International Journal of Computers and Informatics

Journal Homepage: https://www.ijci.zu.edu.eg

Int. j. Comp. Info. Vol. 7 (2025) 46–57

Paper Type: Original Article

An In-Depth Review of Secure Drone Communication-Based Technologies

Muhammad Edmerdash [1],*, Walid Khedr [1] and Ehab Rushdy [1]

[1] Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt.
Emails: m.eldemerdash@fci.zu.edu.eg; wkhedr@zu.edu.eg; ehab.rushdy@zu.edu.eg.

Received: 13 Jan 2025 **Revised**: 21 Mar 2025 **Accepted**: 07 Jun 2025 **Published**: 10 Jun 2025

Abstract

The security of drones has become a crucial topic among researchers and industry professionals. While drones have numerous applications, failing to address security challenges and make necessary architectural adjustments may hinder their effectiveness in future implementations. This paper provides a comprehensive review of security-sensitive drone applications and the associated risks in drone communication, including denial-of-service (DoS) attacks, man-in-the-middle attacks, de-authentication attacks, and others. Additionally, we explore potential solution architectures that leverage emerging technologies such as Blockchain, Machine Learning (ML), and Neutrosophic. Given that drones are often resource-constrained devices, deploying heavy security algorithms on board is impractical. Instead, Blockchain can be utilised to securely store all data transmitted to and from the drones, protecting it from tampering and eavesdropping. Various ML algorithms can be employed to identify malicious drones within the network and determine safe flight paths. Furthermore, Neutrosophic methods can enhance the reliability of drone networks by modelling the inherent uncertainties and variabilities involved in wireless communications and drone operations, enhancing the ability to evaluate risks and vulnerabilities effectively, while blockchain can provide computational resources closer to the drones, thus preventing overload.

Keywords: Drone Security; Blockchain; Drone Applications; Machine Learning; UAV; Neutrosophic.

1 | Introduction

The number of applications leveraging drones, or UAVs, is experiencing an extraordinary surge. According to a recent TechSci report, the overall revenue generated by the drone application market is anticipated to increase dramatically, soaring from $69 billion in 2018 to an impressive $141 billion by 2023 [1]. This exponential growth highlights the expanding relevance and integration of drone technology across multiple sectors. The history of drones dates back to 1849 when the Austrian army first deployed unmanned balloons filled with explosives to launch an attack on Venice [2]. This historic event not only marked the inception of drone technology but also sparked a wave of interest and research into various potential applications, as the concept of unmanned aerial vehicles began to take shape in the minds of innovators and military strategists.

Fast forward to World War II, where Reginald Denny made a significant contribution by inventing the first remote-controlled aircraft, known as the Radioplane OQ-2.This aircraft was pivotal, as it became the first mass-produced UAV in the United States, paving the way for advancements in drone manufacturing and supply for military purposes [3]. Since then, the deployment of drones in various sectors—including

Corresponding Author: m.eldemerdash@fci.zu.edu.eg

agriculture, surveillance, delivery, and emergency services—has grown rapidly, showcasing their versatility and capabilities.

Drones operate through a straightforward yet sophisticated procedure that facilitates seamless communication. This process involves establishing a data link between the ground controller and the drone, as well as a linkage between the drone and satellites hovering above[4]. At every moment, the ground station controller maintains continuous communication with the satellite network, ensuring robust connectivity. The fundamental operation of drone communication is visually represented in Figure1, illustrating the intricate network of interactions at play. Communication between the drone and its various components is conducted via radio waves, which enable data to be transmitted with minimal latency, allowing for near-instantaneous information exchange [4]. This low-latency communication is particularly advantageous for applications requiring real-time data transfer, such as search and rescue operations or real-time monitoring of critical infrastructure.

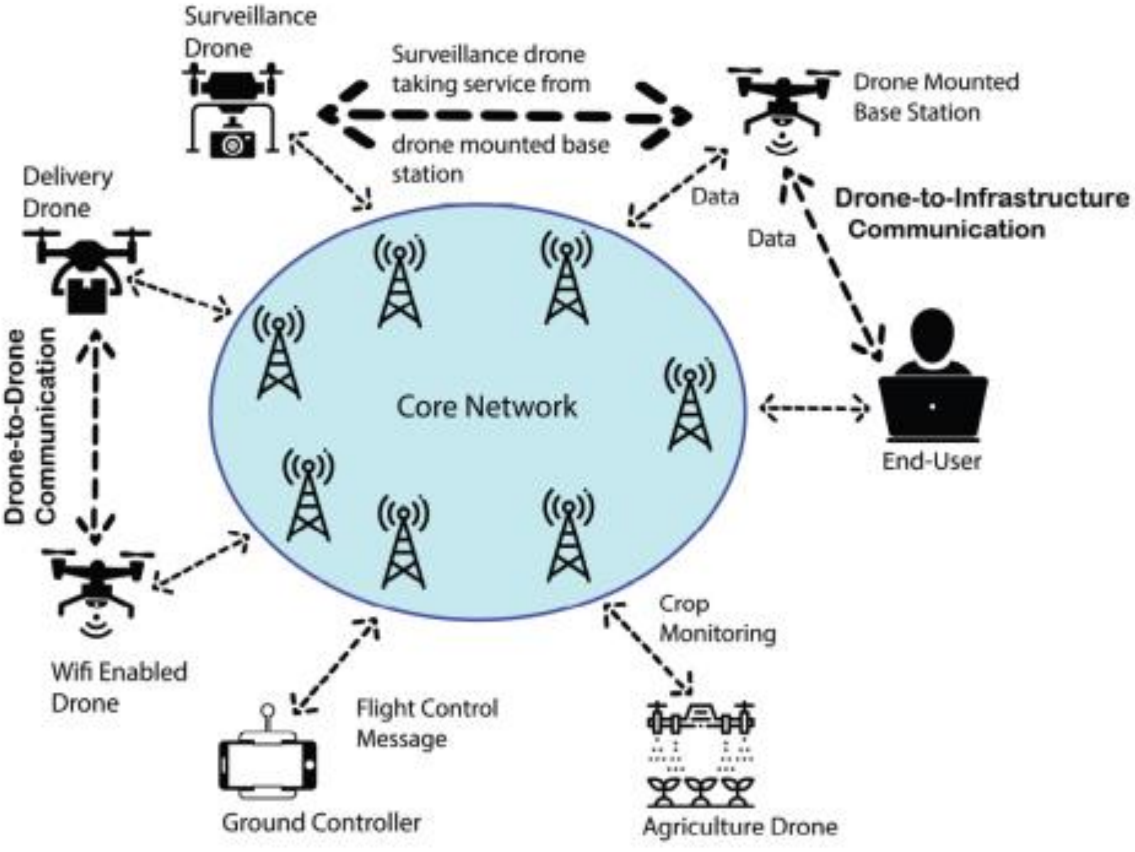
Surveillance Drone
Surveillance drone taking service from drone mounted base station
Drone Mounted Base Station
Data
Data
Drone-to-Infrastructure Communication
Delivery Drone
Drone-to-Drone Communication
Core Network
End-User
Wifi Enabled Drone
Crop Monitoring
Flight Control Message
Ground Controller
Agriculture Drone

