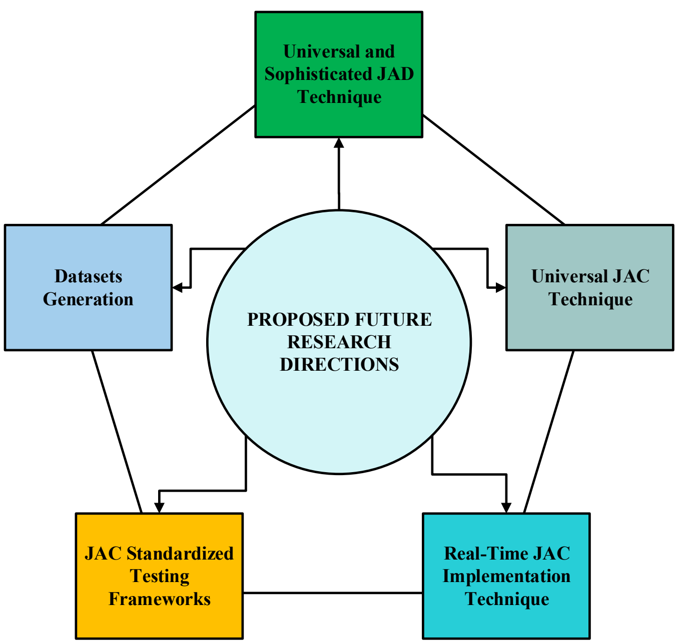

Fig. 5 The Proposed Future Research Directions in UAV's JAD and JAC Schemes

4.5 *JAC Standardized Testing Frameworks*

The challenge of evaluating the effectiveness of the already existing UAV's JAC strategies under various scenarios using standardized testing frameworks is attracting a growing interest. As UAVs become increasingly important across various domains, there is a multiplicity of approaches geared towards developing systems to protect UAVs against JA signals. As a result, there is a need to develop standardized testing frameworks to ensure improved JAC technologies in UAVs. The envisaged comprehensive testing frameworks should include the establishment of benchmarks as performance baseline metrics. The test should replicate real-world conditions, including urban, rural, and military battlefield environments, where different types of JAs might occur. This will ensure that countermeasures are effective across various operational contexts. The performance of different JAC strategies can therefore be determined by comparison against the established benchmarks in order to determine the most effective JAC solutions.

5. *Conclusion*

UAV wireless communication links, which are indispensable for effective operational control, remain highly vulnerable to network JAs security threats. These attacks can lead to DoS conditions with severe consequences such as UAV crashes, loss of control, or even unauthorized takeover. This paper has provided a comprehensive survey of UAV applications, their associated vulnerabilities to JAs, the classification of various JTs, and the range of JAD and JAC strategies. Among the detection and mitigation approaches, ML-based techniques have emerged as the most promising solutions due to their adaptability, pattern recognition strength, and near-human decision-making capability. By incorporating benchmarking criteria such as detection accuracy, false alarm rate, latency, real-time responsiveness, robustness to JA variants, throughput or PDR, energy efficiency, and resource overhead, the study has objectively analyzed existing and emerging JAD/JAC techniques, and has identified trade-offs to guide the development of more effective solutions. Furthermore, this paper highlights the need for creating diverse UAV communication datasets, developing advanced and adaptive JAD methods, implementing real-time JAC mechanisms, establishing universal countermeasure frameworks, and defining standardized testing procedures for UAV anti-jamming systems. Addressing these gaps will be pivotal in ensuring secure, reliable, and resilient UAV operations in the presence of any kind of JA security threat.

References

[1] R. Giulio, C. M. Pinotti, D. D. Bhumika and S. K. Das, "Delivery with UAVs: A Simulated Dataset via ATS," *Proceedings 2022 IEEE 95th Vehicular Technology Conference, Helsinki, Finland*, pp. 1 - 6, 2022.

[2] Y. Li, J. Pawlak, J. Price, K. Al Shamaileh, Q. Niyaz, S. Paheding and V. Devabhaktuni, "Jamming Detection and Classification in OFDM-Based UAVs via Feature-and Spectrogram-Tailored Machine Learning," *IEEE Access*, Vol. 10, pp. 16859 - 16870, 2022.

