

Review Article

A Comprehensive Survey of Low-Complexity High-Security Techniques for UAV Communications

Jolly Ramesh Nikhade¹, Shrikant V. Sonekar²

¹Department of Electronics and Computer Science, RTMNU Nagpur, Maharashtra, India.

²Department of Computer Science and Engineering, J D College of Engineering and Management, Nagpur, Maharashtra, India.

¹Corresponding Author : Jollynikhade21@gmail.com

Received: 05 June 2026

Revised: 02 October 2026

Accepted: 14 October 2026

Published: 28 October 2026

Abstract - Unmanned Aerial Vehicles (UAVs), commonly known as drones, are found to play an important role in the progress of 6G wireless communication technology, including military applications, precision agriculture, intelligent transportation, smart surveillance, and disaster management. UAV-based communication is especially vulnerable to a variety of security risks, including eavesdropping, jamming, spoofing, denial-of-service, and hijacking, because of the wireless channel's intrinsic accessibility and dynamic nature. Strict limitations on energy, compute, latency, and mobility also apply to the UAVs, making the use of traditional sophisticated cryptography methods impractical. Lightweight cryptography, physical layer security, blockchain-based authentication, federated learning, intrusion detection systems, and reinforcement learning-based secure resource allocation are just a few of the low-complexity and high-security solutions for UAV communications that are thoroughly surveyed in this paper. A wide range of UAV designs, including single UAVs, swarm-based UAVs, cellular-connected UAVs, satellite-assisted UAVs, and ad hoc UAV networks, are thoroughly covered in the survey. To offer a cohesive evaluation viewpoint, the performance metrics—such as energy consumption, latency, throughput, dependability, secrecy rate, computational complexity, and packet delivery ratio—are also included. This study provides the reader with organized data on the design of UAV communication systems that are safe, scalable, and energy-efficient for usage in upcoming wireless networks.

Keywords - Unmanned Aerial Vehicles, Physical Layer Security, Satellite-Assisted UAV, Blockchain-based authentication, and Secrecy rate.

1. Introduction

UAVs have been highlighted as critical facilitators of future wireless communication systems, aiding as aerial relays, flying base stations, and mobile edge computing nodes in beyond-5G and 6G networks [1-3]. UAVs are highly useful for disaster relief, smart city surveillance, intelligent transportation systems, military surveillance, and Internet of Things applications because of their rapid deployment, adaptable coverage, and enhanced line-of-sight communication [4, 5]. However, UAV communication is susceptible to a variety of security risks because wireless communication is broadcast and open, such as snooping, jamming, spoofing, hijacking attempts, and denial-of-service attacks [6, 7].

Furthermore, the high frequency of topology changes, dispersed coordination, and energy restrictions in highly dynamic networks like the Flying Ad Hoc Network (FANET) make UAV communication even more susceptible to impersonation, routing, and Sybil attacks [8, 9]. Thus, an effective UAV security mechanism must not only provide

authentication, confidentiality, and resilience against attacks but also operate with reduced computational and communication overhead. This creates a trade-off between security and efficiency in resource-constrained UAV environments.

However, the traditional cryptographic approaches like RSA and traditional AES-based systems offer high confidentiality and integrity but with significant computational and energy overheads, which make them less desirable for lightweight drone communications [10, 11]. Therefore, recent works have focused on developing low-complexity, high-security solutions specifically for UAV wireless communications [12, 13]. Lightweight cryptographic protocols like Elliptic Curve Cryptography (ECC)-based mutual authentication and hash-based key agreement schemes have shown lower computational complexity and energy overheads [14].

Conversely, Reconfigurable Intelligent Surface (RIS)-assisted secure transmission, secure beamforming,



cooperative jamming, artificial noise injection, and other Physical Layer Security (PLS) techniques have taken advantage of the randomness of wireless channels to increase secrecy capacity with minimal protocol overheads [15, 16]. Blockchain-assisted distributed authentication and trust routing protocols have also been presented to improve decentralized security for UAV swarms and FANETs [17, 18]. Furthermore, to identify hostile activity in real-time with effective communication overheads, Machine Learning (ML)-based intrusion detection and anomaly detection schemes have been utilized more often [19]. Figure 1 displays the overall architecture of UAV communication.

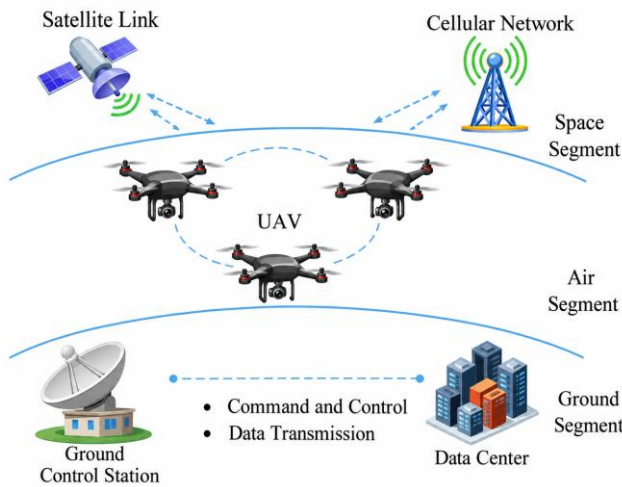


Fig. 1 Overview of UAV communication

Although great progress has been made, the current literature assesses security solutions with isolated performance metrics like secrecy rate, computational complexity, or energy efficiency, without a common assessment framework that combines multiple performance aspects [20]. The methods that ensure strong security might require huge energy and computational demands. Solutions using lightweight mechanisms might provide poor robustness against varied attacks and wireless channel losses.

The diverse variety of UAV applications, like IoT enabled UAV, UAV-assisted 6G systems, FANETs, etc., makes the existing security solutions difficult. The lack of standardized quantitative mechanisms limits the ability of network designers to determine the appropriate security mechanism that provides a balance between security, energy consumption, scalability, robustness, resource consumption, and communication efficiency.

The lack of common assessment criteria makes it challenging to compare and contrast different low-complexity security solutions. Thus, it is necessary to conduct a thorough survey of recent advances in low-complexity high-security methods for UAV wireless communications. To address this research gap, this study presents a quantitative evaluation

framework for various UAV application settings. However, the development of a novel Drone Security Rank Metric that considers security strength, computational complexity, latency, scalability, energy efficiency, and robustness against wireless channel impairments is proposed. By integrating these factors, the study systematically compares various UAV security mechanisms.

This can serve as a methodical, quantitative platform for evaluating and selecting the most effective security measures in future UAV-assisted wireless communications. This is best suited for practical applications where UAV security is not optimized independently of energy, latency, network scalability, and processing capability.

The contributions of this review are discussed as follows: recent UAV security mechanisms are analyzed with the emphasis on providing low complexity and high security. Thus, it is suited for resource-constrained UAV applications. The security and efficiency trade-off between existing approaches is examined to show the practical limitations and trade-offs. The development of a unified ranking metric based on multiple criteria to rank the security mechanisms irrespective of common performance metrics.

The metric provides a basis for selecting the appropriate security mechanism for varied UAV-assisted communication scenarios. The proposed review bridges the gap between practical deployment and security effectiveness in UAV environments by jointly considering the constraints. Thus, the proposed review provides an effective security solution for developing resource-efficient UAV communication systems.

2. Existing Surveys: Scope and Limitations

Some of the recent related studies are surveyed and described in the following section:

Hassija et al. [21] looked at security-critical drone applications and the primary communication dangers they face, including DoS, Man in the Middle, and De Authentication assaults. The methods investigated include Software Defined Networks (SDN) for centralized traffic control, Blockchain for tamper-proof data storage, ML for safe routing and hostile drone detection, and Fog/Edge computing to offload compute closer to drones. However, the limitations noted are that drones are highly resource-constrained, making heavy security algorithms impractical. Scalability, latency, and integration complexity remain challenges when deploying these emerging technologies together.

Trinh et al. [22] reviewed security-critical drone applications in agriculture and focused on communication challenges such as limited range, energy constraints, propagation losses, and latency. The limitations identified are persistent issues in energy management, coverage optimization, and scalability, which hinder large-scale

deployment despite the potential opportunities highlighted. As a result, this integrated study provides a systematic overview of the most recent expansions in drone-assisted agricultural communication systems research.

Ballestrin et al. [23] examined drone-assisted WSNs in precision agriculture with an emphasis on communication issues, including latency, energy efficiency, range, and propagation losses. After screening, 64 relevant papers were discovered.

Notwithstanding the encouraging prospects shown, the constraints include enduring problems with energy management, coverage optimization, and scalability that impede widespread rural implementation. Overall, the study offers a well-organized summary of recent work and potential directions for drone-assisted agricultural communication systems.

Sarkar et al. [24] examined lightweight security solutions for UAV communication and stressed the need for energy-efficient methods because drones have limited resources and depend on open wireless channels. The lack of defined frameworks for post-quantum cryptography in UAV swarms, difficulties with safe rekeying while in flight, and resistance to cross-layer attacks are some of the concerns brought forth. The study provides a comparison of encryption and key distribution methods while highlighting significant research gaps for future UAV security designs.

A study of security issues in the Internet of Drones (IoD) with a focus on access control and authentication in dynamic, heterogeneous networks was provided by Al Majmaie et al. [25]. The dataset was created by thoroughly analyzing cutting-edge PUF-based authentication frameworks and evaluating their resistance to node impersonation, spoofing, and replay attacks.

The limitations mentioned are the environmental sensitivity of PUFs and their vulnerability to modeling attacks, which could compromise reliability. Overall, the results show that PUF-authenticated IoD devices greatly improve security and trust, providing a scalable, resource-efficient alternative to traditional cryptographic techniques.

Dixit et al. [26] suggested a MAVShield, a novel cipher integrated into the MAVLink protocol to secure UAV-GCS communication. This study compared encryption techniques against the conventional unencrypted MAVLink protocol using a real drone testbed dataset. However, there are still issues with algorithm scalability over various UAV platforms, additional energy and area overheads, and possible trade-offs between security strength and real-time speed. For UAV deployments, MAVShield exhibits strong security and effective resource utilization.

Aldossary et al. [27] introduced the Cross-Layer Convolutional Attention Network (CLCAN), a novel intrusion detection method for IoD security. To solve problems with dynamic, high-dimensional transmission data, class imbalance, and inadequate anomaly detection, the system incorporates multi-scale convolution, contextual attention, and adaptive resampling.

This achieves 98.7% recall, 98.4% accuracy, and 98.1% F1-score, outperforming CNN, LSTM, and XGBoost in processing time. Limitations include potential scalability issues for larger datasets, dependency on preprocessing quality, and the need for further validation across diverse IoD environments.

Al-Kamali et al. [28] suggested a novel UAV placement strategy based on spatial threat exclusion. Simulation datasets that mimic single- and multi-threat situations under conservative coverage-edge circumstances are used to verify the technique.

Compared with optimal-placement and PSO baselines, it regularly achieves positive secrecy rates and energy savings, demonstrating strong performance. Nevertheless, there are several drawbacks, such as reliance on simulation assumptions, possible scalability problems in extremely dense networks, and the requirement for further validation in actual UAV installations.

Farajijalal et al. [29] suggested UAV emergency recovery technologies and integrated strategies to improve safety during malfunctions in densely populated locations. They examined datasets of UAV recovery techniques, including parachutes, airbags, software-based, and hybrid systems, for both fixed-wing and multirotor aircraft. Nevertheless, there are still issues with increased payload weight, deployment dependability in a variety of scenarios, and regulatory uniformity among UAV kinds and missions.

Kumar et al. [30] examined a systematic review of UAV-based surveillance technologies, focusing on advancements in AI models, edge computing, and autonomous navigation to enhance situational awareness and public safety.

The study overcomes challenges of bridging academic research with industry practice, handling latency, and improving energy efficiency by comparing lightweight and full-scale solutions.

It highlights persistent limitations, including privacy concerns, energy constraints, and scalability issues in real-time deployments. Overall, the review provides actionable recommendations for researchers, developers, and regulators to design intelligent, reliable, and scalable UAV surveillance systems. Table 1 describes a review of existing surveys.