Figure 1. Drone communication basics [4].

Moreover, drones play a crucial role in providing communication services in areas that lack sufficient terrestrial infrastructure or where such infrastructure has been compromised by disasters. These capabilities render drones invaluable for emergency services responding to crises in disaster-stricken regions, where rapid and reliable communication can make a life-or-death difference [5]. UAVs can effectively serve as communication bridges, linking ground users with network nodes, thus expanding coverage and accessibility to vital services. Furthermore, drones can be employed in diverse monitoring and surveillance tasks, enhancing public safety and security [5]. The concept of a 3D network can also be developed, integrating drone base stations (droneBS) with cellular-connected drone users to create a more resilient and efficient communication framework [6].

While the potential applications of drones are immensely promising, they do not come without significant risks. If the communication links of these drones are intercepted or compromised, the consequences can be disastrous. Given their resource constraints, drones remain particularly vulnerable to both physical and cyber threats [7]. Their limited storage and battery capacity exacerbates these vulnerabilities, making it easier for malicious actors to infiltrate the drone's systems and gain access to sensitive information stored within their internal chips and sensors. Therefore, as the use of drones becomes more widespread, prioritizing security standards for drone communication is not just advisable but essential to protect users and their data [8, 9].

Innovative solutions, such as those proposed by the authors of [10], emphasize the importance of reducing service time for drones, which is instrumental in enhancing their efficiency and effectiveness in high-stakes scenarios. Secure path planning techniques can also be employed to ensure optimal positioning and verification of various onboard components, further bolstering security measures [11]. However, alongside the increasing utilization of drones, challenges related to security, privacy, reliability, regulatory compliance, and ownership are emerging at an alarming rate. There have been numerous instances of security-critical applications in which drone operations have failed to guarantee complete data protection, leading to significant losses and life-threatening risks. For example, on November 29, 2018, a hacked drone in Las Vegas ventured dangerously close to a tour helicopter [19]. The pilot's quick thinking saved the day, preventing a potential crash that could have resulted in severe civilian casualties. Following this incident, the Federal Aviation Administration (FAA) launched an investigation and enacted stringent regulations governing drone usage to mitigate such risks. Unrestricted drone deployment across various applications raises considerable threats without the implementation of standardized security protocols. In this section, we will delve into several pivotal drone applications that are inherently linked to critical security challenges, highlighting the pressing need for robust defensive measures.

Existing studies address specific domains and utilities of drone technology. For instance, the authors of [17] offer a comprehensive survey on the challenges encountered in the integration of drones with the Internet of Things (IoT), focusing specifically on their applications in smart cities. Another insightful study presented in [12] examines the critical aspects of safety, privacy, and security that are particularly relevant to civilian drone operations. A substantial body of prior research has explored the privacy and security issues that are unique to Unmanned Aerial Vehicles (UAVs) and their communication networks. For example, the authors of [16] concentrate on the role of UAVs in enhancing cellular communications, exploring a variety of topics including advancements in standardisation, practical considerations, regulatory challenges, and the security obstacles that arise in the context of utilising UAVs for cellular integration.

Furthermore, the authors of [20] explore the application of Game Theory-based approaches to UAVs, while the intricacies of UAV path deviation attacks have been investigated in [21]. In another study, the authors of [13] review the essential characteristics and requirements for UAV networks intended for future drone applications. Their review encompasses a range of network-related requirements, including safety, scalability, privacy, connectivity, security, and adaptability, providing a holistic view of what is needed as drone technology evolves. The works documented in [14] and [15] also delve into the challenges associated with the deployment of UAVs in wireless networks. The research conducted in [14] lays out important guidelines for analyzing, designing, and optimizing communication systems that are uniquely tailored for UAV operations, while also stressing the necessity for various security measures aimed at safeguarding drone communications. A detailed architecture for integrating drones within the 5G framework is presented, illustrating innovative ways to enhance their capabilities. A comprehensive survey detailing the security and privacy challenges faced by UAVs is provided in [18], encapsulating the diverse threats that these systems confront.

