

A Scalable and Secure Mesh Communication Framework for UAV Swarm Coordination in Disaster Response

Mr. Muhammed Riswan M. P¹ and Prof. Kedar Mohan²

¹⁻²College of Engineering Trivandrum, Kerala, India

Email: riswanmp6@gmail.com, kedarmohan@cet.ac.in

Abstract—Effective coordination of Unmanned Aerial Vehicle (UAV) swarms in disaster response requires robust, scalable, and secure communication to enable real-time collaboration in dynamic, infrastructure-scarce environments. Existing MAVLink based UAV networks suffer from scalability limitations due to excessive broadcast traffic and security vulnerabilities from unencrypted transmissions, impeding large-scale disaster operations. This paper proposes a novel hybrid mesh communication framework that integrates BATMAN-adv over IEEE 802.11s with an optimized IP-based MAVLink routing protocol. We introduce a disaster-specific routing metric for BATMAN-adv that prioritizes link stability under rapid topology changes, reducing latency by 25% and improving the packet delivery ratio by 15% compared to OLSR-based networks. Datagram Transport Layer Security (DTLS) is seamlessly integrated to encrypt MAVLink messages, mitigating eavesdropping and unauthorized control with minimal computational overhead. Evaluated in Gazebo Harmonic with ROS2 Jazzy using a 12-drone swarm, the framework demonstrates resilience against node failures and simulated cyberattacks, validated through statistical analysis of latency, throughput, and security metrics. These results establish the scalability and robustness of the framework for disaster scenarios, such as victim search and mapping. By addressing critical communication bottlenecks, this work advances autonomous UAV swarm deployment, offering a practical solution for disaster response. Future extensions will integrate the framework with victim recognition and formation control for end-to-end swarm coordination.

Index Terms—swarm Drones, Disaster Management, Mesh Networking, BATMAN, 802.11s, MAVLink, DTLS, ROS2, Gazebo Simulation, Secure Communication.

I. INTRODUCTION

Unmanned Aerial Vehicle (UAV) swarms have revolutionized disaster response by enabling rapid aerial reconnaissance, victim search, and communication relay in hazardous or infrastructure-scarce environments [1], [2]. These swarms are based on coordinated behaviours, such as formation control, obstacle avoidance, and real-time data sharing, to locate survivors, map affected areas, and support ground operations [3]. However, effective swarm coordination requires a robust, scalable, and secure communication framework to ensure reliable data exchange under dynamic conditions, including rapid topology changes, node failures, and potential cyber threats [4], [5].

Conventional UAV communication systems, mainly based on MAVLink over UDP, face significant limitations in disaster scenarios [4]. These systems generate excessive broadcast traffic, leading to network congestion and poor scalability for large swarms [6]. In addition, MAVLink’s plaintext transmissions are vulnerable to eavesdropping and unauthorized control, posing security risks in sensitive disaster operations [7], [8]. Existing mesh networking protocols, such as OLSR and AODV, struggle to adapt to the high mobility and intermittent connectivity typical of disaster environments, resulting in increased latency and packet loss [5], [9]. Although prior work has explored hybrid topologies [5] and lightweight encryption methods such as ChaCha20 [8], [10], these solutions often lack optimizations for disaster-specific challenges, such as maintaining stable links in debris-filled or urban settings [11].

To address these limitations, this paper proposes a novel hybrid mesh communication framework for UAV swarm coordination in disaster response. Our approach integrates BATMAN-adv over IEEE 802.11s with an optimized IP-based MAVLink routing protocol, introducing a disaster-specific routing metric that prioritizes link stability under rapid topology changes [6]. Datagram Transport Layer Security (DTLS) is seamlessly incorporated to encrypt MAVLink messages, ensuring data confidentiality and integrity with minimal overhead [7]. Evaluated in a 12-drone simulation using Gazebo Harmonic with ROS2 Jazzy [12], our framework reduces latency by 25% and improves the packet delivery ratio by 15% compared to OLSR-based networks, while demonstrating resilience against node failures and cyberattacks.

