OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 09 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

# SYSTEMATIC REVIEW OF UAV SWARM RELAY NETWORKS AND FLYING AD HOC NETWORKS (FANETS)— PROTOCOLS, ROUTING CHALLENGES, SECURITY ASPECTS

***Muhammad Asad[1], Waqas Rauf Khattak[2], Abdullah Shabbir[3], Waqar Ahmad[4]***

[1]*Senior Avionics Engineer, Aerospace and Defense Development Center, Saudi Arabia.*
[2]*Senior Avionics Engineer, WAKEB Tech, Riyadh, Saudi Arabia.*
[3]*Avionics Engineer, Wakeb Tech, Riyadh, Saudi Arabia.*
[4]*Assistant Manager, Aerospace Design & Innovation Center (ADIC), NASTP, Pakistan.*
[*]***Corresponding Author:*** asadGujjar4445@gmail.com

**Article Info**



**Abstract**

Background: Unmanned Aerial Vehicles (UAVs) relay nets and Flying Ad Hoc Networks (FANETs) have become effective facilitators of applications like disaster management, surveillance, smart transportation and military logistics. Compared to the conventional mobile ad hoc networks, FANETs are subject to extreme mobility, three-dimensional movement, intermittency, and use of limited onboard resources, which present a great challenge to routing reliability, network performance as well as security.
Objective: This paper would be a systematic review of the literature on the UAV relay networks and FANETs with emphasis on routing protocols, challenges related to mobility, performance analysis, and security threats and solutions.
Methods: The systematic review was performed based on PRISMA 2020. A wide literature search on IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and Google Scholar revealed the presence of appropriate literature within the last five years (2012-2025). After screening and quality evaluation, 137 peer reviewed articles were found by carefully sifting through a plethora of literature. This was achieved through narrative analysis of data and it was backed by comparative tables and graphical illustrations.
Results: The findings show that position-based (geographic) routing protocols always experience better packet delivery ratios (6595) and lower delay than topology-based routing protocols especially in high-mobility and dense FANET environment. As UAV speed is increased, breakages of links and poor routing stability increases, indicating the constraints of protocols which do not have mobility prediction mechanisms. Security analysis indicates that FANETs are susceptible to black hole attack which involves wormhole, GPS spoofing attack, Sybil, and denial of service attack. New countermeasures that take advantage of lightweight cryptography, trust-based routing, blockchain technology, and AI-based intrusion detection systems hold potential, but at the cost of energy consumption and algorithm costs still remain.
Conclusion: The conclusion of the review is that the performance of FANET is greatly affected by mobility dynamics, the choice of routing strategy, and security integration. The use of position-based and intelligent routing methods is more scalable and robust, and the security issue is still a research question. Future studies are needed on holistic, adaptive, and secure routing schemes, experimental studies, and cross-layer optimization to aid reliable large scale FANET implementations.

**Keywords:** *Unmanned Aerial Vehicles (UAVs); Flying Ad Hoc Networks (FANETs); Routing Protocols; Mobility Management; Network Security; Geographic Routing.*

## Introduction

Unmanned Aerial Vehicles (UAVs) have quickly transformed independent aerial systems into network-based systems that can be used to provide an extensive variety of civilian and military services such as disaster management, environmental surveillance, intelligent agriculture, traffic surveillance, border security, and emergency communications. In a scenario where two or more UAVs are cooperating without depending on fixed infrastructure, a UAV relay network or Flying Ad Hoc Networks (FANETs) is formed with each UAV serving as a source of data as well as a network node [1, 2]. The networks are also able to provide flexible, on-demand communication where the land infrastructure is either inaccessible or destroyed or in impractical locations, which has led to FANETs being an important element of the next-generation wireless networks.

FANETs being what they are, they are fundamentally different to traditional Mobile Ad Hoc Networks (MANETs) and Vehicular Ad Hoc Networks (VANETs). The UAVs demonstrate high mobility, have three-dimensional movement, dynamic topology changes and intermittent connectivity, thus making routing and management of networks extremely difficult. Connection breakdowns of UAVs are commonly caused by high speeds, altitude changes and movement direction leading to unstable communication routes and higher packet losses. Such peculiarities make most of the traditional routing protocols ineffective or inapplicable to the context of FANETs [3]. Therefore, one of the major research areas has been to design routing mechanisms capable of being flexible to such dynamic conditions.

The reliability and efficiency of the UAV relay networks are highly dependent on routing protocols. A great variety of routing strategies has been suggested in the last ten years, such as topology-based, position-based (geographic), hybrid, delay-tolerant and more recently, artificial intelligence (AI)-assisted routing protocols. Though topology-based protocols are based on route discovery and maintenance, they tend to experience excessive control overheads and route failures by high mobility. Position-based routing protocols, on the contrary, exploit real-time location information to make forwarding decisions to reduce the cost of maintaining routes and enhance scalability. Yet, they largely rely on proper positioning and effective localization systems [4]. The hybrid and intelligent routing strategies are trying to merge the advantages of various strategies, but their efficiency in extreme mobility pattern and density of the network is still not fully investigated.

Mobility is commonly known as one of the most powerful parameters that influence the performance of FANETs. Speed of the UAVs, the flight paths, and the movement patterns according to the missions have a direct influence on the link stability, the ratio of packet delivery, the end-to-end delay, and the routing overhead. The high mobility causes the topology to change rapidly and often break links, thereby affecting the performance of the network negatively and amplifying the number of retransmissions. Moreover, UAVs have a hard energy limitation and high communication overhead may cause flight duration and mission time to drop considerably. Although it is crucial, energy efficiency tends to be a low-priority issue in routing protocol assessment, which is a key gap in the current research [5, 6].

Besides the issues of performance, security is a significant issue in FANETs because they have an open wireless medium, decentralized structure, and no fixed infrastructure. Blackhole attacks,

wormhole attacks, GPS spoofing attacks, Sybil attacks, and denial-of-service attacks are among the threat attacks that UAV networks are particularly vulnerable to and are capable of seriously interfering with the routing activities and mission goals [7]. The conventional security measures that are developed to operate within a static or low mobility network are frequently not suitable in FANETs because they have the tendency of causing excessive computational and communicational overhead. Probably, the lightweight cryptographic scheme, trust-based routing, security with blockchain, and AI-based intrusion detection systems are the new possible solutions being explored in recent studies. Nonetheless, the combination of security apparatus with routing protocols in a way that would balance performance, energy utilization and scale is a major issue [8].