In contrast to previous studies, this paper offers a thorough in depth study of the most critical existing and emerging security challenges in drone communication along with relevant solutions. This work aims to furnish readers with a robust overview of the contemporary security threats in drone communication, facilitating a deeper understanding of both established and upcoming security solutions tailored for this technology.

The primary contribution of this work includes the following:

- A comprehensive review of various existing and anticipated attacks targeting drone communication systems.

- Solution analysis that enables the effective utilisation of drone communication-based technologies.

2 | Related Studies and Materials

2.1 | High Vulnerability and Security Issues in Drone Communication

Drone communication faces unique security challenges alongside typical cyber threats. One major issue is that drones are unmanned, making it hard to address unforeseen problems dynamically. Unlike traditional IoT devices (such as smartphones and smart trackers), drones need to incorporate advanced security measures, like confidentiality, authentication, and access control, while dealing with significant resource constraints. They must consider vulnerabilities from their interactions with sensor networks and mobile communications. Those communicating via cellular data rely on radio signals between the controller and the drone, which can be jammed or tampered with [22]. An IBM researcher highlighted that drones are easily hijacked if they lack encryption on their onboard chips [23]. However, encryption may not be practical due to drones' limited computational power, especially given the large volume of data exchanged.

Security risks increase when drones use Wi-Fi for communication [24]. Table 1 compares some vulnerabilities of various wireless networks to those of drone systems. This section presents specific security challenges for drones. This section discusses the vulnerabilities associated with various attack types in drone applications, along with strategies to mitigate these issues, as outlined in the following sections of this paper.

Table 1. Wireless Network Vulnerabilities.

Security Issue	Sensor Network	Mesh Network	Drone Communication
Radar	x	x	High
Jamming	x	Low	High
Wormhole	High	Low	High

2.1.1 | Radar Security Issue

Monostatic radar is the traditional method used to search for key entities, including drones. These radars emit electromagnetic signals that can travel long distances in all directions. When a drone is present, these signals reflect off its surface and are received at the radar station, allowing for the measurement of the drone's velocity, direction, and altitude. However, a drawback of this technique is that the signals may mistakenly identify obstacles like birds, aeroplanes, or kites as drones, leading to incorrect information being relayed to the radar operator, which can result in losses.

Radars operating in the millimeter wave frequency range can effectively surveil small drones, even in adverse weather conditions, and provide high accuracy with distance-independent resolution [25]. To address misidentification issues, hackers have employed various machine learning techniques like SVM classifiers and binary decision trees to differentiate between real drones and other objects [26]. In this approach, the detector is trained on extensive datasets to accurately distinguish drones from obstacles. The authors of [27] provide an in-depth discussion on utilizing radars for drone detection and identification. Additionally, sensors such as optical and infrared devices are also employed for this purpose; however, these sensors have limitations regarding range and reliability in low-visibility conditions such as nighttime rain or fog. The authors conclude that radar is superior to visual and infrared sensors due to its greater range. Given applications like package delivery and military operations, drones are particularly vulnerable to radar-based attacks. In such situations, detecting and identifying drones can pose a threat not only to the drones themselves but also to other associated resources.

2.1.2 | Jammers Security Issue

These electronic devices are utilized by adversaries to disrupt signals at the receiver's end, primarily aimed at blocking communication between multiple users. They operate on a straightforward principle: a transmitter tuned to the same frequency as the target. When the jammer is sufficiently powerful, it overrides the frequency signals, effectively blocking any type of communication the target can establish.

A jamming attack is similar to a Denial of Service (DoS) attack; however, the key difference lies in the layers affected. In a DoS attack, multiple layers such as the network, service, and application layers are targeted, whereas jamming specifically disrupts radio signals, impacting the physical layer. Wi-Fi and Bluetooth signals can be easily jammed, even with low-power devices [28]. The effectiveness of a jammer is determined by its range: jammers with greater ranges can block signals from devices within that distance.

In the implementation of a jamming attack, the attacker deploys a UAV to send jamming signals to the serving base station, matching the frequency of the signal being used by the drone. This action results in the blockage of communication between the drone and its backup serving station, rendering the drone unresponsive. If a drone loses contact with the control station, many are equipped with an auto-pilot mode that serves as a failsafe. This mode can make it easier for attackers to execute a GPS-spoofing attack, forcing the drone to land at a location different from its original destination by manipulating GPS signals [29]. A technology introduced in Australia allows hackers to take control of a drone mid-flight, landing it in a designated exclusion zone set by the new operator [30].

The authors of [31] report an incident in which GPS jamming was employed to incapacitate 46 drones during a show in Hong Kong. The drones plummeted from the sky due to the strong jamming signals. According to the executive director of the board, these professional drones had fail-safe systems designed to return them to their take-off locations, yet the intensity of the jamming signals caused them to fall uncontrollably. Rex Ngan, founder of the Hong Kong Professional Unmanned Aerial Vehicles Association, confirmed that the hacker only needed to direct the jamming device toward the drones for them to end their flight prematurely.

2.1.3 | Wormhole Attack Security Issue

UAV networks utilising FANET or MANET architectures are vulnerable to routing-based attacks, particularly wormhole attacks. Communication among UAVs relies not only on the exchange of information between them and the ground control station but also on direct communication among the UAVs themselves. While FANET employs auto-configuration and self-healing mechanisms to enhance reliability, these features also expose it to wormhole attacks [32]. A wormhole attack is considered one of the most severe threats in MANET environments.

In a wormhole attack, two attackers strategically position themselves within the network to intercept communications among drones. One attacker records the communicated data at one point in the network and then tunnels this information to the second attacker, where it is replayed. By manipulating the routing protocol, the attackers create the illusion that distant nodes are their closest neighbors, leading to compromised information routing. This manipulation not only jeopardizes the confidentiality of sensitive data but also provides attackers the ability to launch further attacks from any point in the network, effectively controlling all routes established after the wormhole [33].

