SNPSG Journal of Intelligent Unmanned Systems

2026, Vol. 1, No. 1, Article 12
DOI: https://doi.org/10.65218/jius.2026.12

RESEARCH ARTICLE

Evaluating SDN against AODV for dynamic topology management in disaster-relief UAV networks

Antonio Santos da Silva[1, 2, *], Túlio Dapper e Silva[1], Flávio Rech Wagner[1], Alexey Vinel[2, 4], Mauro Tropea[3], Paulo Mendes[5] and Edison Pignaton de Freitas[1,4]

1 Federal University of Rio Grande do Sul, Porto Alegre, Brazil
2 Karlsruhe Institute of Technology, Karlsruhe, Germany
3 University of Calabria, Arcavacata CS, Italy
4 Halmstad University, Halmstad, Sweden
5 Airbus, Taufkirchen, Germany
* Corresponding author(s): Antonio Santos da Silva
Email(s): aassilva@inf.ufrgs.br

Received: 01 December 2025 | Accepted: 06 March 2026 | Published Online: 30 June 2026

Abstract: In the aftermath of natural disasters, the rapid deployment of Unmanned Aerial Vehicles (UAVs) is critical for re-establishing communication services. However, managing the network topology in these scenarios is a significant challenge, primarily due to the high mobility of both the UAVs and the ground users they serve. While dynamic routing protocols have been the traditional approach for ad hoc networks, the centralized control paradigm of Software-Defined Networking (SDN) presents a compelling alternative for dynamic topology management. This paper investigates the efficacy of an SDN-based management solution for UAV networks, a topic for which the existing literature lacks a definitive performance consensus. An SDN architecture tailored for UAV-based emergency networks is proposed and evaluated, with performance benchmarked against the well-established Ad hoc On-Demand Distance Vector (AODV) protocol. Through simulations in the OMNeT++ framework, key performance indicators were analyzed, including end-to-end latency, packet delivery ratio, infrastructure utilization, and packet drop rates, under varying user loads. The results demonstrate a clear performance advantage for the proposed SDN solution. Specifically, the architecture achieved a packet delivery ratio of up to 17.5% higher than AODV and reduced the end-to-end data packet latency by up to 10 ms. These findings provide strong evidence that a centralized software-defined approach can offer superior reliability and efficiency for managing highly dynamic UAV communication networks in critical disaster recovery operations.

Keywords: Unmanned Aerial Vehicles (UAVs), Software Defined Networks (SDN), Natural Disasters

I. Introduction

In the critical 72-hour window following natural disasters, the rapid restoration of communication infrastructure is paramount for effective rescue operations. The absence of reliable communication and situational awareness frequently degrades the effectiveness of post-disaster missions, a challenge highlighted by [1]. In this context, Unmanned Aerial Vehicles (UAVs) have emerged as a key technology for providing rapid network recovery services, enhancing public safety networks, and addressing other emergency scenarios.

The flexibility, ease of deployment, and low operational costs of UAVs have motivated extensive research into their application for delivering wireless communication solutions. Foundational works, such as [2, 3], have investigated the feasibility of integrating UAVs into communication network architectures. While these studies primarily focused on the challenges and standardization trends for UAVs in supporting cellular networks, the encouraging results have provided significant visibility to this domain, as systematically surveyed in [4].

A particularly promising application involves deploying UAVs as flying base stations (BSs) in a three-dimensional (3D) space to provide ubiquitous sky access to ground users during disaster events. With terrestrial BSs often unavailable, UAV-based flying BSs offer a suitable method for dynamically adjusting a network topology to maintain real-time ground communication links [5]. However, the diverse aerodynamic characteristics of conventional UAVs—including flight altitude, energy constraints, payload capacity, and endurance—necessitate adjustable, multi-layer architectures for future UAV networks [3, 6].

Although studies [7–11] have proposed solutions for sustaining network communication among ground nodes via relay nodes, these proposals exhibit limitations, particularly in maintaining reliability and connectivity [12]. A thorough review of the literature reveals a gap in approaches that fully address the problem of dynamic topology management without depending on fixed anchor nodes or pre-configured, inflexible network topologies. To address this gap, this paper presents an evaluation of the trade-offs in a Software-Defined Network (SDN) based approach for managing a dynamic UAV-network topology, drawing inspiration from architectures applied in military scenarios [13].

This article conducts a comparative analysis between an SDN-based and an ad hoc[1] approach to UAV topology management. The evaluation utilizes a UAV topology formation algorithm adapted from Kim and Lee [16], employing three distinct node types: a central controller node, a set of relay nodes, and a set of user nodes. The relay nodes are tasked with maintaining connectivity among user nodes and optimizing their position to meet service requests. In the SDN-based approach, the controller node assumes responsibility for discovering and configuring the optimal network topology and populating the routing tables of the relay nodes.

[1]This paper uses the term ad hoc in accordance with several related works [Kirichek et al. [14] and Misra Sudip et al. [15]].

DOI: https://doi.org/10.65218/jius.2026.12

The proposed architecture is validated through simulation-based experiments implemented in the OMNeT++ simulator[2], which accounts for modeled physical constraints. The simulations model a large urban area where user nodes exhibit random mobility. For topology management, an SDN-based algorithm was developed, with implementation details described in Section 3. Control messages exchanged between the relay and controller nodes adhere to the OpenFlow standard [17]. For the comparative analysis, an ad hoc routing protocol with features analogous to the SDN approach was also implemented, as detailed in Section 5.

The simulation results indicate that the SDN approach provides significant performance improvements in a dynamic UAV network. The end-to-end latency of data packets was reduced by up to 10ms, and the packet delivery ratio was up to 17.5% higher compared to the AODV protocol. Furthermore, the results demonstrate more efficient utilization of network infrastructure under the SDN paradigm. These findings suggest that a centralized control architecture with a global network view is a highly effective method for managing dynamic networks characterized by high traffic flow.

The remainder of this work is organized as follows. Section 2 presents the main concepts of the SDN approach and discusses other related works. Section 3 presents the architecture, providing an overview of resources, node capabilities, the UAV coordination protocol, and topology management. The methodology and mechanisms used in the experiments to evaluate the proposed solution are the subject of Section 4. Section 5 describes the experiments performed to evaluate the proposed solution and discusses the obtained results. Finally, the conclusions and potential future work are presented in Section 6.