[3] S. Y. Nam and G. P. Joshi, "Unmanned Aerial Vehicle Localization Using Distributed Sensors," *Int. J. Dist. Sensor Network*. Vol. 13, No. 9, pp. 1 - 8, 2017.

[4] Z. Kaleem and M. H. Rehmani, "Amateur Drone Monitoring: State-of-the-Art Architectures, Key Enabling

DOI: https://doi.org/10.65218/jius.2026.112

Technologies, and Future Research Directions," *IEEE Wireless Comm.*, Vol. 25, No. 2, pp. 150 - 159, 2018.

[5] M. Z. Anwar, Z. Kaleem, A. Jamalipour, "Machine Learning Inspired Sound-Based Amateur Drone Detection for Public Safety Applications," *IEEE Trans. Vehicle. Technology*, Vol. 68, No. 3, pp. 2526 - 2534, 2019.

[6] H. Kim, L. Mokdad and J. Ben-Othman, "Designing UAV Surveillance Frameworks for Smart City and Extensive Ocean with Differential Perspectives," *IEEE Communication. Magazine*, Vol. 56, No. 4, pp. 98 - 104, 2019.

[7] S. A. Aly, P. Keith, M. Vuk and G. Giovanni, "UAV-Assisted Attack Prevention, Detection, and Recovery of 5G Networks," *IEEE Wireless Communication*, Vol. 27, Issue 4, pp. 40 - 47, 2020.

[8] H. Huang and A. V. Savkin, "An Algorithm of Reactive Collision Free 3-D Deployment of Networked Unmanned Aerial Vehicles for Surveillance and Monitoring," *IEEE Trans Ind. Information*, Vol. 16, No. 1, pp. 132 - 140, 2020.

[9] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models," *IEEE Access*, Vol. 9, pp. 93803 - 93815, 2021.

[10] Q. Wu, W. Mei and R. Zhang, "Safeguarding Wireless Network with UAVs: A Physical Layer Security Perspective," *IEEE Wireless Communication*, Vol. 26, No. 5, pp. 12 - 18, 2019.

[11] S. Hafeez, A. R. Khan, and M. M. Al-Quran, "Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey," *IEEE Open Journal of Vehicular Technology*, Vol. 4, pp. 558 - 580, 2023.

[12] O. M. Ayegun, K. F. Akingbade, J. J. Popoola and B. C. Ubochi, "Investigating a Transparent and Interpretable Deep Learning Model for Enhanced Jamming Attack Detection in UAV Communication Networks," *FUTA Journal of Engineering and Engineering Technology*, Vol. 19, No. 1, pp. 215 - 225, 2025.

[13] C. A. Kozera, "Military Use of Unmanned Aerial Vehicles - A Historical Study," *Scientific and Technical Journal - Safety & Defense*, Vol. 4, No. 1, pp. 17 - 21, 2018.

[14] C. W. Commander, P. M. Pardalos, V. Ryabchenko, O. V. Shylo, S. Uryasev and G. Zrazhevsky, "Jamming Communication Networks under Complete Uncertainty," *Optimization Letters*, Vol. 2, No. 1, pp. 53 - 70, 2008.

[15] C. Gencer, E. K. Aydogan and C. Celik, "A Decision Support System for Locating VHF/UHF Radio Jammer Systems on the Terrain," *Journal of Information Systems Frontiers*, Vol. 10, No. 1, pp. 111 - 124, 2008.

[16] J. Yousaf, H. Zia, M. Alhalabi, M. Yaghi, T. Basmaji, E. Al Shehhi, G. A. Alkhedher and M. Ghazal, "Drone and Controller Detection and Localization: Trends and Challenges," *Journal of Applied Science*s, Vol. 12, Issue No. 24, p. 12612, 2022.

[17] M. Juhlin and A. Jakobsson, "Localization of Multiple Jammers in Wireless Sensor Network," *Proceedings of the 29th European Signal Processing Conference (EUSIPCO), Dublin, Ireland,* pp. 1596 - 1600, 2021.

[18] K. B. Adedeji, A. M. Abu-Mahfouz and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept Research, Perspective and Challenges, networks," *Sensors and Actuator Networks*, Vol. 12, No. 4, pp. 1 - 57, 2023.