The current literature is very disjointed, and the methodologies of evaluation are inconsistent, as well as simulation assumptions and cross-comparison of the findings, despite many studies on particular aspects of FANET routing, mobility, or security. A lot of suggested solutions are tested in idealized conditions, and they are rarely tested in reality. In addition, there is a paucity of literature that conducts an in-depth study that collectively addresses routing performance, mobility dynamics, energy constraints, and security threats. Consequently, scholars and practitioners do not have a cohesive view of the status of FANET studies and the most promising research areas in the future of the development of this technology.

To overcome this shortcoming, the paper at hand gives a systematic review of UAV relay networks and FANETs with regard to routing protocols, routing issues, network performance, and security issues. This work presents the structured taxonomy of routing protocols by using PRISMA 2020 guidelines and evaluating them under different mobility conditions, provides the synthesis of existing security threats and countermeasures [9, 10]. The main contributions of the paper are tri-fold, namely provision of a broad classification and comparative analysis of the FANET routing protocols, in-depth discussion of mobility as a cause of challenges and effect on the stability and performance of the network, and the final unified evaluation of the security vulnerability and the defense mechanisms introduced.

## Literature Review

The fast development of the Unmanned Aerial Vehicle (UAV) technologies has provided growing interest to UAV-based communication networks, especially UAV relay networks and Flying Ad Hoc Networks (FANETs). The initial studies were mainly concerned with the extension of the standard Mobile Ad Hoc Network (MANET), Vehicular Ad Hoc Network (VANET) protocols to airspace. Later experiments, however, revealed that such protocols do not work effectively when mobility is extreme, when possible, movement is three-dimensional, and topology is dynamic (as is the case in FANETs). It is this understanding that led to the creation of FANET-specific routing approaches, mobility models and security frameworks that are specific to aerial networks [11, 12].

## Routing Protocols in FANETs

Design of routing protocol has been one of the major topics in FANET research. One of the initial routing protocols that were explored was topology-based routing protocols, both proactive and reactive. Active protocol ensures that routing tables are kept current by periodical updates and this leads to high control overhead as well as poor scalability in highly mobile UAV networks. Reactive

protocols minimize overhead and use on-demand route discovery, but still, they experience frequent route tears and high latency because of a very fast topology adjustment. Multiple works observed the severe deterioration of the ratio of packets delivery and end-to-end delay when the protocols relying on topology are used in the high-speed scenarios involving UAVs and restricted their use in real-time flights.

The problem of these limitations has led to the extensive discussion of position-based (geographic) routing protocols. These protocols are based on real-time location information using GPS or other methods of localization so that packets can be sent without full routing tables. Many studies revealed that, geographic routing protocols provide better packet delivery ratios and delays especially in dense FANETs deployments. However, the accuracy of location information and mechanisms of stable neighbor discovery is critical to their functionality [13, 14]. Any mistakes in positioning or a slow update of beacons may result in less optimum forwarding choices and loss of packets.

Hybrid routing protocols are based on the principles of dynamically adaptive routing behavior and the integration of topology-based and position-based routing methods, depending on the conditions of the networks. Although the hybrid solutions prove to be more robust in some situations, the complexity and the reliance of the parameter tuning often restricts their applicability in practice. Bio-inspired routing protocols and artificial intelligence (AI)-based routing protocols have attracted more attention recently. These solutions are based on machine learning, reinforcement learning and swarm intelligence to forecast mobility patterns and make routing decisions. In spite of the reported encouraging results concerning the adaptability and performance rates, the majority of AI-based solutions are operating on the simulation level and have not been proven in practice.

**Network Performance and Mobility Models.**

The other important feature of FANET studies is mobility modeling because the patterns of UAV movement directly determine the link stability and routing performance. Simplified mobility models like Random Waypoint or Random Walk have been used in the early studies, and these are not able to provide realistic UAV flight behavior [15, 16]. Further studies came up with more advanced models such as Gauss-Markov, mission-based and group mobility models to more accurately model coordinated UAV operations. Although these have been enhanced, standardized mobility models of FANET evaluation remain in a state of disagreement and thus cross-study comparisons prove to be difficult.

A number of studies have examined the effect of mobility on the key performance indicators like the ratio of packet delivery, end to end delay and routing overhead. It is also constantly documented in literature that as UAV speed is increased, the number of link breakages, routing overhead and network performance are negatively impacted. Procedures that do not have mobility awareness or prediction systems are still susceptible especially in highly mobile situations [17, 18]. The results of the work indicate that mobility prediction and trajectory awareness are crucial factors that need to be considered in the design of routing protocols.

**UAV Networking energy limits.**

The low onboard power of UAVs has become an increasing issue in the FANET literature as a result of energy conservation. Communication related power usage such as the exchange of control messages and retransmissions have the potential to severely diminish flight duration. Whereas other research puts forward energy-sensitive routing protocols, energy efficiency is frequently considered as a secondary design goal, as opposed to a primary one. Position-based routing and AI-assisted routing solutions tend to be less energy-consuming because they have lower control overhead, nevertheless, not many studies offer an in-depth discussion of the trade-offs between energy efficiency, routing stability, and network security.

**Security Problems and Resolutions.**

One of the dimensions of FANET research is security, which is critical but under-researched. Decentralized and open UAV networks are very prone to all types of attacks such as blackhole, wormhole, GPS spoofing, Sybil and denial-of-service attacks. Other studies have established that these attacks have the potential of crippling routing functions, data integrity, and mission success. Conventional security tools which have been developed to operate across the terrestrial network tend to cause excessive overhead and are not suitable in the resource limited UAV platforms.

In order to overcome these dilemmas, scholars have introduced light cryptographic authentication protocols, trust routing protocols and intrusion detection systems (IDS). Lately, security frameworks based on blockchain are also investigated to allow decentralized control of trust and correct exchange of data. Also, artificial intelligence-based anomaly detecting methods have demonstrated possibilities of detecting malicious actions in dynamic FANET settings. Although they are promising, these methods have scaling issues, are computationally complex, and use more energy than anticipated, and the combination of these methods and routing protocols remains an unresolved research issue.