II. Background and Related Work

The integration of UAVs to form Flying Ad Hoc Networks (FANETs) has emerged as a critical solution for establishing communication in scenarios where terrestrial infrastructure is compromised or absent, such as in natural disasters [18]. The management of network topology in these highly dynamic environments, however, presents significant challenges. This section reviews the evolution of research in this domain, from foundational concepts and the limitations of traditional protocols to the rise of Software-Defined Networking (SDN) and the specific research gap this study addresses.

SDN introduces a software abstraction layer that provides a centralized view of the network, enabling unified management and programmatic control over a topology that continuously evolves [19]. The architecture of SDN is founded on four key principles, as defined by Kreutz et al. [20]:

- **Separation of Control and Data Planes:** Network devices are simplified to function primarily as traffic-forwarding elements, with control plane responsibilities offloaded to an external controller.

- **Flow-Based Forwarding:** Routing decisions are made based on flows, where a sequence of packets between a source and destination receives a consistent set of service policies.

- **Software-Based Network Programming:** The network is programmable via software running on the controller, which interacts with the data planes of the network devices. This represents the core value proposition of SDN.

- **Centralized Control Logic:** The network's control logic is managed by one or more external SDN controllers, which possess a global view of the network state.

The unique characteristics of FANETs, high node mobility, frequent topology changes, and low node density, differentiate them from traditional Mobile Ad Hoc Networks (MANETs) and Vehicular Ad Hoc Networks (VANETs). A comprehensive survey by Lakew et al. (2020) provides an exhaustive review of FANET routing protocols, establishing that their routing requirements far surpass those of other ad hoc networks and highlighting significant open research issues [21]. The core challenge lies in maintaining stable and efficient communication amidst constant topological flux. SDN has been proposed as a promising paradigm to address these challenges. SDN decouples the network's control plane from the data plane, enabling centralized network management and programmability. A foundational survey by Haque and Abu-Ghazaleh (2016) reviewed the application of SDN in various wireless settings, noting its potential for centralized control and graceful protocol evolution but also highlighting that, at the time, it was not widely adopted or well-understood in the wireless domain [22].

Traditional ad hoc routing protocols, while foundational, exhibit significant performance degradation in high-mobility context of FANETs. A comparative evaluation by Gupta and Seth (2023) using NS-3 simulations assessed OLSR, DSDV, AODV, and DSR, concluding that while AODV performed best among them in high-mobility scenarios, it still suffered from considerable packet loss and routing overhead [23]. Another performance evaluation of FANET routing protocols in disaster scenarios further confirmed these limitations, analyzing AODV, DSR, OLSR, and ZRP and underscoring the difficulties these protocols face in emergency contexts [24]. These studies collectively demonstrate that even the most optimized traditional protocols struggle to cope with the rapid topological changes inherent to UAV operations, justifying the exploration of alternative network management paradigms.

The application of SDN to FANETs aims to overcome the limitations of distributed routing by centralizing network intelligence. Early conceptual work, such as that by Bupe et al. (2015), proposed autonomous UAV deployment with centralized management for disaster recovery, establishing the value of a central controller without formally employing the SDN paradigm [18]. Subsequent research focused on practical SDN implementations. Sharma et al. (2019) proposed and demonstrated a method for the automatic configuration of OpenFlow in MANETs using the Mininet-WiFi emulator, addressing key deployment challenges [25].

More specific to topology management, Silva et al. (2019) introduced STFANET, an SDN-based protocol that combines construction and adjustment algorithms to maintain FANET topology, achieving notable performance in simulated military scenarios [26]. However, its focus was on topology formation rather than a direct performance benchmark against established ad hoc protocols. Similarly, the ASR-FANET framework proposed by Albu-Salih and Khudhair (2021) presented an adaptive SDN-

[2] Available in: https://omnetpp.org/.

DOI: https://doi.org/10.65218/jius.2026.12

based routing solution, but its performance was only compared against the proactive OLSR protocol, overlooking a comparison with AODV, the most relevant reactive protocol for such dynamic environments [27]. This reveals a critical gap: the lack of a direct, systematic performance comparison between a practical SDN implementation and the most suitable traditional ad hoc protocol.

Recent research has explored more sophisticated aspects of SDN-FANETs. Recognizing the centralized controller as a single point of failure, Uomo et al. (2025) proposed a P4-programmable architecture for fault-tolerant SDN-FANETs, enabling autonomous rerouting when the controller is unreachable [28]. Spina et al. (2024) integrated security into the equation with SURA-LB, an SDN framework featuring an Intrusion Detection System (IDS) and resource-aware load balancing for disaster scenarios [29]. Sun et al. (2025) introduced a hybrid SDN architecture using an Extended Kalman Filter for predictive routing to improve energy efficiency [30]. While these works advance the state-of-the-art in specialized areas, they do not provide the fundamental performance benchmark against AODV.

Concurrently, machine learning has emerged as an alternative, decentralized paradigm. Liu et al. (2023) proposed PARouting, a Deep Reinforcement Learning (DRL) based protocol [31], and Qiu et al. (2023) developed a DRL-based method for adaptive link maintenance [32]. These approaches also aim to solve the high-mobility challenge but through a distributed intelligence model, further highlighting the need to rigorously validate the performance benefits of the centralized SDN approach.

The validity of any comparative network study rests on its simulation methodology. The OMNeT++ simulator, along with the INET framework, is a well-established tool for this purpose. The GrADyS-SIM framework, developed by Lam-enza et al. (2022), is a notable example of an OMNeT++/ INET-based platform built specifically for simulating UAV swarms [33]. Furthermore, comparative studies of network simulators, such as the one conducted by Manzoor et al. (2023) between ns-3 and OMNeT++, provide guidance on simulator selection and validate their use for performance evaluation in wireless networks [34]. The work by Tropea et al. (2025) also contributes by comparing ns-3 and Mininet-WiFi for SDN-FANET emulation, offering insights into the trade-offs of different simulation platforms [35].

Despite the extensive body of work, a definitive performance consensus on the superiority of SDN over optimized ad hoc protocols in highly dynamic UAV networks is conspicuously absent from the literature. While many studies propose advanced SDN features, they often stop short of a direct, empirical comparison against AODV, the most relevant reactive protocol. This work addresses that specific gap by providing a systematic, simulation-based performance evaluation of an SDN-based topology management solution aga-inst the AODV protocol, using metrics critical for disaster recovery scenarios. By doing so, it aims to provide a clear benchmark to justify the adoption of SDN in highly dynamic UAV networks.