Table 1. Survey of existing surveys

Author & Reference	Year	Method	Dataset	Challenges
Hassija et al. [21]	2022	Blockchain, ML, SDN, Fog/Edge computing for UAV security	Conceptual datasets of drone communication flows and traffic patterns	Lacks an integrated security framework; limited quantitative evaluation
Trinh et al. [22]	2025	Drones as mobile data collectors, WSN integration, hybrid architectures, IRSs	Agricultural communication datasets	Insufficient attention to privacy-preserving learning; lack of a survey on a unified framework combining authentication, privacy-preserving encryption, trust management, and AI-based routing.
Ballestrin et al. [23]	2026	Drone-assisted WSNs, hybrid architectures, IRSs	64 screened papers in precision agriculture	The review did not validate an integrated framework that addresses adaptive routing, energy-efficient clustering, privacy preservation, and cross-layer optimization. The paper also insufficiently quantified the energy overhead of security mechanisms and the scalability of routing in large-scale dynamic networks.
Sarkar et al. [24]	2025	Lightweight cryptography (ASCON), post-quantum cryptography, blockchain, PUF-based authentication	Comparative analysis of encryption/key distribution techniques	Lacked a survey on a joint framework performing privacy-preserving learning, adaptive routing, secure aggregation, and cross-layer optimization. The energy and communication overhead of cryptographic mechanisms and distributed learning in large-scale dynamic environments was not quantified.
Al Majmaie et al. [25]	2025	PUF-based authentication frameworks with ML enhancements	Evaluation datasets of PUF resistance to impersonation/spoofing/replay	The review focuses on authentication rather than privacy-preserving routing; environmental sensitivity and vulnerability to attacks are not validated.
Dixit et al. [26]	2025	MAVShield cipher integrated into MAVLink	Real drone testbed dataset	Focused on UAV-GCS security rather than multi-node WSN clustering and routing.
Aldossary et al. [27]	2025	Cross-Layer Convolutional Attention Network (CLCAN)	Real-world drone communication dataset (118,000 records)	The review focused on anomaly detection and did not address privacy-preserving clustering or routing. It also did not address security or the overhead associated with larger networks.
Al-Kamali et al. [28]	2026	UAV placement strategy via spatial threat exclusion	Simulation datasets (single/multi-threat scenarios)	The study focused only on UAV positioning and did not address clustering, multi-hop routing, distributed learning, or privacy preservation. It also did not validate scalability in large-scale WSN environments.
Farajijalal et al. [29]	2025	Emergency recovery systems	UAV recovery datasets (fixed-wing & multirotor)	The review mainly focuses on UAV safety rather than secure and energy-efficient networking. The implications of integrating safety mechanisms remain unexplored.
Kumar et al. [30]	2025	Systematic review of UAV surveillance technologies	Literature and market prototypes	The review analyzed the challenges in efficiency, privacy, latency, etc., individually rather than as an integrated architecture. Further, security and computational overhead are not sufficiently quantified.

The research gaps identified from existing reviews are discussed as follows,

- The existing survey evaluated security using limited parameters such as detection accuracy, secrecy rate, latency, energy consumption, and computational cost.
- The existing reviews identified research challenges through qualitative parameters and do not provide quantitative parameters for evaluating the UAV security.
- Security is rarely evaluated based on computational complexity, scalability, robustness, energy efficiency, etc.

This study's main goal is to provide a thorough overview of high-security, low-complexity UAV communication system strategies. It will discuss the security threats, lightweight security techniques, and other advanced techniques such as blockchain, physical layer security, and Deep Learning (DL) techniques in various types of UAVs.

The aim is to identify the challenges and design a secure, scalable, and energy-efficient network in the context of 6G and beyond 5G networks. The objectives of this research are:

- To offer a comprehensive overview of the latest developments in low-complexity and high-security techniques for UAV communication systems.
- To investigate different UAV communication systems, such as single UAV systems, swarm-based UAVs, cellular-connected UAVs, satellite-assisted UAVs, and flying ad-hoc networks.
- To look at serious security concerns with Unmanned Aerial Vehicles (UAVs), including eavesdropping, jamming, spoofing, denial of service, and hijacking.
- To investigate lightweight cryptography and physical layer techniques for UAVs.
- To investigate blockchain, federated learning, and DL techniques for secure UAVs.
- To evaluate UAVs using key performance parameters such as energy efficiency, latency, throughput, reliability, secrecy rate, computational complexity, and packet delivery ratio.
- To research UAVs in order to identify areas for development and potential paths for safe UAVs beyond 5G and 6G networks.

From analysis of the available review articles, the following research questions were addressed in this review:

- What are the major security threats for UAV communication systems?
- What low-complexity security techniques can be used for UAV systems, considering their resource constraints?
- How can physical layer security improve the secrecy of UAV wireless networks?
- How can blockchain technology be used to improve the authentication, trust management, and data integrity of UAV networks?

- What is the role of DL and federated learning techniques for intrusion detection and resource allocation for UAV systems?
- How do UAV communication architectures impact the security of the system?
- What are the major performance parameters for UAV security systems?
- What are the current research challenges and future directions for UAV communication systems for beyond-5G and 6G wireless networks?

This is how the remainder of the paper is organized. The associated work is introduced in Section 2, where the previously recommended methods are examined critically. Section 3 describes the review methodology, including the systematic search process, criteria for inclusion and exclusion, and the PRISMA-based article selection process for gathering the relevant literature. Section 4 presents several UAV communication architectures. Section 5 describes the blockchain-based UAV-related approaches. Section 6 introduces various security threats in UAV communication. Sections 7 and 8 describe the performance and comparative analysis of UAV communication. Section 9 illustrates the challenges in UAVs. Section 10 shows the future research directions. Finally, Section 11 describes the conclusion.

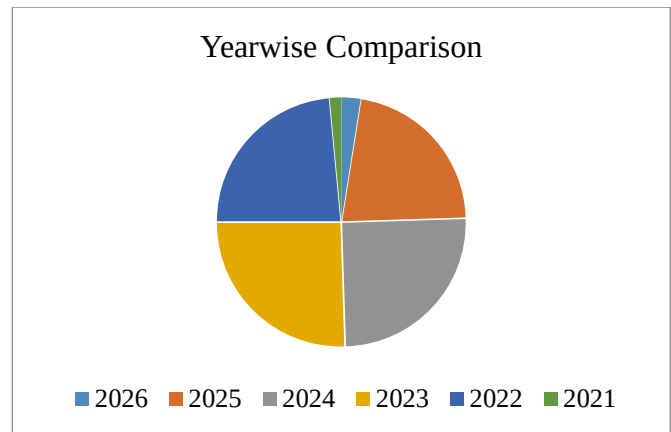


Fig. 2 Analysis of year-wise article selection

3. Review Methodology and Search Strategy

3.1. Review Methodology

This section will deal with the analytical and reporting methods that are often followed by researchers while conducting systematic literature reviews. This systematic review of accessible literature focuses especially on the synthesis of quantitative studies. The selection criteria followed in this study are justified based on the data collected. The technique used in this systematic review could be covered in the parts that follow. The key papers for this study were chosen using strict selection criteria, which explains the research methodology. This systematic review's approach consists of planning, carrying out, and analyzing the findings. The annual selection of papers is shown in Figure 2.

3.2. Search Strategy

The search strategy was planned to retrieve relevant and high-quality research articles related to low-complexity high-security techniques for UAV communications and a novel drone security rank metric. The first step in the search approach was to go through electronic scientific resources, including Wiley Online Library, Google Scholar, ScienceDirect, IEEE Xplore, SpringerLink, and ACM Digital Library. To ensure contemporary technology breakthroughs, the literature search was mostly focused on recent publications from 2021 to 2026. A list of structured keywords and Boolean search combinations was employed to search for relevant studies. The list of keywords included: “UAV”, “Blockchain”, “UAV communication”, “Ad hoc networks”, “deep learning”, “Cellular connected UAV”, “Physical layer security”, and “UAV swarm security”. The keywords were combined using Boolean operators such as: (UAV AND Blockchain AND UAV communication), (UAV AND Physical layer security AND Ad hoc networks), (Cellular connected UAV AND Deep learning), and (UAV swarm security AND blockchain). Duplicated papers were eliminated, and title and abstract searches were conducted to shortlist relevant studies. Only

peer-reviewed journal articles and high-quality conference papers available in English were considered.

3.3. Inclusion and Exclusion Criteria

The first phase should cover a number of questions that must be answered following the systematic review and the criteria for inclusion, exclusion, and quality. Table 2 illustrates the criteria of Inclusion (IC) and Exclusion (EC). Figure 3 describes the number of articles selected during each stage of the selection process.

Table 2. Analysis of Inclusion and Exclusion criteria

Inclusion Criteria	Exclusion Criteria
Searched in Title	Not searched in title
Published in English Language	Not published in the English Language
Studies from Worldwide	-
Published between 2021 and 2026	Published before 2021
Works using DL, ML, and blockchain as the primary technique	Works not using DL, ML, and Blockchain as the secondary technique

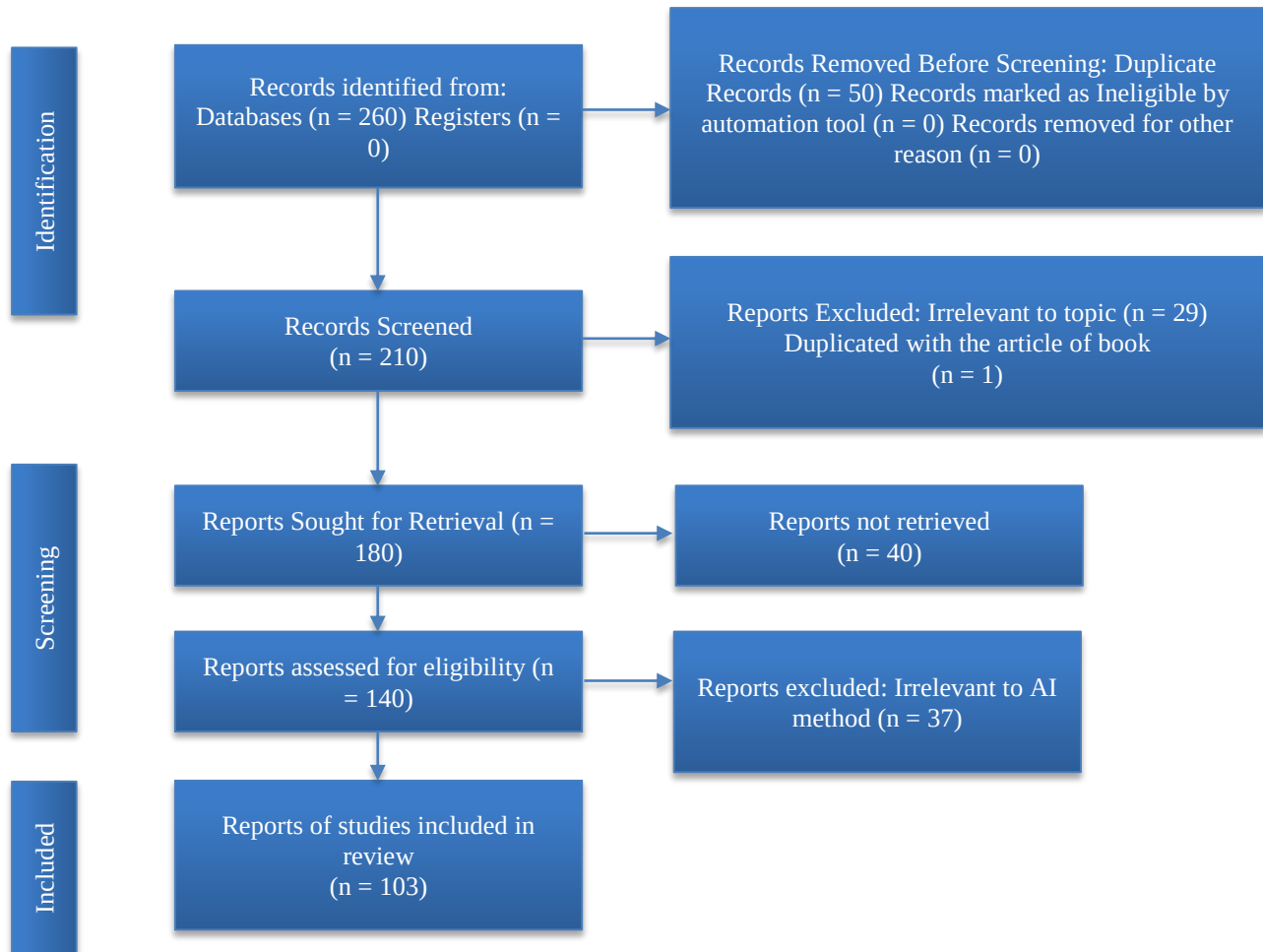


Fig. 3 PRISMA plot

4. UAV Communication Architectures

The communication architectures for UAVs describe how drones communicate with ground stations, other drones, and network systems. The communication architectures for drones include direct communication between the drones and the ground stations (UAV-to-Ground, U2G), direct communication between drones (UAV-to-UAV, U2U), and multi-hop Flying Ad-hoc Networks for swarm drones. In some advanced communication systems, drones communicate with cellular networks (4G/5G/6G networks) and satellite networks to cover wide areas and communicate beyond line-of-sight. The effectiveness of a UAV communication system is greatly influenced by the communication architecture.