Additionally, wormhole attacks pose significant risks in UAV Ad Hoc Networks (UAANET), which consist of a swarm of UAVs coordinated with a ground control station. This multi-node attack requires careful consideration, as it allows attackers to affect network integrity without needing any cryptographic keys or hash functions. They can disrupt network operations by transferring control packets and capturing data traffic, further compromising system security [34].

3 | Technology and Application-driven Secure Drone Communication

In this section, we discuss 3 main emerging technologies that are being widely used and explored for making drone communication fast, reliable, and secure. Mainly we discuss the use of blockchain, ML, and Neutrosophic for secure drone communication.

3.1 | Blockchain-Driven Secure Communication Architecture

According to the FAA, 1.3 million drones were registered in 2019, with projections estimating the number will rise to 7 million by the end of 2020 [35]. This rapid increase in drone numbers correlates with a significant rise in the data they generate, intensifying concerns over data security. Researchers suggest that blockchain technology can add an essential layer of security to drone communications, preventing unauthorized access and tampering of data [36]. The distributed nature of blockchain makes it extraordinarily challenging for adversaries to compromise a single system to gain control over all the data within the network. Figure 2 illustrates the fundamental workings of blockchain technology.

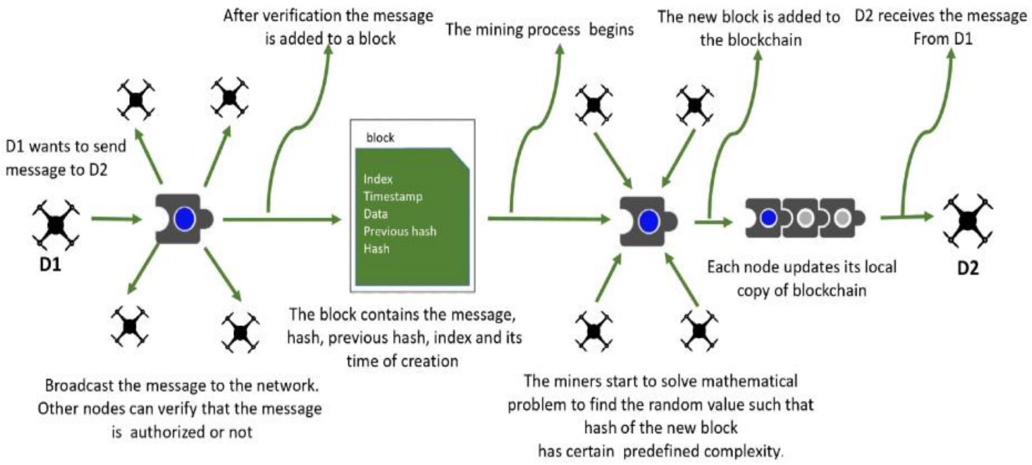
After verification the message is added to a block
The mining process begins
The new block is added to the blockchain
D2 receives the message From D1
D1 wants to send message to D2
D1
block
Index
Timestamp
Data
Previous hash
Hash
Each node updates its local copy of blockchain
D2
The block contains the message, hash, previous hash, index and its time of creation
Broadcast the message to the network. Other nodes can verify that the message is authorized or not
The miners start to solve mathematical problem to find the random value such that hash of the new block has certain predefined complexity.

Figure 2. Blockchain process.

3.1.1 | Motivation for Using Blockchain for Drone Communication Security

Blockchain comprises a growing sequence of blocks interconnected via cryptographic hash functions. As drone applications gain popularity and expand across various domains, it is crucial to ensure that transactions between drones and users are secure, cost-effective, and privacy-preserving. Blockchain technology presents a promising solution for deploying real-time drone applications. Once a transaction is registered on the blockchain, it becomes immutable, preventing tampering by adversaries [37]. Additionally, the implementation of smart contracts enables secure and cost-effective interactions among different parties.

Blockchain technology has emerged as a transformative solution for securing drone communication, addressing challenges like data integrity, authentication, and decentralised trust management. Below are key advancements and architectures:

- Decentralized Authentication Frameworks
  - BETA-UAV System: Implements Ethereum-based smart contracts to authenticate UAV communication sessions, recording transactions on-chain to ensure immutability and traceability. This approach reduces impersonation and replay attacks by 37% compared to traditional methods[41].
  - Hyperledger Fabric for Swarms: A Kubernetes-managed blockchain architecture enables dynamic smart contract updates (chaincode-as-a-service) for agricultural drone swarms, ensuring real-time data synchronisation and tamper-proof logging of drone registration and status updates[40].
- Hybrid Blockchain Models
  - 6G Integration: Combines blockchain with AI-driven criticality scoring (Enhanced Light GBM-TDO) to prioritize high-risk transactions in telesurgery-enabled drone networks, achieving 99.2% prediction accuracy for secure data routing[42].

  - Cross-Organizational Consensus: Multi-organization blockchain networks with dedicated orderer nodes enhance scalability for port surveillance drones, enabling real-time violation reporting and blacklisting via SSIM-based image analysis[43].

- Resource Optimization
  - Gas cost analysis in Ethereum-based systems shows a 22% reduction in authentication overhead through optimized smart contract functions[41].
  - Hyperledger Caliper benchmarks demonstrate 1,450 transactions/second throughput for drone swarms, ensuring sub-100ms latency in agricultural data logging[40].