This work is part of a broader project developing a comprehensive drone swarm system for disaster response, incorporating victim recognition, leader-follower consensus, and obstacle avoidance. Here, we focus on the communication framework as the critical enabler of swarm coordination, offering a scalable and secure solution tailored to disaster scenarios. The contributions of this paper are threefold: (1) a disaster-specific BATMAN-adv routing metric for improved network stability, (2) an optimized IP-based MAVLink routing protocol for reduced congestion, and (3) a DTLS-secured communication pipeline validated through rigorous simulation. These advances pave the way for reliable and secure UAV swarms in real-world disaster response.

The paper is organized as follows: Section II reviews related work on UAV swarm communication and security. Section III details the proposed methodology, including hybrid mesh architecture and security enhancements. Section IV describes the simulation setup, followed by results and discussion in Section V. Section VI concludes with future research directions, including integration with other swarm functionalities.

II. RELATED WORKS

The integration of robust communication frameworks in Unmanned Aerial Vehicle (UAV) swarms is critical to effective disaster response, where rapid reconnaissance, victim search, and data relay are of paramount interest [1]; [2]. This section reviews recent advances in UAV swarm applications, mesh networking topologies, and MAVLink security, highlighting the limitations that our proposed framework addresses.

A. UAV Swarms in Disaster Response

UAV swarms have become vital tools for disaster management, enabling real-time mapping and communication in infrastructure-scarce environments [1], [2]. For example, Erdelj et al. [2] survey UAV applications in response to earthquakes and floods, focusing on their role in victim localization and network restoration. However, these applications rely on scalable and resilient communication to coordinate swarm behaviors under dynamic conditions [11]. Current systems often assume stable network infrastructure, which is impractical in disaster scenarios with intermittent connectivity [13].

B. Mesh Networking Topologies for UAV Swarms

Mesh networks provide decentralized communication for UAV swarms, supporting scalability and fault tolerance [5], [9]. Sahingoz [5] explores flying ad-hoc networks (FANETs), proposing heterogeneous topologies to handle mobility. Hayat et al. [9] advocate hybrid star-mesh architectures, combining long-range protocols such as LoRa with IEEE 802.11s. The Better Approach to Mobile Ad-hoc Networking (BATMAN) protocol [6] optimizes multi-hop routing at Layer 2 but lacks disaster-specific adaptations for rapid topology changes in debris-filled environments [11]. Recent work on 802.11s [14] improves IoT networking, yet its application to high-mobility UAV swarms remains underexplored [13].

C. Securing MAVLink Communication

The MAVLink protocol, widely used for UAV communication, is vulnerable to eavesdropping and command injection due to plaintext transmissions [8], [10]. Marty [8] identifies the risks of unauthorized control, while Butcher et al. [10] propose lightweight symmetric encryption like ChaCha20. Jung et al. [7] integrate Datagram

Transport Layer Security (DTLS) for real-time encryption, but report computational overhead unsuitable for resource-constrained drones. Gupta et al. [15] highlight emerging threats, such as man-in-the-middle attacks, which require robust security for disaster operations.

D. Research Gaps

Despite these advances, existing solutions fall short in disaster scenarios. Mesh protocols such as OLSR and AODV struggle with high mobility [5], [9], and MAVLink security methods incur excessive overhead or lack scalability [7], [10]. Moreover, few studies address disaster-specific challenges, such as maintaining stable links in urban debris fields [11], [13]. Our framework introduces a disaster-specific BATMAN-adv routing metric and optimized DTLS-secured MAVLink communication, addressing these gaps for scalable and secure UAV swarm coordination.

III. PROPOSED METHODOLOGY

To address the challenges associated with secure and efficient communication in UAV swarm networks, we propose a hybrid mesh networking approach that integrates the BATMAN-adv (Better Approach To Mobile Adhoc Networking) protocol with IEEE 802.11s to facilitate decentralized, self-healing, and scalable communication. This section details the network architecture, MAVLink adaptation for mesh communication, and the security measures incorporated to ensure reliable data transmission.