III. Architecture

The proposed architecture is structured into a three-tiered hierarchy comprising a single Controller and Super Orchestrator (CSO), a set of mobile Relay Nodes (RNs), and a set of autonomous User Nodes (UNs), as depicted in Figure 1. This

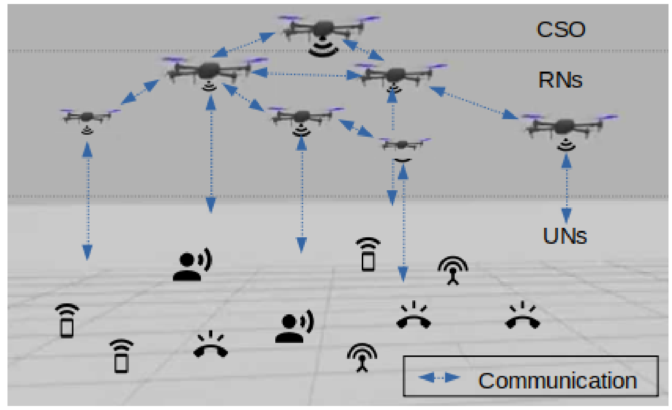


Fig. 1 Application topology divided into three layers. First *CSO* layer contains the controller node, second layer *RNs* contains the relay nodes, and third layer *UNs* contains the user nodes.

model is designed to provide resilient network coverage for ground-based UNs, which are assumed to be executing an arbitrary mission, such as searching for points of interest [9]. Consequently, the mobility of UNs is self-determined and considered unpredictable from the network management perspective.

To maintain robust connectivity, the RNs—implemented as UAVs—are strategically positioned to form a multi-hop backbone. The CSO is responsible for the global optimization of this backbone. It assigns each RN a specific operational area, defined by a central coordinate and a radius, within which the RN has the autonomy to perform minor positional adjustments to enhance local link quality with connected UNs. The overarching topology management and routing logic, however, are centralized at the CSO. This external controller periodically gathers contextual information —such as position, trajectory, and speed—from all nodes to maintain a global network view. Based on this view, the CSO computes and disseminates routing table updates and optimal positions for itself and the RNs.

A. Node Roles and Functionality

The architecture defines three distinct node roles with specialized responsibilities:

a) Controller and Super Orchestrator (CSO)

The CSO functions as the centralized control plane of the network. It is exclusively responsible for allocating RNs to strategic locations to ensure infrastructure-wide connectivity. In accordance with the SDN paradigm, the CSO configures and maintains the flow tables for all RNs and manages the association between RNs and the UNs they serve. To ensure routing decisions reflect the current network state, the CSO periodically receives context updates from the RNs. Its only direct communication is with the RNs, conducted via a secure control channel using a protocol based on OpenFlow [17].

b) Relay Nodes (RNs)

RNs operate primarily within the data plane. Their core function is to forward packets between UNs according to the rules installed in their flow tables by the CSO. They also possess limited autonomy to optimize their position within their designated operational area to improve link quality for associated UNs. Furthermore, RNs are responsible for gathering and periodically transmitting local context information and operational status updates to the CSO, acting as the sensory apparatus of the control

DOI: https://doi.org/10.65218/jius.2026.12

plane. All data traffic forwarded by RNs is routed on a multi-hop basis through the FANET backbone.

c) User Nodes (UNs)

UNs are the end-users of the network infrastructure. Their mobility is dictated by their specific mission objectives and is independent of network control.

B. SDN Implementation and Operation

The architecture explicitly implements the four pillars of SDN as proposed by Kreutz et al. [20], ensuring a clean separation between the control and data planes. As illustrated in Figure 1, the RNs constitute the Infrastructure Layer (data plane), while the CSO embodies the Control and Application Layers (control plane). Communication across this separation is facilitated by a custom, OpenFlow-based protocol that standardizes the exchange of control messages, as detailed in Table 1.

Table 1 Control plane message types exchanged by the CSO, RNs and UNs.

Message	Source	Destination
Hello	UN	RN
Close	UN	RN
Response_KeepAlive	UN	RN
Refresh	UN	RN
Confirmation_Registry	RN	UN
KeepAlive	RN	UN
Response_Close	RN	UN
Register	RN	CSO
Unregister	RN	CSO
Refresh_Register	RN	CSO
Packet_In	RN	CSO
Notify_User_Status	RN	CSO
Notify_Relay_Status	RN	CSO
Update_User	CSO	RN
Update_Routing_Table	CSO	RN
Update_Area	CSO	RN

This separation enables flow-based forwarding. Each RN maintains a Flow Table containing entries that map packet characteristics (Rules) to specific forwarding behaviors (Actions), such as forwarding a packet to a specific port. These entries are populated on-demand. When an RN receives a packet for which no matching rule exists in its Flow Table, it sends a control message (akin to a Packet-In message) to the CSO. The CSO, leveraging its global network view, processes the request, determines the appropriate forwarding rule, and sends it back to the RN. The RN then installs this new rule in its Flow Table and processes the original packet, which was temporarily queued.

The entire logic for network topology management and RN coordination is implemented as software applications running on the CSO. The route selection process, for instance, is handled by an application that executes Dijkstra's algorithm [36] on the global network graph to compute the minimum-cost path for each flow. The dynamic reconfiguration capabilities inherent to SDN allow the CSO to continuously update the Flow Tables across all RNs, ensuring that the data plane always reflects the most current and optimal network state.

IV. Methodology

In order to evaluate the performance of the SDN approach in managing an UAV topology, its efficiency is compared with an alternative solution, the Ad hoc On-Demand Distance Vector Routing (AODV) protocol, having the same objective. Experiments were performed in the Mobile Multimedia Wireless Sensor Network (M3WSN), which is an OMNet++ framework developed over Castalia [37]. OMNet++ is a network simulator which is widely used for implementing and testing novel solutions. In the rest of this section, the AODV protocol is better described, as well as the topology coordination algorithms applied for both construction and maintenance of the network. The simulation setup is described, along with scenario parameters and considered metrics. In the following, results and discussions are also presented.

A. Ad hoc On-Demand Distance Vector (AODV) Routing

The Ad hoc On-Demand Distance Vector (AODV) routing protocol, standardized by the IETF MANET Working Group[3], was developed to provide an efficient and adaptive routing solution for highly dynamic mobile networks. Its primary design goal is to minimize control message overhead, thereby conserving bandwidth and computational resources, by establishing routes only when they are needed. This is achieved through a reactive, or on-demand, mechanism: a route discovery process is initiated only when a source node needs to transmit data to a destination for which it has no valid route [38]. Although it relies on traditional routing tables at each node, it avoids the constant overhead of proactive protocols that maintain routes to all possible destinations. The implementation used in this work adheres to the specifications outlined in RFC 3561 [39].