4.1. Single UAV System

In a highly dynamic context of cache-enabled UAVs serving as aerial base stations for terrestrial users, Muslih et al. [31] investigated the caching problem. In order to diminish the complete transmission delays of the necessary data, UAVs must exchange their caches and modify their locations accordingly. Using ultra-wideband properties and frequency non-stationarity, Hua et al. [32] demonstrated a three-dimensional model communication channel named UAV-to-Ground (U2G). To accurately depict the situation, the 3D model of the U2G channels includes both large-scale and small-scale fading components, such as the UAV posture matrix and bandwidth-dependent route numbers. Channel hardening, UAV 3D motions, and posture variation effects are some of the UWB characteristics of the U2G channels.

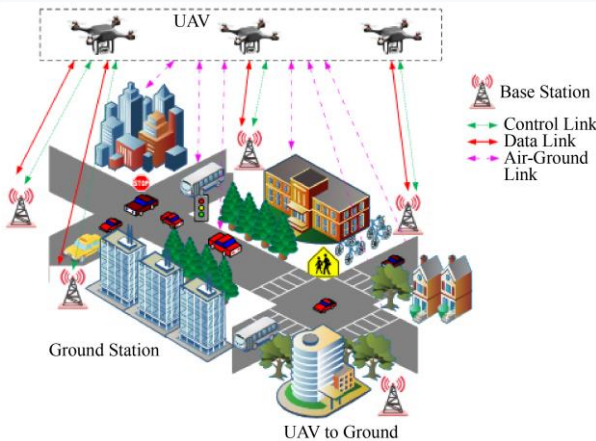


Fig. 4 UAV to Ground communication architecture

The authors Jiang et al. [33] presented a 3D physics-based, dual Reconfigurable Intelligent Surface (RIS)-aided MIMO stochastic channel model for communication systems between an Unmanned Aerial Vehicle (UAV) and a ground receiver. To assist the UAV transmitter in the aforementioned situation in reflecting its signals towards the GR, the double RIS might be positioned on the building's surface. The broadcasts can also be improved via the RIS's beamforming capacity. To show how U2G communication systems are

affected by both large-scale and small-scale fading, the provided channel model is used to compute the route power gains of UAV and GR between diverse propagation connections. The U2G transmission is shown in Figure 4.

Zhang et al. [34] give a novel model based on the characteristics of clusters produced by the ML approach, in addition to offering a four-state Markov chain to characterize the channel clusters. For the U2G MIMO channel, Hua et al. [35] created a non-stationary hybrid model in three dimensions that accounts for both small-scale and large-scale fading. Incorporating the 3D UAV trajectory and posture, the proposed model accounts for the Fuselage Scattering Effect (FSE), Posture Variation Fading (PVF), and other distinctive features of the U2G channel. Dabiri et al. [36] introduced a Modulating Retro-Reflector (MRR)-based FSO communication system for UAV-to-ground communication. As the next sections will demonstrate, the accuracy of the tracking errors has a significant influence on the system's performance. Some factors are considered while assessing the MRR-based UAV FSO channel, including tracking system faults, UAV orientation, length, and height; optical beam divergence; atmospheric turbulence; and optical losses for the double-pass channels. Potential benefits of deploying UAVs based on MRR for FSO communication could be assessed.

4.2. Swarm-based UAV

Self-Adaptive Intrusion Detection (SID)-UAV is a method presented by Fotohi et al. [37] that is resistant to malicious UAV assaults that might compromise UAV-to-UAV communications. Using a self-matching algorithm to find the safest route among UAVs is the foundation of the approach. The many steps that comprise the solution include the information database registration phase, the destructive UAV reaction stage, the route finding and study phase, and the decision-making phase. Zeng et al. [38] developed an arbitrary-elevation two-cylinder reference model for MIMO air-to-air communication in UAV channels. Besides the Line-of-Sight (LoS), the other rays that are considered are the Single-Bounced at the Transmitter (SBT), Double-Bounced (DB), and Single-Bounced at the Receiver (SBR). As a result, it is highly versatile in a range of UAV-to-UAV communication situations. Figure 5 shows how UAVs communicate with one another.



Fig. 5 UAV-UAV communication

Li et al. [39] offer a hierarchical network architecture based on UAV swarms for coordinating the scheduling of sensing, processing, and communication resources. It is especially suggested that the computing groups, which are composed of several UAVs, perform image processing jobs in a pipeline manner in order to maximize the employment of computing resources. A two-layer multi-edge complex network model that considers the swarm's cooperation and communication status for the specific mission is used by Yang et al. [40] to explain the UAV swarm. The function layer and the communication layer make up the model. The UAV swarm model was first presented by Wen et al. [41]. A description of the distributed target-fencing problem is given. Second, based on the notion that certain UAVs are unable to locate the moving target in real time, a Distributed Position Observer (DPO) is presented.

4.3. Cellular-Connected UAVs

A cellular-connected UAV system that achieves accurate detection through cooperative detection among the connected UAV and the base station was presented by Wang et al. [42]. Using deep and ensemble learning, Dang et al. showed how to identify GPS spoofing for cellular-connected UAVs [43]. By arranging mission completion time, UAV trajectories, and communication base station affiliations, Zhan et al. [44] aim to lower the energy consumption of cellular-connected UAVs. Maintaining enough communication contact with the base cellular network is essential when the UAV is in flight. All the practical elements of air-ground communication models, including the base station's antenna design, interference from unrelated base stations, the surrounding environment, and the UAV's energy consumption, are taken into consideration while designing an optimization problem. Maintaining enough communication contact with the base cellular network is essential when the UAV is in flight. An optimization difficult is created that takes into account all the practical features of air-ground communication models, such as the antenna design of the base station, interference from unrelated base stations, the surrounding environment, and the energy consumption of the UAV during flight. Figure 6 shows the architecture of cellular-connected UAVs.

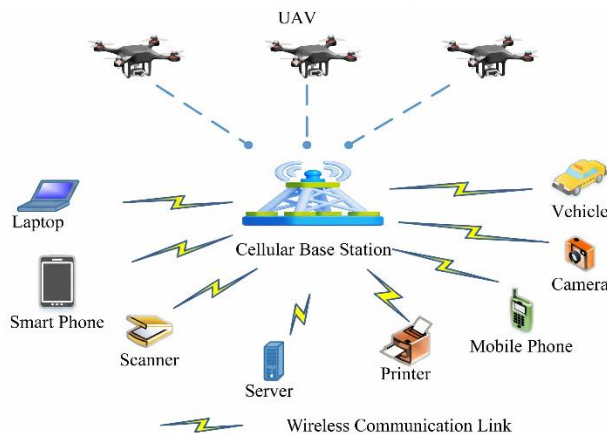


Fig. 6 Cellular-Connected UAVs

Meer et al. [45] suggested two approaches to achieve this goal: 1) A deep Q-network-based model-free method to reduce handovers while preserving high service availability. 2) A model-based approach to service availability-aware Mobility Robustness Optimization (MRO) that aims to provide high service availability with minimal handovers by modifying changeover control parameters. The authors of the study by Dang et al. [46] identify and resist efforts at GPS spoofing in UAVs that are linked to cellular networks by utilizing machine learning algorithms and a 3D radio map. Using deterministic channel models, Kriging algorithms, and ray tracing techniques, the theoretical 3D radio map is generated by the edge UAV flight controller.

4.4. Satellite-Assisted UAV Communication

Liang et al. [47] analyze a satellite UAV-assisted data gathering system in which a remote control center uses a satellite channel to operate the UAV. A reference trajectory is initially created for the UAV based on its hovering locations in order to optimize its Energy Efficiency (EE). Next, the trajectory tracking control's communication and state sensing techniques' power allocation is optimized. Nafea et al. [48] created a unique concept for satellite-assisted UAVs-enabled vehicle networks called Resource Allocation and Edge Computing for Dual Hop Communication (RAEDH). Dual-hop communication between cars and UAVs, resource allocation for vehicles and UAVs, and UAV-assisted mobile computing are the key elements of this innovative concept. Figure 7 depicts the architecture of satellite-to-UAV communication.

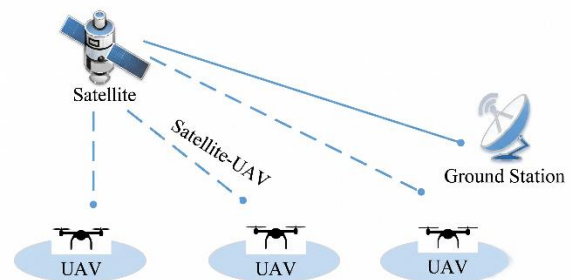


Fig. 7 Satellite-UAV communication

A new approach to Multi-Objective Optimization in Satellite Assisted UAVs (MO-SAUVs) was proposed by Jubair et al. [49] employing an Improved Ant Colony Optimization (IACO) method. Zhou et al. [50] discussed the use of Unmanned Aerial Vehicles (UAVs) and satellites for data collection in IoRT networks. After gathering data from SNs, the UAV determines whether to send it straight to the data processing center or via a satellite channel. Mohamed et al. [51] provide a novel integration technique among a Low-Earth-Orbit Satellite (LEO Sat) and a UAV to assist users in a disaster area. The LEO Sat provides UAVs with backhaul access to the GBS, and many UAVs are dispatched to completely cover each victim.

4.5. Ad-Hoc UAV Networks

An Intelligent Clustering Routing Approach for UANETs (ICRA) was introduced by Guo et al. [52]. The three modules that comprise ICRA are routing, clustering, and clustering strategy modification. The clustering module's functionality is determined by each node. To keep the network stable and extend its lifetime in different states, the reinforcement learning-based clustering strategy adjustment module should continuously learn the benefits of using different strategies to determine the nodes' utility in a given network state. The communication architecture of FANETs in SAGINs was examined by Lu et al. [53]. The various routing protocols and their clusters have been described concurrently. For UAV ad hoc networks, Ren et al. [54] presented a K-means online learning routing protocol technique based on a Markov mobility model.

To precisely determine the UAVs' positions, this approach first employs a 3D Gauss-Markov model. In three distinct scenarios, improving mobility, boosting scalability, and expanding space for UAVs in SAR missions, Wheeb et al. [55] evaluated and analyzed the performance of the original and modified 'Optimal Link State Routing protocols' (OLSR) for UAV ad hoc networks. The primary contribution of Uddin et al. [56] was the development of a cooperative MAC protocol featuring an optimal relay selection method, specifically designed for FANETs operating in challenging environments. A realistic network model that accounts for mobility, distance, and SNR forms the foundation of the adaptive back-off approach. To facilitate reliable connections between source and destination nodes, Arafat and his team [57] developed an innovative Q-learning-based Topology-Aware Routing (QTAR) protocol for FANETs. This proposed method enhances routing decisions by considering nodes located two hops away. Figure 8 depicts the UAV Ad-hoc network.

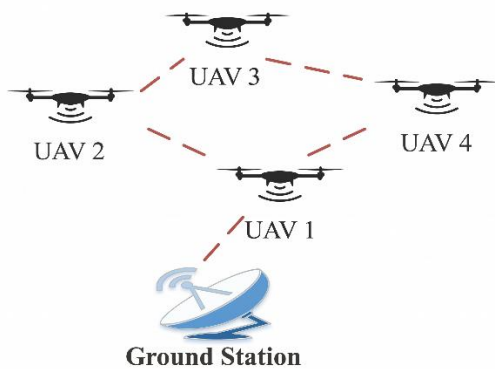


Fig. 8 UAV Ad-Hoc Network

Cui et al. [58] created a Topology-Aware Robust Routing technique based on Adaptive Q-learning (TARRAQ) to make accurate routing decisions while capturing topology changes with the least amount of cost in a distributed and autonomous way. Zhao et al. [59] proposed UAVs that make use of actively

developing unmanned autonomous flight control programs and are provided with radio communication equipment. It has been found to be commercially essential to produce cheap small and micro drones owing to recent developments in embedded systems and the feasible extent of integration. However, the utility of a single UAV is found to be restricted owing to low carrying and cruise capabilities. Jin et al. [60] developed a single UAV that communicates with the ground when operating alone.