[19] D. Kemi, R. Xiaoqiang, E. Q. Daniel, D. Subhrakanti and S. Ling, "Defensive Deception against Reactive Jamming Attacks in Remote State Estimation," *Journal of Automatica*, Vol. 113, pp. 1 - 11, 2020.

[20] V. H. Nguyen, N. N. Diep, T. H. Dinh, X. V. Thang, D. Eryk and C. Symeon, "Defeating Super-Reactive Jammers with Deception Strategy: Modeling, Signal Detection, and Performance Analysis," *IEEE Transaction on Wireless Communication,* Vol. 21, No. 9, pp. 7374 - 7390, 2021.

[21] K. Ibrahim, S. X. Ng, I. M. Qureshi, A. N Malik and S. Muhaidat, "Anti-Jamming Game to Combat Intelligent Jamming for Cognitive Radio Networks," *IEEE Access*, Vol. 9, pp. 137941 - 137956, 2021.

[22] H. T. Thien, V. H. Vu and I. Koo, "A Transfer Games Actor-Critic Learning Framework for Anti-Jamming in Multi-Channel Cognitive Radio Networks," *IEEE Access*, Vol. 9, pp. 47887 - 47900, 2021.

[23] H. Yang, Z. Xiong, J. Zhao, D. Niyato and Q. Wu, "Intelligent Reflecting Surface Assisted Anti-Jamming Communications: A Fast Reinforcement Learning Approach," *IEEE Transaction on Wireless Communications*; Vol. 20, No 3, pp. 1963 - 1974, 2021.

[24] G. Alnifie and R. Simon, "MULEPRO: A Multi- Channel Response to Jamming Attacks in Wireless Sensor Networks," *Wireless Communications and Mobile Computin*g, Vol. 10, No. 5, pp. 704 - 721, 2010.

[25] V. Prisacariu, "The History and the Evolution of UAVs from the Beginning till the 70s," *Journal of Defense Resources Managemen*t, Vol. 8, Issue 1 (14), pp. 181 - 189, 2017.

[26] H. O. Slimane, S. Benouadah, T. T. Khoei and N. Kaabouch, "A Light Boosting-based ML Model for Detecting Deceptive Jamming Attacks on UAVs," *Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0328 - 0333, 2022.

DOI: https://doi.org/10.65218/jius.2026.112

[27] W. Aldosari, M. Moinuddin, A. J. Aljohani and U. M. Al-Saggaf, "Distributed Extended Kalman Filtering Based Techniques for 3-D UAV Jamming Localization," *Sensor*, Vol. 20, No. 22, p. 6405, 2020.

[28] H. Xue, Z. Zhuo, W. Yan, and Y. Zhang, "Research on UAV Jamming Signal Generation Based on Intelligent Jamming", *IEEE Access*, Vol. 13, pp. 14686 - 14701, 2025.

[29] J. Li, L. Yang, Q. Wu, X. Lei, F. Zhou, F. Shu, X. Mu, Y. Liu, and P. Fan, ''Active RIS-aided NOMA-Enabled Space-Air-Ground Integrated Networks with Cognitive Radio,'' *IEEE Journal on Selected Areas in Communication*, Vol. 43, No. 1, pp. 314 - 333, 2025.

[30] I. H. Sarker, ''Machine Learning: Algorithms, Real-World Applications and Research Directions,'' *Social Network Computer Science*, Vol. 2, No. 3, p. 160, 2021.

[31] L. Benos, A. C. Tagarakis, G. Dolias, R. Berruto, D. Kateris, and D. Bochtis, ''Machine Learning in Agriculture: A Comprehensive Updated Review,'' *Sensors*, Vol. 21, No. 11, p. 3758, 2021.

[32] R. Rai, M. K. Tiwari, D. Ivanov, and A. Dolgui, ''Machine Learning in Manufacturing and Industry 4.0 Applications,'' *International Journal on Production Research*, Vol. 59, No. 16, pp. 4773 - 4778, 2021.

[33] J. F. Hwaidi and T. M. Chen, ''Classification of Motor Imagery EEG Signals Based on Deep Autoencoder and Convolutional Neural Network Approach,'' *IEEE Access*, Vol. 10, pp. 48071 - 48081, 2022.