To cope with the high mobility inherent to FANETs, AODV incorporates mechanisms for both route discovery and route maintenance. The route discovery process is initiated by the source node broadcasting a Route Request (RREQ) packet. As the RREQ propagates through the network, intermediate nodes create reverse paths back to the source. Upon reaching the destination, a Route Reply (RREP) packet is unicast back along the established reverse path, creating the forward path in the process.

Route maintenance is critical for detecting link failures. This is primarily achieved through periodic local connectivity checks using "Hello" messages. If a node fails to receive several consecutive Hello messages from a neighbor, it assumes the link is broken. When a link failure is detected along an active route, the node upstream of the break broadcasts a Route Error (RERR) message. This message propagates back towards the source, notifying all affected nodes to invalidate the routes that depend on the broken link. Upon receiving an RERR message, a source node can then choose to re-initiate the route discovery process if the path is still required.

B. Topology Coordination Model

The primary objective of the topology coordination model is to dynamically construct and maintain a robust communication network connecting all User Nodes (UNs), either directly or via multi-hop relay paths. This is achieved by optimizing the spatial positions of the UAVs, which serve as relay nodes and a central controller. The optimization process is driven by a cost function, adapted from the work of Kim and Lee [16], which is minimized using a Particle Swarm Optimization (PSO) algorithm. The PSO algorithm iteratively adjusts the positions of

[3] Available at: https://www.ietf.org/wg/manet/.

 DOI: https://doi.org/10.65218/jius.2026.12

the UAVs (the particle swarm) to find a quasi-optimal network topology that balances connectivity, signal quality, and physical constraints.

The cost function, denoted as $f(X,P)$, quantifies the suitability of a given UAV deployment configuration. It is defined as a weighted sum of three distinct components, as shown in Equation (1). Each component represents a critical aspect of the network's performance and stability.

$$f(X,P) = f_1(X,P) + f_2(X,P) + f_3(X,P). \tag{1}$$

Here, X represents the set of all node positions, and P is the set of all communication paths within the network topology.

The first component, $f_1(X,P)$, promotes network compactness by minimizing the total length of all communication links in the topology. This encourages shorter, more energy-efficient links, which inherently lead to lower latency and higher signal integrity. The function is defined as:

$$f_1(X,P) = \psi \sum_{p\in P} \sum_{k=1}^{|p|-1} \delta(p_k, p_{k+1}), \tag{2}$$

where P is the set of all end-to-end communication paths, p is a single path within that set (represented as a sequence of nodes $(p_1, p_2, \ldots, p_{|p|})$), $\delta(u,v)$ is the Euclidean distance between any two nodes u and v, and ψ is a weighting coefficient that controls the relative importance of network compactness in the overall cost function.

The second component, $f_2(X,P)$, introduces a significant penalty for any communication link that exceeds the maximum effective communication range, denoted as d_r^*. This term ensures that the optimized topology consists only of viable links, preventing the formation of paths that are too long to sustain reliable communication. The penalty is quadratic, meaning that even small violations are heavily penalized, driving the optimization algorithm to prioritize link feasibility above all else. The function is formulated as:

$$f_2(X,P) = \lambda \sum_{p\in P} \left(\max\left\{0, \max_{k=1,\ldots,|p|-1} \delta(p_k, p_{k+1}) - d_r^* \right\} \right)^2, \tag{3}$$

where d_r^* is the maximum ideal distance for a reliable communication link. The inner $\max$ function identifies the longest link within each path p, and the outer $\max\{0,\ldots\}$ ensures that a penalty is applied only if this longest link exceeds d_r^*. The term is weighted by λ, a large coefficient designed to make this penalty dominant, ensuring that solutions with invalid link lengths are strongly disfavored.

The third component, $f_3(X,P)$, enforces a minimum safety distance, d_s, between any two nodes (UAVs or UNs) in the network. This is a critical physical constraint to prevent collisions and mitigate signal interference between co-located nodes. Similar to f_2, this function applies a quadratic penalty if any two nodes are closer than the defined safety threshold. The function is defined as:

$$f_3(X,P) = \mu \left(\max\left\{0, d_s - \min_{\substack{u,v\in C\cup R\cup I \\ u\neq v}} \delta(u,v) \right\} \right)^2, \tag{4}$$

where d_s is the minimum required safety separation distance. The sets C, R, and I represent the controller node, relay nodes (UAVs), and user nodes (UNs), respectively. The $\min$ function finds the shortest distance between any pair of distinct nodes in the entire network, and the $\max\{0,\ldots\}$ function ensures a penalty is applied only if this minimum distance is less than d_s. The entire term is weighted by μ, a large coefficient that heavily penalizes any violation of the safety distance to ensure the physical feasibility of the UAV deployment.

The iterative optimization process executed by the CSO is illustrated in the block diagram in Figure 2. The algorithm begins by initializing a swarm of particles, where each particle represents a complete candidate topology defined by a set of positions for all RNs. For each particle in the swarm, a fitness evaluation is performed by calculating the total cost using the function $f(X,P)$ from Equation (1). This core step aggregates the values from the three distinct components: network compactness (f_1), penalties for exceeding the maximum communication range (f_2), and penalties for violating the minimum safety distance (f_3). Based on this cost, each particle's personal best position (pbest) and the swarm's global best position (gbest) are updated. The algorithm then adjusts the velocity and position of each particle, pulling it towards these best-known positions. This loop continues until a termination condition is met, such as a maximum number of iterations or convergence of the solution. The final output is the global best position, which represents the quasi-optimal set of coordinates for the RNs to be deployed.

C. Simulation Setup

The performance evaluation of the proposed SDN architecture against the AODV benchmark was conducted using a discrete-event network simulator. The simulation environment was designed to represent a challenging disaster recovery scenario characterized by high mobility and variable user density. This section details the simulation parameters, mobility and traffic models, and the performance metrics used for the comparative analysis.

The simulated environment consists of a flat, obstacle-free terrain with dimensions of 10 km x 10 km. A fixed set of 10 Relay Nodes (RNs) was deployed to provide network connectivity for a variable number of User Nodes (UNs). To assess the scalability of each approach, three distinct scenarios were simulated, with the number of UNs set to 15, 30, and 45, respectively. All nodes were configured with a nominal communication range of 100 meters. Each simulation was run for a total duration of 30 minutes, a timeframe deemed sufficient to allow the network to reach a steady state and to gather statistically significant results. A drop-tail queuing mechanism was implemented on all nodes to manage buffer overflow, where incoming packets are discarded when a node's buffer is full.

