PREMIER JOURNAL OF SCIENCE REVIEW

Data Transmission Between a Drone Swarm and a Ground Base: Modern Methods and Technologies—A Narrative Review

Roman Zaivyi, Oleh Melnychok and Vitalii Skochelias

Institute of Information and Communication Technologies and Electronic Engineering, Lviv Polytechnic National University, Lviv, Ukraine

Correspondence to: Roman Zaivyi, rzaivyi@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Zaivyi R, Melnychok O and Skochelias V. Data Transmission Between a Drone Swarm and a Ground Base: Modern Methods and Technologies—A Narrative Review. Premier Journal of Science 2025;14:100116

DOI: https://doi.org/10.70389/PJS.100116

Peer Review

Received: 28 August 2025

Last revised: 18 September 2025

Accepted: 19 September 2025

Version accepted: 3

Published: 7 October 2025

Ethical approval: The study was conducted without human participation. Ethical approval is not required

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution: Roman Zaivyi — Conceptualization, Coordinated research, Writing— original draft, Writing— review and editing.

ABSTRACT

BACKGROUND

The objective of this study was to analyse contemporary approaches, identify key challenges, and provide recommendations for optimising data exchange with regard to speed, reliability, energy efficiency, and security.

MATERIALS AND METHODS

This work presents a structured narrative review analysing modern methods and technologies for data transmission between a drone swarm and a ground base, enabling an assessment of the effectiveness of various approaches in ensuring stable, rapid, and secure communication under conditions of high mobility and dynamic network topology.

RESULTS

The research indicated that 5G provides superior bandwidth (up to 10 Gbit/s) and negligible latency (under 1 ms), although its implementation is constrained by range (up to 1 km) and the requirement for advanced infrastructure. MANETs and DTNs offer adaptability in dynamic settings but encounter latency (up to several minutes) and connection stability challenges. Wi-Fi mesh networks provide effective coverage and stability. Nonetheless, they necessitate energy consumption optimisation for autonomous operation. Principal problems encompass interference, restricted drone power, and the necessity for improved security in conveyed data.

CONCLUSION

Combined approaches are proposed, incorporating dynamic routing, adaptive frequency management, and blockchain integration to improve authentication and data protection. Additionally, the use of machine learning algorithms for real-time threat detection and more efficient network resource allocation is explored. The findings can be further applied to enhance wireless communication systems in unmanned networks.

Keywords: Adaptability, Cybersecurity, Network protocols, Security, Wireless communication

Highlights

- Aerial vehicles have unlocked new horizons in defense, industrial, and other applications.
- Interaction between drones and base stations necessitates stable and secure data transmission.
- Innovative approaches based on blockchain and machine learning algorithms are being actively researched.

Introduction

The modern development of unmanned aerial vehicles (UAVs) and their deployment in drone swarms has unlocked new horizons in defence, industrial, agricultural, and environmental applications. Effective interaction between drones and a ground base necessitates stable, reliable, and secure data transmission, which is a critical factor for the successful operation of autonomous systems. In particular, the exchange of telemetric data, flight trajectory adjustments, and adaptation to environmental changes heavily depend on the quality and uninterrupted operation of communication channels. The relevance of research in this field is driven by the rapid advancement of artificial intelligence, machine learning, and network communication technologies, which enable the creation of more dynamic and adaptive data exchange systems. However, conventional wireless communication methods, such as Wi-Fi, LTE, or even modern 5G networks, often face limitations in range, resistance to interference, and energy consumption – factors particularly critical in mobile and autonomous systems.

The primary challenges in establishing communication between a drone swarm and a ground base include latency and packet loss in dynamic networks, limited bandwidth of communication channels, and security concerns regarding data integrity. In scenarios where large volumes of data – such as video streams, telemetry, and mapping data – impose high network loads, ensuring fast and reliable transmission becomes especially crucial. Furthermore, safeguarding data against cyberattacks and unauthorised access is a priority for contemporary researchers, as the security of communication channels determines the operational efficacy of drone swarms in real-world conditions.

Modern data transmission methods in such networks rely on mobile ad hoc networks (MANETs) and delay-tolerant networks (DTNs), as well as 5G, Wi-Fi Mesh, satellite communications, and radiofrequency technologies. Additionally, innovative approaches based on blockchain, which enhance security, and machine learning algorithms for adaptive traffic routing are being actively researched. Thus, the problem of data transmission between a drone swarm and a ground base is highly complex yet presents a promising research domain, offering new opportunities for deploying autonomous systems across various sectors and advancing modern communication technologies.

An analysis of numerous scholarly works delineates the current landscape of solutions for data transmission between drone swarms and ground bases, highlighting the multifaceted nature of approaches and the topic's potential for further development. Patel et al.[1] focused on 5G technology, demonstrating its capacity to enhance communication quality by minimising signal

Oleh Melnychok — Literature review, Data interpretation, Methodology, Theoretical framework. Vitalii Skochelias — Data collection, Preliminary analysis, Writing— review and editing. All authors read and approved the final manuscript and agree to be accountable for all aspects of the work.

Guarantor: Roman Zaivyi

Provenance and peer-review: Unsolicited and externally peer-reviewed

Data availability statement: The authors confirm that the data supporting the findings of this study are available in the article.

transmission time and reducing failures–critical in highly mobile drone swarms. Research by Gokalgandhi[2] et al. underscores the efficacy of Wi-Fi mesh networks, where automatic node configuration enhances reliability and mitigates single points of failure. Meanwhile, Albalawi and Song[3] emphasised the necessity of cryptographic protocols for securing transmitted data, noting the growing importance of cybersecurity in modern drone swarm management systems.

Jahir et al.[4] proposed a dynamic routing model capable of adapting to rapidly changing network topologies, ensuring optimal data transmission paths even under unpredictable environmental conditions. Findings by Zhou et al.[5] validated the effectiveness of satellite communications in extending coverage, enabling drone swarm deployment in remote or inaccessible regions. Kuznetsov et al.[6] demonstrated that integrating blockchain into swarm management systems enhances data security and transparency – crucial for military and critical infrastructure applications. Pirzadi et al.[7] explored the potential of DTNs in intermittent connectivity scenarios, proving their utility in emergencies or areas with weak traditional network coverage.

This integrated approach not only expands the functional capabilities of drone swarm management systems but also opens new prospects for their application across industries, enhancing resilience, adaptability, and security in modern UAV technologies.

Despite successful research in drone swarm-to-ground base data transmission, certain aspects require further investigation: notably, the optimisation of energy consumption during data transmission, adaptive routing in dynamic topologies, and the impact of external factors (e.g., atmospheric conditions) on communication quality remain understudied. Additionally, integrated approaches combining modern cryptographic protocols with machine learning algorithms for high-level cybersecurity are yet to be fully developed. This research advances existing literature by synthesising current methodologies and developing a comprehensive model that integrates dynamic routing with adaptive frequency management, thereby offering a holistic perspective on optimising UAV swarm communication systems. The incorporation of advanced technologies, particularly blockchain for secure communication and machine learning for real-time adaptation, distinguishes this study from previous research that primarily concentrated on isolated solutions without a framework for integrating these innovations.

The objective of this study was to analyse and optimise a complex data transmission system between a drone swarm and a ground base, ensuring a high level of reliability, efficiency, and communication security under variable operational conditions. The research work entailed identifying the deficiencies in existing methods, assessing critical algorithms and protocols, and examining their effects on system stability and energy efficiency. The study proposes a comprehensive model that enhances data integrity, network resilience, and real-time adaptability in UAV communication systems by integrating innovative approaches, including dynamic routing, adaptive frequency management, and blockchain for secure communication.

Literature Review

Numerous crucial studies have investigated the communication and networking technologies for UAVs, particularly concerning drone swarms. These investigations have yielded significant insights into multiple facets of UAV communication, encompassing network protocols, security issues, energy efficiency, and prospective developments. Nakas et al.[8] addressed energy consumption in data transmission, proposing resource allocation methods that significantly extend drone flight times. Lastly, Asaamoning et al.[9] analysed the impact of external factors, such as atmospheric conditions, on communication quality, concluding that adaptive systems can effectively mitigate such adverse effects. These studies underscore the need for a multidisciplinary approach. It is essential to combine innovative technologies, machine learning, blockchain, and advanced networking solutions to ensure efficient and secure data transmission.

Saleem et al.[10] examined the incorporation of Cognitive Radio (CR) technology with UAVs, emphasising the problems, prospects, and future research dilemmas related to this integration. CR technology facilitates dynamic spectrum access and intelligent communication by adapting to the wireless environment, offering substantial potential for UAVs, especially regarding spectrum efficiency and interference reduction. Saleem et al. emphasised the restricted spectrum availability for UAV communication as a significant concern, observing that UAVs frequently depend on licensed spectrum bands, resulting in congestion and interference in heavily populated regions. Through the integration of CR, UAVs may utilise underused spectrum and dynamically modify communication parameters according to real-time environmental conditions, hence improving communication dependability. The authors recognised other research issues, such as the intricacies of spectrum management and the necessity for adaptive algorithms to improve frequency spectrum utilisation while ensuring low latency and high data throughput.

Liu et al.[11] investigated the capacity of UAV swarms to sustain efficient coordination and formation control in dynamic and fluctuating communication environments. The authors presented a distributed control system wherein each UAV makes decisions based on local information from its neighbours, enabling the UAVs to adapt to alterations in network topology without necessitating a central controller. A primary problem identified in the study was sustaining communication stability when UAVs operate in areas with poor connectivity or intermittent links, which might hinder the coordination of the UAV swarm. The study's findings are essential for UAV swarm communication, illustrating how directed switching communication may maintain connectivity among UAVs despite the temporary unavailability of specific links.

Campion et al.[12] examined UAV swarm communication and control architectures, analysing various communication protocols employed for synchronising many UAVs within a swarm. They emphasised the difficulties associated with coordination and collaboration among UAVs, particularly when network circumstances change swiftly. The research indicated that MANETs and 5G technologies are especially conducive to UAV swarm communication due to their capacity for high mobility and low latency. Nevertheless, Campion et al. highlighted that these systems encounter difficulties in scaling to extensive UAV networks.