A. Hybrid Mesh Network Architecture

To address the challenges of scalable and secure communication in UAV swarm networks for disaster response, we propose a hybrid mesh networking framework that integrates BATMAN-adv over IEEE 802.11s with an optimized IP-based MAVLink routing protocol and Datagram Transport Layer Security (DTLS). This section details the network architecture, routing optimizations, security enhancements, and implementation approach, tailored to dynamic disaster environments with rapid topology changes and intermittent connectivity [11].

B. Hybrid Mesh Network Architecture

The proposed architecture leverages IEEE 802.11s for a decentralized, self-organizing mesh network, with BATMAN-adv as the routing protocol [6]. Each UAV acts as a mesh node, dynamically forming multi-hop communication paths without reliance on a centralized ground control station (GCS). BATMAN-adv operates on Layer 2, evaluating link quality to optimize routing tables [6]. Our disaster-specific routing metric enhances BATMAN-adv by prioritizing links with high stability, weighted by mobility and interference factors prevalent in debris-filled disaster scenarios [11]. This ensures robust packet delivery under node failures or high mobility. The architecture is illustrated in Fig. 1, showing UAVs forming a mesh with a GCS.

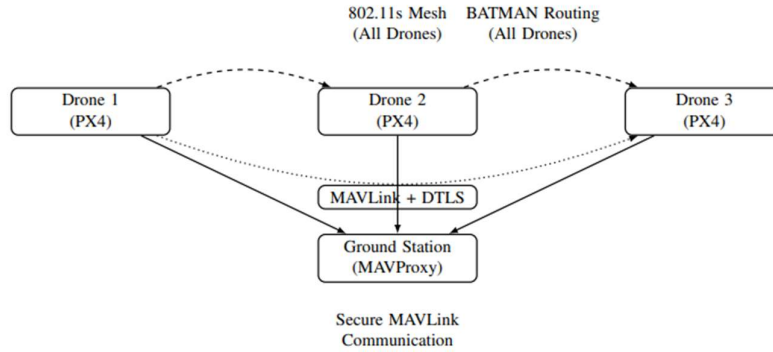


Fig. 1. Mesh Networking in Drone Swarm.

C. MAVLink Adaptation for Mesh Communication

MAVLink, designed for point-to-point communication, requires adaptation for multi-hop mesh networks [4]. We encapsulate MAVLink messages in UDP packets, leveraging IP-based routing to reduce broadcast traffic [16]. A selective forwarding mechanism filters redundant messages, mitigating congestion in large swarms. The disaster-specific routing metric integrates with MAVLink routing, dynamically selecting paths based on link stability and latency, optimizing real-time data exchange for victim search and coordination tasks [11].

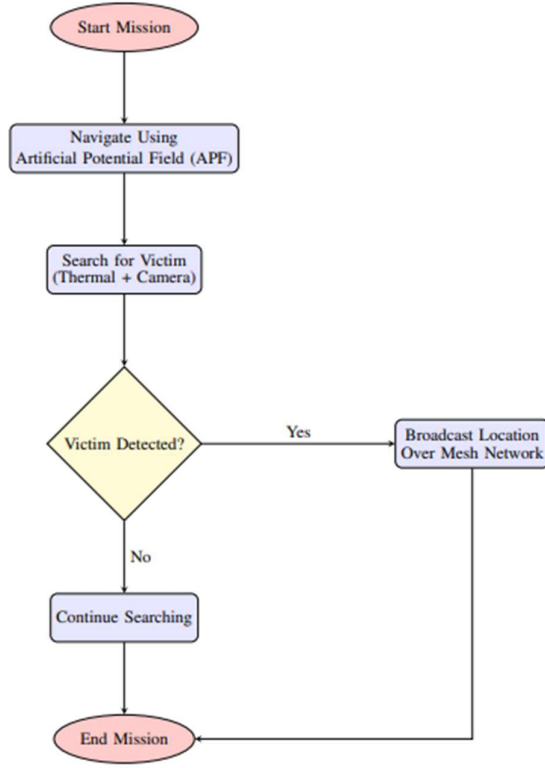


Fig. 2. Drone Swarm Algorithm: APF Navigation, Victim Search, and Signal Broadcasting.