A Random Waypoint (RWP) mobility model was used for all UNs, which moved at speeds randomly selected from a uniform distribution between 5 m/s and 10 m/s. The RNs and the CSO, while managed by their respective positioning algorithms, were assigned a maximum operational speed of 20 m/s. The traffic

DOI: https://doi.org/10.65218/jius.2026.12

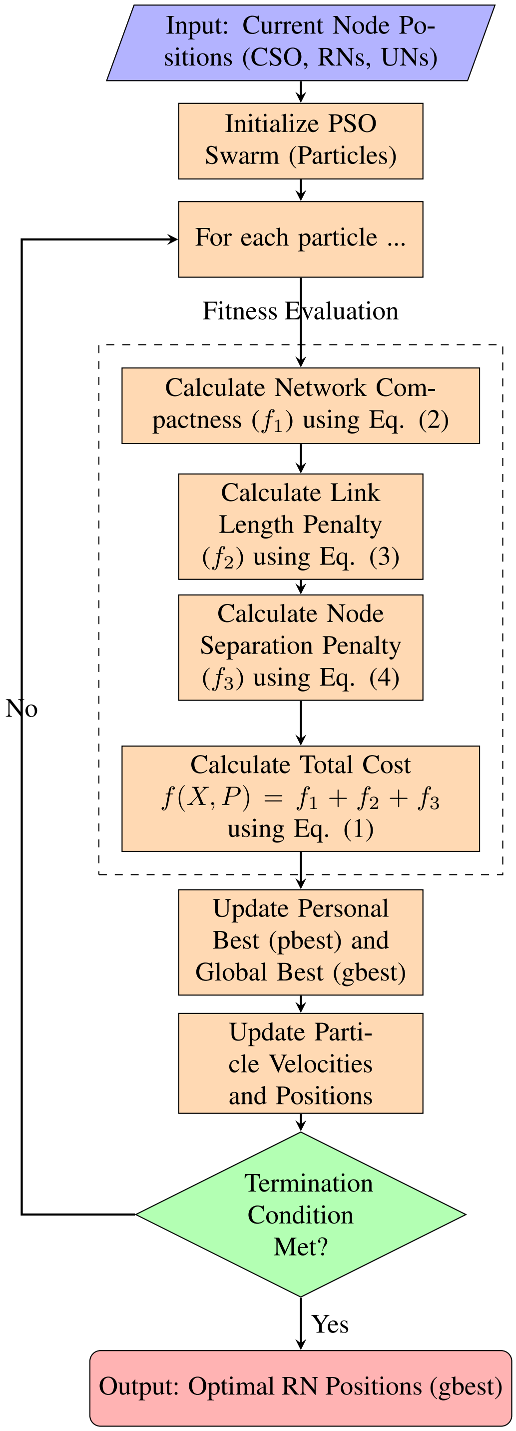


Fig. 2 Block diagram of the iterative algorithm evaluates each candidate topology (particle) by calculating a total cost based on network compactness (f_1), link length penalties (f_2), and node separation penalties (f_3).

generation model involved each UN transmitting data packets to another randomly selected UN at intervals uniformly distributed between 50 ms and 200 ms. This model simulates a constant-bit-rate (CBR) traffic pattern with varied destinations, creating a dynamic and demanding communication load on the network backbone.

The parameters for the AODV protocol were configured in strict accordance with the recommendations outlined in RFC 3561 [39]. For the proposed SDN-based solution, the control loop periodicity and other relevant parameters were optimized for the target scenario. A comprehensive summary of all simulation parameters is presented in Table 2.

Table 2 Simulation parameters.

Simulation Parameters	Value
Coordination and Exploration Model	
Inertia weight (w)	[0.9 ... 0.4]
Cognitive parameter (C_1)	1.4962
Social parameter (C_2)	1.4962
Infrastructure	
Radio	802.11g
Mode	11 Mbps

V. Results and Discussion

This section presents a comparative performance analysis of the proposed SDN-based topology management architecture against the benchmark AODV protocol. The evaluation is based on key performance indicators (KPIs) crucial for disaster recovery scenarios: control plane overhead, packet delivery ratio (PDR), packet drop rate, and end-to-end latency. The results are analyzed across three scenarios with increasing network density (15, 30, and 45 User Nodes).

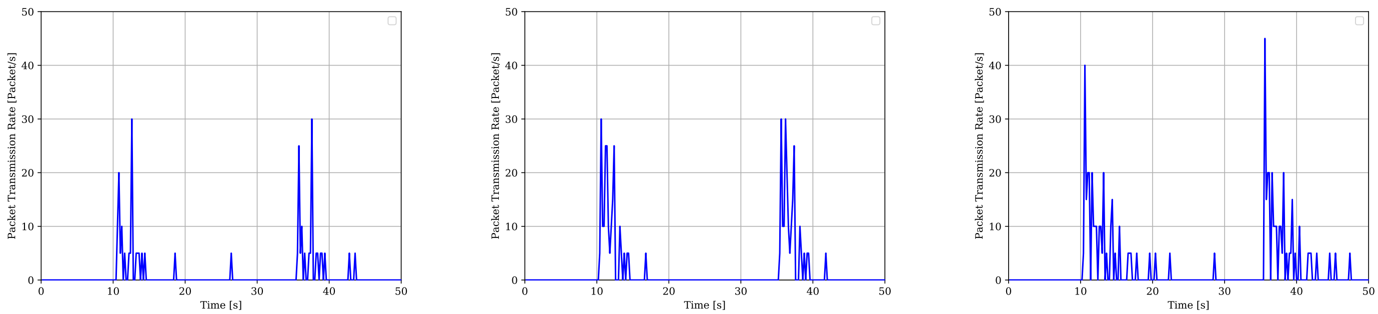
A. Control Plane Overhead and Infrastructure Usage

A fundamental difference between the two approaches lies in their management of control plane traffic. AODV relies on a proactive link maintenance mechanism, where nodes periodically exchange `AODV_HELLO_PACKET` messages to validate established routes [39]. Figure 3 illustrates the transmission rate of these packets. The results show that this control overhead scales linearly with the number of active links, reaching a constant rate of approximately 45 packets/s in the 45-user scenario. While essential for the distributed nature of AODV, this continuous exchange of maintenance packets creates significant background channel contention, which can degrade the performance of data-intensive applications, as discussed in [15].