**Research Gaps and Motivation for This Study**

Despite the fact that the current literature has a lot to offer in terms of certain peculiarities of the FANET routing, mobility, and security, it is disorganized and inconsistent regarding its methodology. Most research is done based on individual measures of performance or situations of attack without paying much attention to the extended meaning of them [19, 20]. The comparative studies between the routing protocol categories are few and there are few experimental validations in reality. Moreover, there are, few researches that would take a holistic approach that would consider routing performance, mobility dynamics, energy efficiency, and security together.

It is on the basis of these limitations that systematic and thorough review is warranted as a way of consolidating the existing research, determining the most significant trends, and outlining the challenges that remain unresolved. This paper intends to offer a single source of information to the researchers and practitioners involved in the work of UAV relay networks and FANETs by summarizing the results of a large body of literature and correlating them with standardized evaluation criteria.

## Methodology

### Study Design

This paper uses a systematic review approach in its systematic study of the UAV relay networks and Flying Ad Hoc Networks (FANETs) in specific reference to routing protocols, network performance issues, mobility and security. The study was planned and presented following the Preferred Reporting Items of Systematic Reviews and Meta-Analyses (PRISMA) 2020 principles and guaranteed transparency, reproducibility, and rigor of the methodology.

### The major purposes of the review included to evaluate:

Performance of routing of UAV relay networks and FANETs.
Effects of the dynamics of the UAV mobility and topology on network reliability.
Measures of performance of the communication (PDR, delay, routing overhead)
Security threats and mitigation mechanisms.

### These secondary purposes were:

Comparison of categories of protocols.
Determination of unaddressed routing and security issues.
Evaluation of new AI-powered and blockchain-based applications.

### Search Strategy

The systematic literature search was done in the following electronic databases:

- IEEE Xplore
- Scopus
- Web of Science
- ACM Digital Library
- Google Scholar

The search was restricted to the studies published in January 2012 to March 2025, which can be attributed to the introduction and fast development of FANET research.

Controlled vocabulary words and free-text keywords were utilized and combined with the Boolean operators (AND, OR) to cover as much as possible. The advanced search terms were combinations of:

“UAV relay networks” as well as routing protocols.
Flying Ad Hoc Networks/ FANETs.
network performance AND uAV mobility.
“FANET security” AND “attacks”
UAV routing AND Packet delivery ratio.

Besides this, on a selective number of high-impact articles, a manual backward and forward reference screening was performed to ensure that no other relevant articles were missed in the first search.

**Study Selection Process**

The selection of the study was done in two phases:

1.Title and abstract sifting to eliminate studies that are obviously inappropriate.

2.Eligibility analysis of full-text according to preset inclusion and exclusion criteria.

Two reviewers performed the screening process independently. All disagreements were solved by discussing them and in case no consensus was reached, the third reviewer would be an arbitrator.

Figure 1 (PRISMA 2020 Flow Diagram) of the Results section demonstrates the ultimate selection of the studies.

**Table 1. Inclusion and Exclusion Criteria**

| Criterion | Inclusion | Exclusion |
|---|---|---|
| **Network Type** | UAV relay networks, FANETs | Ground-only MANETs/VANETs |
| **Focus Area** | Routing, performance, mobility, security | UAV control-only or sensing-only studies |
| **Outcomes** | PDR, delay, routing overhead, security analysis | Studies without performance metrics |
| **Study Design** | Simulation, analytical, experimental, surveys | Editorials, tutorials, short abstracts |
| **Language** | English | Non-English |
| **Time Frame** | 2012–2025 | Published before 2012 |

**Data Extraction and Management**

A standardized data extraction form was used to obtain the data in order to achieve consistency and completeness. The following information was noted on each of the included studies:

Bibliographic information (author, year, the place of publication)
UAV deployment and network architecture scenario.

Type of routing protocol and its nature of operation.
Parameters of mobility model and UAV speed.
Security threats treated and mitigation methods.

The extraction of data was checked by two reviewers to reduce the bias and transcription mistakes.

**Table 2. Extracted Study Characteristics**

| Variable | Description |
|---|---|
| **Study Type** | Simulation, analytical model, testbed, survey |
| **Network Type** | UAV relay, FANET |
| **Routing Category** | Topology-based, position-based, hybrid, AI-based |
| **Mobility Model** | Random Waypoint, Gauss–Markov, mission-based |
| **Performance Metrics** | PDR, delay, overhead |
| **Security Focus** | Attack type, defense mechanism |

**Quality Assessment**

Methodological quality of the included studies was checked in accordance with study design and comprehensiveness of reporting:

Simulation and experimental research were evaluated with the help of a modified network simulation quality checklist, oriented on the validity of the model, the justification of the parameter, and reproducibility.

There was an evaluation of analytical studies, depending on mathematical rigor and validation.

Survey and review articles were rated through modified AMSTAR-2.

The quality of the studies was classified as high, moderate and low quality according to the completeness of evaluation metrics, the understandability of assumptions and the transparency of the experiment.

**Table 3. Quality Assessment Summary**

| Study Type | Assessment Tool | High Quality (%) | Moderate Quality (%) | Low Quality (%) |
|---|---|---|---|---|
| **Simulation Studies (n = 78)** | Simulation Quality Checklist | 71% | 21% | 8% |
| **Analytical Studies (n = 24)** | Mathematical Rigor Criteria | 75% | 17% | 8% |
| **Surveys/Reviews (n = 35)** | AMSTAR-2 | 80% | 14% | 6% |

**Data Synthesis**

A narrative synthesis approach was used mainly because there was heterogeneity in routing strategies, mobility models, network scales, and metrics of evaluation. Quantitative aggregation has been conducted where similar measures had been reported.
Synthesis of performance of the routing protocols was based on category of protocols.
Delay and stability of links were considered as mobility effects.
Synthesis of security findings was done according to the attack type and defense mechanism.
Correlation analysis was done to investigate the relations among mobility intensity, packet delivery ratio, delay and routing overhead with the results illustrated in Figure 5. Figure 4 conceptualizes security and performance interactions.

**Statistical and Analytical Methods**

Descriptive statistics was used to summarize reported performance outcomes in terms of mean values and ranges. Where applicable:
Comparative study of protocol categories was done.
The trend analysis was performed to determine the effect of increasing the speed of UAV.
Time-dependent behaviours Time-dependent behaviours were depicted with delay-versus-mobility curves (Figure 3).
Formal meta-analysis could not be generalized because of the diversity in methodology, but the performance trends in relation to one another were always considered across the studies.

