Veerendra Ahirwar, 2026, 14:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Review of Different Attacks for Secure Routing in FANET

Veerendra Ahirwar[1], Arjun Rajput[2]
Department Of Computer Science And Engineering Technocrats Institute Of Technology And Excellence, Bhopal, Madhya Predesh, India

Abstract— Aerial Aerial networks, specifically Flying Ad Hoc Networks (FANETs), are gaining importance for real-time applications in military, disaster management, and surveillance. The high mobility and dynamic topology of FANETs make secure routing a challenging task. To address these challenges, researchers are exploring advanced algorithms that can adapt to changing network conditions while ensuring data integrity and confidentiality. Enhancing the resilience and efficiency of routing protocols will be crucial for the successful deployment of FANETs in critical scenarios. Various attacks, such as black hole, wormhole, Sybil, and Denial-of-Service (DoS), threaten FANET routing protocols. These attacks can lead to packet loss, network partitioning, and data leakage. Black hole attacks drop data packets by falsely advertising optimal paths. Wormhole attacks create a tunnel between malicious nodes to manipulate traffic. Sybil attacks introduce multiple fake identities to disrupt network operations. Traditional security mechanisms for MANETs and VANETs often prove inadequate in FANET scenarios because of the unique constraints posed by UAVs. Effective solutions must address high mobility, limited resources, and real-time requirements. Recent research focuses on lightweight cryptographic methods, trust management, and anomaly detection. Comprehensive attack analysis is key to developing robust routing protocols. Ensuring secure routing is critical for the reliability and safety of FANET-based missions. Enhancing these protocols requires a multi-faceted approach that considers the technical capabilities of UAVs and incorporates adaptive strategies to respond to emerging threats. As the field evolves, collaboration between researchers and industry practitioners will be essential in creating resilient frameworks that can withstand the dynamic challenges of aerial networks.

Keywords— Attack, Routing, Security, UAVs, FANET,

I. INTRODUCTION

The continuous movement of UAV nodes further complicates the process of maintaining secure and reliable communication links [1][2]. Addressing these concerns, recent research emphasizes the integration of security measures within routing protocols to reduce attack surfaces. Solutions such as intrusion detection methods, authentication schemes, and trust-based models are increasingly adopted [3][4]. However, the application of these solutions is often constrained by the limited energy and computational resources available on aerial nodes. Intrusion detection systems tailored for FANET environments have also gained momentum in the literature. These systems aim to identify and respond quickly to abnormal behaviors or potential intrusions critical in mission-centric FANET deployments where delay or data loss is unacceptable [5][6][7]. Balancing security and performance remain a persistent challenge. Heavy security mechanisms may bolster defenses but often lead to increased overhead and reduced network efficiency. Thus, there is a pressing need for lightweight, agile security protocols that can be dynamically adjusted based on network conditions and mission priorities. Another layer of complexity arises from the heterogeneity of FANET components, as different UAVs may have varied capabilities and resources [8]. Therefore, adaptive routing strategies that account for these discrepancies are essential for optimal network performance and resilience to attacks.

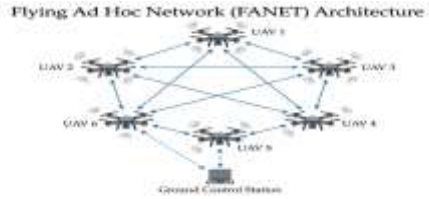


Figure 1 FANET Architecture

© 2026 Veerendra Ahirwar, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

The figure illustrates a Flying Ad Hoc Network (FANET) composed of six unmanned aerial vehicles (UAVs) communicating wirelessly with one another and with a ground control station.

1. Uav Nodes

The six drones—UAV 1 through UAV 6—are the primary nodes of the network. Each UAV can:

- Collect data through onboard sensors
- Process and store information
- Communicate with neighboring UAVs
- Forward messages across the network
- Adapt its position according to the mission

Unlike a fixed terrestrial network, the UAVs are mobile and may change their positions during flight.

2. Wireless Mesh Connections

The blue lines between the UAVs represent wireless communication links. Together, these links create a mesh topology. In this topology

UAVs communicate directly with nearby drones.

- Data can travel through multiple intermediate UAVs.
- If one connection fails, information may be routed through another path.
- The network does not depend on a single central communication tower.

For example, a message from UAV 1 to UAV 5 may travel directly if they are within range, or it may be relayed through UAV 2, UAV 3, or another neighboring drone.

3. Multi-Hop Communication

FANETs commonly use multi-hop communication. This means that a UAV can act as both:

- An end device that generates or receives data
- A router that forwards data for other UAVs
- This extends the communication range beyond the direct radio range of an individual drone.