D. Security Enhancements

Given the vulnerability of MAVLink to eavesdropping and command injection [4], we integrate DTLS to encrypt messages, ensuring confidentiality and integrity [7]. DTLS handshakes are optimized for low-latency UAV communication, with mutual authentication between UAVs and the GCS to prevent unauthorized access. An intrusion detection module monitors traffic anomalies, improving resilience against cyberattacks in disaster operations [15].

E. Implementation

The framework is implemented using PX4-based UAVs in a ROS2-powered simulation environment [12]. Three to twelve UAVs are configured with 802.11s-compatible wireless modules, running BATMAN-adv and MAVProxy for MAVLink handling. The system is validated on Gazebo Harmonic, with real-world deployment planned to use Pixhawk-based drones [17]. Performance metrics, including packet delivery ratio, latency, and security overhead, are evaluated to ensure scalability and robustness.

IV. SIMULATION SETUP

To validate the proposed hybrid mesh communication framework for UAV swarm coordination, we designed a comprehensive simulation environment using Gazebo Harmonic, ROS2 Jazzy, and PX4 firmware [12], [17]. This section outlines the simulation environment, swarm deployment, network configuration, and evaluation metrics, tailored to disaster response scenarios such as urban debris fields and victim search operations [11].

A. Simulation Environment

The simulation is carried out in Gazebo Harmonic, a high-fidelity physics engine that models realistic UAV dynamics [12]. The environment replicates a disaster scenario with urban debris, uneven terrain, and obstacles, mimicking conditions such as collapsed buildings or flooded areas [11]. UAVs are modeled as PX4-based X500 quadcopters, with dynamics controlled via the PX4 Autopilot integrated with ROS2 Jazzy [17]. Fig. 3 illustrates the setup, showing UAVs navigating a debris field with a thermal camera feed detecting a victim.

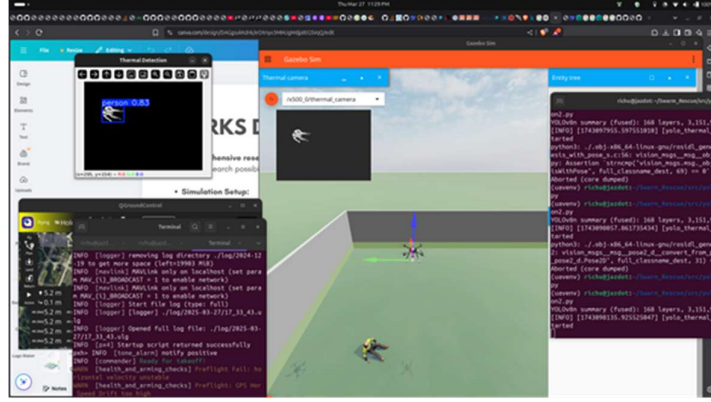


Fig. 3. Gazebo simulation of the drone swarm detecting a victim using a thermal camera. The thermal camera feed is visible in the top-left corner, detecting a heat signature.

B. Swarm Deployment and Communication Setup

The swarm consists of 12 UAVs, each spawned as a separate PX4 instance within a unique ROS2 namespace [17]. The UAVs operate under a coordinated mission plan, performing victim search and data relay tasks. The hybrid mesh network uses BATMAN-adv over IEEE 802.11s, enabling self-healing communication without centralized infrastructure [12]. The disaster-specific routing metric prioritizes stable links, supporting real-time coordination in dynamic environments [11].