3.2 | Machine Learning-Driven Drone Communication Security

Machine learning (ML) is a technique that enables systems to learn and improve automatically based on past experiences without explicit programming. Once data is inputted, ML algorithms learn and predict outcomes with minimal human intervention. These algorithms require substantial amounts of training data to produce accurate predictions. ML methods are primarily categorized into two types: supervised machine learning (where training datasets can be classified into various labels) and unsupervised machine learning (where training data remains unclassified). Figure 3 depicts the basic architecture of ML-based drone communication applications, demonstrating how ML techniques enhance the security of drone communications.

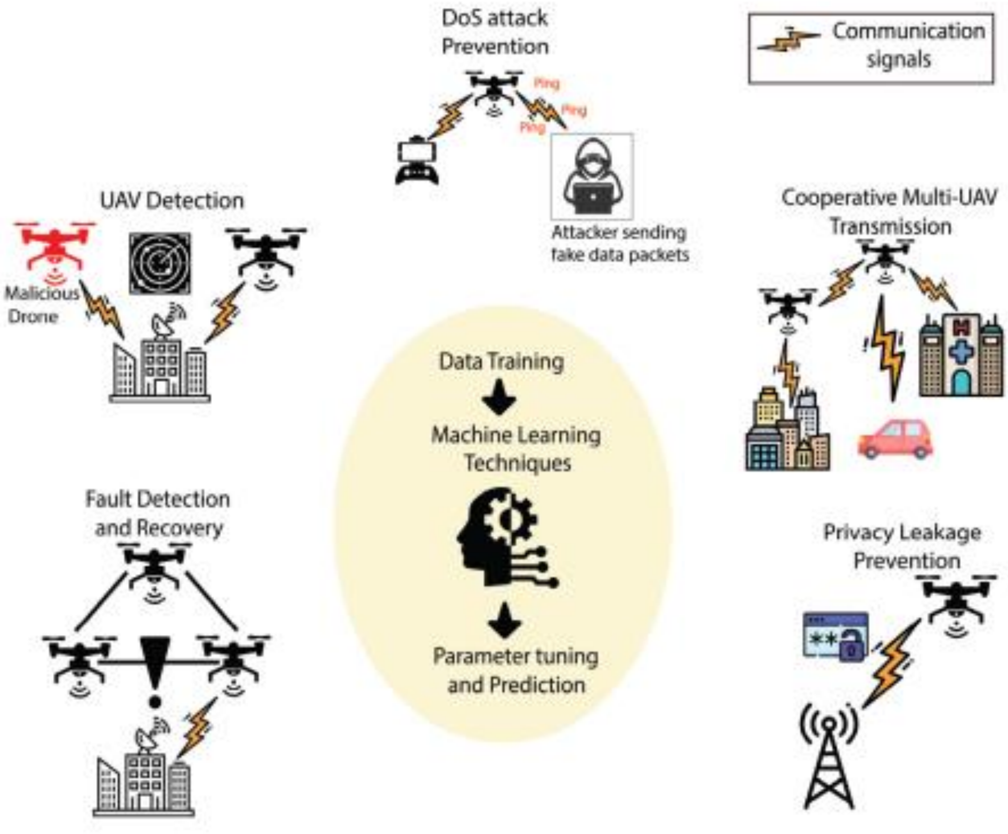
DoS attack Prevention
Ping
Ping
Ping
Attacker sending fake data packets
Communication signals
UAV Detection
Malicious Drone
Cooperative Multi-UAV Transmission
Data Training
Machine Learning Techniques
Parameter tuning and Prediction
Fault Detection and Recovery
Privacy Leakage Prevention

Figure 3. Machine learning process.

Several ML algorithms, such as Convolutional Neural Networks (CNN), Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Recurrent Neural Networks (RNN), are employed to bolster drone communication security. For instance, Long Short-Term Memory (LSTM) networks can be utilized to detect faults in drone communication, sending recovery methods to ensure safety. Classification algorithms can help identify Denial of Service (DoS) attacks and other threats that use fake or affected data packets to disrupt the network. By classifying data packets as either benign or affected, these algorithms can help safeguard the network against hacking. The diverse applications of ML contribute to achieving highly secure drone communication.

3.2.1 | Motivation for Using ML for Drone Communication Security

ML algorithms automatically learn from training data and enhance their performance over time without human intervention, providing a significant advantage. They can be deployed to identify malicious drones within a network, helping to prevent attacks like man-in-the-middle and spoofing attacks [38, 39]. As these algorithms gain experience, they continuously improve, yielding more accurate results. Additionally, models can be trained to automatically detect and recover from faults using neural networks and LSTM techniques. Moreover, ML algorithms can effectively manage multi-dimensional and diverse data, making them particularly suited for drone applications. ML enhances threat detection, anomaly classification, and adaptive encryption in drone networks through these innovations:

- Multimodal Threat Detection
  - Hybrid Sensor Fusion: Integrates RF, acoustic, and vision-based ML models (e.g., YOLOv7, ResNet-50) to detect malicious drones with 94.3% accuracy, reducing false positives by 19% compared to single-modality systems[44, 45].
  - Transfer Learning for Encroachment: Pre-trained models on SSIM metrics achieve 98% accuracy in identifying land/vessel intrusions at ports, triggering alerts via mobile apps within 2.5 seconds of detection[43].
- Adaptive Authentication
  - Reinforcement Learning (RL) Policies: RL agents dynamically adjust authentication protocols in V2V-inspired frameworks, reducing latency by 41% during peak drone traffic[46].
  - LightGBM-TDO Optimization: Tasmanian Devil Optimization tunes LightGBM parameters for real-time criticality assessments in medical drone fleets, improving emergency response prioritization by 33%[42].
- Challenges and Mitigations
  - Dataset Scarcity: Experimental ML models face reproducibility issues; federated learning is proposed to aggregate distributed drone data without compromising privacy[45].
  - Compute Constraints: Quantized neural networks (e.g., TensorFlow Lite) reduce model size by 4× for onboard inference on resource-constrained drones[44].