4. *Ground Control Station*

The Ground Control Station (GCS) at the bottom of the figure is connected to the UAV network by a dashed link. It can be used to:

- Monitor UAV locations and status
- Send commands and mission instructions
- Receive sensor data and video
- Coordinate the movements of the UAVs
- Manage network and flight operations

The dashed line represents a communication link between the GCS and the nearest UAV. That UAV can relay commands to the other drones through the mesh network.

5. Wireless Signal Indicators

The signal symbols around the drones indicate radio communication coverage. Communication is possible when UAVs are within one another's transmission range. The effective range depends on factors such as:

- Distance between UAVs
- Antenna characteristics
- Transmission power
- Frequency band
- Obstacles and interference
- UAV altitude and orientation

6. Distributed Network Architecture

The figure represents a distributed FANET architecture. No single UAV is necessarily responsible for all communication. Instead, the network is formed dynamically as the UAVs exchange information and establish links with their neighbors. This architecture provides:

- Flexibility
- Scalability
- Fault tolerance
- Rapid deployment
- Support for changing network conditions

7. Dynamic Topology

Because the UAVs are moving, the network topology can change frequently. A link may disappear when two UAVs move out of range, while a new link may form when other UAVs approach each other. Therefore, FANET routing protocols must handle:

- Frequent link breaks
- Rapid changes in network structure
- Variable communication delays
- Limited bandwidth
- Energy constraints

- High mobility

8. Overall Data Flow

A typical communication process is:

- A UAV collects information using its s2ensors.
- The data is transmitted to a neighboring UAV.
- Intermediate UAVs forward the data through the mesh network.
- The information reaches the GCS.
- The GCS analyzes the data or sends instructions back to the UAVs.

Thus, the figure demonstrates how six UAVs cooperate as a self-organizing aerial network while remaining connected to a ground control station.

Continuous innovation is required as attackers evolve their tactics to exploit new vulnerabilities in both established and emerging FANET protocols. Simulation-based studies prove useful in identifying potential weaknesses, but real-world validation is necessary to ensure practical applicability. As FANETs are further integrated into society's critical infrastructures, ongoing research into scalable, secure, and efficient communication protocols will determine the future success and safety of these networks. The ultimate goal is to enable dependable, secure, and mission-effective FANET operations, facing both present and future threats.

Section 2 describes the security issues in FANET 3 discusses the limitations.in FANET. Section 4 mentioned the overview of routing protocols in FANET. literature survey is mentioned in section 5. The expected outcome or scheme that we will propose is mentioned in section 6 and the conclusion of the research is mentioned in figure 7.

II. SECURITY ISSUE IN FANET

Security issues in Flying Ad Hoc Networks (FANETs) arise because drones communicate wirelessly while moving rapidly and operating with limited computing, energy, and communication resources [3][9][10]. The network may face risks to confidentiality, integrity, availability, authentication, and privacy. Attackers can intercept sensitive data, alter messages, impersonate legitimate drones, disrupt communication, or access information such as locations, images, and flight plans. Frequent changes in network topology and dependence on wireless links make FANETs more difficult to protect than traditional networks. Therefore, secure routing, encryption, authentication, intrusion detection, and privacy-preserving mechanisms are essential for reliable and safe FANET operation.



Figure 2. Security Issues in FANET

1. *Confidentiality*

Confidentiality in FANET ensures that information exchanged among drones and ground stations is accessible only to authorized users. Because wireless communication can be intercepted, attackers may capture sensitive data such as flight plans, location information, video, or mission instructions. Encryption and secure communication protocols help protect this information from unauthorized access.

2. *Integrity*

Integrity ensures that messages and data remain accurate and unchanged during transmission. In a FANET, an attacker could modify navigation commands, sensor readings, or routing information, causing drones to make incorrect decisions. Authentication methods, message verification, and digital signatures can help detect and prevent unauthorized changes.

3. *Availability*

Availability means that FANET services, communication links, and drone resources remain operational when needed. Wireless interference, network congestion, or malicious disruption can prevent drones from communicating with one another or with the control station. Reliable routing, redundant communication links, and resistance to interference are important for maintaining network availability.

4. *Privacy*
Privacy protects sensitive information collected and transmitted by drones. FANETs may handle user identities, locations, images, videos, and environmental data, which could be misused if exposed. Limiting data collection, anonymizing information, controlling access, and using secure storage can help protect the privacy of users and surrounding environments.