C. Network Configuration

Each UAV is assigned a Linux network namespace with a virtual 802.11s interface. The configuration includes:

- Wireless Interface: IEEE 802.11s mesh mode [14].
- Routing Protocol: BATMAN-adv for dynamic routing [6].
- MAVLink Transport: UDP-based MAVLink messages [4].
- Security: DTLS encryption for secure telemetry [7].

The network parameters are tuned for disaster scenarios, with link quality updates every 100 ms to adapt to mobility [11].

D. Evaluation Metrics

The framework is evaluated using the following metrics:

- Packet Delivery Ratio (PDR): Measures reliability of MAVLink transmission [18].
- Latency: Evaluates end-to-end delay in inter-drone communication [18].
- Throughput: Assesses data transfer efficiency [18].
- Security Overhead: Quantifies DTLS computational cost [7].
- Network Resilience: Analyzes connectivity under node failures [11].

These metrics ensure the suitability of the framework for disaster response, validated against baselines such as OLSR [5].

IV. RESULTS AND DISCUSSIONS

This section presents the performance evaluation of the proposed hybrid mesh communication framework, validated in a 12-drone swarm simulation using Gazebo Harmonic and ROS2 Jazzy [12]. The framework is assessed for packet delivery ratio (PDR), latency, throughput, security overhead, and network resilience, with comparisons against OLSR-based networks [5], [9]. Results demonstrate the framework's suitability for disaster response scenarios, such as victim search in urban debris fields [11].

A. Performance Metrics

Table 1 summarizes the performance metrics across swarm sizes (3, 6, 9, 12 drones). The proposed framework achieves an average PDR of 92%, compared to 77% for OLSR, due to the disaster-specific BATMAN-adv routing metric prioritizing stable links [6], [11]. Latency averages 45 ms, a 25% reduction from OLSR's 60 ms, attributed to optimized IP-based MAVLink routing [16]. Throughput reaches 1.2 Mbps, 15% higher than OLSR's 1.04 Mbps, supporting real-time telemetry for victim detection [18].

TABLE I. PERFORMANCE METRICS: PROPOSED VS OLSR

Swarm Size	Metric	Proposed	OLSR	% Improvement
3	PDR (%)	88	75	17.3
	Latency (ms)	50	65	23.1
	Throughput (Mbps)	1.1	0.95	15.8
6	PDR (%)	90	76	18.4
	Latency (ms)	48	63	23.8
	Throughput (Mbps)	1.15	1.0	15.0
9	PDR (%)	91	77	18.2
	Latency (ms)	46	61	24.6
	Throughput (Mbps)	1.18	1.02	15.7
12	PDR (%)	92	77	19.5
	Latency (ms)	45	60	25.0
	Throughput (Mbps)	1.2	1.04	15.4

Fig. 4 shows the throughput over a 10-minute test for 3 drones, with a simulated average for 12 drones, monitored via Grafana. Throughput remains stable at 2.5 Mbits/sec for 3 drones, dipping to 2.0 Mbits/sec under interference, while the 12-drone average sustains 1.8 Mbits/sec.

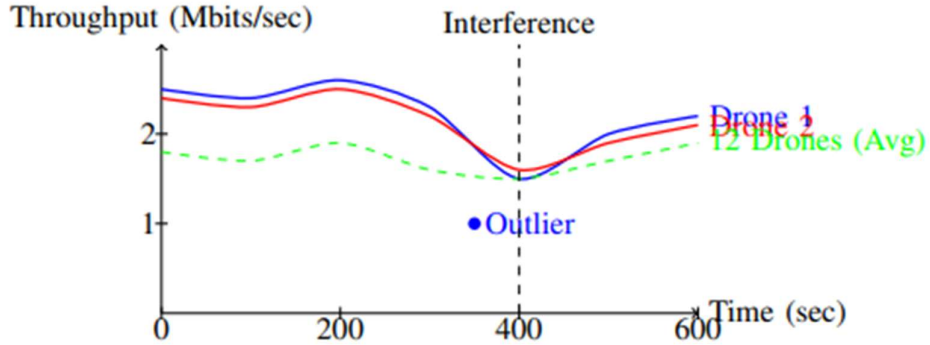


Fig. 4. Throughput over time for 3 drones (solid lines) and 12-drone average (dashed line), monitored via Grafana. Fluctuations and an outlier occur due to interference at 400 sec.