This overhead's impact on overall network traffic is further detailed in Figures 4 and 5, which depict the composition of network traffic over time for a 15-user scenario. In the AODV approach (Figure 4), the control packet traffic for route maintenance constitutes a persistent and significant portion of the total traffic, competing directly with the application data flow. This leads to an unstable data transmission rate throughout the simulation.

Conversely, the SDN approach (Figure 5) exhibits a different traffic profile. A significant burst of control traffic is observed during the initial 10 seconds of the simulation. This corresponds to the network bootstrapping phase, where UNs register with the CSO, and the initial topology and flow rules are established. After this initial phase, the control traffic becomes minimal, occurring only when necessary to handle topological changes or new flow requests. This behavior allows the communication channel to become almost exclusively available for application data traffic, leading to a more stable and efficient use of network resources over the long term, a critical factor for mission success in post-disaster operations [1].

 DOI: https://doi.org/10.65218/jius.2026.12



(a) 15 connected users. **(b)** 30 connected users. **(c)** 45 connected users.

Fig. 3 Control plane overhead in AODV, showing the constant transmission rate of `AODV_HELLO_PACKET` messages for route maintenance across different network densities.

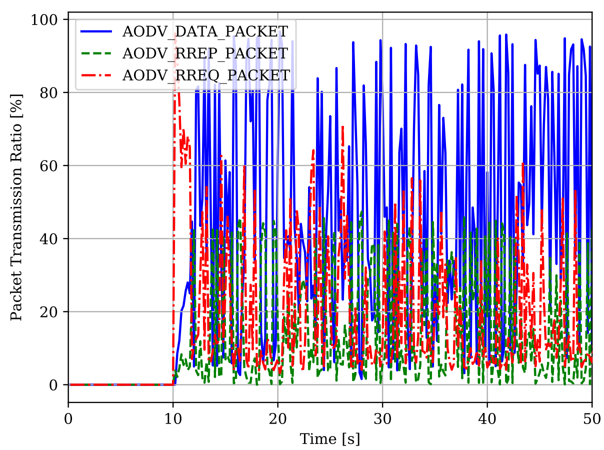


Fig. 4 Infrastructure usage over time with the AODV protocol, showing persistent control packet overhead competing with data traffic.

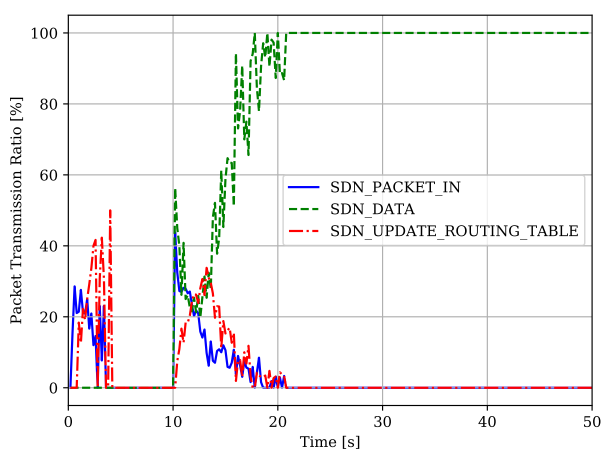


Fig. 5 Infrastructure usage over time with the SDN approach, showing an initial control traffic burst for setup, followed by stable data transmission.

B. *Packet Delivery Ratio and Drop Rate*

The efficiency of network resource utilization directly impacts the Packet Delivery Ratio (PDR) and packet drop rate. Figures 6 and 7 illustrate the PDR for the SDN and AODV approaches, respectively. For both approaches, the PDR is highest in the least dense scenario (15 users) and decreases as the network scales. However, a clear trend emerges: the PDR for the SDN approach consistently outperforms AODV and tends to improve over time as the network stabilizes. In contrast, the PDR for AODV remains relatively static or degrades slightly, burdened by the persistent control plane overhead.

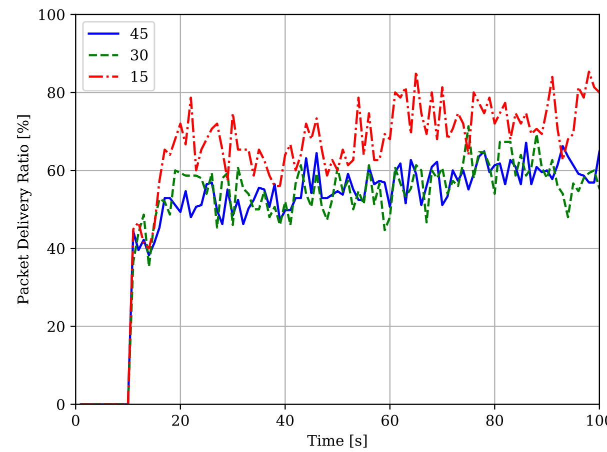


Fig. 6 Data packet delivery ratio over time for the SDN-based approach across three different user densities.

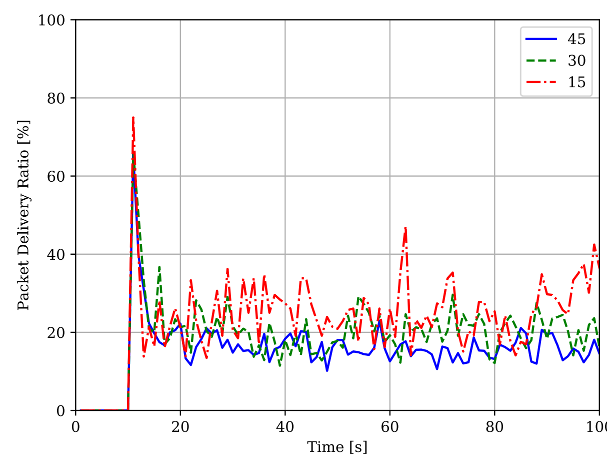


Fig. 7 Data packet delivery ratio over time for the AODV protocol across three different user densities.

This performance disparity is further explained by the packet drop rates shown in Figure 8. Packet drops are primarily caused by buffer overflows resulting from network congestion. For

DOI: https://doi.org/10.65218/jius.2026.12

the AODV protocol, packet drops begin to occur after approximately 20 seconds and increase with network density. This is a direct consequence of the high channel contention caused by the combination of data traffic and the continuous stream of `HELLO` packets, which leads to buffer saturation.

In the SDN approach, packet drops are minimal and are concentrated almost exclusively during the initial network setup phase (around the 10-second mark), particularly in the higher-density scenarios (30 and 45 users). This initial burst of drops corresponds to the period when UNs begin transmitting data while the initial flow rules are still being computed and disseminated by the CSO. Once the primary routes are established, the drop rate falls to near-zero, demonstrating the superior efficiency of centralized management in a steady-state network.