III. LIMITATIONS IN FANET

The communication between the UAVSA in FANET are ot easy due to the high mobility speed of UAVs [2][3][11].

1. High Mobility And Dynamic Topology
UAVs move rapidly and unpredictably, causing frequent topology changes and link breakages. This dynamic environment presents major obstacles to communication protocols and network management. Adaptability and robust algorithms are essential to maintain connectivity and ensure efficient operation in such conditions.

2. *Limited Energy Resources*
UAVs are battery-powered, restricting flight and operation time, which impacts network longevity and performance. These challenges necessitate the development of adaptive routing protocols that can efficiently manage network dynamics while conserving energy. Researchers are exploring innovative solutions to enhance the resilience and efficiency of UAV networks, ensuring reliable communication even in the face of these constraints.

3. *Bandwidth Constraints*
Wireless links in FANETs are typically bandwidth-limited, which can degrade communication quality, especially with high data transmission.

4. High Probability Of Link Failure
Due to obstacles, weather, or interference, links between UAVs may frequently fail, disrupting network connectivity. To address these challenges, robust error correction mechanisms and dynamic link adaptation strategies are being developed. These measures aim to maintain a stable communication flow, even under fluctuating conditions, thereby enhancing the overall performance of the network.

5. Security And Privacy Issues
Open wireless channels are vulnerable to eavesdropping, jamming, spoofing, and various cyber-attacks. To mitigate these challenges, robust encryption protocols and adaptive routing algorithms must be implemented to maintain secure and efficient communication. Additionally, developing intelligent algorithms that can dynamically adjust to changing network conditions will be crucial for sustaining reliable operations in UAV networks.

6. *Limited Payload Capacity*
Most UAVs can only carry lightweight communication hardware, restricting computational and communication capabilities.

7. Synchronization And Coordination Challenges
Coordinating and synchronizing multiple UAVs is complex, especially in real-time and in large swarms. These challenges necessitate the development of robust protocols and innovative technologies to enhance resilience and security in UAV networks. Addressing these issues will be crucial for the successful implementation of UAV systems in various applications, from military operations to commercial delivery services.

IV. ROUTING PROTOCOLS IN FANET

The primary routing protocol types used in Flying Ad Hoc Networks (FANETs) are shown in figure 3. The way data packets move between unmanned aerial vehicles (UAVs) is determined by FANET routing protocols [12][13][14]. Routing is a significant challenge because drones move quickly and the network topology changes often. Proactive, reactive, and hybrid protocols are the three primary groups of routing protocols are mentioned ion figure 3.

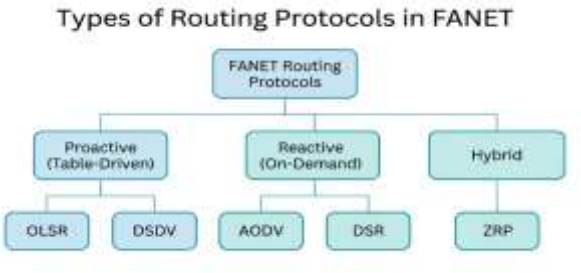


Figure 3. Routing Protocols in FANET

Table-driven protocols are another name for proactive protocols. Before data transmission starts, they keep the network's routing information up to date. Every drone shares updates with nearby drones on a regular basis. Because a route is already available, this method offers quick route access. Continuous updates, however, use battery life, processing power, and bandwidth. One proactive routing protocol is OLSR. To cut down on pointless control messages, it makes use of specific relay nodes. Another proactive protocol that keeps routing tables up to date with destination information is DSDV. On-demand protocols are another name for reactive protocols.

Only when a source drone needs to transmit data do they generate a route. Network resources are saved and superfluous control traffic is decreased as a result. However, there is a delay before communication can begin due to route discovery. A popular reactive protocol that finds routes when needed is called AODV. Another reactive protocol that makes use of route maintenance and route discovery techniques is DSR. Proactive and reactive approaches are combined in hybrid protocols. Within a small neighborhood, they proactively maintain routes, and outside of it, they find routes reactively. This approach aims to strike a balance between minimal control overhead and minimal delay. One hybrid routing protocol is ZRP.

All things considered, each category has unique benefits and drawbacks. Although proactive protocols facilitate rapid communication, they necessitate frequent updates. Although reactive protocols lower overhead, they may cause delays in route discovery. A middle ground between these two methods is offered by hybrid protocols. Drone speed, network size, traffic load, energy availability, and communication needs all influence the best protocol.

V. LITERATURE SURVEY

The authors contributions are effective and giving ideas of innovative research. In this section describe the security scheme of different researches in field of security against dropping attack in FANET.