[34] J. Lai, X. Wang, and Q. Xiang, ''A Review of Autoencoders and their Applications,'' *J. Commun*., Vol. 42, No. 9, pp. 218 - 230, 2021.

[35] Y. Wang, L. Liu, and H. Xu, ''Noisy Gravity Data Reconstruction using Convolutional Autoencoder,'' *Geomatic and Information Science of Wuhan University*, Vol. 47, No. 4, pp. 543 - 550, 2022.

[36] A. S. Banu and G. Padmavathi, "Taxonomy of UAVs GPS Spoofing and Jamming Attack Detection", *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*, pp. 167 - 201, 2022.

[37] D. Sathyamoorthy, Z. Fitry, E. Selamat, S. Hassan, A. Firdaus and Z. Zaimy, "Evaluation of the Vulnerabilities of Unmanned Aerial Vehicles (UAVs) to Global Positioning System (GPS) Jamming and Spoofing", *Defence S and T Technical Bulletin*, Vol. 13, pp. 333 - 343, 2020.

[38] N. Z. B. Taufik, G. E. Mustafa, A. S. Hafeez and M. A. Zulkifley, "Simulation-Driven Analysis of GPS Jamming and Spoofing Effects on UAV Flight Stability", *2025 IEEE 15th International Conference on System Engineering and Technology (ICSET)*, pp. 429 - 433, 2025.

[39] S. R. Ratna and R. Ravi, "Survey on Jamming Wireless Networks: Attacks and Prevention Strategies," *World Academy of Science Engineering and Technology International Journal of Computer and Information Engineering*, Vol. 9, No. 2, pp. 1 - 7, 2015.

[40] A. Pourranjbar, G. Kaddoum and W. Saad, "Jamming Pattern Recognition over Multi-Channel Networks: A Deep Learning Approach," *Proceedings of the 55th Asilomar Conference on Signals, System, and Computers*, pp. 305 - 308, 2021.

[41] P. Mykytyn, M. Brzozowski, Z. Dyka and P. Langendoerfer, "Jamming Detection for IR-UWB Ranging Technology in Autonomous UAV Swarms," *Proceedings of the 10th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1 - 6, 2021.

[42] S. Sivaprakash, U. V. Anbazhagu, I. Perumal, V. V. Kumar, T. R. Mahesh and S. Guluwadi, "Analysis and Attack Detection in GSM Mobile Network with an Intelligent Jammer Using ANFIS Classifier," *IEEE Access*, Vol. 11, pp. 118962 - 118972, 2023.

[43] F. T. Zahra, Y. S. Bostanci and M. Soyturk, "Real-Time Jamming Detection in Wireless IoT Networks," *IEEE Access*, Vol. 11, pp. 70425 - 70442, 2023.

[44] B. Upadhyaya, S. Sun and B. Sikdar, "Machine Learning-Based Jamming Detection in Wireless IoT Networks." *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, pp. 1 - 5, 2019.

[45] F. Alrefaei, "Machine Learning for Intrusion Detection into Unmanned Aerial System 6G Networks," *Ph.D. dissertation, Dept. Elect. Eng & Comp. Sci., Embry-Riddle Aeronautical University*, 2024.

[46] J. Pawlak, Y. Li, J. Price, M. Wright, K. Al Shamaileh, Q. Niyaz and V. Devabhaktuni, "A Machine Learning Approach for Detecting and Classifying Jamming Attacks Against OFDM-based UAVs," *Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning*, pp. 1 - 6, 2021.

[47] O. M. Ayegun, K. F. Akingbade, J. J. Popoola and B. C. Ubochi, "Leveraging on Artificial Intelligence for Jamming Attacks Detection in Unmanned Aerial Vehicles Communications," *Computers and Electrical Engineering*, Vol. 127, Part B, pp. 1 - 15, 2025.

[48] A. Eshmawi, M. Umer, I. Ashraf and Y. Park, "Enhanced Machine Learning Ensemble Approach for Securing Small Unmanned Aerial Vehicles from GPS Spoofing Attacks", *IEEE Access*, Vol. 12, pp. 27344 - 27355, 2024.