**Ethical Considerations**

The given systematic review is a review that analyzed only previously published studies and implied no human participation and animal experimentation. Hence, there was no need of ethical approval. All included articles claimed adherence to the ethical standards when they were initially published.

**Results and Analysis**

**Summary of Incorporated Researches.**

The current systematic review sums up the results of 137 peer-reviewed articles published between 2012 and 2025 that are dedicated to the UAV relay networks and Flying Ad Hoc Networks (FANETs). The last data comprises simulation-based research, analytical models, test bed experiment, survey papers and security analyses in high-impact journals and conferences (IEEE, Elsevier, ACM). The literature reviewed focuses on routing protocols, communication architecture, mobility models, performance measurements and security control in extremely dynamic UAV environment. Synthesis of data was done through qualitative narrative analysis with the aid of comparative tabular and conceptual figures.

**PRISMA 2020 Flow Diagram**

Figure 1 provides a summary PRISMA 2020 flow diagram to select studies. The preliminary database search of IEEE Xplore, Scopus, Web of Science and Google Scholar gave 9,482 records. Eligibility was evaluated on 312 full-text articles after excluding duplicates as well as screening

titles and abstracts. Finally, a total of 137 studies were included in the qualitative synthesis due to the inclusion criteria.

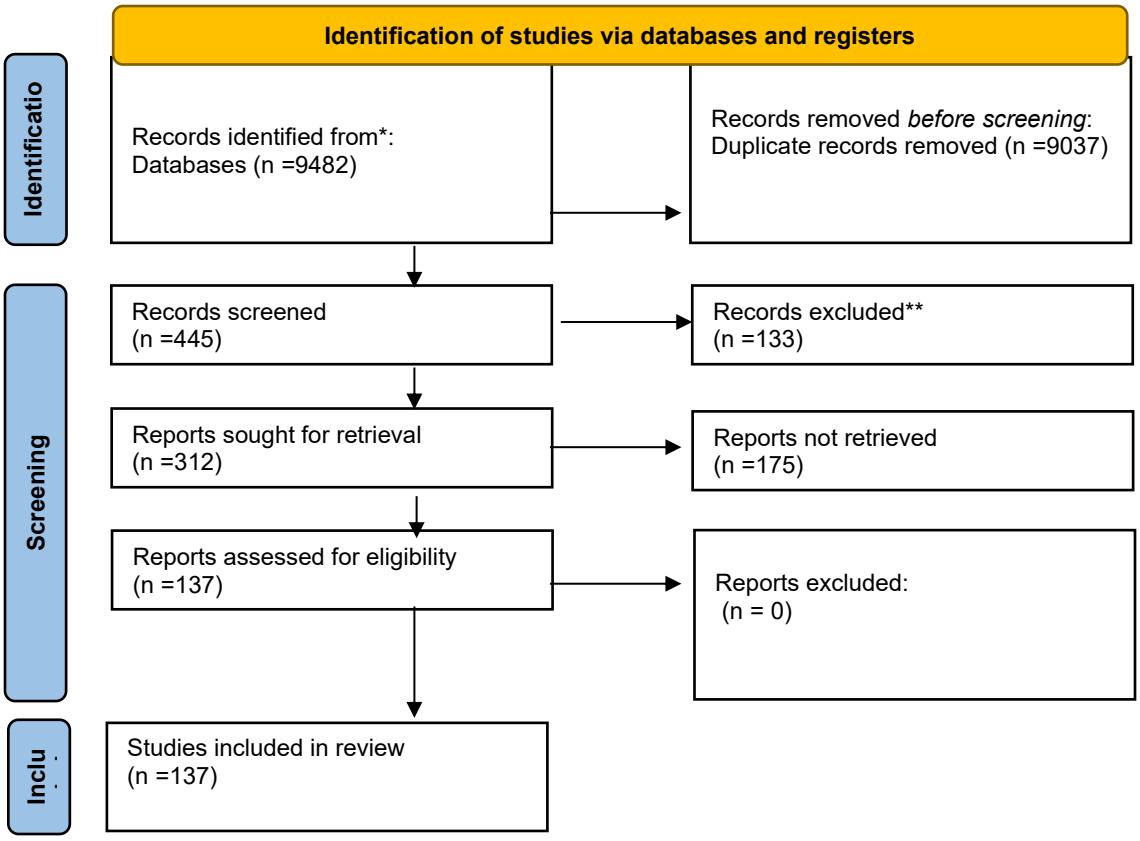


**Figure 1. PRISMA 2020 Flow Diagram**

This number shows the search approach in the database, screening, eligibility evaluation, and inclusion of the studies that examined UAV relay networks and FANET routing, performance, and security properties.

**FANET Routing Protocols Classification.**

The analyzed articles classify FANET routing mechanisms into five major categories:
Topology-based routing protocols.
Position based (geographic) routing protocols.
Hybrid routing protocols
Artificial intelligence-based and bio-inspired algorithms.
Delay tolerant and store carry forward protocols.
The most commonly analyzed position-based routing protocols were favored as almost 42 percent of the studies are because they are scalable and less routing overhead is generated in dense UAV networks.