High power consumption, a high packet loss rate, and a high propagation delay are found to be the consequences of radio transmission over a long distance. Moreover, the whole communication system becomes immobile if one link fails. Hence, operating together with multiple UAVs forms a network that has greater utility than a single drone. Inter-group communication was the focus of the research conducted by Chandran et al. [61]. The GS does not support intra-group communication within the UAV ad hoc network. Nevertheless, this paradigm lacks resilience due to its semi-centralization. The study by Lakhwani et al. [62] examined all of the group's linked backbone UAVs that are part of the top layer. Nevertheless, only one of the group's primary UAVs is linked to the GS.

5. Blockchain-based UAV Security

Intelligence distillation utilizing ML-based techniques is crucial in large-scale, dynamic, heterogeneous, and complex UAV-based MEC-enabled IoT networks, according to previous studies. However, by guaranteeing decentralization, immutability, transparency, and safe and authentic data, the creation of blockchain has transformed the security industry. This section highlights current research that focuses on blockchain, machine learning, or both. The FEEL approach was employed in the study reported in Feng et al. [63] to ensure data privacy and prevent UAVs from sharing raw data. Both computing power and wireless bandwidth were allocated simultaneously. A DRL-based Deep Deterministic Policy Gradient (DDPG) technique, first presented by Kaewdornhan et al. [64], was used to create and solve a non-convex optimization problem. In order to optimize the computation offloading process, bandwidth allocation, and the safe and environmentally friendly design of the MEC network, Gao et al. [65] combined the latest findings in Deep Neural Networks (DNNs) with those in RL-based Q-learning algorithms to create an effective Deep Q-network (DQN) algorithm. To address the issue of partial compute offloading in UAV-assisted MEC-enabled IoT networks, Gao et al. [66] presented an online Differential Privacy-based Deep Q-Learning (DP-DQL) method to ensure privacy. To safeguard the offloading preference, this strategy used the Prioritized Experience Replay method, as explained by Luo et al. [67]. This approach accelerates the learning mechanism and DQL, which represent the main learning process. A safe offloading method for multiple UAVs in MEC-enabled networks was shown by Lu et al. [68].

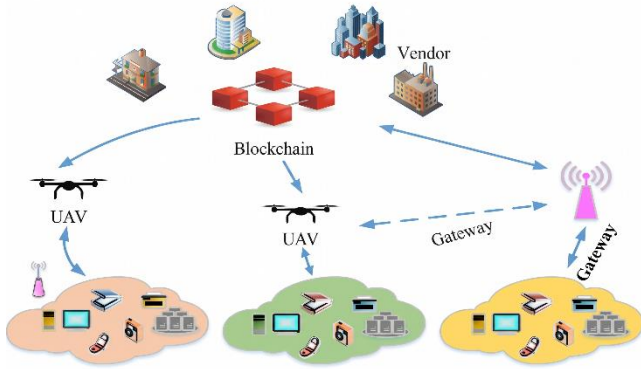


Fig. 9 Blockchain-based UAV security

Figure 9 illustrates the blockchain-based UAV security. A decentralized Blockchain-based FL solution was given in Fan et al. [69], where the UAVs learned the data locally to overcome some security and privacy concerns. The FL method and blockchain were successfully combined in Islam et al. [70] to create FBI, a secure drone-assisted IoT architecture for data aggregation. IoT devices in outlying locations were able to avoid connection problems and keep end-to-end communication going by using drones as intermediary nodes in conjunction with edge servers. For remote locations inaccessible to traditional cellular networks,

Heidari et al. [71] looked into the possibility of using drones to increase the radio coverage of an IoT network that is enabled by MEC.

The smart contracts were tested on the Ropsten test network, which is based on Ethereum. Solidity, a high-level object-oriented programming language, was used for this. The STRIDE threat model developed by Yarden et al. [72] is used to identify security risks. UAVs have recently been acknowledged as an affordable, sustainable, and cost-effective alternative to traditional ground vehicles in parcel delivery systems, according to Stuiwe et al. [73]. An optimal technique for resource pricing and trading was proposed by Xu et al. [74] for a network that is enabled by Unmanned Aerial Vehicles (UAVs) and uses MEC. Client service quality was continuously improved by adjusting the distribution of edge computing resources across neighboring UAVs and Edge Computing Stations (ECSs). A Stackelberg dynamic game was used by Wang et al. [75] to explain how edge computing resources are traded. ECSs and UAVs were seen as the leaders and followers in the development of the optimization problem. Karmakar et al. [76] presented a blockchain-based data collecting system and investigated using a swarm of UAVs to gather data from IoT devices. The blockchain-based security strategy for UAV communication is contrasted in Table 3.

Table 3. Comparative analysis of blockchain-based security approaches in UAV communication

Ref. No	Author (Year)	Technique / Approach	Application	Key Contribution	Limitations
[63]	Feng et al. (2022)	Federated Edge Learning (FEEL)	UAV-assisted MEC	Decentralized training with joint resource allocation	Non-convex optimization complexity
[64]	Kaewdornhan et al. (2024)	DRL (DDPG)	Energy management in UAV systems	Deep RL for predictive energy optimization	Training overhead, convergence issues
[65]	Gao et al. (2024)	Deep Q-Network (DQN)	Secure UAV-enabled MEC	Joint trajectory & resource optimization	High computational training cost
[66]	Gao et al. (2025)	Differential Privacy-based DQL	Privacy-preserving offloading	Secure computation offloading with DP noise	Accuracy vs privacy trade-off
[67]	Luo et al. (2024)	Prioritized Experience Replay (TD3)	UAV path planning	Faster RL convergence for dynamic routing	Requires careful parameter tuning
[68]	Lu et al. (2022)	Secure multi-UAV transmission (RL-based)	MEC-enabled UAV networks	Artificial noise & optimal UAV placement	LoS assumption limits realism
[69]	Fan et al. (2023)	Blockchain-based Federated Learning	Decentralized UAV learning	Anonymous & secure FL authentication	Blockchain latency overhead
[70]	Islam et al. (2022)	FL + blockchain (FBI Framework)	Drone-assisted IoT	Secure data accumulation & decentralized storage	Scalability challenges
[71]	Heidari et al. (2023)	Private blockchain + IDS	UAV-assisted IoT	Secure offloading with smart contracts	Blockchain processing delay

[72]	Yerden et al. (2025)	STRIDE Threat Model	UAV threat identification	Structured UAV threat modeling	Conceptual, limited performance analysis
[73]	Stuive et al. (2024)	Secure UAV logistics design	UAV parcel delivery	Secure urban airspace network modeling	Focus on logistics, not communication security
[74]	Xu et al. (2024)	Blockchain-based resource trading	Multi-UAV MEC	Dynamic edge resource pricing	Transaction latency
[75]	Wang et al. (2024)	Stackelberg Game + blockchain	UAV-MEC resource allocation	Game-theoretic optimization	Leader-follower assumption
[76]	Karmakar et al. (2023)	Blockchain-based clustering authentication	UAV swarms	Distributed secure clustering protocol	Energy overhead in large swarms
Proposed review		UAV security techniques analysis	UAV, FANET, IoT and UAV-assisted communication	Unified framework for comparing and ranking heterogeneous UAV security solutions	Designed to balance both security and resource requirements rather than evaluating security.

6. Security Threats in UAV Communication

6.1. Eavesdropping

The flow of private information between the legal nodes is being intercepted by aerial and ground intruders, which is a regular security issue. This security vulnerability affects private data such as access codes, control instructions, navigational information, etc., as well as access to the source and destination nodes.

FANETS and cellular communication, for example, are subject to intruder assaults that are difficult to track since they do not broadcast any signals and hence have a negative impact on network security [77]. Additional encryption can prevent eavesdropping, and more sophisticated security mechanisms in the PHY layer can be a universal solution.

6.2. Jamming

The communication channels between the authorized nodes are disrupted by the jamming assault. The genuine nodes' ability to share information is hampered by this interference. In a jamming attack, the attacker transmits interference signals to the legitimate node [78]. The genuine node's SINR is disturbed by this influence. The original message was not received as intended as a result. The respondent takes a while to recognize the response. An intruder, either airborne or terrestrial, might take advantage of the easily accessible A2G link of UAVs and their radial coverage to jam the communication link. In the publication [79], a report on GPS jamming was discussed. In the paper, the GPS jamming was discussed, and the crashing of the small drone was analyzed. To calculate the likelihood of invasions, a number of techniques have been suggested. A strong defense against the jamming attack can be achieved by increasing the SNR. However, the UAV has an energy constraint, which limits the increase in the transmitted signal. In order to control the interference signals, scientists investigated UAV-specific jammers for generating energy-constrained waveforms [80].

6.3. Denial of Service Assault

Network congestion may result from the adversaries sending copies of several service interruptions to the genuine network's wireless access point in this type of attack. Service requests, acknowledgments, or adverts from unexpected sources can all be examples of service interruptions [81]. This might result in a delay in the terrestrial base station's ability to provide the UAVs with control and command responses. The genuine UAV nodes may likewise be the target of a security assault by the attacker. Consequently, the service will no longer be provided by the authorized service provider. Malicious UAVs may use the powerful LoS link to increase their radial coverage and launch a denial-of-service attack. DDoS attacks, which target a single target by coordinating several systems, are one type of Denial-Of-Service attack. Using repeated copies of the requests to gain control of the UAV, an experiment was conducted in [82] to demonstrate that Telnet software is utilized to block the UAV controller network link during the AR Discovery process. The de-authentication assault, which aims to authenticate the genuine user, might come after the DoS or DDoS attack.

6.4. Hijacking

Hijacking is the term used to describe gaining complete control. In other words, an attacker gains complete access to the wireless connection after taking it over. For instance, Wi-Fi makes it easier for the GCS and the UAV nodes to communicate and access each other. To begin the hijacking attempt, an attacker may detach the drone from the connected GCS using de-authentication management frames. Additionally, it may use IEEE 802.11 protocols to remotely operate the drone. A number of security measures have been put in place to stop an attacker from initiating a de-authentication attack. Detection mechanisms and encryption of the frames have been made possible. Furthermore, the authors in [83] have suggested the WPA2 encryption utilizing IEEE 802.11i-2004 to stop an attacker from starting a hijacking attempt that provides the right key length.

Nonetheless, the authors in [84] have shown that an additional level of security is provided to the attacker by encryption employing a dynamic secret key. The drone connected to the network may also be safer if the Wi-Fi access points' MAC addresses are restricted. Additionally, by blocking the SSID broadcast, IEEE 802.11 protocols can make the Wi-Fi connection secure.

6.5. Spoofing

To compromise data or gain unauthorized access, spoofing attackers insert false identification information into a valid communication channel. To gain access to and control over the source nodes, it employs a strong false misleading signal [85]. Gaining entry to emails, phone conversations, address resolution protocol cache poisoning, and more are examples of common spoofing attacks. However, another common issue with UAVs is GPS spoofing. It is achieved by sending a high-power, illegal signal inside the working frequency band. Therefore, the hacker can use GPS spoofing to change the GPS position, get personal information, or infect the system with a virus. The two most popular spoofing techniques are identity spoofing and Sybil attacks. By using a fictitious MAC or IP address of a real user, the attacker poses as a legitimate user in an identity spoofing attack. Thus, after

gaining illegal access, the hacker may initiate sophisticated operations like DoS and man-in-the-middle attacks. In contrast, Sybil attacks involve a single device acting maliciously by taking on several fake identities of other nodes [86].

7. Performance Evaluation of Existing Studies

The performance of existing studies is analyzed in this section based on the following parameters: energy consumption, latency, throughput, reliability, computational complexity, secrecy rate, and PDR.

7.1. Energy Consumption

The UAV's battery capacity is a crucial component that permits extended operations. It has been noted that as the UAV's weight increases with battery capacity, it requires more power for a given function. The endurance of the UAV with the restricted power supply is still a major concern, despite the fact that power storage systems have significantly improved over the last few decades Yu et al [87]. The UAVs must then be run with little energy usage. Figure 10 shows the energy consumption performance evaluation.