Singh et al. [15], proposed an RDSBP security framework for FANET Sybil attacks. The main goal of RDSBP is to identify the attacker. Network integrity and fleet communication depend on identity verification. The proposed solution uses advanced behaviour analysis to strengthen FANETs against malicious functioning.

V Chandrasekar [16] proposed Secure AODV approach that reduces packet loss and routing overhead while increasing throughput compared to TAODV and AODV. This detection approach in FANET is able to improved real-time security breach detection and prevention, boosting FANET dependability and security.

Singh [17], proposed a fuzzy trust mechanism with direct and indirect recommendations is proposed. The proposed scheme assesses network node trustworthiness using trust. A decay function accelerates trust convergence to node behaviour in the network. The decay function uses past trust, weighted trust, rewards, and punishment. Trust ratings are more accurate and responsive to node behaviour changes with this method. Therefore, the network can provide more reliable and secure connection and data sharing.

Buksh et al. [18] proposed the trust-oriented peered customized mechanism (TOPCM) in FANETs to evaluate UAV trustworthiness and detect and isolate hostile UAVs. To evaluate UAV trust, the trust evaluator considers broadcast ID, destination address, next-hop ID, and current node ID. Each UAV's trust is then recorded in a trust table. RREQ is monitored to determine assessment parameters.

Mauro et al. [19], proposed Greedy Perimeter Stateless Routing (GPSR) protocol is used for network deployment to enable drone communication. This paper provides a thorough analysis of Gray Hole and Sybil attacks on a network vulnerable to the GPSR protocol. SecGPSR uses lightweight public key cryptographic primitives, including Elliptic Curve

Cryptography (ECC), to detect fake drone IDs without ML/DL models or specific hardware. This approach is crucial to preventing Sybil attacks. A distributed and collaborative trustworthiness evaluation method for FANET drones to identify a gray hole-like hostile drone.

V. Ananthi et al. [20] proposed the hierarchical energy-efficient secure routing (HEESR) protocol for relay-mobile node communication. This method selects cluster heads using Low-Energy Adaptive Hierarchy Media Access Control (LEACH). For secure data transfer, Huffman coding is used. HEESR routing reduces body area network throughput and security. The right route selection improves data transmission reliability and energy efficiency.

1. Expected Outcome

A robust security scheme to mitigate Sybil packet dropping attacks involves multiple layers of authentication and monitoring within the network. Sybil attackers create multiple fake identities to gain trust and disrupt routing by selectively dropping packets. To counter this, the scheme begins with strong node authentication, leveraging cryptographic techniques such as public key infrastructure (PKI) to ensure a unique identity per node. Implementing neighbor watch protocols empowers nodes to monitor the forwarding behavior of their neighbors. Suspicious activity, such as packet dropping above a certain threshold, triggers local alarms.

The scheme incorporates trust management systems that assign and update trust scores based on node reputation and behavior. Nodes falling below a trust threshold are isolated or denied routing privileges. Additionally, periodic challenge-response tests can distinguish genuine nodes from Sybil entities. The system employs resource testing by making nodes prove costly computational, memory, or bandwidth commitments—further deterring would-be Sybils. Multipath routing is adopted to minimize the impact of dropped packets, ensuring successful data delivery even if some routes are compromised. Intrusion detection systems (IDS) continuously analyze network traffic to spot irregularities tied to Sybil behavior. Regular key refreshment and revocation prevent compromised or Sybil-faked identities from persisting. Collectively, these measures create a holistic defense, maintaining data integrity and robust routing even in the presence of Sybil packet dropping attackers.

VI. CONCLUSION AND FUTURE WORK

Flying Ad Hoc Networks) play an increasingly critical role in applications such as surveillance, disaster management, and military operations. Their inherent characteristics—such as high-speed mobility, frequent topology changes, and three-dimensional operation—set them apart from traditional MANETs and VANETs. These unique features, however, create significant challenges in both security and routing. FANETs are exposed to a spectrum of cyber threats, especially due to their dynamic network topologies and open wireless communications.

Common attacks include blackhole, grayhole, wormhole, Sybil, and denial-of-service incidents, each capable of compromising network integrity and reliability. Traditional routing protocols often fail in FANET scenarios due to their reliance on stable and predictable network architectures. As a result, numerous routing strategies have been developed to meet FANET-specific requirements. Proactive, reactive, hybrid, and most notably, geographic and position-based routing protocols are frequently considered for their adaptability and speed.