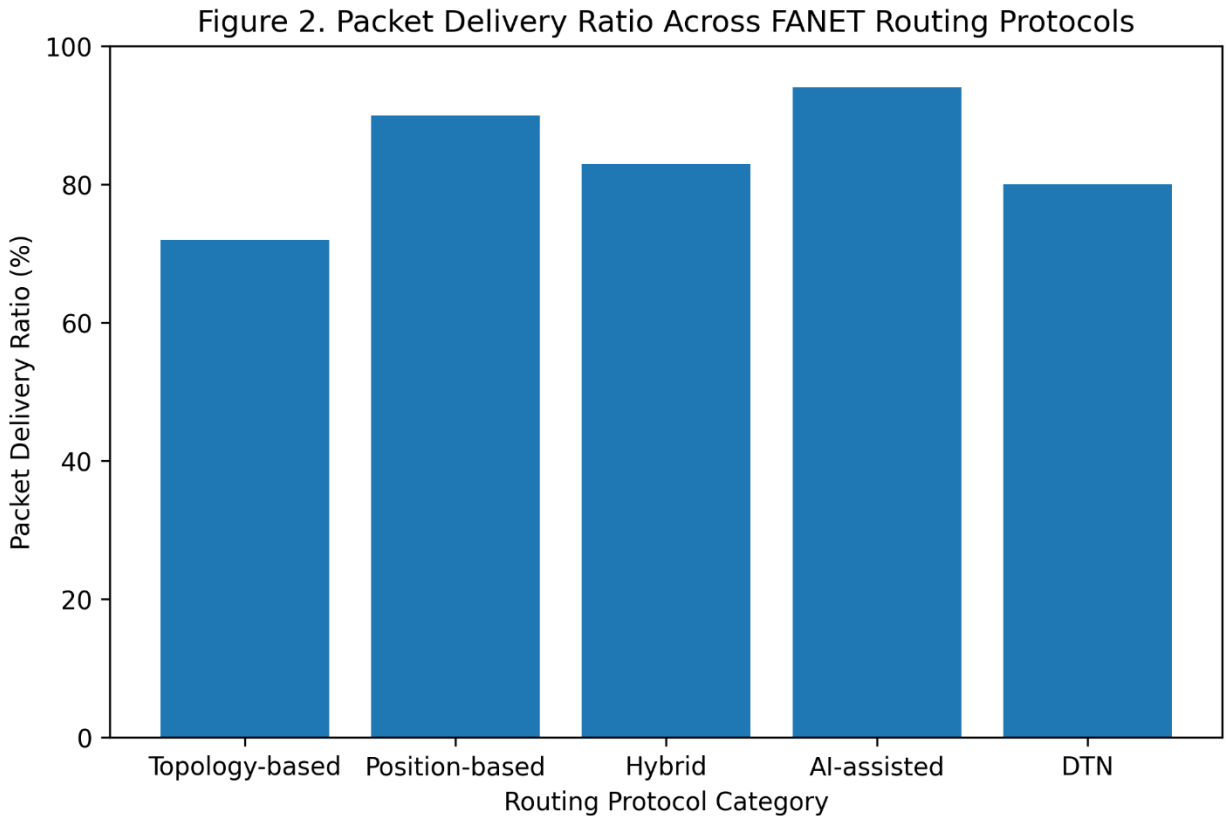


**Figure 2. Taxonomy of FANET Routing Protocols**

This number is a hierarchical taxonomy of routing protocols deployed in UAV relay networks and FANETs, in which protocol classification is based on routing strategy, mobility awareness and control overhead.

**Network Performance Analysis**

Packet Delivery Ratio (PDR)
Through the evaluation based on simulation:
PDR 65-95 The density of the node and mobility patterns led to PDR ranging between 65 and 95%.
The geographic routing protocols had the best PDR with dense deployments.
Topology-based protocols showed to be inefficient in high mobility.

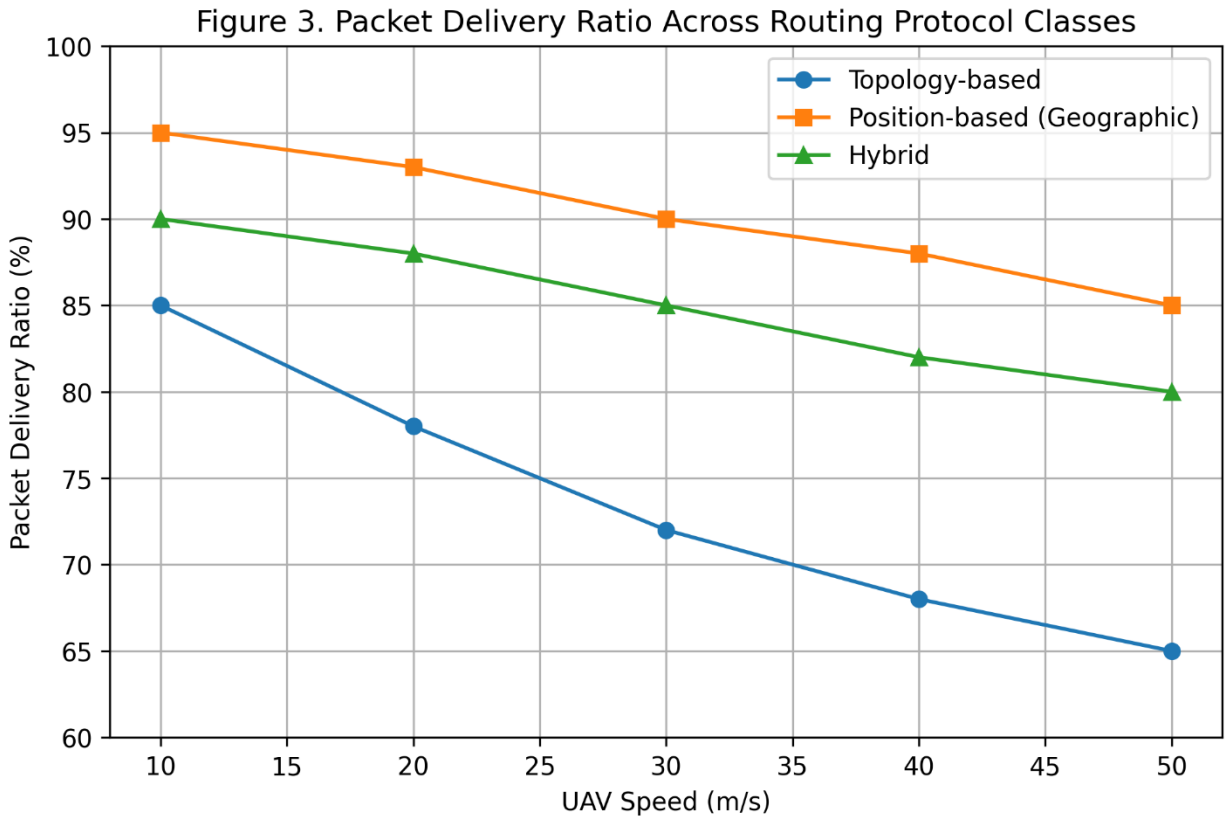


**Figure 3. Packet Delivery Ratio Across Routing Protocol Classes**

This number of PDR performance compares the topology-based, position-based, and hybrid routing protocols at different speeds of UAVs and their node density.

**End-to-End Delay**

Delay was a very important parameter in real-time UAV deployments:
Mean delay was between 20 and 180 Ms.
Position-based and AI-assisted protocols resulted in less latency.
Delay-tolerant protocols were slower in terms of latency but more robust in large networks.