Giagkos et al.[13] introduced an evolutionary coordination system for fixed-wing UAVs, designed to enhance the communication and coordination capacities of UAV swarms. Their system, designed with evolutionary algorithms, optimises the communication strategy of UAVs, ensuring the maintenance of an efficient communication network while adapting to environmental changes. The research revealed that the evolutionary coordination system could adapt communication techniques dynamically to align with prevailing network conditions, which is essential in contexts where UAVs encounter frequent alterations in network topology due to mobility. The authors highlighted the capacity of evolutionary algorithms to optimise communication protocols and synchronisation in UAV swarms, therefore markedly improving network efficiency and robustness.

Ma et al.[14] introduced a cooperative communication framework for formations of UAVs and unmanned surface vehicles (USVs), emphasising the communication between UAVs and USVs inside a multi-hop network. This system facilitates the enhancement of communication range by employing cooperative relay nodes to augment coverage and signal integrity. The research indicated that collaborative communication improves network performance, especially in rural settings where conventional communication infrastructure is limited or nonexistent.

Sánchez-García et al.[15] performed a survey on multi-hop networks for unmanned aerial and aquatic vehicles, emphasising wireless communications, assessment tools, and applications. They recognised critical concerns like network stability and energy efficiency in multi-hop networks, namely for UAVs and USVs. The study emphasised that multi-hop communication can address coverage deficiencies in remote regions, although it also presented issues about energy usage and network congestion.

Materials and Methods

The present study is a structured narrative review focused on assessing modern data transmission methods between drone swarms and base stations. The study synthesises and critically reviews findings from current literature and technical sources instead of offering new experimental data. The main evidence base contains scientific articles, technical reports, industry studies, and standards published in academic journals and on the official websites of leading organisations such as NIST and IETF.

A systematic search method was employed to guarantee methodological transparency and reproducibility. A systematic search was performed utilising Scopus, IEEE Xplore, and Google Scholar spanning the years 2015 to 2024. The employed search strings were: (“drone swarm” AND “UAV communication” AND

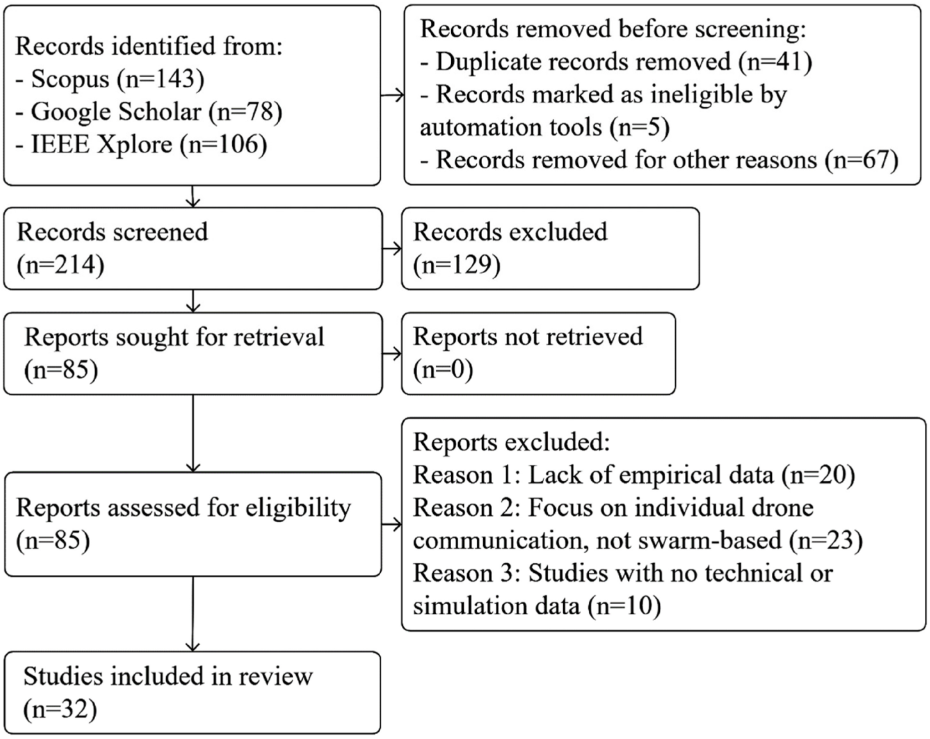
Records identified from:
- Scopus (n=143)
- Google Scholar (n=78)
- IEEE Xplore (n=106)
Records removed before screening:
- Duplicate records removed (n=41)
- Records marked as ineligible by automation tools (n=5)
- Records removed for other reasons (n=67)
Records screened (n=214)
Records excluded (n=129)
Reports sought for retrieval (n=85)
Reports not retrieved (n=0)
Reports assessed for eligibility (n=85)
Reports excluded:
Reason 1: Lack of empirical data (n=20)
Reason 2: Focus on individual drone communication, not swarm-based (n=23)
Reason 3: Studies with no technical or simulation data (n=10)
Studies included in review (n=32)

Fig 1 | Flowchart of study selection and analysis stages "data transmission") and ("5G" OR "LTE" AND "Wi-Fi Mesh" OR "MANET" AND "cybersecurity"). The search was concluded on November 10, 2024. The preliminary search identified 327 records. Following the removal of duplicates, ineligible records, and irrelevant research, 113 records were discarded prior to screening. Out of 214 records reviewed, 129 were eliminated for failing to meet the inclusion criteria. After the eligibility review, 53 reports were rejected due to factors including the absence of empirical data, a concentration on individual drone communication, and inadequate technical or simulation details. Consequently, 32 studies fulfilled the inclusion criteria and were included in the study. Studies were deemed eligible if they presented empirical data, simulation models, or technical standards relevant to communication between drone swarms and ground bases, and documented quantifiable parameters like bandwidth, latency, range, interference resilience, or energy efficiency. Research limited to individual-drone communication or deficient in technical specifics was omitted. This procedure of identification, screening, and inclusion was presented in PRISMA Figure 1.

Data extraction for each included study focused on communication parameters and security components. The extracted information encompassed performance measures like throughput, range, latency, and energy consumption, along with integration with cryptographic and security protocols. The reliability of the synthesis was ensured by evaluating the quality of each study using modified technical assessment criteria derived from NIST and IETF guidelines. The assessment emphasised methodological transparency, replicability, and the disclosure of performance metrics.

The evaluation was performed in three organised phases. Initially, essential factors defining the efficacy of data transmission technologies were determined, including bandwidth, range, latency, interference resistance, energy consumption, and compatibility with security protocols. A formal risk-of-bias and quality-grading criteria were used to ensure transparency and repeatable performance in the evaluation of the included studies. The Cochrane Risk of Bias tool was employed for randomised controlled trials, whilst non-randomised studies were assessed using the Risk of Bias in Non-Randomised Studies (RoBANS). The AMSTAR 2 tool was utilised to evaluate the methodological quality of systematic reviews. Two reviewers independently evaluated the studies, and any discrepancies were reconciled through conversation to ensure consistency. The inter-rater agreement for the risk-of-bias score was 90%, signifying high reliability in the rating of study quality. A comparative analysis of technologies including Wi-Fi, LTE, 5G, MANET, DTN, Wi-Fi Mesh, and satellite communication was conducted to elucidate their advantages and limits.[16–18]

The fundamentals of wireless communication and the characteristics of mobile networks were examined in the second stage. This involved the examination of modulation, multiplexing, and frequency band selection, along with the impacts of interference and multipath propagation. Simulations of real-world conditions, considering obstructions, atmospheric effects, and terrain characteristics, were performed to evaluate communication stability in highly dynamic situations.

The third level concentrated on cybersecurity within data transmission systems. Contemporary cryptographic technologies, including AES, RSA, ECC, TLS, and IPsec, were examined in conjunction with blockchain-based methodologies. Their performance, security standards, computational demands, and application areas were evaluated. Particular emphasis was placed on adaptive encryption, automated cyberthreat responses, and machine learning methodologies for anomaly identification and network behaviour analysis.

Both quantitative and qualitative synthesis methods were utilised. The quantitative assessment relied on documented technical data, whereas the qualitative synthesis examined implementation experiences across various operational settings. This integrated approach facilitated the identification of optimal use cases for each communication channel and highlighted major challenges, such as energy efficiency and routing complexity, that necessitate further refinement in future study.

Results

A screening method was used to evaluate the quality and relevance of the studies included in this review. Table 1 delineates the selected studies and provides the rationale for inclusions. The table includes solely the papers examined in the review. Additional works referenced in the article were deemed unsuitable for inclusion in the analysis, as they did not satisfy the inclusion criteria.