Nevertheless, these approaches are not without their own risks. For instance, position-based routing, while efficient, introduces vulnerabilities such as location spoofing and increased susceptibility to location-dependent attacks. In conclusion, the landscape of FANET security and routing is complex and multifaceted. Effective solutions necessitate a holistic approach—one that merges robust routing design with proactive, context-aware security strategies. Strengthening collaboration across networking, cybersecurity, and UAV development disciplines will be fundamental.

REFERENCES

1. O. Bekmezci, K. Sahingoz, S. Temel, "Flying Ad-hoc Networks (FANETs): A Survey," Ad Hoc Network, Vol. (11), pp.1254–1270, 2013.
2. O.K Sahingoz, "Routing Protocols in flying Ad-hoc Networks (FANETs): Concepts and Challenges,"

Journal of Intelligent Robot System, Vol. (74), pp.513–527, 2014.

3. G. Soni, M. K. Jhariya, K. Chandravanshi and D. Tomar, "A Multipath Location based Hybrid DMR Protocol in MANET," 2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), pp. 191-196, 2020.
4. D. Anwekar and S. Phulre, "Analysis of Congestion Control Techniques to Improve QoS and Frequent Communication in FANET," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-7.
5. K. Chandravanshi, G. Soni, D.K. Mishra, "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET," IEEE Access, Vol. 10, pp. 110003 – 110025, 2022.
6. M.F Khan, Kok-Lim Alvi Yau, Rafidah Md Noor, Muhammad Ali Imran, "Routing Schemes in FANETs: A Survey," Sensors, MDPI, pp. 1-33, 2019.
7. J. Jiang, G. Han, "Routing Protocols for Unmanned Aerial Vehicles. IEEE Communication Magine, Vol. 56, pp. 58–63, 2018.
8. Ceviz, O., Sadioglu, P., Sen, S.. "Analysis of Routing Attacks in FANETs," Ad Hoc Networks and Tools for IT. ADHOCNETS TridentCom 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 428. Springer, 2022.
9. Ren, D. Li, Q. Hu, Y. Liu and J. Liu, "An Improved Security OLSR Protocol against Black Hole Attack based on FANET," 2022 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, 2022, pp. 383-388.
10. Altaweel, H. Mukkath and I. Kamel, "GPS Spoofing Attacks in FANETs: A Systematic Literature Review," in IEEE Access, vol. 11, pp. 55233-55280, 2023.
11. G. Soni, K. Chandravanshi, D. Deoskar, S. Parashar and R. Thakur, "Design and Develop an Efficient Load Balancing Approach with AOMDV Routing in 7G-FANET," 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, , pp. 1-7, 2024.
12. Kai-Yun Tsao, Thomas Girdler, Vassilios G. Vassilakis , "A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-Hoc Networks," Ad Hoc Networks, Vol. 133, pp. 1-36, 1 August 2022.
13. A.S Kaurav, S. R Dutt, "Detection and prevention from different attacks in VANET: A Survey," Journal of Physics: Conference Series, Volume 2040, International Conference on Physics and Energy 2021 (ICPAE 2021), Kancheepuram, India, 2021.
14. Sayani Sarkar, Sima Shafaei, Trishtanya S. Jones, Michael W. Totaro, "Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques", Drones, vol.9, no.8, pp.583, 2025.
15. A. Singh, A. Pandey, Detecting and protecting from hostile behavior in flying ad hoc networks for data and route security, IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG), pp. 1-7 (2025).
16. V. Chandrasekar, V. Shanmugavalli, T.R. Mahesh, , "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm. Sci Rep 14, 7818 (2024).
17. K. Singh,, A.K. Verma, "TBCS: A trust-based clustering scheme for secure communication in flying ad-hoc networks.," Wireless Personal Communnication , vol.114, pp.3173–3196 (2020).
18. W. Buksh, Y. Guo, S. Iqbal, K.N. Qureshi, J. Lloret, "Trust-oriented peered customized mechanism for malicious nodes isolation for flying ad hoc networks," Transactions on Emerging Telecommunications Technologies (ETT), (2022)..
19. Mauro Tropea, Mattia Giovanni Spina, Abderrahmane Lakas, Panagiotis Sarigiannidis, Floriano De Rango, "SecGPSR: A Secure GPSR Protocol for FANET against Sybil and Gray Hole Attacks," IEEE Access, Vol. 12, pp. 186909- 186925, 2024.
20. J. Vijitha Ananthi, P. Subha Hency Jose, "Performance of unique and secure routing protocol (USRP) in flying Ad hoc Networks for healthcare applications," High-Confidence Computing, Vol.4, pp. 1-8, 2024.