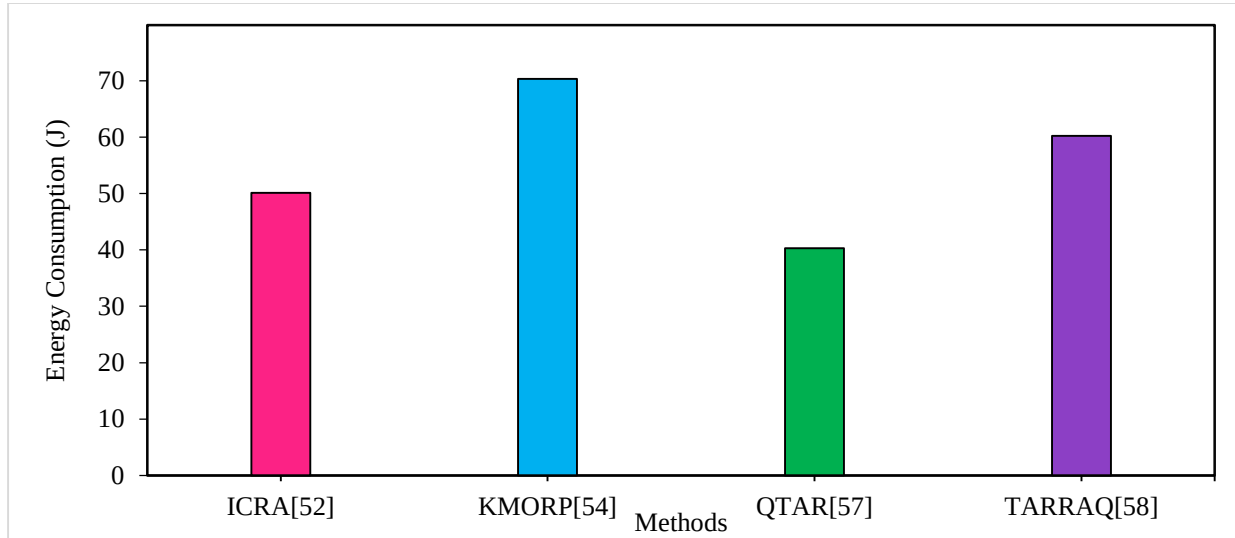


Fig. 10 Performance evaluation of energy consumption

7.2. Latency

In their study, García-Gil et al. [88] tackled the issue of offloading ultra-reliable computations with minimal latency with the help of US aircraft. The study shows that employing UAVs is an issue for ultra-reliable low-latency computation offloading. The admittance rate can be supported to a higher degree by increasing the computing resources, because the tasks can be completed ahead of schedule by making the best use of the existing resources.

The performance evaluation of latency is displayed in Figure 11. To calculate latency, Hossain et al. [89] defined it

as the total time required for a transaction to be verified on a blockchain network. The delay between submitting a transaction and having it verified on the blockchain is known as Latency (L), and it is determined by:

$$L = \frac{B_s}{R} + \frac{N_t T_s}{R} + D_p \quad (1)$$

where N_t is the number of transactions in a block, B_s is the block size, and R is the transmission rate (bandwidth). T_s represents the average transaction size, while D_p represents the network propagation latency.

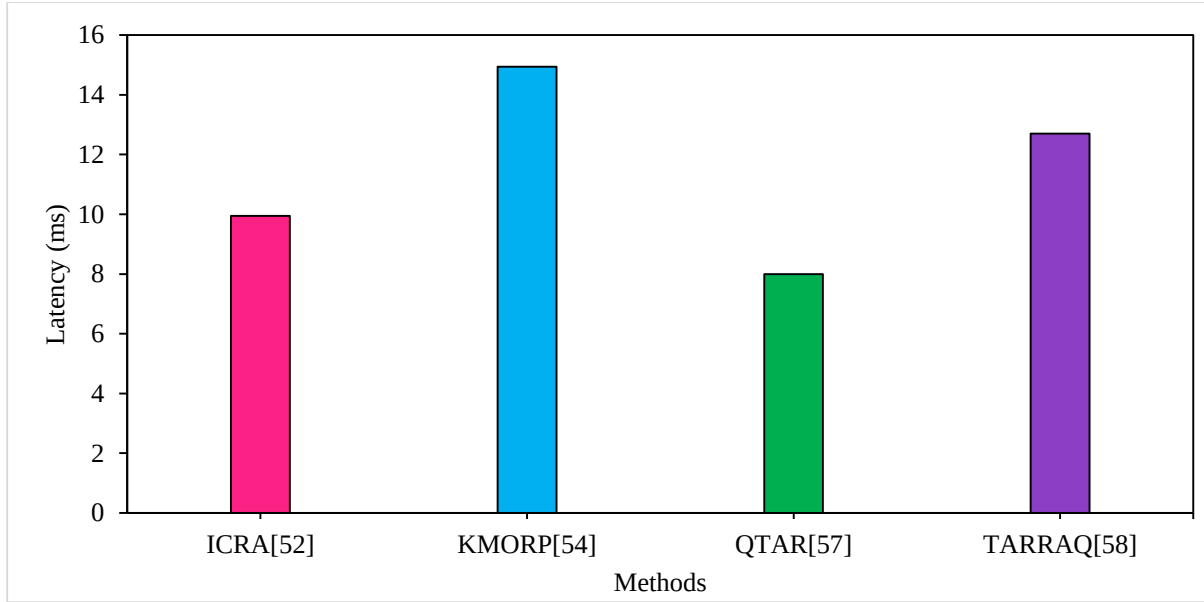


Fig. 11 Performance evaluation of latency

7.3. Throughput

To exploit the general system throughput, the UAV route and Dynamic Time Splitting (DTS) ratio were computed. An optimization problem was formulated by Tran et al. [90] to maximize the total gathered throughput at the destination,

taking into consideration the DTS ratio in each time slot, the maximum speed of the UAV, its path, and the limited flight period. To enhance network performance, Li et al. [91] looked into the matter of deploying a heterogeneous UAV network during a crisis.

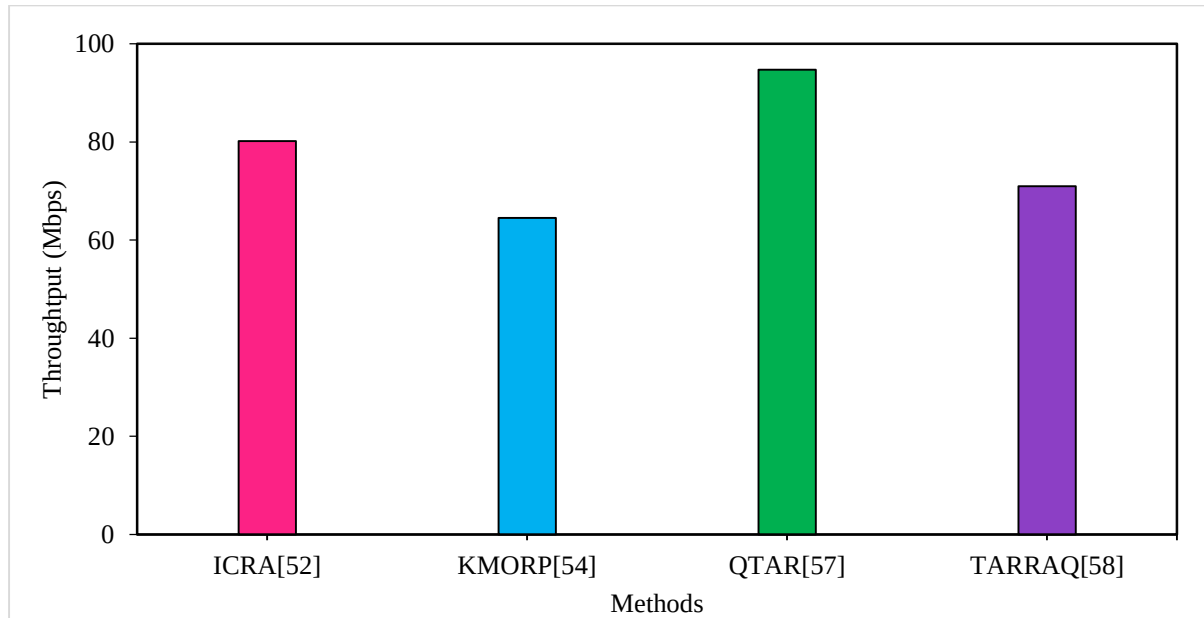


Fig. 12 Performance evaluation of throughput

The performance of the throughput is shown in Figure 12. This determines the blockchain network's overall efficiency, depending on how many transactions it can handle in a second.

The following formula is used to determine throughput [89] (TPS):

$$TPS = \emptyset \times S \quad (2)$$

A blockchain's primary performance metric is transactions per second or TPS. The chance of producing a block $\emptyset$ is multiplied by the number of transactions per block S to determine the TPS.

7.4. Reliability

Hao et al. [92] present a combined optimization problem for work offloading, communication resources, and UAV trajectories while accounting for system dependability to increase the long-term average task success rate. The two components of a system's dependability are transmission

reliability and compute unit reliability. This reliability model can reflect both hardware problems and soft failures by adjusting the failure-rate parameter. Long-term unavailability is frequently caused by equipment malfunctions. The UAV is deemed offline in this scenario and is not given any new missions. Figure 13 displays the reliability performance.

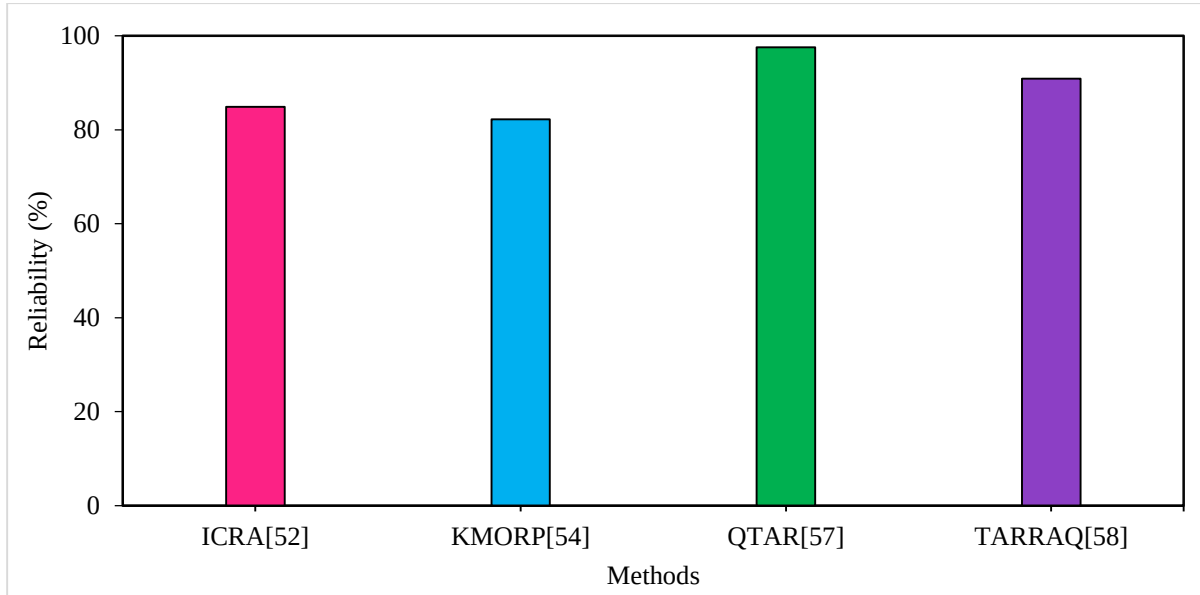


Fig. 13 Performance evaluation of reliability

7.5. Computational Complexity

The necessity to handle massive volumes of heterogeneous data in real-time makes integrating numerous sensors, such as cameras, LiDAR, RADAR, and IMUs,

computationally challenging [93]. The type of sensor directly affects computational complexity. The performance of computational complexity is shown in Figure 14.