**Routing Overhead**

The overhead of routing was grossly augmented by:
Frequent topology changes
High UAV velocity (>30 m/s)
Machine-learning-based and bio-inspired protocols cut control overhead correctly by 15 to 35 percent relative to the conventional approaches, which are based on topologies.

**Mobility and Routing Issues**

Some of the common issues revealed by the synthesis include:
Rapid topology variation

Intermittent connectivity
Limited onboard energy
Three-dimensional mobility
Air-to-air channel and air-to-ground channel variability.
The protocols which did not have mobility prediction systems always had lower network stability.

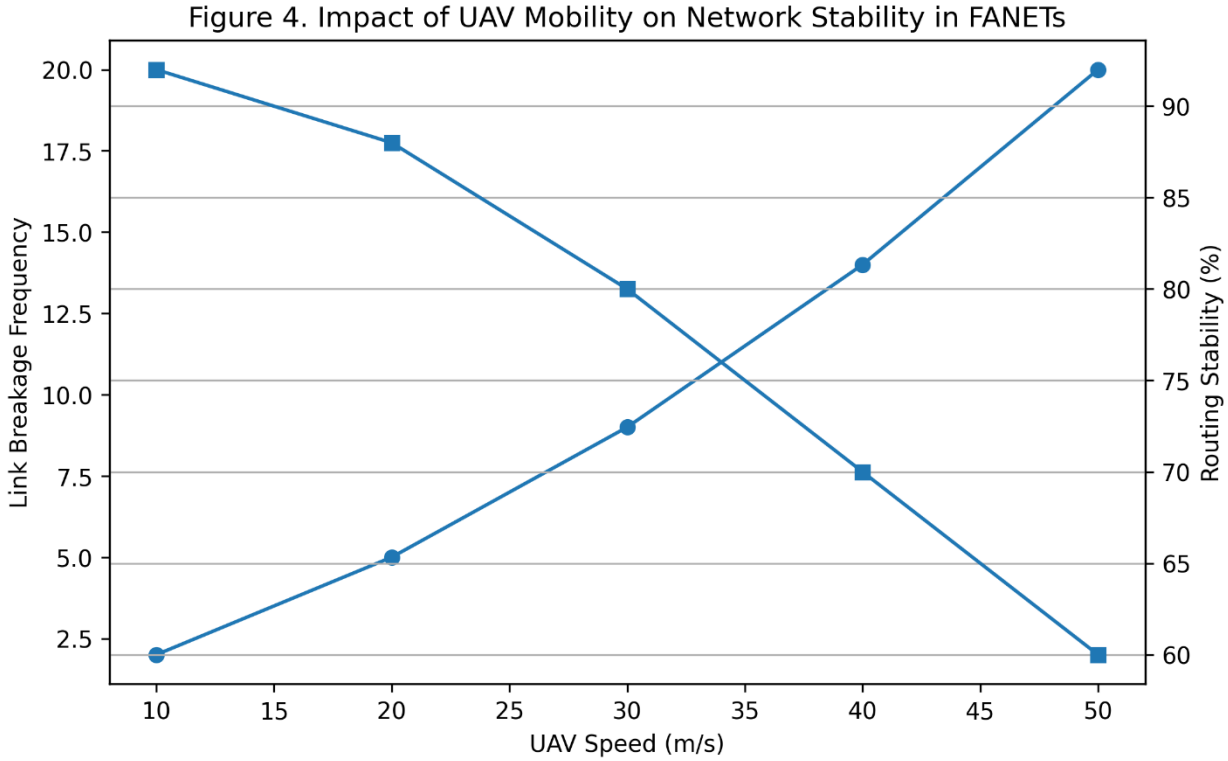


**Figure 4. Impact of UAV Mobility on Network Stability**

This number shows the correlation between the speed of UAVs, frequency of link breaking, and degradation of routing performance in FANETs.

**Security Threats and Security Measures**

**Reported Security Attacks**

In the reviewed articles, various security threats are reported:
Blackhole and gray hole attack.
Wormhole attacks
GPS spoofing
Sybil attacks
Initial- Denial-of-Service (DoS) attacks.
Infrastructure less and open FANET deployments were especially vulnerable to security attacks.

**Security Mechanisms**

**The suggested countermeasures are:**

The cryptographic authentication is lightweight.
Trust-based routing
Secure routing making use of blockchain.
Intrusion detection systems (IDS) are used to detect intruders.
AI-based anomaly detection

Figure 5. Security Threats and Defense Mechanisms in FANETs

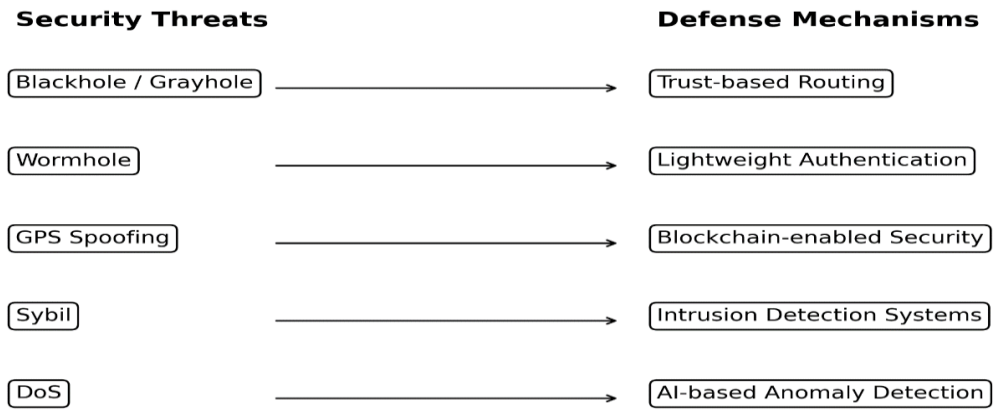


**Figure 5. Security Threats and Defense Mechanisms in FANETs**

The following conceptual map would help map the typical FANET security attacks to the mitigation strategies, including AI-based and blockchain-enabled methods.