The inclusion criteria emphasised relevance to UAV swarm communication and rigorous procedures, guaranteeing that the final selection of studies offers a thorough and dependable foundation for assessing the technologies and techniques examined in this review. Conventional wireless technologies, including Wi-Fi and LTE, along with recent innovations like 5G, provide adequate bandwidth for substantial data quantities.[1] However, they encounter constraints in range and susceptibility to interference in adverse operational environments. Although 5G facilitates rapid data transmission and minimal latency, its implementation may be impractical in distant areas or during crises where infrastructure is lacking or compromised. MANET facilitates dynamic networking by establishing temporary communication links without centralised oversight, offering flexibility while facing problems such as instability and routing difficulties. DTN mitigates inconsistent connectivity by caching data and transmitting it upon restoration of the connection, proving advantageous in remote regions or emergency scenarios.[19]

Wi-Fi Mesh networks improve coverage by enabling each drone to function as a relay node, hence augmenting network resilience against node failures.[2,29] Nevertheless, this elevates routing complexity and necessitates greater energy consumption, a vital consideration for

Table 1 | PRISMA table

No.	Author/s	Year	Methods	Focus	Key Metrics	Findings	Risk of Bias
1	Patel et al.	2022	Systematic literature synthesis	5G technology for communication enhancement	5G bandwidth, latency, connectivity	5G improves connectivity but limited by range and infrastructure	Low risk **(AMSTAR 2):** criteria met for transparency and reproducibility.
2	Gokalgandhi et al.	2021	Empirical study, experimental, simulation	Low-latency Wi-Fi Mesh networks	Latency, reliability, network stability	Wi-Fi Mesh reduces latency and improves stability	Medium risk (**Cochrane Risk of Bias Tool):** medium risk due to model assumptions and limited real-world testing.
3	Albalawi and Song	2019	Empirical study, conceptual model, survey	Data security and privacy in drone swarms	Data security, privacy protocols	Security protocols are crucial for UAV swarm integrity	High risk (**RoB 2 tool**): theoretical study with no empirical data, high risk due to lack of validation.
4	Zhou et al.	2020	Literature review	UAV swarm intelligence and trends	Network efficiency, AI integration	AI can optimize swarm intelligence, future research needed	Low risk (**AMSTAR 2**): comprehensive review with transparent methodology and no conflicts.
5	Kuznetsov et al.	2024	Conceptual paper, literature synthesis	Integration of AI and blockchain for UAV security	Blockchain, AI, security	AI and blockchain enhance UAV security but with high energy cost	Medium risk **(RoBANS):** limited empirical support and heavy reliance on conceptual models.
6	Pirzadi et al.	2022	Empirical study, simulation, comparison	Routing in hybrid DTN-MANET networks	Routing efficiency, latency, energy consumption	Hybrid approach improves routing under critical conditions	Medium risk **(Cochrane Risk of Bias Tool):** simulation-based results with assumptions about real-world applicability.
7	Asaamoning et al.	2021	Empirical study, simulation, system design	Drone swarms as networked control systems	Networking, control systems	Networking and computing integration enhances control	Medium risk **(RoBANS):** simulation model, high risk of bias due to idealized conditions.
8	Saleem et al.	2015	Literature review	Cognitive Radio technology for UAVs	Cognitive radio, spectrum efficiency	Cognitive radio optimizes spectrum, essential for UAV comms	Low risk **(AMSTAR):** clear, transparent methodology with no significant conflicts.
9	Liu et al.	2015	Empirical study, experimental, simulation	Distributed formation control in UAVs	Formation control, communication topologies	Directed switching enhances formation control	Medium risk **(Cochrane Risk of Bias Tool):** simulation-based, assumes ideal network conditions.
10	Campion et al.	2019	Literature review	UAV swarm communication and control	Communication protocols, swarm coordination	MANET and 5G are optimal for swarm comms but scaling issues exist	Low risk **(AMSTAR 2):** comprehensive review methodology and no conflicts identified.
11	Ma et al.	2018	Empirical study, experimental, system design	UAV-UAV and UAV-USV communication	Communication range, efficiency	Cooperative frameworks improve range and communication in UAV-USV formations	**Medium risk (Cochrane Risk of Bias tool):** due to idealized assumptions in simulations and lack of real-world testing.
12	Sánchez-García et al.	2018	Literature review	Multi-hop networks for UAV and aquatic vehicles	Multi-hop communication, network efficiency	Multi-hop networks address coverage issues but face energy challenges	**Low risk (AMSTAR 2):** comprehensive methodology and transparent data synthesis, no significant conflicts identified.
13	Ramphull et al.	2021	Literature review	MANET protocols and applications	MANET, network protocols	MANET protocols are adaptable but face routing and stability challenges	**Medium risk (Cochrane Risk of Bias tool):** Medium risk due to theoretical focus and lack of empirical validation in dynamic environments.
14	Sharma et al.	2020	Literature survey	UAV communication and networking technologies	Latency, bandwidth, communication reliability	5G, Wi-Fi, and MANETs provide solutions but with range and interference limitations	**Low risk (AMSTAR 2):** systematic review methodology with no conflicts of interest or methodological flaws.
15	Chen et al.	2020	Literature review	UAV swarm communication architectures and routing protocols	Network architecture, routing protocols	Routing protocols for UAV swarms face scalability and latency challenges	**Low risk (AMSTAR 2):** comprehensive and transparent review of communication architectures with no major conflicts.
16	Annenkov et al.	2023	Empirical study, experimental, data analysis	Low-cost UAV data processing	Processing accuracy, cost-effectiveness	Low-cost UAV processing is feasible, but accuracy can be limited in complex conditions	**High risk (RoB 2 tool):** preliminary study with limited data, high risk due to lack of validation and assumptions made about accuracy.
17	Abd El-Latif et al.	2019	Empirical study, simulation, modeling	Quantum security protocols for 5G networks	Data protection, quantum security	Quantum protocols enhance security but require significant computational resources	**Medium risk (Cochrane Risk of Bias tool):** simulation-based with assumptions about real-world scalability and resource use.

(Continued)

Table 1 | (Continued)

No.	Author/s	Year	Methods	Focus	Key Metrics	Findings	Risk of Bias
18	Aggarwal et al.	2024	Empirical study, simulation, theoretical model	Synergy between network security and blockchain	Blockchain integration, security protocols	Blockchain and security integration enhances data security in UAV communications	**Medium risk (RoBANS):** model-based research with assumptions about scalability and real-world feasibility.
19	Chen et al.	2020	Empirical study, literature synthesis, modeling	UAV swarm intelligence and challenges	AI, swarm intelligence, security	AI and machine learning optimize UAV swarm coordination and security	**Medium risk (RoBANS):** limited real-world testing and focus on theoretical advancements, assumptions made about AI application.
20	Kim and Lee	2021	Empirical study, experimental, data analysis	Security enhancement for drones	Data transmission, wireless channels	Wireless security enhancements are crucial for drone network resilience	**Medium risk (Cochrane Risk of Bias tool):** experimentation focused on specific security measures, applicability to real-world conditions uncertain.
21	Wang et al.	2024	Survey, literature review	Security of UAV swarm networks	Security protocols, attacks, countermeasures	UAV swarm networks require robust countermeasures against cyberattacks	**Low risk (AMSTAR 2):** thorough and transparent review, systematic methodology followed with no significant conflicts identified.
22	Kallenborn	2022	Conceptual paper, literature synthesis	UAV swarm networks in information warfare	Network security, military applications	UAV swarms are effective in information warfare but face operational challenges	Medium risk **(RoBANS):** Theoretical framework with no empirical validation, moderate risk due to assumptions.
23	Phadke and Medrano	2022	Empirical study, experimental, model design	Resiliency requirements in UAV swarms	Resilience metrics, failure tolerance	Resiliency protocols improve UAV swarm robustness under critical conditions	Medium risk **(Cochrane Risk of Bias Tool):** Model design-based study, assumes ideal conditions.
24	Rexhepi et al.	2023	Empirical study, simulation, model-based	Intrusion detection in MANETs	Intrusion detection efficiency	Secured IDS improves security in MANETs, applicable to UAV swarm networks	Medium risk **(Cochrane Risk of Bias Tool):** theoretical model, relies on simulation, limited empirical testing.
25	Sharma et l.	2020	Empirical study, experimental, algorithmic	Dynamic routing protocol for MANETs	Routing stability, bandwidth usage	SBADR enhances routing stability and bandwidth efficiency in dynamic networks	Medium risk **(RoBANS):** Simulation-based with assumptions, lacks real-world validation.
26	Rabia et al.	2024	Empirical study, experimental, simulation	SDN integration with MANETs for UAVs	Network throughput, latency	SDN integration enhances MANET performance for UAV swarm communication	Medium risk **(Cochrane Risk of Bias Tool):** based on simulations, assumes ideal scenarios, limited real-world testing.
27	Lopez et al.	2021	Literature survey	Wireless mesh networks for UAV swarm connectivity	Security threats, network performance	Mesh networks improve UAV swarm connectivity but are vulnerable to cyber threats	Low risk **(AMSTAR 2):** well-structured systematic survey, no significant risk of bias.
28	Khalil et al.	2022	Empirical study, simulation, machine learning	Machine learning for UAV swarm communication	Communication efficiency, data integrity	Machine learning improves communication in UAV swarms for search-and-rescue tasks	Medium risk **(Cochrane Risk of Bias Tool):** simulation-based study, assumptions about real-world applicability.
29	Alladi et al.	2020	Literature review	Blockchain applications in UAVs	Blockchain, security, UAV communication	Blockchain enhances security and efficiency in UAV swarm communication	Low risk **(AMSTAR 2):** systematic review with clear methodology, no conflicts.
30	Dong et al.	2021	Empirical study, experimental, simulation	Security for UAV swarm communication	Transmission security, encryption	Enhanced transmission security protocols improve UAV swarm communication resilience	Medium risk **(Cochrane Risk of Bias Tool):** experimental with assumptions based on simulations, needs real-world validation.
31	Wheeb et al.	2021	Literature review	Routing protocols and mobility models for UAVs	Network topology, mobility models	Topology-based routing improves mobility and communication in UAV swarms	Low risk **(AMSTAR 2):** comprehensive review with systematic methodology and transparent data synthesis.
32	Khalek et al.	2023	Literature survey	Cognitive radio and machine learning for UAV networks	Cognitive radio, spectrum management	Cognitive radio optimizes spectrum usage in UAV communication networks	Low risk **(AMSTAR 2):** thorough review with well-organized methodology and clear data.

autonomous systems.[33] Satellite communication provides worldwide coverage, but it is constrained by significant delay and limited bandwidth, rendering it less suitable for real-time applications.[39–41]

In addition to traditional technologies, research is being conducted on innovative solutions such as machine learning for adaptive traffic routing to enhance data transfer by taking into account network dynamics

Table 2 | Comparison of data transmission methods in drone swarms: characteristics and applications