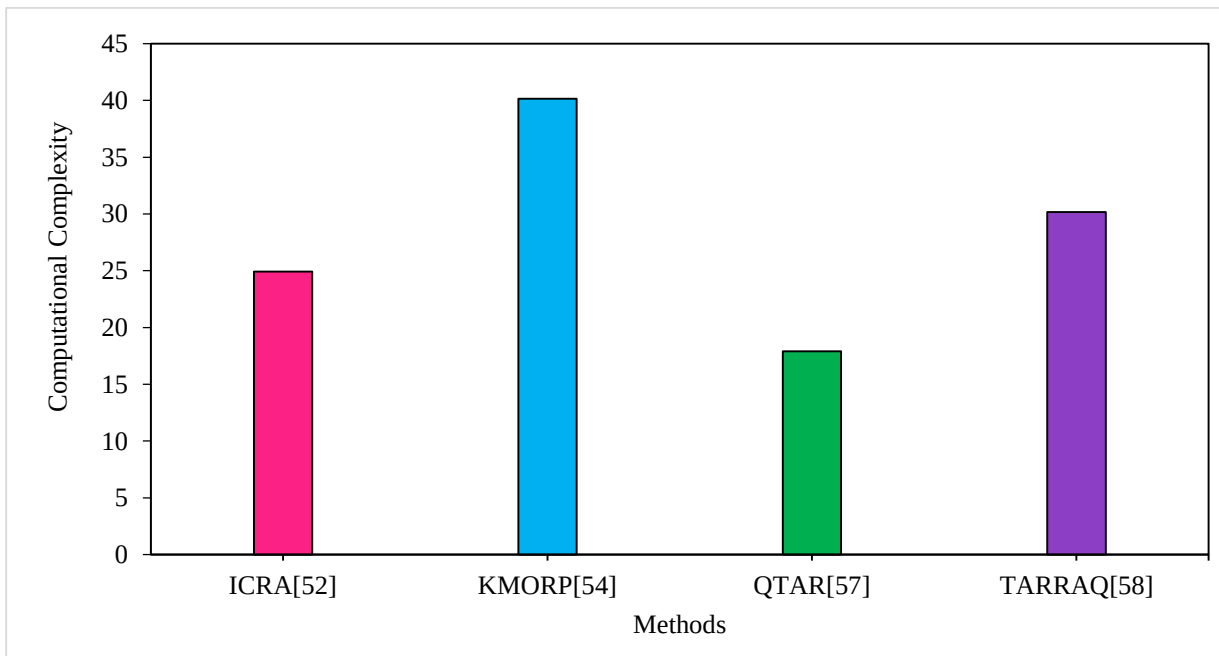


Fig. 14 Performance evaluation of computational complexity

Thus, despite its potentially large volume of information, LiDAR-based approaches can potentially match and exceed the performance of other approaches, for example, Visual SLAM. However, it is important to process these heterogeneous information flows efficiently using sophisticated algorithms, for example, employing DL, Kalman filters, and other recursive filters for reliable multi-modal sensor fusion.

7.6. Secrecy Rate

Secure UAV-assisted communication is necessary for a number of applications, including defense, healthcare monitoring, and mission-critical communication. In order to ensure dependable communication, Pandey et al. [94] have proposed a technique to evaluate the secrecy performance criteria. The difference between the achievable rate of the eavesdropping channel and the feasible rate of the legal channel is known as the Secrecy Rate. R_s . The following is an expression for the Secrecy Rate. R_s [95]:

$$R_s = [R_b - R_w]^+ \quad (3)$$

where

$$[x]^+ = \max[x, 0] \quad (4)$$

$$R_b = \log_2(1 + \gamma_b) \quad (5)$$

$$R_w = \log_2(1 + \gamma_w) \quad (6)$$

The attainable rate of the UAV's legal channel is represented by the Secrecy Rate (R_s), R_b r, formula above. The wiretap channel's attainable rate is shown by R_w . Additionally, γ_b and γ_w and stMoreover, for the instantaneous SINR of the signal received via the wiretap channel and the legal channel, respectively. Figure 15 displays the secrecy rate's performance.

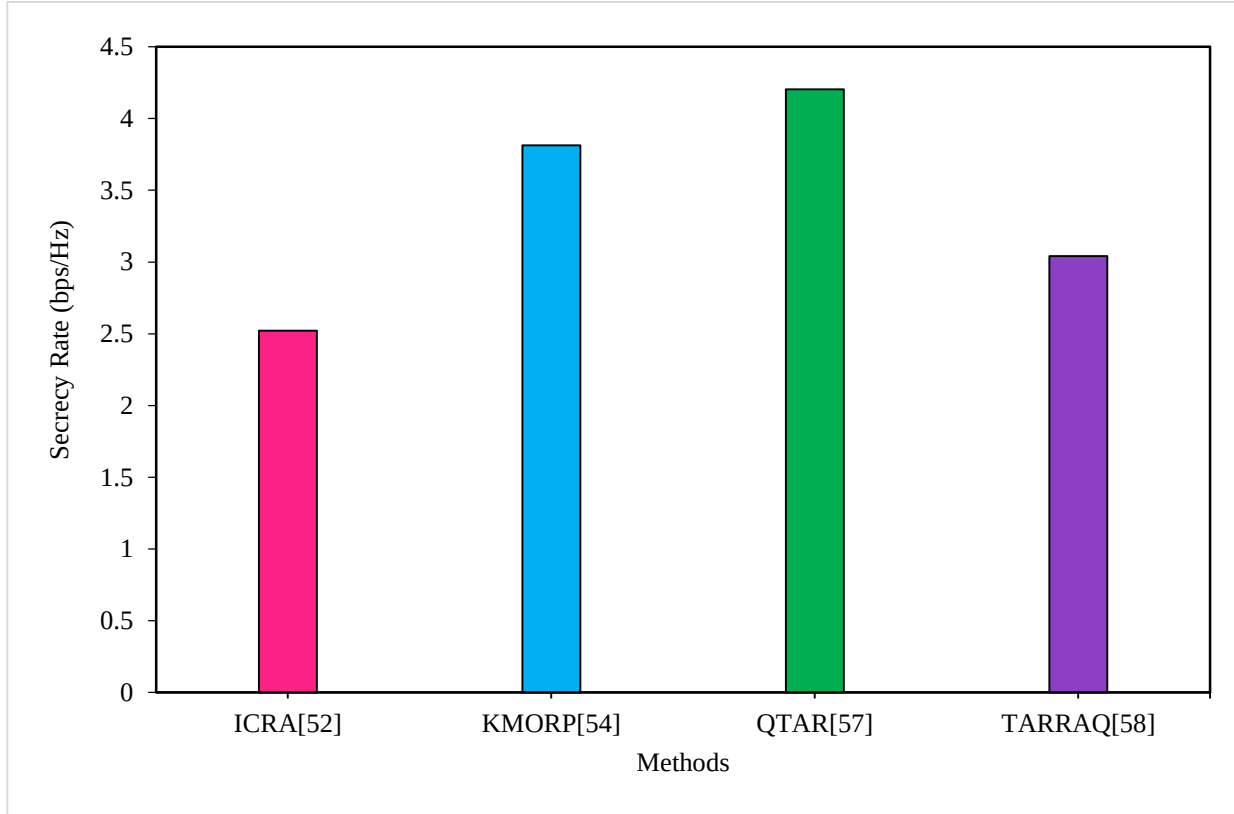


Fig. 15 Performance evaluation of secrecy rate

7.7. Packet Delivery Ratio

The ratio of data packets sent by the source to those received at the destination is displayed by the packet delivery ratio, or PDR. Naser et al. [96] show that the equation below is used as the basis for measuring this parameter.

$$PDR = \frac{R_{pkt}}{T_{pkt}} \quad (7)$$

where, R_{pkt} is the entire data packet received at the destination UAV.

T_{pkt} is the data packet conveyed at the source UAV. The performance of the PDR is shown in Figure 16. The performance values measured are shown in Table 4.

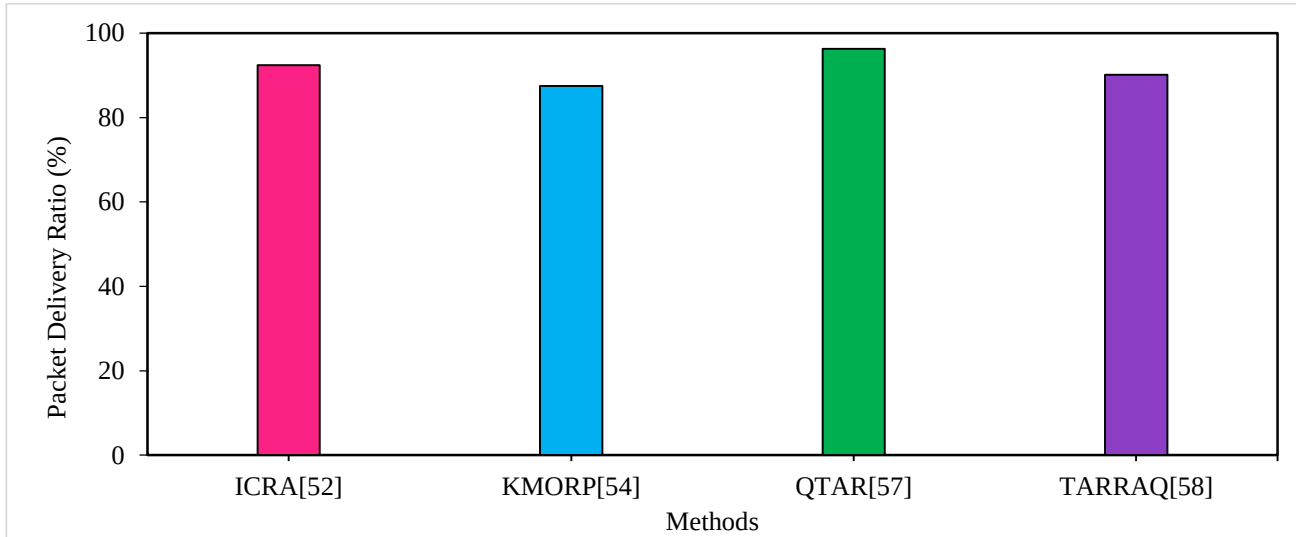


Fig. 16 Performance evaluation of PDR

Table 4. Performance values measured

Metrics/Method	ICRA	KMORO	QTAR	TARRAQ
Energy	50.10	70.35	40.33	60.22
latency	9.94	14.94	7.99	12.69
Throughput	80.19	64.544	94.74	70.96
Reliability	84.84	82.18	97.57	90.84
Computational Complexity	24.93	40.16	17.89	30.17
Secrecy Rate	2.52	38.16	4.20	3.04
Packet Delivery Ratio	92.36	87.438	96.30	90.14

8. Comparative Analysis of UAV Communication

Yu et al. [87] adopted NOMA based URLLC optimization method, which considered energy efficiency, throughput, reliability, and security, but not latency. This was a major limitation; however, UAV-based applications require low-latency communications in addition to energy efficiency. The proposed review is framed to provide all metrics for fair evaluation of performance.

García-Gil et al. [88] and Hao et al. [92] introduced swarm assisted UAV based communication offloading and trajectory optimization. This demonstrated the importance of task offloading and reliable UAV communication. Throughput and security are not addressed; this remains a major limitation. The proposed review addresses this limitation by evaluating throughput and security in addition to other metrics.

Hossain et al. [89] introduced blockchain based UAV framework. The study enhances trust authentication and data integrity through blockchain, which results in additional latency. The energy efficiency and reliability are not addressed. The UAVs are constrained by battery and changing

communication links. Ignoring efficiency and reliability limits practical deployment. The proposed framework extends the work by incorporating efficiency and latency alongside other metrics.

Tran et al. [90] presented Joint Trajectory & Time Allocation Optimization. This improved resource utilization, but security and reliability are not reported. This limits the ability to determine reliable communication. The proposed review suggested improving this by evaluating all performance metrics.

Li et al. [91] studied the heterogeneous UAV deployment strategies. This showed the advantages of heterogeneous networks in improving resource utilization. However, latency and security are not evaluated.

The advantage of the proposed review is that it evaluates not only individual UAV communication parameters but also combined parameters in terms of energy efficiency and security. Thus, it provides a basis for examining communication and the trade-off between these factors. This helps select appropriate security mechanisms for resource-constrained environments. The proposed review provides a broader evaluation of security across UAV-assisted MEC,

FANET, UAV swarm, IoT-enabled UAV, and beyond 5G/6G systems, where security and communication efficiency are important.

The techniques and performance metrics comparison of the UAV communication is defined in Table 5.