DOI: https://doi.org/10.65218/jius.2026.112

[49] J. Viana, H. Farkhari, L. M. Campos, P. Sebastião, F. Cercas, L. Bernardo and R. Dinis, "Two methods for Jamming Identification in UAVs Networks using New Synthetic Dataset," *Proceedings of the 2022 IEEE 95th Vehicular Technology Conference: (VTC2022 - Spring)*, pp. 1 - 6, 2022.

[50] B. M. Kouassi, V. Monsan, A. B. Ballo, K. J. Ayikpa, D. Mamadou and K. J. Adou, "Application of the Learning Set for the Detection of Jamming Attacks in 5G Mobile Networks," *International Journal of Advanced Computer Science and Application*, Vol.14, No. 6, pp. 715 - 723, 2023.

[51] C. Gudla, M. S. Rana and A. H. Sung, "Defense Techniques Against Cyberattacks on Unmanned Aerial Vehicles," *Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS), The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)*, pp. 110 - 116, 2018.

[52] A. A. Laghari, A. K. Jumani, R.A. Laghari and H. Nawaz, "Unmanned aerial vehicles: A review," *Cognitive Robotics*, Vol. 3, pp. 8 - 22, 2023.

[53] C. Propper, M. Strasser and S. Capkun, "Anti-Jamming Broadcast Communication Using Uncoordinated Spread Spectrum Techniques," *IEEE Journal on Selected Areas in Communications*, Vol. 28 (5), pp. 703 - 715, 2010.

[54] R. Ali, M. Farooq and M. Basit, "Systemic Study of Anti-Jamming Strategies Using Direct Sequence Spread Spectrum," *Journal of Artificial Intelligence and Computing,* Vol. 3 (1), pp. 15 - 19, 2025.

[55] H. Jung, B. V. Nguyen, I. Song and K. Kim, "Design of Anti-Jamming Waveforms for Time-Hopping Spread Spectrum Systems in Tone Jamming Environments," *IEEE Transaction on Vehicular Technology*, Vol. 69 (1), pp. 728 - 737, 2020.

[56] Y. Chen and A. Arora, "QF-MAC: Adaptive, Local Channel Hopping for Interference Avoidance in Wireless Meshes," *Networking and Internet Architecture*, pp. 1 - 12, 2023.

[57] J. D. Lohn, J. M. Becker and D. S. Linden, "An Evolved Anti-Jamming Adaptive Beamforming Network," *Genetic Programming and Evaluable Machines,* Vol. 12 (3), pp. 217 - 234, 2011.

[58] S. A. Khan and S. A. Malik, "Adaptive Beamforming Algorithms for Anti-Jamming," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 4 (1), pp. 95 - 106, 2011.

[59] X. Fang, D. Zhao and L. Zhang, "Unimodular MIMO Waveform Design for Saturated Forwarded Jammer Suppression," *2023 IEEE International Radar Conference (RADAR)*, pp. 1 - 6, 2023.

[60] Y. Zhang, M. Tan and Z. Tan, "Anti-Jamming Performance Analysis of FDA-MIMO Based Sidelobe Cancellation with Minimum Mean Square Error Algorithm," *2023 8th International Conference on Intelligent Computing and Signal Processing (ICSP)*, pp. 1401 - 1405, 2023.

[61] K. Yu, Y. Niu, H. Yao and K. Zhang, "Anti-Jamming Power Control Algorithm for Wireless Communication Systems Based on MPC", *Electronics*, Vol. 13, p. 4567, 2024.

[62] H. Wang, G. ding, J. Chin, Y. Zou and F. Gao, "UAV Anti-Jamming Communications with Power and Mobility Control", *IEEE Transactions on Wireless Communications,* Vol. 22 (7), pp. 4729 – 4744, 2022.

[63] D. T. Hoang, D. N. Nguyen, M. A. Aisheikh, S. Gong, E. Dutkiewicz, D. Niyato and Z. Han, ""Borrowing Arrows with Thatched Boats": The Art of Defeating Reactive Jammers in IoT Networks," *IEEE Wireless Communication*, Vol. 27, No. 3, pp. 79 - 87, 2020.

[64] P. Ali, K. Georges, F. Aidin and S. Walid, "Reinforcement Learning for Deceiving Reactive Jammers in Wireless Networks," *IEEE Transaction on Communication*, Vol. 69, Issue 6, pp. 3682 - 3697, 2021.