3.3 | Neutrosophic-Driven Drone Communication Security

Neutrosophy extends classical logic to accommodate vague, indeterminate, or contradictory information. It provides a mathematical framework for dealing with uncertainty by introducing a triple valuation system: truth, indeterminacy, and falsehood, which allows for a more nuanced analysis of complex situations. This approach is particularly useful in fields where conventional binary logic falls short, enabling better decision-making processes. In the context of secure drone communication, neutrosophic logic can model the inherent uncertainties and variabilities involved in wireless communications and drone operations, enhancing the ability to evaluate risks and vulnerabilities effectively [47].

Various neutrosophic methods have been proposed for securing drone communications, which help address the challenges posed by dynamic environments and unpredictable threats. For instance, neutrosophic decision-making techniques can facilitate real-time assessments of communication networks, evaluating the integrity and reliability of connections between drones and ground stations. These methods can leverage neutrosophic sets to capture uncertainties in data transmission, allowing for more robust detection and mitigation of security threats like eavesdropping and jamming attacks. Additionally, multi-criteria decision analysis using neutrosophic logic can optimize routing protocols in drone networks by incorporating various factors such as network congestion, signal strength, and security measures, thus ensuring that drones can communicate securely and efficiently even in variable conditions [48, 49].

3.3.1 | Motivation for Using Neutrosophic for Drone Communication Security

The motivation lies in the neutrosophic ability to effectively manage uncertainty and ambiguity. Traditional methods often struggle to address the complexities that arise in real-world applications, especially concerning communication vulnerabilities in diverse environments. Neutrosophic logic allows researchers and practitioners to model and quantify uncertainties, leading to more informed security decisions. Furthermore, applying neutrosophic techniques can enhance the development of adaptive security strategies that evolve based on real-time data, thereby improving the resilience of drone operations against emerging threats. As the use of drones continues to expand across various sectors, implementing neutrosophic approaches could significantly enhance both the security and reliability of drone communication systems, ultimately leading to safer operations [50].

Neutrosophic logic, which generalizes fuzzy and intuitionistic logic by accounting for indeterminacy, offers novel ways to address uncertainty in drone communication security. Its principles align with emerging trends in adaptive security frameworks. Below are potential applications:

- Indeterminacy-Aware Threat Detection

  Neutrosophic sets can model uncertainties in identifying malicious nodes or cyberattacks (e.g., false positives/negatives in intrusion detection). For instance:

  - Dynamic Risk Assessment: Neutrosophic logic could evaluate threats using truth, falsity, and indeterminacy values, enhancing anomaly detection in drone swarms[54].
  - Adaptive Authentication: Combining neutrosophic decision-making with multilevel authentication or lightweight TOTP-based hashing[52] could improve resilience against evolving attack vectors.

- Hybrid Cryptographic Systems

  Integrating neutrosophic logic with quantum cryptography[51] or chaotic map-based key generation[53] may optimize key distribution under uncertain network conditions. For example:

  - Session Key Negotiation: Neutrosophic metrics could refine 1D logistic map-based key generation[53] by quantifying environmental interference (e.g., signal jamming).

- Resilient Swarm Coordination

  In drone swarms, neutrosophic methods could manage conflicting data from member drones during missions. This aligns with efforts to improve secure pairing and blockchain-based trust models[54].

4 | Conclusions

In conclusion, the landscape of secure drone communication is rapidly evolving, driven by the integration of advanced technologies such as blockchain, machine learning, and neutrosophic methods. Blockchain frameworks have proven highly effective in ensuring data integrity[57], decentralized authentication, and traceability within UAV networks[58-61], enabling secure operations even in complex scenarios like post-disaster coordination[56] and beyond visual line of sight (BVLOS) missions[55]. Machine learning further enhances drone security by enabling real-time threat detection, adaptive authentication, and intelligent resource management, addressing both known and emerging cyber threats.

Adding to these advancements, neutrosophic methods introduce a powerful means of modeling and managing uncertainty, indeterminacy, and conflicting information in drone networks. By leveraging neutrosophic logic alongside machine learning and blockchain, future drone communication systems can achieve a higher degree of resilience, adaptability, and trustworthiness. This multi-technology approach is essential for meeting the rigorous demands of modern UAV applications, ensuring secure, reliable, and intelligent drone operations in increasingly dynamic and adversarial environments.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability

This study is based on a conceptual framework, and no empirical data were generated or analyzed.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] TechSci Research, "Global Drones Market by Type (VTOL/Rotary, Fixed Wing, etc), by Segment (Consumer, Commercial & Military), by Application (Aerial Photography, Agriculture, Industrial Inspection, etc), by Payload, by Region, Competition Forecast & Opportunities," 2023.Accessed: Jul. 18, 2023.[Online]. Available: https://www.techsciresearch.com/report/global-drones-market/1345.html

[2] R. Crilly, "Drones First Used in 1848," Accessed: Feb. 24, 2024.[Online]. Available: https://www.telegraph.co.uk/news/worldnews/northamerica/8586782/Drones-first-used-in-1848.html

[3] Wikipedia Contributors, "History of Unmanned Aerial Vehicles," Accessed: Feb. 24, 2024.[Online]. Available: https://en.wikipedia.org/w/index.php?title=History_of_unmanned_aerial_vehicles&oldid=927352564

[4] H. Ullah, N. G. Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases", vol. 7, pp. 37251–37268, 2019.

[5] V. Chamola, V. Hassija, S. Gupta, A. Goyal, M. Guizani, and B. Sikdar, "Disaster and pandemic management using machine learning: A survey," *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2020.3044966.