Table 5. Techniques and performance metrics comparison of the UAV communication

Ref. No	Author (Year)	Technique / Approach	Performance Metrics				
			Energy Efficiency	Latency	Throughput	Reliability	Security
[87]	Yu et al. (2024)	Secure NOMA-based URLLC Optimization	✓	✗	✓	✓	✓
[88]	García-Gil et al. (2024)	UAV Swarm-assisted Computation Offloading	✓	✓	✗	✓	✗
[89]	Hossain et al. (2024)	Blockchain-based UAV Framework	✗	✓	✓	✗	✓
[90]	Tran et al. (2022)	Joint Trajectory & Time Allocation Optimization	✓	✗	✓	✗	✗
[91]	Li et al. (2024)	Heterogeneous UAV Deployment Strategy	✓	✗	✓	✓	✗
[92]	Hao et al. (2025)	Reliability-aware Resource & Trajectory Optimization	✓	✓	✗	✓	✗
Proposed	-	UAV communication security evaluation	✓	✓	✓	✓	✓

9. Challenges in UAV

The UAVs' transmission systems have essential parts that enable the control and communication required for the UAVs' function [97]. However, because the aerial environment necessitates real-time communication, the transmission systems face particular difficulties [98]. UAVs need low-latency and low delay connections for real-time control and data transfer, including 3D point cloud video, NLP, transformers, encoding, and decoding [99]. Since precise activity timing depends on real-time data delivery, edge computing and low-latency communication protocols are essential. The HD and UHD videos require large amounts of bandwidth; thus, there is a need to employ high-bandwidth communication techniques such as 5G, mmWave, and antenna techniques to support the large amounts of data to be transmitted [100].

Particularly for real-time video transmission in UAVs, precise and dependable data transfer without duplication is

crucial [101]. To guarantee dependable communication in various settings, error correction, mesh networks, and multi-link communication are advised. Because UAVs have limited power sources and can operate only for a short time, energy efficiency is crucial. It is highly recommended that, to tackle this issue, energy-efficient communication algorithms and hardware be developed [102]. Utilizing secure communication protocols and procedures can mitigate signal attenuation, noise, and distortion while also reducing its vulnerability to interference and intrusions [103].

10. Future Research Directions

The development of scalable, lightweight, and flexible security mechanisms that can manage the extremely dynamic nature of UAV communications should be the main goal of future research on UAV communication security. Although considerable progress has been reported in terms of integrating blockchain technology, physical layer security, and DL-based intrusion detection systems, there are still many open issues in

terms of energy constraints, computational overhead, and real-time processing requirements that must be addressed in the near future. Additionally, the security of UAV communications against multi-vector attacks can be greatly enhanced by cross-layer security models that optimize routing, authentication, and transmission security in a single framework. Moreover, the integration of UAV networks with 5G, beyond 5G, and upcoming 6G networks, including mmWave and terahertz communications, will require the development of sophisticated security mechanisms in terms of beamforming and anti-jamming security in UAV communications. Additionally, explainable AI-based intrusion detection systems and lightweight cryptography based on quantum computing may be used in the near future to provide reliable, autonomous, and energy-efficient UAV communication security.

11. Conclusion

The rapid development of wireless communication systems using UAVs has created significant opportunities and complex security concerns. This survey has comprehensively reviewed the latest developments in low-complexity and high-security technologies to protect UAV communication networks. UAV communication networks, including UAV-to-Ground, UAV-to-UAV, swarm-based networks, cellular-connected UAVs, satellite-assisted UAV networks, and ad hoc networks, have been thoroughly examined to determine their particular operational challenges and security issues. A number of lightweight cryptographic systems have been studied, such as physical layer security technologies,

authentication protocols based on blockchain technology, intrusion detection systems that use DL technologies, and privacy preservation systems that use federated learning. The following metrics are measured: energy efficiency, computational complexity, reliability, secrecy rate, throughput, latency, and packet delivery ratio. The results demonstrate that, while AI- and blockchain-based advanced security models are very secure, real-world implementations of these models require fine-tuning to meet the energy- and computationally intensive demands of real-time communication. However, developing UAV security systems that are effective, adaptable, scalable, and energy efficient remains a challenging task. The future of UAVs' communication systems will be based on developing cross-layer, intelligent, and lightweight security solutions that are efficient and reliable for beyond 5G and 6G wireless networks. This survey provides a technical base and direction for developing efficient and secure UAV communication infrastructures for future work.

Conflict of Interest

The authors declare no conflict of interest.

Funding Information

No funding is provided for the preparation of the manuscript.