[65] H. Wang, J. Wang, G. Ding, J. Chen, Y. Li, and Z. Han, "Spectrum Sharing Planning for Full-duplex UAV Relaying Systems with under Laid D2D Communications", *IEEE J. Sel. Areas Communication*, Vol. 36, No. 9, pp. 1986 - 1999, 2018.

[66] V. H. Nguyen, T. H. Dinh, N. N. Diep, D. Eryk and M. Markus, "Defeating Smart and Reactive Jammers with Unlimited Power," *IEEE Transactions on Wireless Communications*, Vol. 16, No. 3, pp. 1412 - 1422, 2017.

[67] V. H. Nguyen, D. N. Nguyen, D. T. Hoang, E. Dutkiewicz, M. Mueck and S. Srikanteswara, "Ambient Backscatter: A Novel Method to Defend Jamming Attacks for Wireless Networks," *IEEE Wireless Communication Letters*, Vol. 9, No. 2, pp. 175 - 178, 2020.

[68] K. N. Vaishnavi, R. Kishore and S. Gurugopinath, "Energy Efficiency of Ambient Backscattering-Based Cognitive Radio Networks Under Jamming Attack," *Proceedings of the 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Technique, Mysuru, India*, pp. 491 - 496, 2021.

[69] W. Li, Y. Xu, Q. Guo, Y. Zhang, D. Liu, Y. Li and W. Bai, "A Q-Learning-Based Channel Selection and Data Scheduling Approach for High-Frequency Communications in Jamming Environment," *Conference*

DOI: https://doi.org/10.65218/jius.2026.112

on Machine Learning and Intelligent Communications, pp. 145 - 160, 2019.

[70] S. Ak and S. Bruggenwirth, "Avoiding Jammers: A Reinforcement Learning Approach," *IEEE International Radar Conference (RADAR)*, pp. 321 - 326, 2020.

[71] X. Lu, L. Xiao, C. Dai and H. Dai, "UAV-Aided Cellular Communications with Deep Reinforcement Learning Against Jamming," *IEEE Wireless Communications*, Vol. 27, Issue 4, pp. 48 - 53, 2020.

[72] F. Yao and L. Jia, "A Collaborative Multi-Agent Reinforcement Learning Anti-Jamming Algorithm in Wireless Networks," *IEEE Wireless Communication Letter*, Vol. 8, No. 4, pp. 1024 - 1027, 2019.

[73] Z. Feng, G. Ren, J. Chen, X. Zhang, Y. Luo, M. Wang and Y. Xu, "Power Control in Relay-Assisted Anti-Jamming Systems: A Bayesian Three-Layer Stackelberg Game Approach," *IEEE Access*, Vol. 7, pp. 14623 - 14636, 2019.

[74] Q. Zhou, Y. Li and Y. Niu, "Intelligent Anti-Jamming Communication for Wireless Sensor Networks: A Multi-Agent Reinforcement Learning Approach," *IEEE Open Journal of Communication Society*, Vol. 2, pp. 775 - 784, 2021.

[75] L. Jia, N. Qi, F. Chu, S. Fang, X. Wang, S. Ma and S. Feng, "Game-theoretic Learning Anti-jamming Approaches in Wireless Networks," *IEEE Communications Magazine*, Vol. 60, Issue 5, pp. 60 - 66, 2022.

[76] H. Yang, Z. Xiong, J. Zhao, D. Niyato and Q. Wu, "Intelligent Reflecting Surface Assisted Anti-Jamming Communications: A Fast Reinforcement Learning Approach," *IEEE Transaction on Wireless Communications*, Vol. 20, Issue 3, pp. 1963 - 1974, 2021.

[77] Z. Ji, W. Yang, X. Guan, X. Zhao, G. Li and Q. Wu, "Trajectory and Transmit Power Optimization for IRS-Assisted UAV Communication under Malicious Jamming," *IEEE Transactions on Vehicular Technology*, Vol. 71, Issue 10, pp. 11262 - 11266, 2022.

[78] T. Xiao, W. Dawei, Z. Ruonan, C. Zheng and H. Zhu, "Jamming Mitigation via Aerial Reconfigurable Intelligent Surface: Passive Beamforming and Deployment Optimization," *IEEE Transaction on Vehicular Technology*, Vol. 70, No. 6, pp. 6232 - 6237, 2021.