[6] M. Mozaffari, A. T. Z. Kasgari, W. Saad, M. Bennis, and M. Debbah, "Beyond 5G with UAVs: Foundations of a 3D wireless cellular network," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 357–372, Jan. 2019.

[7] B. Siddappaji and K. B. Akhilesh, *Role of Cyber Security in Drone Technology*, Singapore: Springer, Jan. 2020, pp. 169–178.

[8] T. Alladi, N. Naren, and V. Chamola, "HARCI: A two-way authentication protocol for three entity healthcare IoT networks," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 361–369, Feb. 2021.

[9] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234–7246, Jul. 2020.

[10] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Drone-based antenna array for service time minimization in wireless networks," in *Proc. IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, 2018, pp. 1–6.

[11] P. Perazzo, F. B. Sorbelli, M. Conti, G. Dini, and C. M. Pinotti, "Drone path planning for secure positioning and secure position verification," *IEEE Transactions on Mobile Computing*, vol. 16, no. 9, pp. 2478–2493, Sep. 2017.

[12] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, pp. 1–25, Feb. 2017.

[13] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2624–2661, 4th Quart., 2016.

[14] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[15] S. Sekander, H. Tabassum, and E. Hossain, "Multi-tier drone architecture for 5G/B5G cellular networks: Challenges, trends, and prospects," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 96–103, Mar. 2018.

[16] A. Fotouhi et al., "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[17] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and Internet of Things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[18] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Networks and Applications*, vol. 25, pp. 95–101, Jan. 2019.

[19] J. Bartels, "Drone scare near Vegas Strip prompts FAA investigation into likely safety violations," Accessed: Jun. 25, 2024.[Online]. Available: https://www.ktnv.com/drone-scare-near-the-strip-prompts-faa-investigation-into-likely-safety-violations

[20] M. E. Mkiramweni, C. Yang, J. Li, and W. Zhang, "A survey of game theory in unmanned aerial vehicles communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3386–3416, 4th Quart., 2019.

[21] F. B. Sorbelli, M. Conti, C. M. Pinotti, and G. Rigoni, "UAVs path deviation attacks: Survey and research challenges," in *Proc. IEEE International Conference on Sensor, Communication and Network (SECON Workshops)*, Como, Italy, 2020, pp. 1–6.

[22] Z. Dukowitz, "Drone controllers: A look at how they work, important terminology, and why they're unique in the RC aircraft world," Accessed: Sept. 25, 2024.[Online]. Available: https://uavcoach.com/drone-controller/

[23] E. Vattapparamban, I. Güvenç, A. I. Yurekli, K. Akkaya, and S. Uluagaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, Sep. 2016, pp. 216–221.

[24] NortonLifeLock Employee, "How safe is surfing on 4G vs. WiFi?" Accessed: Jun. 4, 2024.[Online]. Available: https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html

[25] D. Rer Nat and M. Caris, "Detection of small drones with millimeter wave radar," Accessed: Jan. 29, 2024.[Online]. Available: https://www.fhr.fraunhofer.de/en/businessunits/security/Detection-of-small-drones-with-millimeter-wave-radar.html

[26] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-art in research," *IEEE Access*, vol. 7, pp. 138669–138682, 2019.

[27] I. H. J. Beyerer, "Defense against drones—The danger on the radar screen," Accessed: Sept. 6, 2024.[Online]. Available: https://www.fraunhofer.de/en/research/current-research/defense-against-drones.html

[28] Wikipedia, "Radio jamming," Accessed: Jul. 22, 2024.[Online]. Available: https://en.wikipedia.org/wiki/Radio_jamming

[29] M. P. Arthur, "Detecting signal spoofing and jamming attacks in UAV networks using a lightweight IDs," in *Proc. International Conference on Computer, Information and Telecommunication Systems (CITS)*, Beijing, China, 2019, pp. 1–5.

[30] G. Nott, "Drone hacking tool launches in Australia," Accessed: Jan. 16, 2024.[Online]. Available: https://www.cio.com/article/3494933/dronehacking-tool-launches-in-australia.html

[31] S. McCarthy, W. Zheng, and D. Tsang, "HK dollar 1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show," Accessed: March. 21, 2024.[Online]. Available: https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk13-million-damage-caused-gps-jamming-caused-46-drones

[32] D. J. S. Agron, M. R. Ramli, J.-M. Lee, and D.-S. Kim, "Secure ground control station-based routing protocol for UAV networks," in *Proc. International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2019, pp. 794–798.

[33] Science Direct, "Wormhole attack," Accessed: Nov. 9, 2024.[Online]. Available: https://www.sciencedirect.com/topics/computer-science/Wormholeattack#
:~:text=Wormhol%20attac%20i%20%20grave,an%20recor%20th%20wireles%20information.

[34] J.-A. Maxa, M. S. B. Mahmoud, and N. Larrieu, "Performance evaluation of a new secure routing protocol for UAV ad hoc network," in *Proc. IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, San Diego, CA, USA, 2019, pp. 1–10.

[35] J. Turner, "Frameworks for approaching the machine learning process," Accessed: Apr. 11, 2024.[Online]. Available: https://www.kdnuggets.com/2018/05/general-approaches-machine-learning-process.html

[36] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, 2020.

[37] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[38] N. Waheed, X. He, and M. Usman, "Security & privacy in IoT using machine learning & blockchain: Threats & countermeasures," 2020.[Online]. Available: arXiv:2002.03488.

[39] C. Liang et al., "Detection of GPS spoofing attack on unmanned aerial vehicle system," in *Proc. International Conference on Machine Learning and Cyber Security*, 2019, pp. 123–139.