Acknowledgement

None

References

- [1] Kaitao Meng et al., "UAV-Enabled Integrated Sensing and Communication: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 97-104, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Hongyang Pan et al., "Joint Power and 3D Trajectory Optimization for UAV-Enabled Wireless Powered Communication Networks with Obstacles," *IEEE Transactions on Communications*, vol. 71, no. 4, pp. 2364-2380, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [3] Ruhui Ma et al., "A UAV-Assisted UE Access Authentication Scheme for 5G/6G Network," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2426-2444, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Yuxuan Song et al., "An Overview of Cellular ISAC for Low-Altitude UAV: New Opportunities and Challenges," *IEEE Communications Magazine*, vol. 63, no. 12, pp. 88-95, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Javad Sabzehali et al., "Optimizing Number, Placement, and Backhaul Connectivity of Multi-UAV Networks," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21548-21560, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Syed Agha Hassnain Mohsan et al., "Unmanned Aerial Vehicles (UAVs): Practical Aspects, Applications, Open Challenges, Security Issues, and Future Trends," *Intelligent Service Robotics*, vol. 16, no. 1, pp. 109-137, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Trung Duc Tran et al., "A Cybersecurity Risk Framework for Unmanned Aircraft Systems under Specific Category," *Journal of Intelligent & Robotic Systems*, vol. 104, no. 1, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Omer T. Abdulhae, Jit Singh Mandeep, and Mt Islam, "Cluster-Based Routing Protocols for Flying Ad Hoc Networks (FANETs)," *IEEE Access*, vol. 10, pp. 32981-33004, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] M. Usha et al., "EOEEORFP: Eagle Optimized Energy Efficient Optimal Route-Finding Protocol for Secure Data Transmission in FANETs," *IETE Journal of Research*, vol. 70, no. 5, pp. 4867-4879, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Praveen Kumar Sandanamudi et al., "Securing UAV Communications Using Lightweight Cryptography Algorithms," *Proceedings of Tenth International Congress on Information and Communication Technology*, pp. 121-132, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [11] Dauriya Zhaxygulova et al., "Secure and Energy-Aware Cryptographic Framework for IoT-Enabled UAV Systems," *Symmetry*, vol. 17, no. 11, pp. 1-26, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [12] Saeed Ullah Jan et al., "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET," *IEEE Access*, vol. 10, pp. 95321-95343, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] Image Bhattarai et al., "A Lightweight and Anonymous Application-Aware Authentication and Key Agreement Protocol for the Internet of Drones," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 19790-19803, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Wali Ullah Khan et al., "Opportunities for Physical Layer Security in UAV Communication Enhanced with Intelligent Reflective Surfaces," *IEEE Wireless Communications*, vol. 29, no. 6, pp. 22-28, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Peishun Yan et al., "Securing UAV-Aided NOMA Wireless Powered Communications via Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 24, no. 6, pp. 4809-4823, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Yixin Shang, "RIS-Assisted Secure UAV Communication Scheme Against Active Jamming and Passive Eavesdropping," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 16953-16963, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Nilesh Kumar Jadav et al., "Blockchain-Based Secure and Intelligent Data Dissemination Framework for UAVs in Battlefield Applications," *IEEE Communications Standards Magazine*, vol. 7, no. 3, pp. 16-23, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] Sihem Benfriha et al., "A Survey on Trust Management in Flying Ad Hoc Networks: Challenges, Classifications, and Analysis," *2023 Tenth International Conference on Software Defined Systems (SDS)*, San Antonio, TX, USA, pp. 107-114, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Rui Fu et al., "Machine-Learning-Based UAV-Assisted Agricultural Information Security Architecture and Intrusion Detection," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18589-18598, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] Li Wang et al., "Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 41-47, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [21] Vikas Hassija et al., "Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2802-2832, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [22] Mien L. Trinh et al., "Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-based Approaches," *Algorithms*, vol. 18, no. 5, pp. 1-62, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Rogerio Ballestrin et al., "Drone-Based Data Acquisition for Digital Agriculture: A Survey of Wireless Network Applications," *AgriEngineering*, vol. 8, no. 2, pp. 1-25, 2026. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [24] Sayani Sarkar et al., "Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques," *Drones*, vol. 9, no. 8, pp. 1-58, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Sufian Al Majmaie et al., "PUF-Based Hardware Security for Trusted Internet of Drones: Challenges and Future Directions," *2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC)*, Dayton, OH, USA, pp. 1-7, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [26] Bhavya Dixit et al., "A Novel Cipher for Enhancing MAVLink Security: Design, Security Analysis, and Performance Evaluation Using a Drone Testbed," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 9027-9051, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [27] Mohammad Aldossary, Ibrahim Alzamil, and Jaber Almutairi, "Enhanced Intrusion Detection in Drone Networks: A Cross-Layer Convolutional Attention Approach for Drone-To-Drone and Drone-To-Base Station Communications," *Drones*, vol. 9, no. 1, pp. 1-29, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] Faisal Al-Kamali et al., "Optimizing UAV Placement with Spatial Threat Exclusion for Secure and Energy-Efficient Wireless Communications," *IEEE Open Journal of the Communications Society*, vol. 7, pp. 539-558, 2026. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] Mohsen Farajijalal et al., "Safety Systems for Emergency Landing of Civilian Unmanned Aerial Vehicles (UAVs)—A Comprehensive Review," *Drones*, vol. 9, no. 2, pp. 1-59, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [30] Sudesh Kumar et al., "The Rise of UAV-Based Smart Surveillance: A Systematic Review of Trends and Technologies," *IEEE Access*, vol. 13, pp. 181553-181575, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [31] Hamidullah Muslih et al., "Cache Sharing in UAV-Enabled Cellular Network: A Deep Reinforcement Learning-Based Approach," *IEEE Access*, vol. 12, pp. 43422-43435, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [32] Boyu Hua et al., "Ultra-Wideband Non-Stationary Channel Modeling for UAV-to-Ground Communications," *IEEE Transactions on Wireless Communications*, vol. 24, no. 5, pp. 4190-4204, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [33] Hao Jiang et al., "Physics-Based 3D End-to-End Modeling for Double-RIS Assisted Non-Stationary UAV-to-Ground Communication Channels," *IEEE Transactions on Communications*, vol. 71, no. 7, pp. 4247-4261, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [34] Zhaolei Zhang et al., "Machine Learning Based Clustering and Modeling for 6G UAV-to-Ground Communication Channels," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 10, pp. 14113-14126, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [35] Boyu Hua et al., "Channel Modeling for UAV-to-Ground Communications with Posture Variation and Fuselage Scattering Effect," *IEEE Transactions on Communications*, vol. 71, no. 5, pp. 3103-3116, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [36] Mohammad Taghi Dabiri et al., "Modulating Retroreflector Based Free Space Optical Link for UAV-to-Ground Communications," *IEEE Transactions on Wireless Communications*, vol. 21, no. 10, pp. 8631-8645, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [37] Reza Fotuhi, Masoud Abdan, and Sanaz Ghasemi, "A Self-Adaptive Intrusion Detection System for Securing UAV-to-UAV Communications Based on the Human Immune System in UAV Networks: A Self-adaptive Intrusion Detection System for Securing UAV-to-UAV Communications Based on the Human Immune System in UAV Networks," *Journal of Grid Computing*, vol. 20, no. 3, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [38] Linzhou Zeng et al., "Three-Dimensional UAV-to-UAV Channels: Modeling, Simulation, and Capacity Analysis," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10054-10068, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [39] Tianyang Li et al., "Intelligent Resource Allocation Schemes for UAV-Swarm-Based Cooperative Sensing," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21570-21582, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [40] Yuheng Yang et al., "Modeling and Vulnerability Analysis of UAV Swarm Based On Two-Layer Multi-Edge Complex Network," *Reliability Engineering & System Safety*, vol. 256, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [41] Liangdong Wen et al., "Distributed Cooperative Fencing Scheme for UAV Swarm Based on Self-Organized Behaviors," *Aerospace Science and Technology*, vol. 138, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [42] Yi Wang et al., "ISAC Enabled Cooperative Detection for Cellular-Connected UAV Network," *IEEE Transactions on Wireless Communications*, vol. 24, no. 2, pp. 1541-1554, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [43] Yongchao Dang et al., "Deep-Ensemble-Learning-Based GPS Spoofing Detection for Cellular-Connected UAVs," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25068-25085, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [44] Cheng Zhan, and Yong Zeng, "Energy Minimization for Cellular-Connected UAV: From Optimization to Deep Reinforcement Learning," *IEEE Transactions on Wireless Communications*, vol. 21, no. 7, pp. 5541-5555, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [45] Irshad A. Meer et al., "Mobility Management for Cellular-Connected UAVs: Model-based Versus Learning-Based Approaches for Service Availability," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 2125-2139, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [46] Yongchao Dang et al., "3D Radio Map-Based GPS Spoofing Detection and Mitigation for Cellular-Connected UAVs," *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 1, pp. 313-327, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [47] Tianhao Liang et al., "Satellite-Assisted UAV Control: Sensing and Communication Scheduling for Energy Efficient Data Collection," *IEEE Internet of Things Journal*, vol. 13, no. 4, pp. 5694-5707, 2026. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [48] Ahmed Adil Nafea, Mustafa Maad Hamdi, and Sami Abduljabbar Rashid, "Resource Allocation and Edge Computing for Dual Hop Communication in Satellite Assisted UAVs Enabled VANETs," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 3, pp. 1-21, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [49] Mohammed Ahmed Jubair et al., "Multi-Objective Optimization in Satellite-Assisted UAVs," *Journal of Intelligent Systems & Internet of Things*, vol. 16, no. 1, pp. 189-198, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [50] Weijie Zhou et al., "Satellite-Assisted UAV Data Collection for Information Freshness in IoRT Networks," *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, Dubai, United Arab Emirates, pp. 1-6, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [51] Ehab Mahmoud Mohamed et al., "LEO Satellite Assisted UAV Distribution Using Combinatorial Bandit with Fairness and Budget Constraints," *PLoS One*, vol. 18, no. 8, pp. 1-17, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [52] Jingjing Guo et al., "ICRA: An Intelligent Clustering Routing Approach for UAV ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2447-2460, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [53] Yuxi Lu et al., "UAV Ad Hoc Network Routing Algorithms in Space-Air-Ground Integrated Networks: Challenges and Directions," *Drones*, vol. 7, no. 7, pp. 1-26, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [54] Saifullah et al., "K-Means Online-Learning Routing Protocol (K-MORP) for Unmanned Aerial Vehicles (UAV) Adhoc Networks," *Ad Hoc Networks*, vol. 154, pp. 1-15, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [55] Ali H. Wheeb et al., "Performance Evaluation of Standard and Modified OLSR Protocols for Uncoordinated UAV Ad-Hoc Networks in Search and Rescue Environments," *Electronics*, vol. 12, no. 6, pp. 1-23, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [56] Salah Uddin et al., "Cooperative MAC Protocol with Optimal Relay Selection Algorithm for UAVs Ad Hoc Network in Disasters," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 9, pp. 14445-14456, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [57] Muhammad Yeasir Arafat, and Sangman Moh, "A Q-Learning-Based Topology-Aware Routing Protocol for Flying Ad Hoc Networks," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 1985-2000, 2021. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [58] Yanpeng Cui et al., "Topology-Aware Resilient Routing Protocol for FANETs: An Adaptive Q-Learning Approach," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18632-18649, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [59] Zhuo Zhao et al., "Lightweight Ring-Neighbor-Based User Authentication and Group-Key Agreement for Internet of Drones," *Cybersecurity*, vol. 7, no. 1, pp. 1-14, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [60] Huilong Jin et al., "A Survey of Energy Efficient Methods for UAV Communication," *Vehicular Communications*, vol. 41, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [61] Indu Chandran, and Kizheppatt Vipin, "Multi-UAV Networks for Disaster Monitoring: Challenges and Opportunities from a Network Perspective," *Drone Systems and Applications*, vol. 12, pp. 1-28, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [62] Kamlesh Lakhwani, Tejpreet Singh, and Orchu Aruna, "Multi-Layer UAV Ad Hoc Network Architecture, Protocol and Simulation," *Artificial Intelligent Techniques for Wireless Communication and Networking*, pp. 193-209, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [63] Jie Feng et al., "Heterogeneous Computation and Resource Allocation for Wireless Powered Federated Edge Learning Systems," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3220-3233, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [64] Niphon Kaewdornhan, and Rongrit Chatthaworn, "Predictive Energy Management for Microgrid Using Multi-Agent Deep Deterministic Policy Gradient with Random Sampling," *IEEE Access*, vol. 12, pp. 95071-95090, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [65] Yuan Gao et al., "Deep Reinforcement Learning-Based Trajectory Optimization and Resource Allocation for Secure UAV-Enabled MEC Networks," *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Vancouver, BC, Canada, pp. 1-5, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [66] Chao Gao et al., "UAV-Centric Privacy-Preserving Computation Offloading in Multi-UAV Mobile Edge Computing," *Drones*, vol. 9, no. 10, pp. 1-21, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [67] Xuqiong Luo et al., "UAV Path Planning based on the Average TD3 Algorithm with Prioritized Experience Replay," *IEEE Access*, vol. 12, pp. 38017-38029, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [68] Weidang Lu et al., "Secure Transmission for Multi-UAV-Assisted Mobile Edge Computing based on Reinforcement Learning," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1270-1282, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [69] Mochan Fan et al., "Blockchain-based Decentralized and Lightweight Anonymous Authentication for Federated Learning," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 12075-12086, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [70] Anik Islam, Ahmed Al Amin, and Soo Young Shin, "FBI: A Federated Learning-Based Blockchain-Embedded Data Accumulation Scheme Using Drones for Internet of Things," *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 972-976, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [71] Arash Heidari, Nima Jafari Navimipour, and Mehmet Unal, "A Secure Intrusion Detection Platform using Blockchain and Radial Basis Function Neural Networks for Internet of Drones," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8445-8454, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [72] Aytac Ugur Yerden et al., "xT-STRIDE Threat Model for Unmanned Air Vehicle Security," *International Journal of Information Security*, vol. 24, no. 4, pp. 1-22, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [73] Leanne Stuive, and Fatma Gzara, "Airspace Network Design for Urban UAV Traffic Management with Congestion," *Transportation Research Part C: Emerging Technologies*, vol. 169, no. 1, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [74] Runchen Xu et al., "Blockchain-Based Resource Trading in Multi-UAV Edge Computing System," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 21559-21573, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [75] Die Wang et al., "Resource Allocation in Blockchain Integration of UAV-Enabled MEC Networks: A Stackelberg Differential Game Approach," *IEEE Transactions on Services Computing*, vol. 17, no. 6, pp. 4197-4210, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [76] Raja Karmakar, Georges Kaddoum, and Ouassima Akhrif, "A Blockchain-Based Distributed and Intelligent Clustering-Enabled Authentication Protocol for UAV Swarms," *IEEE Transactions on Mobile Computing*, vol. 23, no. 5, pp. 6178-6195, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [77] Elmehdi Illi et al., "Physical Layer Security for Authentication, Confidentiality, and Malicious Node Detection: A Paradigm Shift in Securing IoT Networks," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 347-388, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [78] Hossein Pirayesh, and Huacheng Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [79] Xiaomin Wei, Jianfeng Ma, and Cong Sun, "A Survey on Security of Unmanned Aerial Vehicle Systems: Attacks and Countermeasures," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34826-34847, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [80] Muhammad Majid Aziz et al., "Anti-Jamming Radar Waveform Design for Repeater Jammer using Reinforcement Learning," *Vehicular Communications*, vol. 47, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [81] Vanlalruata Hnamte et al., "DDoS Attack Detection and Mitigation Using Deep Neural Network in SDN Environment," *Computers & Security*, vol. 138, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]

- [82] Muhammet A. Sen, Saba Al-Rubaye, and Antonios Tsourdos, "Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications," *Sensors*, vol. 25, no. 4, pp. 1-26, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [83] Navid Ali Khan et al., "A Secure Communication Protocol for Unmanned Aerial Vehicles," *Computers, Materials, & Continua*, vol. 70, no. 1, pp. 601-618, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [84] Tasneem Assaf et al., "High-Rate Secret Key Generation Using Physical Layer Security and Physical Unclonable Functions," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 209-225, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [85] Rajnish Kumar, and Shlomi Arnon, "Improving Physical Layer Security of Ground Stations Against GEO Satellite Spoofing Attacks," *International Symposium on Cyber Security, Cryptology, and Machine Learning*, pp. 458-470, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [86] Seda Dogan-Tusha, Saud Althunibat, and Marwa Qaraqe, "Doppler-Shift-Based Sybil Attack Detection for Mobile IoT Networks," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1136-1147, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [87] Kan Yu et al., "Secure Ultra-Reliable and Low Latency Communication in UAV-Enabled NOMA Wireless Networks," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 10, pp. 14908-14922, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [88] Santiago García-Gil, Juan Manuel Murillo, and Jaime Galán-Jiménez, "Enabling Ultra Reliable Low Latency Communications in Rural Areas using UAV Swarms," *Ad Hoc Networks*, vol. 163, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [89] Md Imran Hossain et al., "Blockchain Integration in UAV Networks: Performance Metrics and Analysis," *Sensors*, vol. 24, no. 23, pp. 1-22, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [90] Dinh-Hieu Tran, Symeon Chatzinotas, and Björn Ottersten, "Throughput Maximization for Backscatter-and Cache-Assisted Wireless Powered UAV Technology," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5187-5202, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [91] Shuyue Li et al., "Maximizing Network Throughput in Heterogeneous UAV Networks," *IEEE/ACM Transactions on Networking*, vol. 32, no. 3, pp. 2128-2142, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [92] Hao Hao et al., "Reliability-Aware Optimization of Task Offloading for UAV-Assisted Edge Computing," *IEEE Transactions on Computers*, vol. 74, no. 11, pp. 3832-3844, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [93] Imen Jarraya et al., "Gnss-Denied Unmanned Aerial Vehicle Navigation: Analyzing Computational Complexity, Sensor Fusion, and Localization Methodologies," *Satellite Navigation*, vol. 6, no. 1, pp. 1-32, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [94] Gaurav Kumar Pandey et al., "Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 112858-112897, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [95] Aanchal Gupta, Divya Dhawan, and Neena Gupta, "Review on UAV-Based FSO Links: Recent Advances, Challenges, and Performance Metrics," *Optical Engineering*, vol. 63, no. 4, pp. 1-29, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [96] Marwa T. Naser, and Ali H. Wheeb, "Implementation of RWP and Gauss Markov Mobility Model for Multi-UAV Networks in Search and Rescue Environment," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 23, pp. 125-137, 2022. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [97] Abiodun Esther Omolara, Moatsum Alawida, and Oludare Isaac Abiodun, "Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey," *Neural Computing and Applications*, vol. 35, no. 31, pp. 23063-23101, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [98] Altaf Hussain et al., "Computing Challenges of UAV Networks: A Comprehensive Survey," *Computers, Materials & Continua*, vol. 81, no. 2, 1999-2051, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [99] Christoph Torens et al., "Runtime Monitoring of Operational Design Domain to Safeguard Machine Learning Components," *CEAS Aeronautical Journal*, vol. 16, no. 3, pp. 973-991, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [100] Zefang Lv et al., "Multi-Agent Reinforcement Learning based UAV Swarm Communications against Jamming," *IEEE Transactions on Wireless Communications*, vol. 22, no. 12, pp. 9063-9075, 2023. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [101] Alberto Boretto et al., "Navigating the Future: The Expanding Role of Unmanned Surface Vehicles in Maritime Security," *Journal of Transportation Security*, vol. 18, no. 1, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [102] Magdalena Garvanova, Ivan Garvanov, and Daniela Borissova, "Unmanned Aerial Vehicles: A Regulatory Compliance Perspective," *International Symposium on Business Modeling and Software Design*, pp. 291-299, 2025. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [103] Weizheng Wang et al., "Lightweight Blockchain-Enhanced Mutual Authentication Protocol for UAVs," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9547-9557, 2024. [[CrossRef](#)] [[Google Scholar](#)] [[Publisher Link](#)]