C. End-to-End Latency

End-to-end latency, measured as the average time for a data packet to travel from source to destination, is a critical metric for real-time applications. Figure 9 presents the average latency as a function of the number of hops for both approaches. The results clearly indicate that the SDN-based solution achieves consistently lower latency across all scenarios. The maximum observed latency reduction was approximately 10 ms in the 30-user scenario (Figure 9-(b)).

This latency improvement is directly correlated with the reduced channel contention in the SDN model. With fewer control packets competing for the wireless medium, data packets experience shorter queuing delays at each hop. In contrast, the higher infrastructure usage in the AODV network leads to longer buffering times as packets wait for transmission opportunities, thereby increasing the overall end-to-end latency. This establishes a clear relationship: the higher control overhead of AODV leads to increased channel contention, which in turn results in higher packet drop rates and increased end-to-end latency, particularly as network density and traffic load increase.

VI. Conclusion and Future Work

In this work, an SDN-based solution was proposed to autonomously manage an UAV topology for providing a network infrastructure to users in a post-disaster scenario. The evaluation of this proposal was performed through several simulation in OMNet++ by comparing it with an alternative and distributed protocol. Both SDN and AODV protocols are reactive, multi-hop and support nodes' mobility. Consequently, AODV was considered suitable for comparison.

The obtained results has demonstrated the efficiency of the proposed solution up to 17.5% packet delivery ratio in comparison to the AODV protocol. In addition, the end-to-end latency of data packets was up to 10ms lower in SDN approach than by using the AODV protocol. Finally, the lower network infrastructure usage obtained in the proposed solution over. Although SDN approach has presented a higher ratio of topology maintenance packets at the topology formation startup, the packet transmissions stabilizes over time. On its turn, the AODV management protocol increases those packets considerably.

Based on the obtained results and a detailed observation over the SDN and AODV features, the SDN approach has proven to manage a network structure more efficiently in post-disaster operations. The efficient use of the network resources is strongly linked to efficiency and success of the mission. The proposed SDN-based solution was proven to be more efficient in managing such a dynamic topology considering high data traffic rate. Future works will be focused in adding telemetry feature [40] in data traffic, hence the controller is able to perform a more complete flow analysis and a more efficient topology management, which enables the SDN dynamic reconfiguration capability. As a consequence, the controller is then able to perform load balancing and ensure Quality of Experience (*QoE*) and Quality of Service (*QoS*), while using the resources of the infrastructure consciously.

Acknowledgment

This study was financed in part by the Brazilian Federal Agency for Support and Evaluation of Graduate Education (CAPES) - Finance Code 001, in part by National Council for Scientific and Technological Development (CNPq) - Projects 309505/2020-8 and 311773/2023-0, and the National Institute of Science and Technology (INCT-Signals) grant no. 406517/2022-3, and by the ELLITT Strategic Research Network, Sweden.

References

[1] S. F. Ochoa and R. Santos, "Human-centric wireless sensor networks to improve information availability during urban search and rescue activities," *Information Fusion*, vol. 22, pp. 71 – 84, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1566253513000687

[2] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on uav cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2019.

[3] S. Sekander, H. Tabassum, and E. Hossain, "Multi-tier drone architecture for 5g/b5g cellular networks: Challenges, trends, and prospects," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 96–103, March 2018.

[4] F. Pasandideh, J. P. J. d. Costa, R. Kunst, W. Hardjawana, and E. P. de Freitas, "A systematic literature review of flying ad hoc networks: State-of-the-art, challenges, and perspectives," *Journal of Field Robotics*, vol. 40, no. 4, pp. 955–979, 2023.

[5] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, and M. Debbah, "A tutorial on uavs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2334–2360, thirdquarter 2019.

[6] I. Bor-Yaliniz and H. Yanikomeroglu, "The new frontier in ran heterogeneity: Multi-tier drone-cells," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 48–55, November 2016.

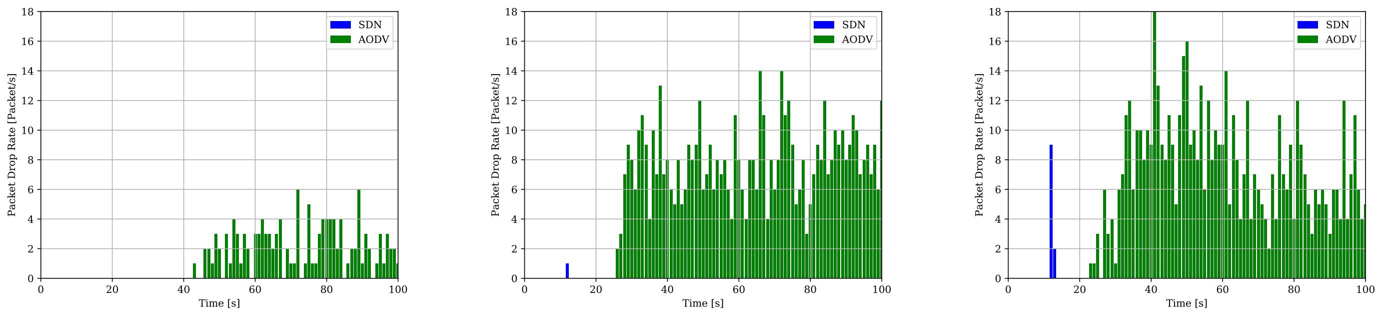
[7] M. Erdelj, E. Natalizio, K. R. Chowdhury, and I. F. Akyildiz, "Help from the sky: Leveraging uavs for disaster management," *IEEE Pervasive Computing*, vol. 16, no. 1, pp. 24–32, Jan 2017.

[8] G.-H. Kim, J.-C. Nam, I. Mahmud, and Y.-Z. Cho, "Multi-drone control and network self-recovery for flying ad hoc networks," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2016, pp. 148–150.