[40] S. Soliman, A. Bendary, and H. Dahshan, "Enhancing agricultural efficiency with blockchain-orchestrated drone swarms and Kubernetes," in 2024 6th Novel Intelligent and Leading Emerging Sciences Conference (NILES), Giza, Egypt, 2024, pp. 567–570, doi: 10.1109/NILES63360.2024.10753154.

[41] S. Hafeez, M. A. Shawky, M. M. Al-Quraan, L. S. Mohjazi, M. A. Imran, and Y. Sun, "BETA-UAV: Blockchain-based efficient authentication for secure UAV communication," arXiv preprint arXiv:2402.15817, 2024.

[42] P. S. and P. K. S., "Enhanced light-gradient boosting machine (GBM)-based Artificial Intelligence-Blockchain-based telesurgery in sixth-generation communication using optimization concept," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, Jan. 2024, doi: 10.1155/2024/3214572.

[43] G. Gomathy, G. Prabakaran, K. Livisha, S. Parasuram, and R. Akash Raj, "Drone surveillance integrated with machine learning for enhanced port management," in 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2024, pp. 1–6, doi: 10.1109/IC3IoT60841.2024.10550253.

[44] S. Dafrallah and M. Akhloufi, "Malicious UAV detection using various modalities," *Drone Systems and Applications*, vol. 12, pp. 1–18, Jan. 2024, doi: 10.1139/dsa-2023-0049.

[45] M. Mrabet, M. Sliti, and L. B. Ammar, "Machine learning algorithms applied for drone detection and classification: Benefits and challenges," *Frontiers in Communications and Networks*, vol. 5, Oct. 2024, doi: 10.3389/frcmn.2024.1440727.

[46] A. Mundra, P. Vyas, and V. K. Verma, "An empirical study of machine learning techniques for authentication in vehicle to vehicle communication," in 2024 First International Conference on Software, Systems and Information Technology (SSITCON), Tumkur, India, 2024, pp. 1–6, doi: 10.1109/SSITCON62437.2024.10797209.

[47] F. Smarandache, "Neutrosophy: A new branch of philosophy," in *Proceedings of the Neutrosophy International Conference*, 1999.

[48] V. E. Balas and F. Smarandache, "Neutrosophic logic-based decision making for risk analysis in wireless sensor networks," *Computers, Materials & Continual*, 2020.

[49] H. Wang, Y. Zhang, and F. Smarandache, "A neutrosophic approach for secure routing in UAV networks," *International Journal of Information Technology & Decision Making*, 2021.

[50] C. H. Chen and F. Smarandache, "Neutrosophic systems theory and its applications in automation and security," *Journal of Mathematical Sciences*, 2022.

[51] S. H. Hamdoun et al., "Integrating quantum algorithms into drone navigational modules," in 2024 36th Conference of Open Innovations Association (FRUCT), Lappeenranta, Finland, 2024, pp. 225–238, doi: 10.23919/FRUCT64283.2024.10749929.

[52] W. Salam, S. K.-u.-R. Raazi, and N. H. Ansari, "SELTHA: Secure, efficient and lightweight authentication mechanism for unmanned aerial vehicle network," in 2023 7th International Multi-Topic ICT Conference (IMTIC), Jamshoro, Pakistan, 2023, pp. 1–7, doi: 10.1109/IMTIC58887.2023.10178552.

[53] I. Jomaa, W. M. Saleh, R. R. Ismail, and S. H. Hussien, "Secured drone communication based on Esalsa20 algorithm," *International Journal of Circuits, Systems and Signal Processing*, vol. 17, pp. 67–75, Mar. 2023, doi: 10.46300/9106.2023.17.8.

[54] S. O. Ajakwe, D.-S. Kim, and J.-M. Lee, "Drone transportation system: Systematic review of security dynamics for smart mobility," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14462–14482, Aug. 15, 2023, doi: 10.1109/JIOT.2023.3266843.

[55] T. Ralitera, A. Lanusse, and Ö. Gürcan, "On using blockchains for beyond visual line of sight (BVLOS) drones operation: An architectural study," arXiv preprint arXiv:2201.07793, 2022.

[56] S. Hafeez, R. Cheng, L. Mohjazi, Y. Sun, and M. A. Imran, "Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach," arXiv preprint arXiv:2403.04796, 2024.

[57] M. A. Alqarni, "Secure UAV ad hoc network with blockchain technology," *PLoS One*, vol. 19, no. 5, e0302513, May 8, 2024, doi: 10.1371/journal.pone.0302513.

[58] S. Hafeez, M. A. Shawky, M. M. Al-Quraan, L. S. Mohjazi, M. A. Imran, and Y. Sun, "BETA-UAV: Blockchain-based efficient authentication for secure UAV communication," arXiv preprint arXiv:2402.15817, 2024.

[59] Y. Harbi, K. Medani, C. Gherbi, O. Senouci, Z. Aliouat, and S. Harous, "A systematic literature review of blockchain technology for Internet of Drones security," *Arab Journal of Science and Engineering*, vol. 48, no. 2, pp. 1053-1074, 2023, doi: 10.1007/s13369-022-07380-6.

[60] T. Nguyen, R. Katila, and T. N. Gia, "A novel Internet-of-Drones and blockchain-based system architecture for search and rescue," arXiv, 2021, doi: 10.48550/ARXIV.2108.00694.

[61] Y. Gao, Y. Liu, Q. Wen, H. Lin, and Y. Chen, "Secure drone network edge service architecture guaranteed by DAG-based blockchain for flying automation under 5G," *Sensors (Basel, Switzerland)*, vol. 20, no. 21, 6209, 2020, doi: 10.3390/s20216209.