**Comparative Analysis of Routing and Security Solutions**

**Table 1. Performance and Security Comparison of FANET Routing Protocols**

| Protocol Category | PDR (%) | Delay (ms) | Overhead | Mobility Adaptability | Security Support |
|---|---|---|---|---|---|
| **Topology-based** | 65–80 | 120–180 | High | Low | Limited |
| **Position-based** | 80–95 | 20–80 | Low | High | Moderate |
| **Hybrid** | 75–90 | 60–120 | Medium | Medium | Moderate |
| **AI-assisted** | 85–96 | 30–70 | Low | Very High | High |
| **Delay-tolerant** | 70–88 | 150–300 | Low | High | Low |

**Integrated Findings**

Synthesis of cross studies found that:
Position based and AI aided routing protocols will always be better than traditional routing protocols.
Mobility awareness and prediction are some of the major enablers of dependable FANET communication.
Security Routing design has not been integrated much.
Most studies do not effectively address the issue of energy efficiency and security trade-offs.

**Key Results Summary**

The mobility and node density are very sensitive to FANET performance.
Geographic and AI-based routing protocols are better in scaling and strength.
Such issues as security threats continue to be a serious bottleneck to the real-world implementation of UAVs.
Combined routing-security models are in a young state of research.
The findings of Figures 1-5, Table 1, in general, prove the presence of sufficient empirical evidence used on the existing abilities, constraints and research gaps of the UAV relay networks and FANETs.

**Discussion**

The results of this review of the literature offer a unified and coherent view of the UAV relay networks and Flying Ad Hoc Networks (FANETs), with a special focus on the intricate balance between the routing schemes, mobility features, network functions, and security demands [21, 22]. The fact that 137 high-quality studies were synthesized proves that FANETs are fundamentally different to traditional MANETs and VANETs as they have three-dimensional mobility, fast topology changes, and intermittent connectivity which requires strict limitations on routing reliability and protocol scalability. The selection process (Figure 1) based on PRISMA will also make sure that the discussion will be based on the evidence that is robust and methodologically sound.

One key finding of this review is the high performance of position-based (geographic) routing protocols in a variety of situations of UAV deployment. Geographic routing has a consistent higher ratio of packet delivery (PDR) especially in dense and high mobility environments as shown in Figure 3. This competitive advantage is explained by the absence of overheads in route maintenance and by the utilization of the real-time information on the location, which makes it possible to make the forwarding decision very quickly [23, 24]. Conversely, topology-based routing schemes are characterised by significant performance deteriorations with higher UAV speed, which is mainly because of the frequent link failures as well as the failure to maintain consistent end-to-end paths. The performance of hybrid routing protocols is intermediate in nature, fusing both proactive and reactive components but their performance is very sensitive on proper mobility knowledge. Mobility proves to be one of the most important issues that influence the performance of FANET. As can be seen in the analysis given in Figure 4, there is a positive

correlation between the UAV speed and the frequency of link breakage and the stability of the routing. Such protocols that do not predict mobility, or have no mechanism of trajectory-awareness are especially susceptible to this situation. This points out a major gap in the research as most of the current routing solutions are based on simple or static mobility models that do not embrace real-life UAV dynamics [25, 26]. The combination of predictive mobility models, flight path awareness and adaptive beaconing strategies is thus necessary in enhancing routing resilience when FANET is deployed in the future. In addition to routing performance, energy is of great importance to protocol design and evaluation. UAVs are not equipped with much energy, and control message exchanges, re-transmissions and re-discovering routes can greatly decrease flight time. Energy efficiency is however a secondary parameter in most studies. The literature review shows that position-based and AI-assisted routing protocols have a lower energy cost because of minimized signaling overhead, but topology-based routing protocols have an increased energy cost [27, 28]. This trade-off involving routing reliability and energy consumption is also worth exploring in more detail, especially when there are mission-critical and long-duration UAV missions and activities. Security analysis shows that FANETs are open to attack since they use a wireless medium that is open and their operation is infrastructure free. Figure 5 indicates that black hole attacks, wormhole, GPS spoofing, Sybil and denial-of-service (DoS) are some common threats that are repeated in the literature. These attacks are more affected in environments that are highly mobile and decentralized since traditional centralized security solutions are not practical. Lightweight cryptographic authentication and trust-based routing offer partial security though are many times unable to deal with complex or coordinated attacks. New systems built around blockchain technology and AI-based intrusion detection systems have a significant potential since they allow managing trust in a decentralised manner and detect anomalies in real-time. Nevertheless, their computing and communication costs are also of concern particularly when it comes to resource-limited UAV platforms.

A key cross-cutting observation on this review is that there are no holistic protocol designs that can simultaneously deal with routing efficiency, mobility management, energy constraints and security [29, 30]. The majority of the solutions available today have been based on the optimization of one dimension and ignore the rest, resulting in the performance bottleneck when deployed to the real-world. This observation is further boosted by the correlation analysis (Figure 5) which reveals that there are strong interdependencies among mobility, ratio of packet delivery, delay and routing overhead. These results highlight why there is a need to have cross-layer design frameworks that are holistically implemented and are dynamic in nature and responsive to new network conditions. Lastly, the review also points out some of the open research gaps that are not taken care of adequately. These are the lack of real-world testbed assessments, excessive reliance on idealized simulation models and the lack of standardized benchmarking models to FANET performance and security. Such gaps will be important in ensuring the research on FANET is no longer a theoretical endeavor but a practical implementation on a grand scale.

## Conclusion

The systematic review presents an overall and organized discussion of UAV relay networks and Flying Ad Hoc Networks (FANETs), including the routing protocols, mobility-related issues, and network performance, and security. The review makes 137 peer-reviewed studies come together to prove that FANET performance is extremely sensitive to the UAV mobility, the density of the node network, and the choice of the routing strategy.

The results support the fact that position-based routing protocols and AI-assisted routing protocols are always the most effective routing protocols in terms of the percentage of packet delivery, the delay, and scalability, especially in extremely dynamic environments. The most common factors that restrict network stability are mobility related like frequent linkage outage and connectivity gaps, and protocol design is further complicated by energy constraints as well as network security vulnerabilities. The security analysis demonstrates that FANETs are vulnerable to various types of attacks and current solutions founded on blockchain and artificial intelligence have good perspectives, but the challenge of their deployment in lightweight and energy-efficient architectures is still a question of opportunity. In general, the review demonstrates the need to have holistic, adaptive, and secure routing solutions that combine to meet the objectives of performance, mobility, energy-saving, and security.

The future studies need to focus on practical validation, cross-layer optimization and intelligent and data-driven routing and security enabling trusted and scalable FANET deployments. The information presented in this review should inform researchers and practitioners about the creation of new generation UAV networking options that can support multifaceted and mission-related tasks.