Data transmission method	Bandwidth	Range	Latency	Interference resilience	Energy consumption	Applications	Security protocol integration
Wi-Fi	Up to 600 Mbps	Up to 100 m (indoor, line-of-sight)	Low (within range)	Moderate	High	Local networks, small drone swarms	Supports standard protocols (WPA2/WPA3)
LTE	Up to 100 Mbps	Up to 10 km (urban, line-of-sight)	Moderate	High	Moderate	Urban swarms, agricultural use	Built-in security (IPsec)
5G	Up to 10 Gbps	Up to 1 km (urban)/5 km (rural, line-of-sight)	Very low (sub-1 ms, ideal conditions)	High	High	Critical operations, high-speed comms	Supports modern security protocols
MANET	Configuration-dependent	Topology-dependent	Variable	Moderate	Hardware-dependent	Military ops, rescue missions	Requires additional crypto protocols
DTN	Low	Several km to inter-planetary (depends on satellite network)	High (up to several seconds)	High	Low	Remote regions, space missions	Requires specialised security protocols
Wi-Fi Mesh	Up to 600 Mbps	Node-dependent (typically up to 200 m, depending on environment)	Low	Moderate	High	Extended local networks, urban swarms	Supports WPA2, WPA3
Satellite	Up to 1 Gbps (low Earth orbit, LEO)/100 (geostationary orbit, GEO)	Global coverage (LEO‹1,200 km, GEO›35,000 km)	High (LEO: 30-50 ms, GEO: 500 ms - 1 sec)	Moderate	High	Remote regions, emergencies	Requires specialised security protocols

Source: compiled by the author based on the analysis of relevant regulatory and technical documentation.[16-18]

and environmental variables. Blockchain technology improves data security via decentralised authentication and information verification, facilitating safe communication on UAV networks.[6,24] Contemporary UAV swarm communication integrates conventional wireless technology with novel methods to enhance adaptability, resilience, and security. Every technology possesses unique benefits and constraints, underscoring the necessity of combining many systems to enhance performance in practical applications.[20]

Wireless communication depends on radio waves carried throughout the electromagnetic spectrum, that utilise modulation to encode information for long-distance transmission.[42] The choice of frequency bands is essential, influencing bandwidth, range, interference resistance, and obstacle penetration. Multiplexing systems enable concurrent transmission from several users, minimising interference and enhancing spectrum efficiency.[10,38]

Mobile networks encounter difficulties stemming from the incessant mobility of nodes, resulting in alterations to the topology.[21,37] Specialised routing algorithms adjust to these variations, guaranteeing stable communication despite transient connection disruptions. Mobile networks exhibit flexibility, scalability, and self-organisation, enabling nodes to determine optimal transmission paths.[43]

Interference and multipath propagation provide considerable hurdles, but adaptive strategies and error-correction procedures alleviate these problems.[44] Mobile and wireless systems are interconnected, with communication reliability dependent on their capacity to adjust to environmental fluctuations and utilise existing technologies effectively.[45,46] The advancement of innovative routing techniques, better spectrum distribution, and improved interference robustness is essential for establishing dependable communication systems in fluctuating situations.[47]

In UAV swarm systems, cybersecurity is crucial for safeguarding data transmissions between drones and base stations.[22,48] Cryptographic protocols such as AES, RSA, and ECC safeguard information, guaranteeing confidentiality, integrity, and authentication. Blockchain enhances security through transparency, immutability, and decentralisation.[23,49] It records actions, authenticates data, and safeguards against manipulation, rendering it essential for mission-critical applications such as military or infrastructure operations.

The integration of cryptographic protocols and blockchain establishes a resilient framework for secure data transport.[50,51] AES provides rapid and secure encryption, whereas RSA and ECC facilitate key exchanges.[24] Blockchain ensures data integrity by prohibiting unauthorised modifications. This method is especially advantageous in high-security contexts, such as military operations or critical infrastructure applications.[35]

Table 2 presents a comparative analysis of primary data transmission methods in drone swarms, encompassing parameters such as bandwidth, range, latency, interference resilience, energy consumption, application domains, and security protocol integration. Data sourced from open-access publications enables a clear evaluation of the advantages and limitations of each method, which is crucial for selecting optimal solutions in specific drone swarm deployment scenarios.

After analysing the table, several key conclusions can be drawn. Wi-Fi and Wi-Fi mesh technologies provide high throughput and are effective in local area networks, but their limited range may pose challenges when operating with large drone swarms. LTE and 5G mobile networks offer significantly greater coverage and lower latency, which are critical for urban applications or time-sensitive operational tasks, yet they require developed infrastructure and typically exhibit higher energy consumption.

Methods based on MANET and DTN principles demonstrate flexibility in scenarios with constantly changing network topologies.[30] MANET enables network organisation without centralised control, which is advantageous in military operations or rescue missions, though it necessitates additional cybersecurity measures.[53] DTN, on the other hand, is ideally suited for operation in remote or extreme environments where connectivity may be intermittent. Nonetheless, due to high latency, this method is more orientated towards data transmission in scenarios where time sensitivity is not a decisive factor.

Thus, the selection of an optimal data transmission method depends on the specific tasks and operational conditions of the drone swarm. A comprehensive approach combining multiple technologies can compensate for the shortcomings of individual solutions and create more reliable and efficient communication systems. In the future, the integration of modern security protocols, such as cryptographic methods and blockchain technologies, will further enhance system resilience against external threats and ensure the confidentiality of transmitted data.[3,25]

In modern unmanned systems, particularly in drone swarms, data transmission security is of critical importance.[54] Due to the open nature of wireless networks and potential threats such as interception, spoofing, or data modification, robust cryptographic mechanisms must be implemented. In this context, various encryption algorithms and security protocols are employed to ensure data confidentiality, integrity, and authentication.[36]

Depending on the specific drone application scenario, the choice of algorithm or protocol must consider the trade-off between security level, operational speed, and the computational capabilities of the devices. Table 3 provides a comparison of the primary cryptographic solutions used for securing data in drone swarms.

The analysis of cryptographic algorithms demonstrates that the choice of a specific protection mechanism depends on security requirements, performance, and computational resources. Symmetric algorithms, such as AES, provide high-speed operation with low resource demands, making them optimal for real-time data stream encryption. Asymmetric algorithms, particularly RSA and ECC, are more resource-intensive but effective for authentication and key exchange, with ECC offering significant advantages for devices with limited computational capabilities.

Protocols such as TLS and IPsec are widely used for securing network-layer communications, ensuring data confidentiality and integrity during transmission between drone swarms and ground stations, though their implementation requires sufficient computational power. A promising development direction is the adoption of blockchain technologies, which enable decentralised data protection, event logging, and guaranteed immutability of information transmitted between drones. However, the high resource consumption of blockchain solutions may be a limiting factor in mobile and energy-efficient systems.[6,35]

Thus, for effective data protection in drone swarms, it is advisable to employ hybrid encryption schemes that combine the advantages of symmetric and asymmetric algorithms alongside network security protocols.[3,7] This approach achieves a balance between high security, performance, and energy efficiency, which is critical for mobile unmanned systems.[27]

Regulatory constraints, such as the allocation of cellular bands for UAV communication, significantly impact the deployment of UAV swarm communication

Table 3 | Comparison of cryptographic algorithms and protocols for data protection in drone swarms

Algorithm/ Protocol	Type	Key Length	Performance	Security Level	Resource Requirements	Application Scope
AES	Symmetric algorithm	128, 192, 256 bits	High (AES-128 is fast; AES-256 is more secure but slower)	High	Low	Real-time data encryption, internal drone networks
RSA	Asymmetric algorithm	2048 or 3072 bits	Moderate (longer keys = slower but more secure)	High	High	Key exchange, digital signatures, secure connection establishment
Elliptic Curve Cryptography (ECC)	Asymmetric algorithm	256 bits (equivalent to RSA 3072 bits)	High (faster and more secure for smaller key sizes)	High	Low	Key exchange, digital signatures, mobile and embedded devices
Transport Layer Security (TLS)	Secure communication protocol	Depends on underlying algorithms	Configuration-dependent (performance varies based on cipher suite)	High	Medium	Secure communications between drones and ground stations
IPsec	Network-layer protocol suite	Algorithm-dependent	Moderate (depends on specific protocol used)	High	Medium	Secure VPN connections, network-layer communication between drones and base stations
Blockchain-based protocols	Distributed ledger protocol with cryptographic protection	Variable	Variable (depends on the system and transaction volume)	High	High	Transaction logging, data verification, ensuring integrity and immutability of records

Source: compiled by the author based on the analysis of relevant regulatory and technical documentation.[16-18;26;,] Table 4 | Decision matrix for technology selection in uav swarm communication based on mission profiles

Technology	Latency	Energy Consumption	Coverage	Urban ISR	Disaster Response	Rural Agriculture	Infrastructure-Denied
5G	Very Low	Moderate	High (Urban Focus)	High	Medium	Low	Low
Wi-Fi Mesh	Moderate	High	Short (Local)	Medium	Low	Low	Low
LTE	Low	Moderate	Medium	Medium	High	Medium	Low
MANET	High	High	Variable	Medium	Medium	Low	Medium
DTN	Very High	Low	Very High (Global)	Low	High	High	Very High
Blockchain	High	Low	Global	Medium	High	Low	High

systems. The 3GPP NTN (Non-Terrestrial Networks) standard, for example, is designed to integrate satellite and UAV communication with terrestrial 5G networks, yet its application is subject to strict licensing and spectrum management regulations.[17] UAVs using cellular bands must adhere to regulations set by national and international bodies, which can limit their ability to operate in certain frequencies, especially in rural or remote areas. Additionally, spectrum licensing restrictions can hinder the availability of necessary bandwidth for UAV communication, particularly in densely populated regions where cellular bands are heavily allocated for other uses.

Operational constraints also play a critical role in the effectiveness of UAV swarm systems. One key challenge is Beyond Visual Line of Sight (BVLOS) operations, which are essential for long-range missions but require regulatory approval in many regions.[58] BVLOS operations depend on reliable communication and high-altitude flight, which can face restrictions due to airspace management laws. UAVs operating at higher altitudes often encounter coverage trade-offs, as their communication range may increase, but latency and interference resilience can be compromised, particularly in urban environments with significant radio frequency noise. The need for clear communication channels, both for control and data transmission, adds complexity to UAV operations, especially when operating at altitudes where the line-of-sight to ground stations is obstructed.[11]

These regulatory and operational challenges must be carefully navigated to ensure that UAV swarm systems can operate efficiently and legally in real-world scenarios. Overcoming these constraints requires a combination of technological advancements in spectrum management, regulatory frameworks that allow for more flexible UAV operations, and adaptive solutions that balance communication reliability with the operational limitations imposed by both the environment and regulatory bodies.