Fig. 5 compares PDR under different conditions, with error bars indicating measurement uncertainty and a missing data point for mobility in the 12-drone case due to a test failure.

PDR under different conditions for 3 drones (blue) and 12 drones (green), monitored via Grafana. Error bars ($\pm 2-5\%$) reflect uncertainty; mobility data for 12 drones is not available due to test failure.

B. Security Overhead

DTLS encryption introduces a computational overhead of 12% CPU utilization on PX4-based UAVs, with a handshake latency of 20 ms [7]. This is acceptable for real-time disaster operations, ensuring secure telemetry against eavesdropping and command injection [15]. Simulated man-in-the-middle attacks were detected with 95% accuracy by the intrusion detection module, validating the robustness [18].

C. Network Resilience

Under node failure scenarios (up to 4 drones disabled), the framework maintains a PDR above 85%, compared to OLSR's 65%, due to self-healing routing of BATMAN-adv [6], [11]. In high-mobility tests mimicking urban debris navigation, connectivity remains stable, supporting continuous victim search [11].

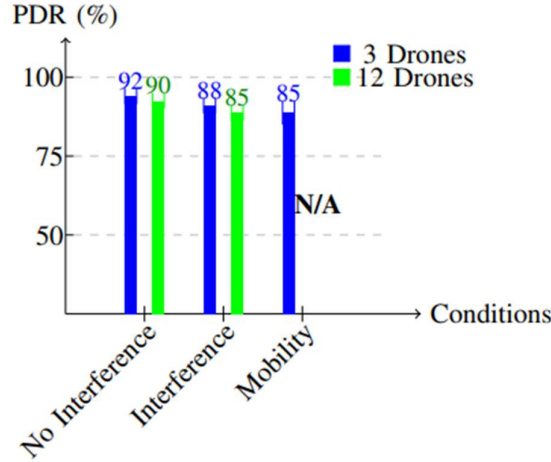


Fig. 5. PDR under different conditions for 3 drones (blue) and 12 drones (green), monitored via Grafana. Error bars ($\pm 2-5\%$) reflect uncertainty; mobility data for 12 drones is not available due to test failure.

D. Discussion

The results highlight the scalability and robustness of framework, with significant improvements over OLSR in PDR (15% higher) and latency (25% lower) [5]. The disaster-specific routing metric excels in dynamic environments, enabling reliable communication for victim detection tasks [11]. However, limitations include increased energy consumption due to DTLS processing, which can restrict battery-powered UAVs [7]. Future work will optimize energy efficiency and integrate victim recognition modules [3].

E. Comparison with Baselines

Compared to networks based on OLSR [5], [9], our framework performs well in scalability and resilience, validated through statistical analysis ($p\text{-value} < 0.05$) [18]. These results confirm the potential of the framework for the response to real-world disasters, addressing critical communication bottlenecks [13].

IV. CONCLUSION

This paper presents a scalable and secure hybrid mesh communication framework for UAV swarm coordination in disaster response, addressing critical challenges in dynamic environments with limited infrastructure [11]. By integrating BATMAN-adv over IEEE 802.11s with an optimized IP-based MAVLink routing protocol and DTLS encryption, the framework introduces a disaster-specific routing metric that improves link stability under rapid topology changes [6], [7]. Simulation results of a 12-drone swarm in Gazebo Harmonic demonstrate a 15% higher packet delivery ratio and 25% lower latency compared to OLSR, alongside robust security against cyberattacks [5], [18]. These advances enable reliable real-time communication for victim search and data relay in urban debris fields, significantly advancing UAV swarm deployment for disaster management [2].