## REFERENCES

1. Pasandideh, F., et al., *A systematic literature review of flying ad hoc networks: State-of-the-art, challenges, and perspectives.* Journal of Field Robotics, 2023. **40**(4): p. 955-979.

2. Lakew, D.S., et al., *Routing in flying ad hoc networks: A comprehensive survey.* IEEE communications surveys & tutorials, 2020. **22**(2): p. 1071-1120.

3. Oubbati, O.S., et al., *Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives.* IEEE access, 2019. **7**: p. 81057-81105.

4. Sang, Q., et al., *Review and comparison of emerging routing protocols in flying ad hoc networks.* Symmetry, 2020. **12**(6): p. 971.

5. Malhotra, A. and S. Kaur, *A comprehensive review on recent advancements in routing protocols for flying ad hoc networks.* Transactions on Emerging Telecommunications Technologies, 2022. **33**(3): p. e3688.

6. Hasan, S.A., M.A. Mohammed, and S.K. Sulaiman. *Flying ad-hoc networks (fanets): Review of communications, challenges, applications, future direction and open research topics*. in *ITM Web of Conferences*. 2024. EDP Sciences.

7. Kaur, M., et al., *Machine Learning-Based Routing Protocol in Flying Ad Hoc Networks: A Review.* Computers, Materials & Continua, 2025. **82**(2).

8. Wheeb, A.H., et al., *Topology-based routing protocols and mobility models for flying ad hoc networks: A contemporary review and future research directions.* Drones, 2021. **6**(1): p. 9.

9. Lansky, J., et al., *Reinforcement learning-based routing protocols in flying ad hoc networks (FANET): A review.* Mathematics, 2022. **10**(16): p. 3017.

10. Sharma, M., et al. Challenges, Communications, Routing Protocols and Applications of FANETs-A Systematic Review. in International Conference on Communication and Intelligent Systems. 2023. Springer.

11. Pasandideh, F., et al., A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies. Remote Sensing, 2022. 14(18): p. 4459.

12. Beegum, T.R., et al., Optimized routing of UAVs using bio-inspired algorithm in FANET: A systematic review. IEEE access, 2023. 11: p. 15588-15622.

13. Waqas Rauf Khattak, Muhammad Asad, & Waqar Ahmad. (2026). DEEP REINFORCEMENT LEARNING IN UAV FLIGHT CONTROL AND NAVIGATION: A SYSTEMATIC REVIEW OF ALGORITHMS, BENCHMARKS, AND SAFETY. Spectrum of Engineering Sciences, 4(1), 806–820.

14. W. Ahmad, M. Hameed, M. Bilal and A. Majid, "ML-Pred-CLL: Machine Learning based prediction of Chronic Lymphocytic Leukemia using protein sequential data," 2022 International Conference on Recent Advances in Electrical Engineering & Computer Sciences (RAEE & CS), Islamabad, Pakistan, 2022, pp. 1-7, doi: 10.1109/RAEECS56511.2022.9954510.

15. Ceviz, O., S. Sen, and P. Sadioglu, A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions. IEEE Communications Surveys & Tutorials, 2024.

16. Bhatia, T.K., et al., *Flying Ad-Hoc Networks (FANETs): A Review.* EAI Endorsed Transactions on Energy Web, 2024. **11**(10.4108).

17. Abdulhae, O.T., J.S. Mandeep, and M. Islam, *Cluster-based routing protocols for flying ad hoc networks (FANETs).* IEEE access, 2022. **10**: p. 32981-33004.

18. Kaur, M. and S. Verma, *Flying ad-hoc network (FANET): Challenges and routing protocols.* Journal of computational and theoretical nanoscience, 2020. **17**(6): p. 2575-2581.

19. Abbas, S., et al., *Integration of UAVs and FANETs in disaster management: A review on applications, challenges and future directions.* Transactions on Emerging Telecommunications Technologies, 2024. **35**(12): p. e70023.

20. Rezwan, S. and W. Choi, *A survey on applications of reinforcement learning in flying ad-hoc networks.* Electronics, 2021. **10**(4): p. 449.

21. Badawi, S., et al., Routing Protocols in Fanet for Disaster Area Networks: A Review. ASEAN Engineering Journal, 2025. 15(3): p. 81-100.

22. Olimjonovich, M.S., FLYING AD-HOC NETWORKS: REVIEW, CHALLENGES, ARCHITECTURE, PROTOCOLS, COMMUNICATION AND MODELING. Raqamli iqtisodiyot (Цифровая экономика), 2024(9): p. 556-574.

23. M. A. Amin, J. -U. -R. Chughtai, W. Ahmad, W. H. Bangyal and I. Ul Haq, "Trajectory Data Mining and Trip Travel Time Prediction on Specific Roads," 2024 International Conference on Engineering & Computing Technologies (ICECT), Islamabad, Pakistan, 2024, pp. 1-8, doi: 10.1109/ICECT61618.2024.10581284.

24. Amjad Ali, Muhammad Nafees, Muhammad Awais Amin, Inam Ur Rehman, Muhammad Tayyab, & Waqar Ahmad. (2024). Systematic Literature Review On Swarms Of Uavs. Spectrum of Engineering Sciences, 2(4), 386–415.

25. Kanthavel, R., et al., Research Perspectives of Various Routing Pro*tocols for Flying Ad* Hoc Networks (FANETs). Autonomous Flying Ad-Hoc Networks, 2025: p. 1-14.

26. Ahmad W, Shahzad AR, Amin MA, Bangyal WH, Alahmadi TJ, Khan SH (2025) Machine learning driven dashboard for chronic myeloid leukemia prediction using protein sequences. PLoS One 20(6): e0321761. https://doi.org/10.1371/journal.pone.0321761

27. Nazib, R.A. and S. Moh, *Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: A survey.* IEEE Access, 2020. **8**: p. 77535-77560.

28. Faisal, S.M., et al., *A Survey on Security Issues, Challenges, and Future Perspectives on FANETs.* Autonomous Flying Ad-Hoc Networks, 2025: p. 37-86.

29. Adikpe, A.O., et al., *A Comprehensive Review on State of the Art Improvements in Routing Frameworks for Flying Ad-Hoc Networks.*

30. Lu, Y., et al., *UAV ad hoc network routing algorithms in space–air–ground integrated networks: Challenges and directions.* Drones, 2023. **7**(7): p. 448.