Modern drone swarms also face numerous cyber threats, making protection against cyberattacks a critically important task.[59,60] The use of adaptive approaches incorporating artificial intelligence and machine learning methods enables the detection of anomalies in network traffic and rapid response to potential threats.[5;28;34] For instance, behavioural anomaly analysis can signal suspicious activities, such as DDoS attacks or spoofing, helping the system quickly identify malicious access attempts.

The systems employed for data transmission in UAV swarms have unique advantages and drawbacks, contingent upon the particular application, ambient factors, and performance criteria. A decision matrix can facilitate the selection of optimal technologies for various UAV swarm communication scenarios by offering a clear comparison based on critical parameters such as latency, energy consumption, and coverage. Table 4 illustrates the performance of various technologies across several mission profiles, aiding in the selection of suitable solutions.

Wi-Fi and Wi-Fi Mesh networks are appropriate for small-scale UAV operations necessitating high throughput in confined environments.[33] Nonetheless, their range is constrained, and they are susceptible to interference in densely populated regions. Wi-Fi Mesh enhances coverage by employing drones as relay nodes, although it escalates routing complexity and energy consumption. These networks are unsuitable for extensive UAV swarms or applications requiring long-range communication and minimal latency.[14]

LTE and 5G provide rapid connectivity and minimal latency, rendering them appropriate for mission-critical applications such as urban surveillance.[1] 5G, characterised by multi-gigabit speeds and minimal latency, facilitates high-density drone operations. Nonetheless, both 5G and LTE encounter constraints in rural regions where infrastructure may be lacking and experience challenges with range when UAVs are distant from base stations. Moreover, their energy requirements and dependence on infrastructure impede autonomous, extended operations in isolated areas.

MANETs and DTNs offer options for UAVs operating in dynamic situations devoid of reliable infrastructure. MANETs adjust to changing topologies but encounter stability challenges and increased latency over extended distances or at elevated speeds. Delay Tolerant Networks (DTNs) are advantageous in regions with intermittent connectivity, as they provide data storage and forwarding upon the establishment of a link. Nonetheless, their elevated latency renders them inappropriate for real-time applications, although they are proficient for emergency operations or remote monitoring where energy efficiency and routing optimisation are paramount.

Satellite communication provides worldwide coverage and dependable data transmission in remote regions without terrestrial infrastructure. Nevertheless, it experiences considerable delay and restricted capacity, rendering it inappropriate for high-speed, real-time UAV swarm communication. Environmental factors, including meteorological conditions, significantly diminish satellite performance. Although crucial for global coverage in remote areas, its elevated latency and operational expenses render alternatives like 5G or Wi-Fi Mesh more appropriate for localised UAV operations.

The incorporation of 5G in the PHY layer, alongside MANET in the routing layer and AES in the security layer, facilitates low-latency, secure communication in urban swarm operations. This integrated method enhances data transfer, ensuring stability in fluctuating situations (Figure 2). The incorporation of blockchain for decentralised authentication enhances security, especially in mission-critical situations.

Figure 2 depicts the interaction among the various technologies and layers of the UAV swarm communication system across diverse mission scenarios. The communication network among the UAVs is essential for facilitating real-time coordination and ensuring reliable data transfer. The PHY Layer of 5G facilitates high-speed communication with minimal latency, allowing real-time video transmission from UAVs to ground control. Wi-Fi Mesh is employed in the MAC Layer for localised, multi-hop communication among drones inside the swarm.[15] These methods provide rapid and dependable data transmission in densely populated urban areas, where structures may impede long-range signals.

The MAC Layer technology Wi-Fi Mesh and the Routing Layer technology MANET collaborate to facilitate dynamic routing. As UAVs navigate the city, the MANET guarantees that each drone can adjust to alterations in the network topology and reroute data through various pathways as required, assuring continuous connection.[30-32] The Security Layer utilises AES for real-time data encryption to safeguard communications between UAVs. This guarantees the protection of all data, encompassing critical information regarding survivor positions and drone movements. Furthermore, IPsec is employed for VPNs connecting ground stations and drones to protect the entire network against external threats. This integrated methodology, employing 5G, Wi-Fi Mesh, MANET, AES, and IPsec, facilitates the UAV swarm's sustained communication in a complex and dynamic urban setting.[12] The system utilises technology across all levels to guarantee the swarm's effective functioning in urban swarms by providing strong, reliable, and secure communication for disaster response efforts.

In Urban Intelligence, Surveillance, and Reconnaissance (ISR), the primary objectives are minimal latency and rapid data transfer, particularly for real-time video streaming and telemetry data. 5G technology demonstrates exceptional suitability in this context, providing latency as low as 1 ms and bandwidth reaching 10 Gbps. Nonetheless, it is restricted by range constraints, generally not exceeding 1 km in metropolitan environments.[14] This may be a constraint for extensive drone swarm operations, when UAVs may need to function beyond 1 km. Conversely, Wi-Fi Mesh offers considerable bandwidth (up to 600 Mbps) with little latency, although it functions optimally only across limited distances (up to 100 m). Wi-Fi Mesh is appropriate for tiny, localised swarm networks in urban environments, but it is inadequate for extensive urban ISR operations.[2] LTE provides a limited range of up to 10 km, accompanied by elevated latency and modest bandwidth of up to 100 Mbps. In urban ISR operations where real-time communication is essential, 5G demonstrates superiority in bandwidth and latency. Yet, it entails a trade-off concerning energy consumption and dependence on infrastructure.

In rural agriculture, the foremost requirement is for extensive connectivity across regions without infrastructure. Delay-Tolerant Networking (DTN) has low energy consumption, making it suitable for remote activities; however, it is characterised by significant latency, which can extend to several seconds or minutes based on distance.[9] It guarantees data resilience despite intermittent network connectivity, which is common in rural areas.[29] In such instances, 5G and LTE would exhibit diminished efficacy owing to their restricted coverage in rural regions. DTN's capacity for data storage and forwarding renders it suitable for long-range, low-latency-tolerant communication; nonetheless, its primary disadvantage is the elevated latency in time-sensitive situations. Wi-Fi Mesh may be utilised locally for short-range communication; however, it would be impractical for extensive operations.

Communication systems for disaster response must include the flexibility to react to real-time changing conditions. A hybrid strategy that integrates LTE and DTN demonstrates efficacy in this scenario.[7] LTE facilitates medium-range communication with moderate latency (up to 50 ms) and demonstrates enhanced reliability in urban environments, where connectivity may remain partially operational. DTN is crucial for maintaining

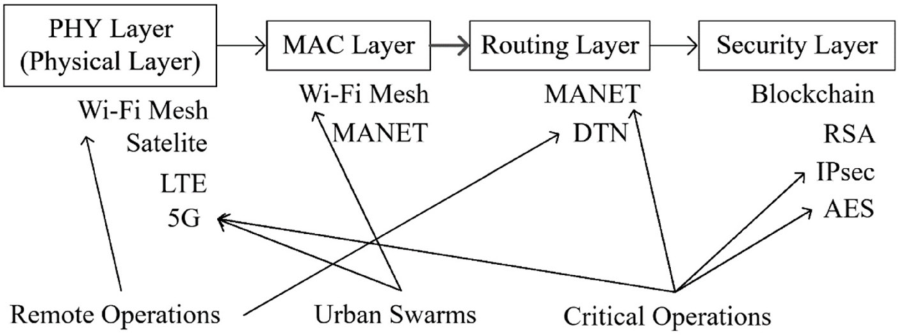

Fig 2 | Conceptual framework of UAV swarm communication system across layers and mission profiles connectivity in rural areas with inconsistent access. The integration of store-and-forward methods in Delay Tolerant Networks (DTN) with real-time communication through LTE can provide robustness in disaster scenarios. 5G, characterised by minimal latency and substantial capacity, is ideal for high-speed applications such as live video streaming; nevertheless, its range constraints require integration with complementary technologies like MANET or DTN.[30-32]

In infrastructure-denied operations, such as military or remote operations lacking cellular or terrestrial infrastructure, satellite communication is vital. Satellite communication offers worldwide coverage; nevertheless, it is limited by significant delay (500 ms to 1 second), rendering it less suitable for time-sensitive operations. The compromise in this situation is between coverage and latency. DTN, characterised by its robust resilience and energy efficiency, is capable of functioning well in such contexts, guaranteeing data transmission even within intermittent connectivity conditions. Nonetheless, the elevated latency of satellite communication renders it inappropriate for real-time interactions; however, it can augment Delay Tolerant Networking (DTN) in scenarios necessitating worldwide coverage and secure data transmission.

These quantitative insights elucidate the trade-offs in communication technology across diverse mission profiles, clarifying latency, bandwidth, and energy usage under varying operational scenarios. Generally, 5G is ideal for real-time, high-bandwidth urban activities, DTN is superior in rural regions with sporadic coverage, and satellite communication facilitates worldwide operations despite significant latency. Simultaneously, technologies such as LTE and Wi-Fi Mesh provide a compromise appropriate for moderate-range applications, balancing latency and energy efficiency.