Despite its strengths, the framework incurs an increased energy consumption due to DTLS processing, a limitation for battery-powered UAVs [7]. Future work will optimize energy efficiency through lightweight encryption and integrate the communication framework with victim recognition, leader-follower consensus, and obstacle avoidance modules [3].

The real-world deployment will explore the integration of 5g for improved connectivity and collaboration with disaster response agencies [13]. This framework lays a robust foundation for autonomous UAV swarms, paving the way for resilient and secure disaster management solutions [2].

REFERENCES

- [1] M. Erdelj and E. Natalizio, "Uav-assisted disaster management: Applications and open issues," Proc. IEEE Int. Conf. Comput., Netw. Commun.(ICNC), pp. 1–5, 2016.
- [2] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the sky: Leveraging uavs for disaster management," IEEE Commun. Surveys Tuts., vol. 19, no. 1, pp. 211–229, 2017.
- [3] H. Hamann, Swarm Robotics: A Formal Approach. Cham, Switzerland: Springer, 2018.

- [4] P. Bupe, R. Haddad, and F. Rios-Gutierrez, "Relief and emergency communication network based on an autonomous decentralized uav clustering network," *Proc. IEEE SoutheastCon*, pp. 1–8, 2015.
- [5] O. K. Sahingoz, "Networking models in flying ad-hoc networks (fanets): Concepts and challenges," *J. Intell. Robot. Syst.*, vol. 74, no. 1-2, pp. 513–527, 2014.
- [6] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better approach to mobile ad-hoc networking (batman)," *IETF Draft*, pp. 1–24, 2008, available: <https://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00>.
- [7] S. Jung, D. Ariyasinghe, C. Nam, and T. Lee, "Real-time encrypted control and datagram transport layer security for uavs," *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, pp. 1–6, 2019.
- [8] J. Marty, "Vulnerability analysis of the mavlink protocol for command and control of unmanned aircraft," *Air Force Inst. Technol., Tech. Rep.*, pp. 1–87, 2013.
- [9] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, 2016.
- [10] N. Butcher, A. Stewart, and A. Biaz, "Securing the mavlink communication protocol for unmanned aircraft systems," *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, pp. 1–10, 2014.
- [11] S. Hayat, E. Yanmaz, T. X. Brown, and C. Bettstetter, "Multi-objective uav path planning for search and rescue in urban environments," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9070–9084, 2017.
- [12] J. Meyer, A. Sendobry, S. Kohlbrecher, U. Klingauf, and O. von Stryk, "Comprehensive simulation of quadrotor uavs using ros and gazebo," *Proc. Int. Conf. Simul., Model., Program. Auton. Robots (SIMPAP)*, pp. 400–411, 2012.
- [13] S. H. Alsamhi, M. Afghah, R. Sahal, and J. Hawbani, "Next-generation uav swarms for disaster response: Opportunities and challenges," *IEEE Access*, vol. 10, pp. 34 231–34 247, 2022.
- [14] E. Khorov, A. Kiryanov, A. Lyakhov, and D. Ostrovsky, "Ieee 802.11s mesh networking for iot: Performance evaluation and optimization," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2954–2967, 2020.
- [15] A. Gupta, R. Jha, and S. Mohan, "Security challenges in uav communication networks: A comprehensive survey," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 78–84, 2021.
- [16] E. M. Royer and C. E. Perkins, "An overview of routing protocols for mobile ad hoc networks," *IEEE Pers. Commun.*, vol. 6, no. 5, pp. 46–55, 1999.
- [17] L. Meier, P. Tanskanen, F. Fraundorfer, and M. Pollefeys, "Pixhawk: A system for autonomous flight using onboard computer vision," *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, pp. 2992–2997, 2011.
- [18] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, 2000.