[79] S. Mehreen and H. S. Abid, "A Survey on Jamming Attacks, Detection and Defending Strategies in Wireless Sensor Networks," *International Journal of Research in Engineering and Technology*, Vol. 3, Issue 3, pp. 558 - 5561, 2014.

[80] V. K. Riddhi and K. Sukanya, "Software Defined Radio Based Global Positioning System Jamming and Spoofing for Vulnerability Analysis," *Proceedings of the 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE*; pp. 881 - 888, 2020.

[81] Y. Arafat, K. S. Yeaser, A. Rahman and A. Dasgupta, "A Machine Learning based Approach for Protecting Wireless Networks Against DoS Attacks," *Proceedings of the 7th International Conference on Networking, Systems and Security*, pp. 126 - 132, 2020.

[82] H. Huang and A. V. Savkin, "An Algorithm of Reactive Collision Free 3D Deployment of Networked Unmanned Aerial Vehicles for Surveillance and Monitoring," *IEEE Trans Ind. Information*, Vol. 16, No. 1, pp. 132 - 140, 2020.

Declarations:

Ethics approval and consent to participate*: Not Applicable*

Consent for publication*: All authors have approved the research's manuscript for publication.*

Availability of data and material*: Data is available upon request from the corresponding author.*

Competing Interests*: The authors have nothing to declare.*

Funding*: This research work did not receive any funding.*

Author contributions*:* ***AYEGUN Oluwadare Michael****: Articles review, Formal analysis, Methodology, Resources, Writing (Original draft), Correspondence author.* ***UBOCHI Brendan Chijioke****: Conceptualization, Supervision, Writing (Review and Editing).* ***AKINGBADE Kayode Francis****: Conceptualization, Supervision, Corrected the final draft of the manuscript.* ***POPOOLA Jide Julius****: Methodology, Resources, Supervision, Corrected the final draft of the manuscript.*

DOI: https://doi.org/10.65218/jius.2026.112

Dr. Oluwadare Michael AYEGUN received his National Diploma certificate in Electrical and Electronics Engineering from the Federal Polytechnic Auchi, Edo State in 2001. He later proceeded to the Federal University of Technology Akure (FUTA), where he obtained his B.Eng., M.Eng., and PhD degrees in Electrical and Electronics Engineering in 2009, 2019, and 2025, respectively. He also obtained MTech. degree in Satellite Communication in 2021 at the African Regional Centre for Space Science Education - English, Obafemi Awolowo University, Ile-Ife in conjunction with FUTA. He is a serving military officer in the Armed Forces of Nigeria with specialization in Weapon Electrical Engineering. His research focuses on UAV wireless network security, systems automation, satellite communication, maritime domain awareness capability systems, artificial intelligence, weapon fire control system, ship's navigation and communication systems.

Prof. Kayode Francis AKINGBADE received his National Diploma and Higher National Diploma certificates from Ondo State Polytechnic Owo (1992) and Polytechnic Ibadan (1996), respectively. He earned his PGD and M.Eng. degrees from the Federal University of Technology Akure (FUTA) in 1999 and 2003 respectively, and later completed his Ph.D. degree from FUTA in 2011. His research focuses on signal processing, wireless communications, and control systems engineering.

Dr. Brendan Chijioke UBOCHI received his B.Eng. degree in Electrical and Electronics Engineering from the Federal University of Technology, Owerri, in 2008. He obtained the M.Sc. degree in Communications Engineering from the University of Manchester in 2011, and the Ph.D. degree in Electronic and Electrical Engineering from Swansea University, Wales, United Kingdom in 2018. He is currently a Reader (Associate Professor) and his research focuses primarily on embedded systems technologies and applications, power electronics and compound semiconductor devices for radio frequency and power applications.

Prof. Jide Julius POPOOLA obtained his B.Eng. and M.Eng. degrees from the Federal University of Technology Akure (FUTA) in 1999 and 2003 respectively. He subsequently obtained his Ph.D. degree in communications Engineering from the University of Witwatersrand, Johannesburg, South Africa in 2012. He has research interests in signal processing, spectrum management, and cognitive radio technology.