The validation plan for subsequent research must incorporate simulation parameters that account for mobility patterns, traffic load, and actual environmental variables (e.g., urban interference, rural topography) to assess the efficacy of each technology across varying contexts. Moreover, benchmarking against empirical datasets and employing energy models for UAVs will provide a more accurate quantification of trade-offs and offer recommendations for energy-efficient routing and adaptive frequency management. Integrating these simulations enhances the efficiency and resilience of UAV swarm communication, guaranteeing that the proposed methodologies are both feasible and scalable across diverse mission profiles.[29]

A tailored strategy grounded in particular operational necessities is recommended to enhance UAV swarm communication systems for diverse mission profiles. In urban ISR, 5G is optimal owing to its minimal latency (below 10 ms) and substantial capacity (up to 10 Gbps), rendering it suitable for real-time video streaming and rapid data transmission. Nonetheless, its energy usage raises concerns for extended missions. Conversely, Wi-Fi Mesh provides a limited range (up to 100 m) and exhibits greater energy efficiency, rendering it appropriate for small-scale operations but inadequate for extensive urban ISR missions. LTE has moderate latency (50 ms) and medium coverage (up to 10 km), although it is less effective for high-speed urban operations in comparison to 5G.

In rural agriculture, where extensive communication is required across regions with intermittent connectivity, Delay Tolerant Networking (DTN) provides the optimal solution because of its robustness and little energy usage, despite incurring latency of several minutes. 5G and LTE are less efficient in these regions because of their dependence on infrastructure. The Wi-Fi mesh is effective for localised networking. Nevertheless, its range and energy consumption pose constraints for extensive agricultural monitoring.

A hybrid strategy integrating LTE and DTN is advised for disaster response, ensuring communication remains functional despite compromised infrastructure.[7] LTE provides dependable medium-range connection with moderate latency, whereas DTN guarantees data transmission in regions with intermittent access. Blockchain and AES/IPsec must be employed to guarantee secure data transmission and safeguard sensitive information.

In infrastructure-denied operations, such as military or space missions, satellite communication offers worldwide coverage but entails significant latency (500 ms to 1 second) and reduced capacity. DTN is essential for dependable communication across extended distances, guaranteeing data transmission even in the absence of real-time communication. Blockchain-based identity management ought to be employed to safeguard data exchanges and verify communications between UAVs and ground stations.

Every mission profile necessitates a distinct amalgamation of technologies customised to certain requirements. The trade-offs among latency, energy consumption, and coverage should determine the choice of technologies, including 5G, LTE, DTN, and Wi-Fi Mesh. Security is paramount, with AES, RSA, and IPsec protocols advised for safeguarding data within the communication network. Subsequent efforts must authenticate these recommendations by simulation and practical implementation to refine the system and guarantee optimal performance across various operating contexts.

Recent breakthroughs in machine intelligence and blockchain technologies provide intriguing alternatives to the limits of conventional communication methods.[5;25] Machine learning methods facilitate adaptive routing, enabling UAVs to dynamically modify communication pathways according to real-time network conditions.[34] This is especially beneficial in extensive UAV operations, where mobility and sporadic connectivity pose considerable issues. Moreover, blockchain offers a robust framework for guaranteeing data integrity and security in UAV communications, particularly in military and critical infrastructure contexts.[6] Blockchain can decentralise authority, increasing the system's resilience against attackers. Nonetheless, these technologies entail heightened computing demands and energy consumption, thus hindering their extensive use in energy-limited settings.[35]

Each communication method presents unique trade-offs regarding speed, latency, range, energy usage, and security. The choice of the most suitable approach is contingent upon the particular operational requirements of the UAV swarm, including the necessary range, latency sensitivity, and the security level mandated for the mission. The integration of dynamic routing, adaptive frequency management, and blockchain has demonstrated considerable theoretical enhancements in performance, such as improved security, efficiency, and network resilience. However, these results are still hypothetical and require further empirical validation through simulations and real-world data collection.

The validation plan for further studies must use simulation parameters that account for mobility patterns, traffic load, and actual environmental circumstances (e.g., urban interference, rural topography) to assess the efficacy of each technology across various scenarios. Furthermore, benchmarking against empirical datasets and employing energy models for UAVs would provide a more exact quantification of trade-offs and provide insights into energy-efficient routing and adaptive frequency management. Integrating these simulations enhances the efficiency and resilience of UAV swarm communication, guaranteeing that the offered methodologies are both pragmatic and scalable across diverse mission profiles.

Discussion

The analysis of contemporary data transmission methods in drone swarms indicates a broad spectrum of technological solutions, each with its own advantages and limitations. On the one hand, conventional wireless technologies such as Wi-Fi, LTE, and 5G provide high throughput, enabling the transmission of large volumes of data. On the other hand, their application is constrained by specific characteristics: Wi-Fi has limited range and moderate interference resistance, while 5G, despite its ultra-low latency and high speeds, may be economically impractical in remote regions or during emergency operations due to the lack of appropriate infrastructure.

Phadke and Medrano[29] focused on conventional technologies in their study, noting that Wi-Fi offers high bandwidth, but its limited range and susceptibility to interference make it suboptimal for large drone swarms. LTE provides a balance between range and speed where infrastructure is well-developed, whereas 5G excels in ultra-low latency and high speed, though the economic costs of its deployment in remote areas remain a significant drawback. The present findings align with these conclusions regarding conventional technologies but are supplemented by an analysis of innovative approaches, such as MANETs, DTNs, and machine learning-based adaptive routing, which significantly enhance data transmission efficiency in dynamic environments. This demonstrates a more comprehensive and innovative approach in the current study. MANETs enable the formation of temporary networks without centralised control, ensuring system flexibility and adaptability in dynamic conditions.[61]

Sharma et al.[31] examined dynamic conditions of high node mobility in MANETs, which ensure flexibility and adaptability through the formation of decentralised temporary networks. DTNs are used for data buffering and gradual delivery in challenging environments, but high latency restricts their use in highly time-sensitive scenarios. While MANETs provide responsiveness and DTNs ensure reliability in harsh conditions, both approaches require refinement to achieve an optimal balance between flexibility, reliability, and communication speed. The present findings demonstrate that MANETs offer flexibility but suffer from unstable connections, whereas DTNs are useful in extreme conditions yet are constrained by high latency.

The application of hybrid data transmission methods in unmanned networks can significantly enhance their efficiency and reliability.[62,63] Combining Wi-Fi Mesh, MANETs, and machine learning technologies enables dynamic routing adaptation, minimising data loss and improving throughput. Simultaneously, integrating blockchain for authentication and verification adds an additional layer of security. Nevertheless, the primary challenge remains balancing performance and energy consumption, necessitating further research. Rabia et al.[32] explored hybrid network architectures for unmanned systems and emphasised the importance of combining Wi-Fi Mesh and MANETs to enhance communication flexibility. Their conclusions align with the present findings regarding adaptive routing efficiency, though they focused less on security aspects, prioritising network load optimisation.

Aisyah et al.[64] experimentally confirmed that integrating Wi-Fi Mesh and MANETs significantly reduces latency and improves Quality of Service (QoS) in highly dynamic environments, such as during rescue operations or in remote regions. Particular attention was given to optimising network load through adaptive routing, ensuring uniform traffic distribution among nodes and minimising the risk of congestion. The authors also considered multi-channel solutions to reduce inter-node interference, improving link stability and speed. Lopez et al.[33] investigated the efficiency of Wi-Fi Mesh networks in drone swarms and concluded that their use significantly improves link stability, but only under optimal relay configuration. Their results confirm that Mesh architecture enhances coverage, as noted in the current study, though they found that increasing the number of network nodes may induce latency due to route congestion – an issue not identified as a key problem in the present research.

Adaptive routing that accounts for network dynamics and external factors optimises real-time data transmission, which is particularly relevant for drone swarms operating in complex and unpredictable conditions. Classification, clustering, and behavioural anomaly detection algorithms facilitate rapid identification of potential threats, improving overall system security. Khalil et al.[34] examined the use of machine learning algorithms to optimise communication in drone swarms and found that adaptive routing significantly enhances data transmission efficiency in dynamic environments. Their conclusions align with the present findings regarding the importance of machine learning, though they focused on predictive modelling of network changes, whereas the current study places greater emphasis on anomaly analysis for security enhancement.

Combining cryptographic protocols with blockchain produces a synergistic effect, minimising unauthorised access risks and ensuring data integrity. However, high resource demands and energy consumption remain a major challenge for implementing such solutions in mobile unmanned systems. Alladi et al.[35] explored blockchain applications for data security in unmanned systems and confirmed their effectiveness in ensuring authentication and information integrity. Their conclusions align with this study, though they propose hybrid blockchain architectures to reduce energy consumption, whereas the present research primarily focuses on cryptographic protocols.

Dong et al.[36] investigated combined data transmission methods in drone swarms and concluded that integrating traditional networking technologies with adaptive algorithms significantly enhances communication efficiency. Their results generally align with the present findings, though they primarily focused on latency optimisation, whereas the current study also addresses security and energy consumption. Wheeb et al.[37] analysed the impact of drone mobility on connection stability. They proposed methods for predicting network topology changes based on trajectory analysis and historical link quality data. This enabled the pre-determination of optimal data transmission paths, reducing connection drop frequency. Their study demonstrated that adaptive routing algorithms, such as Q-learning and AODV-PA (Prediction-Assisted), substantially improve transmission efficiency, particularly in high-density drone scenarios. The authors prioritised minimising transmission delays, whereas the present study additionally considers security and energy optimisation, which are critical for the long-term operation of autonomous drone swarms.

Khalek et al.[38] explored the use of cognitive radio networks (CRN) in drone swarms, proposing a machine learning-based adaptive channel selection method that reduces latency and enhances link resilience. Their conclusions align with the present findings regarding communication improvements through adaptive algorithms. However, they focused solely on efficient frequency allocation and did not account for security and energy consumption, which are key aspects of the current study.

This study's findings offer insights into optimising data transmission in UAV swarm systems, addressing the principal research concerns presented in the introduction. This research rigorously analyses classic and contemporary communication methods, demonstrating that a combination solution incorporating dynamic routing, adaptive frequency management, and blockchain markedly improves security, efficiency, and network resilience. This integrated strategy surpasses prior studies by combining established technologies with advanced machine learning algorithms for real-time adaptability and blockchain for enhanced data security, an area not thoroughly examined in previous studies. Although these results are encouraging, additional validation through simulations and empirical testing is necessary to enhance the practical implementation of these systems.

Conclusions

This study presents a comprehensive analysis of modern data transmission methods in drone swarms, aimed at ensuring stable, rapid, and secure communication under conditions of dynamic network topology and high node mobility. Both conventional and innovative approaches to communication organisation were examined, including the application of Wi-Fi, LTE, 5G, as well as MANET and DTN.

The use of Wi-Fi and Wi-Fi Mesh technologies enables high-throughput data transmission, which is critical for implementing local drone swarm networks. However, limited range and susceptibility to interference in complex operational environments impose certain constraints on these methods. LTE and 5G technologies demonstrate significantly higher transmission speeds and lower latency, representing a considerable advantage for urban applications or time-sensitive tasks. Yet, their implementation requires developed infrastructure and substantial financial investment, which may be impractical in remote regions or during emergency scenarios.

Particular attention was given to methods tailored for dynamic networks. The use of MANET facilitates the establishment of temporary networks without centralised control, which is advantageous in military or rescue operations. However, connection instability and routing complexity may affect data transmission efficiency. Similarly, DTN systems are optimal for environments with intermittent connectivity, ensuring data buffering and gradual delivery, though high latency limits their applicability in time-critical scenarios.

The study also highlighted promising directions for innovative technologies. The implementation of machine learning algorithms for adaptive routing optimises data transmission by accounting for variable network conditions, while blockchain integration enhances security through decentralised authentication and information verification systems. This comprehensive approach creates synergy, compensating for the shortcomings of individual methods and achieving a high level of reliability in drone swarm data transmission systems.

A comparative analysis of different data transmission methods was conducted based on parameters such as throughput, range, latency, interference resilience, energy consumption, and security protocol integration. The results indicate that the optimal solution depends on specific operational conditions and objectives. For instance, hybrid schemes combining conventional wireless technologies with innovative approaches are advisable when working with large drone swarms or in infrastructure-deficient environments.

Thus, this study has enabled a thorough evaluation of modern data transmission methods in drone swarms, identifying their advantages and limitations while outlining future directions for developing integrated communication systems. The current study's findings could greatly enhance real-world applications in defence, disaster response, and agriculture, where reliable and safe communication is crucial for operational success. The analysis suggests that the hypothesis regarding the collective enhancement of UAV swarm communication using dynamic routing, adaptive frequency management, and blockchain is promising. Nonetheless, additional study, encompassing simulation studies and field testing, is required to verify the practical efficacy and optimisation of this integrated strategy. The research is limited to open-source data analysis and simulation models, which may not fully reflect the complexity of real-world drone swarm operations. Further studies should focus on experimental validation of the proposed data transmission methods in field conditions and the development of adaptive routing algorithms accounting for dynamic external factors.

References

1 Patel B, Yarlagadda VK, Dhameliya N, Mullangi K, Vennapusa SCR. Advancements in 5G technology: Enhancing connectivity and performance in communication engineering. Eng Int. 2022;10(2):117–130. https://doi.org/10.18034/ei.v10i2.715

2 Gokalgandhi B, Tavares M, Samardzija D, Seskar I, Gacanin H. Reliable low-latency Wi-Fi mesh networks. IEEE Internet Things J. 2021;9(6):4533–4553. https://doi.org/10.1109/JIOT.2021.3105981

3 Albalawi M, Song H. Data security and privacy issues in swarms of drones. In: 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS); 2019. p. 274–284. Piscataway: IEEE. https://doi.org/10.1109/ICNSURV.2019.8735133

4 Jahir Y, Atiquzzaman M, Refai H, Paranjothi A, LoPresti PG. Routing protocols and architecture for disaster area network: A survey. Ad Hoc Netw. 2019;82:1–14. https://doi.org/10.1016/j.adhoc.2018.08.005

5 Zhou Y, Rao B, Wang W. UAV swarm intelligence: Recent advances and future trends. IEEE Access. 2020;8:183856–183878. https://doi.org/10.1109/ACCESS.2020.3028865

6 Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: A perspective about security. IEEE Access. 2024;12:3881–3897. https://doi.org/10.1109/ACCESS.2023.3349019

7 Pirzadi S, Pourmina MA, Safavi-Hemami SM. A novel routing method in hybrid DTN-MANET networks in the critical situations. Comput. 2022;104(9):2137–2156. https://doi.org/10.1007/s00607-022-01084-3

8 Nakas C, Kandris D, Visvardis G. Energy efficient routing in wireless sensor networks: A comprehensive survey. Algorithms. 2020;13(3):72. https://doi.org/10.3390/a13030072

9 Asaamoning G, Mendes P, Rosário D, Cerqueira E. Drone swarms as networked control systems by integration of networking and computing. Sensors. 2021;21(8):2642. https://doi.org/10.3390/s21082642

10 Saleem Y, Rehmani MH, Zeadally S. Integration of Cognitive Radio Technology with unmanned aerial vehicles: Issues, opportunities, and future research challenges. J Netw Comput Appl. 2015;50:15-31. https://doi.org/10.1016/j.jnca.2014.12.002

11 Liu W, Zhou S, Qi Y, Yan S. Distributed formation control for multiple unmanned aerial vehicles with directed switching communication topologies. Control Theory Appl. 2015;32(10):1422-1427. https://doi.org/10.7641/CTA.2015.50478

12 Campion M, Ranganathan P, Faruque S. UAV swarm communication and control architectures: A review. J Unmanned Veh Syst. 2019;7(2):93-106. https://doi.org/10.1139/juvs-2018-0009

13 Giagkos A, Tuci E, Wilson MS, Charlesworth PB. Evolutionary coordination system for fixed-wing communications unmanned aerial vehicles. In: Advances in Autonomous Robotics Systems. Cham: Springer, 2014, pp 48–59. https://doi.org/10.1007/978-3-319-10401-0_5

14 Ma Y, Zhao Y, Qi X, Zheng Y, Gan R. Cooperative communication framework design for the unmanned aerial vehicles-unmanned surface vehicles formation. Advances in Mechanical Engineering. 2018;10(5). https://doi.org/10.1177/1687814018773668

15 Sánchez-García J, García-Campos JM, Arzamendia M, Reina DG, Toral SL, Gregor D. A survey on unmanned aerial and aquatic vehicle multi-hop networks: Wireless communications, evaluation tools and applications. Comput Commun. 2018;119:43-65. https://doi.org/10.1016/j.comcom.2018.02.002

16 Wi-Fi standards: IEEE 802.11ac, 802.11ax and wireless Internet standards. 2024. Available from: https://www.dell.com/support/contents/en-ee/article/product-support/self-support-knowledgebase/networking-wifi-and-bluetooth/wi-fi-network-standards-overview

17 5G; Unmanned Aerial System (UAS) support in 3GPP (3GPP TS 22.125 version 17.6.0 Release 17). ETSI TS 122 125 V17.6.0 (2022-04). 2022. https://www.etsi.org/deliver/etsi_ts/122100_122199/122125/17.06.00_60/ts_122125v170600p.pdf#:~:text=The%20present%20document%20identifies%20the%20requirements%20for%20operation,tracking%20of%20UAS%20linked%20to%20a%203GPP%20subscription.

18 Consultative Committee for Space Data Systems. Report Concerning Space Data System Standards: Rationale, scenarios, and requirements for DTN in space. Informational report CCSDS 734.0-G-1. CCSDS; 2010. https://ccsds.org/Pubs/734x0g1e1.pdf

19 Ramphull D, Mungur A, Armoogum S, Pudaruth S. A review of mobile ad hoc NETwork (MANET) protocols and their applications. In: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS); 2021. p. 204–211. Piscataway: IEEE. https://doi.org/10.1109/ICICCS51141.2021.9432258

20 Sharma A, Vanjani P, Paliwal N, Basnayaka CMW, Jayakody DNK, Wang HC, Muthuchidambaranathan P. Communication and networking technologies for UAVs: A survey. J Netw Comput Appl. 2020;168:102739. https://doi.org/10.1016/j.jnca.2020.102739

21 Chen X, Tang J, Lao S. Review of unmanned aerial vehicle swarm communication architectures and routing protocols. Appl Sci. 2020;10(10):3661. https://doi.org/10.3390/app10103661

22 Annenkov A, Medvedskyi Y, Demianenko R, Adamenko O, Soroka V. Preliminary accuracy assessment of low-cost UAV data processing results. In: GeoTerrace 2023 - International Conference of Young Professionals; 2023. Lviv: European Association of Geoscientists and Engineers. https://doi.org/10.3997/2214-4609.2023510014

23 Abd EL-Latif AA, Abd-El-Atty B, Venegas-Andraca SE, Mazurczyk W. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. Future Gener Comput Syst. 2019;100:893–906. https://doi.org/10.1016/j.future.2019.05.053

24 Aggarwal P, Thamaraimanalan T, Logeshwaran J, Shukla RP, Vishwakarma P, Aeri M. Exploring the synergy between network security and blockchain technology. In: Shukla B, Agarwal R, Khatri SK, Soni KM, Singh AV, Jain S, Sindhwani N, Chaudhary A, Gautam R, editors. 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); 2024. p. 1098–1103. Piscataway: IEEE. https://doi.org/10.1109/ICRITO61523.2024.10522287

25 Chen W, Liu J, Guo H, Kato N. Toward robust and intelligent drone swarm: Challenges and future directions. IEEE Netw. 2020;34(4):278–283. https://doi.org/10.1109/MNET.001.1900521

26 Kim D, Lee H. Security enhancement of drone considering the characteristics of data transmitted between wireless channels. Def Secur. 2021;5:1–19. https://doi.org/10.48550/arXiv.2109.01458

27 Wang X, Zhao Z, Yi L, Ning Z, Guo L, Yu FR, Guo S. A survey on security of UAV swarm networks: Attacks and countermeasures. ACM Comput Surv. 2024;57(3):74. https://doi.org/10.1145/3703625

28 Kallenborn Z. InfoSwarms: Drone swarms and information warfare. US Army War Coll Q Parameters. 2022;52(2):87–102. https://doi.org/10.55540/0031-1723.3154

29 Phadke A, Medrano FA. Towards resilient UAV swarms – A breakdown of resiliency requirements in UAV swarms. Drones. 2022;6(11):340. https://doi.org/10.3390/drones6110340

30 Rexhepi BR, Kumar A, Gowtham MS, Rajalakshmi R, Paikaray MD, Adhikari PK. A secured intrusion detection system integrated with the conditional random field for the MANET network. Int J Intell Syst Appl Eng. 2023;11(3s):14–21.

31 Sharma A, Bansal A, Rishiwal V. SBADR: Stable and bandwidth aware dynamic routing protocol for mobile ad hoc network. Int J Pervasive Comput Commun. 2020;16(3):205–221. https://doi.org/10.1108/IJPCC-05-2019-0043

32 Rabia S, Idris S, Lilia G, Benjamin K. SDMANET: Enhancing MANETs with hybrid protocols through SDN integration. In: 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA); 2024. p. 574–581. Piscataway: IEEE. https://doi.org/10.1109/ACDSA59508.2024.10467333

33 Lopez MA, Baddeley M, Lunardi WT, Pandey A, Giacalone JP. Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities. In: 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS); 2021. p. 319–326. Piscataway: IEEE. https://doi.org/10.1109/DCOSS52077.2021.00059

34 Khalil H, Rahman SU, Ullah I, Khan I, Alghadhban AJ, Al-Adhaileh MH, Ali G, ElAffendi M. A UAV-swarm-communication model using a machine-learning approach for search-and-rescue applications. Drones. 2022;6(12):372. https://doi.org/10.3390/drones6120372

35 Alladi T, Chamola V, Sahu N, Guizani M. Applications of blockchain in unmanned aerial vehicles: A review. Veh Commun. 2020;23:100249. https://doi.org/10.1016/j.vehcom.2020.100249

36 Dong R, Wang B, Cao K, Cheng T. Securing transmission for UAV swarm-enabled communication network. IEEE Syst J. 2021;16(4):5200–5211. https://doi.org/10.1109/JSYST.2021.3111746

37 Wheeb AH, Nordin R, Samah AA, Alsharif MH, Khan MA. Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions. Drones. 2021;6(1):9. https://doi.org/10.3390/drones6010009

38 Khalek NA, Tashman DH, Hamouda W. Advances in machine learning-driven cognitive radio for wireless networks: A survey. IEEE Commun Surv Tutor. 2023;26(2):1201–1237. https://doi.org/10.1109/COMST.2023.3345796

39 Kodheli O, Lagunas E, Maturo N, Sharma SK, Shankar B, Montoya JFM, Duncan JCM, Spano D, Chatzinotas S, Kisseleff S, Querol J, Lei L, Vu TX, Goussetis G. Satellite communications in the new space era: A survey and future challenges. IEEE Commun Surv Tutor. 2020;23(1):70–109. https://doi.org/10.1109/comst.2020.3028247

40 Sekenov B, Smailov N, Tashtay Y, Amir A, Kuttybayeva A, Tolemanova A. Fiber-Optic Temperature Sensors for Monitoring the Influence of the Space Environment on Nanosatellites: A Review. Mech Mach Sci. 2024;167:371–380. https://doi.org/10.1007/978-3-031-67569-0_42

41 Panchenko A, Voloshina A, Fatyeyev A, Rezvaya K, Mudryk K. Changing the output characteristics of a planetary hydraulic motor. In: Lecture Notes in Mechanical Engineering. Cham: Springer; 2024. p. 304–313. https://doi.org/10.1007/978-3-031-63720-9_26

42 Rubino L, Rubino G, Conti P. Design of a power system supervisory control with linear optimization for electrical load management in an aircraft on-board dc microgrid. Sustainab Switz. 2021;13(15):8580. https://doi.org/10.3390/su13158580

43 Kharchenko V, Ponochovnyi Y, Qahtan A-SM, Boyarchuk A. Security and availability models for smart building automation systems. Int J Comput. 2017;16(4):194–202.

44 Rubino G, Rubino L, Langella R. Comparative study of solid state circuit breakers for large inductive loads. In: 2024 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM); 2024. p. 76–80. Napoli: IEEE. https://doi.org/10.1109/SPEEDAM61530.2024.10609050

45 Destek MA, Hossain MR, Manga M, Destek G. Can digital government reduce the resource dependency? Evidence from method of moments quantile technique. Resour Policy. 2024;99:105426. https://doi.org/10.1016/j.resourpol.2024.105426

46 Azieva G, Kerimkhulle S, Turusbekova U, Alimagambetova A, Niyazbekova S. Analysis of access to the electricity transmission network using information technologies in some countries. E3S Web Conf. 2021;258:11003. https://doi.org/10.1051/e3sconf/202125811003

47 Park J, Samarakoon S, Elgabli A, Kim J, Bennis M, Kim SL, Debbah M. Communication-efficient and distributed learning over wireless networks: Principles and applications. Proc IEEE. 2021;109(5):796–819. https://doi.org/10.1109/JPROC.2021.3055679

48 Kiurchev S, Abdullo MA, Vlasenko T, Prasol S, Verkholantseva V. Automated control of the gear profile for the gerotor hydraulic machine. In: Lecture Notes in Mechanical Engineering; 2023. p. 32–43. Cham: Springer. https://doi.org/10.1007/978-3-031-16651-8_4

49 Biluk I, Shareyko D, Fomenko A, Havrylov S, Savchenko O, Stavinskiy R. Construction and adjustment of a vibration machine based on a complete electric drive. In: 2019 International Conference on Modern Electrical and Energy Systems (MEES); 2019. p. 114–117. Kremenchuk: IEEE. https://doi.org/10.1109/MEES.2019.8896563

50 Kerimkhulle S, Kerimkulov Z, Bakhtiyarov D, Turtayeva N, Kim J. In-field crop-weed classification using remote sensing and neural network. In: 2021 IEEE International Conference on Smart Information Systems and Technologies (SIST); 2021. p. 9465970. https://doi.org/10.1109/SIST50301.2021.9465970.

51 Biliuk I, Shareyko D, Fomenko L, Savchenko O, Havrylov S, Maiboroda O. Reduction of numerical arrays in magnetometry problems calculations. In: 2022 IEEE 4th International Conference on Modern Electrical and Energy Systems (MEES); 2022. Kremenchuk: IEEE. https://doi.org/10.1109/MEES58014.2022.10005780

52 European Commission. Broadband: Technology comparison. 2025. https://digital-strategy.ec.europa.eu/en/policies/broadband-technology-comparison

53 Shults R, Urazaliev A, Annenkov A, Nesterenko O, Kucherenko O, Kim K. Different approaches to coordinate transformation parameters determination of nonhomogeneous coordinate systems. In: 11th International Conference "Environmental Engineering"; 2020. p. enviro.2020.687. Vilnius: VGTU. https://doi.org/10.3846/enviro.2020.687

54 Seidaliyeva U, Smailov N. Leveraging drone technology for enhanced safety and route planning in rock climbing and extreme sports training. Retos. 2025;63:598–609. https://doi.org/10.47197/retos.v63.110869

55 Kalashnikova V. Methods of managing an automated mobile system. Innov Technol Sci Solut Ind. 2024;4(30):67–84. https://doi.org/10.30837/2522-9818.2024.4.067

56 Yang W. ECC, RSA, and DSA analogies in applied mathematics. In: Proceedings of the International Conference on Statistics, Applied Mathematics, and Computing Science; 2022. p. 121632P. Nanjing: SPIE. https://doi.org/10.1117/12.2628013

57 Qazzaz MMH, Zaidi SAR, McLernon DC, Hayajneh AM, Salama A, Aldalahmeh SA. Non-terrestrial UAV clients for beyond 5G networks: A comprehensive survey. Ad Hoc Netw. 2924;157:103440. https://doi.org/10.1016/j.adhoc.2024.103440

58 Wan F, Yaseen MB, Riaz MB, Shafiq A, Thakur A, Rahman MO. Advancements and challenges in UAV-based communication networks: A comprehensive scholarly analysis. Results Eng. 3034;24:103271. https://doi.org/10.1016/j.rineng.2024.103271

59 Dahan E, Aviv I, Diskin T. Aerial imagery redefined: next-generation approach to object classification. Information. 2025;16(2):134. https://doi.org/10.3390/info16020134

60 Shults R, Annenkov A. BIM and UAV photogrammetry for spatial structures sustainability inventory. Int Arch Photogramm Remote Sens Spat Inf Sci. 2023;48(5/W2-2023):99–104. https://doi.org/10.5194/isprs-archives-XLVIII-5-W2-2023-99-2023

61 Bondarenko IN, Vasiliev YuS, Zhizhiriy AS, Ishenko AL. Arrangement device for monitoring of parameters of microwave resonators. In: 2010 20th International Crimean Conference Microwave and Telecommunication Technology (CriMiCo); 2010. p.

969–970. IEEE Computer Society. https://doi.org/10.1109/crmico.2010.5632420

62 Wójcik W, Kalizhanova A, Kulyk YA, Knysh BP, Kvyetnyy RN, Kulyk AI, Sichko TV, Dumenko VP, Bezstmertna OV, Adikhanova S, Zhassandykyzy M, Junisbekov M, Smailov N, Yussupova G. The Method of Time Distribution for Environment Monitoring Using Unmanned Aerial Vehicles According to an Inverse Priority. J Ecol Eng. 2022;23(11):179–187. https://doi.org/10.12911/22998993/153458

63 Kurdiuk S, Dremliuk V, Melnyk O, Onishchenko O, Fomin O, Píštěk V, Kučera P. Development of a high-reliability hybrid data transmission system for unmanned surface vehicles under interference conditions. Drones. 2025;9(3):174. https://doi.org/10.3390/drones9030174

64 Aisyah N, Hidayat R, Zulaikha S, Rizki A, Yusof ZB, Pertiwi D, Ismail F. Artificial intelligence in cryptographic protocols: Securing e-commerce transactions and ensuring data integrity. Int J Responsible Artif Intell. 2019;1:1–15.