[9] R. S. Moraes and E. P. Freitas, "Distributed control for groups of unmanned aerial vehicles performing surveillance missions and providing relay communication network services," *Journal of Intelligent & Robotic Systems*, Nov 2017. [Online]. Available: https://doi.org/10.1007/s10846-017-0726-z

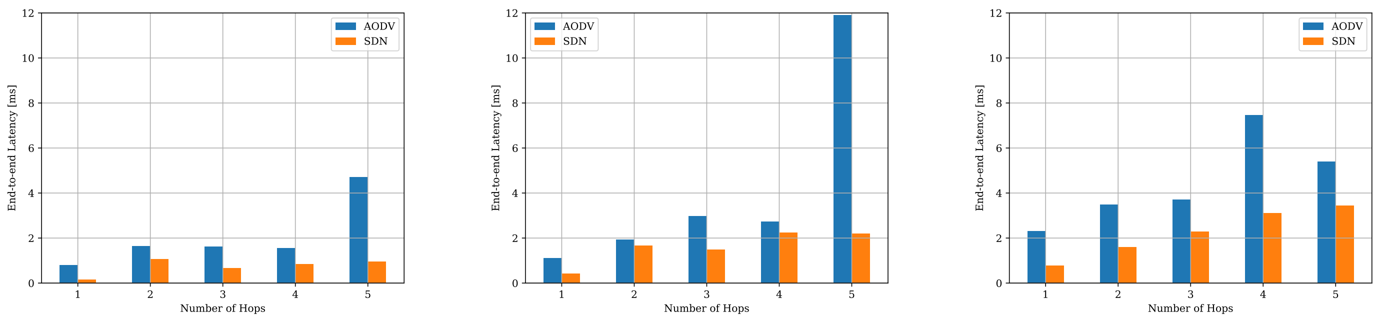
[10] D. Orfanus, E. P. de Freitas, and F. Eliassen, "Self-organization

DOI: https://doi.org/10.65218/jius.2026.12



(a) 15 connected users. **(b)** 30 connected users. **(c)** 45 connected users.

Fig. 8 Packet drop rate over time, comparing the SDN and AODV approaches. AODV exhibits continuous packet drops due to control overhead, while SDN drops are concentrated during the initial setup phase.



(a) 15 connected users. **(b)** 30 connected users. **(c)** 45 connected users.

Fig. 9 Average end-to-end data packet latency per number of hops. The SDN approach consistently demonstrates lower latency compared to AODV across all user densities.

as a supporting paradigm for military uav relay networks," *IEEE Communications Letters*, vol. 20, no. 4, pp. 804–807, April 2016.

[11] S. Rosati, K. Krużelecki, G. Heitz, D. Floreano, and B. Rimoldi, "Dynamic routing for flying ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1690–1700, March 2016.

[12] J. Wang, C. Jiang, Z. Han, Y. Ren, R. G. Maunder, and L. Hanzo, "Taking drones to the next level: Cooperative distributed unmanned-aerial-vehicular networks for small and mini drones," *IEEE Vehicular Technology Magazine*, vol. 12, no. 3, pp. 73–82, Sept 2017.

[13] T. Dapper e Silva, C. F. Emygdio de Melo, P. Cumino, D. Rosário, E. Cerqueira, and E. Pignaton de Freitas, "Stfanet: Sdn-based topology management for flying ad hoc network," *IEEE Access*, vol. 7, pp. 173 499–173 514, 2019.

[14] R. Kirichek, A. Vladyko, A. Paramonov, and A. Koucheryavy, "Software-defined architecture for flying ubiquitous sensor networking," in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Feb 2017, pp. 158–162.

[15] S. Misra, I. Woungang, and S. C. Misra, *Guide to wireless ad hoc networks*. Springer Science & Business Media, 2009.

[16] D. Kim and J. Lee, "Integrated topology management in flying ad hoc networks: Topology construction and adjustment," *IEEE Access*, vol. 6, pp. 61 196–61 211, 2018.

[17] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008. [Online]. Available: http://doi.acm.org/10.1145/1355734.1355746

[18] P. Bupe, R. Haddad, and F. Rios-Gutierrez, "Relief and emergency communication network based on an autonomous decentralized uav clustering network," in *SoutheastCon 2015*. IEEE, 2015, pp. 1–8.

[19] V. Sharma, F. Song, I. You, and H. Chao, "Efficient management and fast handovers in software defined wireless networks using uavs," *IEEE Network*, vol. 31, no. 6, pp. 78–85, November 2017.

[20] D. Kreutz, F. M. V. Ramos, P. Veríssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *CoRR*, vol. abs/1406.0440, 2014. [Online]. Available: http://arxiv.org/abs/1406.0440

[21] D. S. Lakew, U. Sa'ad, N.-N. Dao, W. Na, and S. Cho, "Routing in flying ad hoc networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1071–1120, 2020.

[22] I. T. Haque and N. Abu-Ghazaleh, "Wireless software defined networking: A survey and taxonomy," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2713–2737, 2016.

[23] V. Gupta and D. Seth, "Unmanned aerial vehicles (uavs): Evaluation of olsr, dsdv, aodv, and dsr dynamic routing protocols," in *2023 International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*. IEEE, 2023, pp. 1–6.

[24] S. B. M. Ahmed, S. A. Hussain, L. A. Latiff, N. Ahmad, and S. M. Sam, "Performance evaluation of fanet routing protocols in disaster scenarios," in *2021 IEEE Symposium On Future Telecommunication Technologies (SOFTT)*. IEEE, 2021, pp. 46–51.

[25] S. Sharma, A. Nag, P. Stynes, and M. Nekovee, "Automatic configuration of openflow in wireless mobile ad hoc networks," in *2019 International Conference on High Performance Computing Simulation (HPCS)*. IEEE, 2019, pp. 485–492.

DOI: https://doi.org/10.65218/jius.2026.12

[26] T. D. e. Silva, C. F. E. de Melo, P. Cumino, D. Ros 'ario, E. Cerqueira, and E. P. de Freitas, "Stfanet: Sdn-based topology management for flying ad hoc network," *IEEE Access*, vol. 7, pp. 173 499–173 514, 2019.

[27] A. T. Albu-Salih and H. A. Khudhair, "Asr-fanet: An adaptive sdn-based routing framework for fanet," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 5, pp. 4403–4412, 2021.

[28] D. Uomo, A. Sgambelluri, L. Ismail, and F. Paolucci, "P4 programmability for fault-tolerant software defined flying ad-hoc network," *Computer Networks*, vol. 270, p. 111572, 2025.

[29] M. G. Spina, M. Tropea, and F. De Rango, "Sura-lb: Software-defined ids with uav resource aware load-balancing in fanet disaster scenarios," *Computer Communications*, vol. 223, pp. 101–114, 2024.

[30] K. Sun *et al.*, "Adaptive extended kalman prediction-based sdn-fanet routing scheme," *Sensors*, vol. 25, no. 5, p. 1417, 2025.

[31] C. Liu, Y. Ding, and J. Li, "Parouting: Prediction-supported adaptive routing protocol for fanets with deep reinforcement learning," *International Journal of Intelligent Networks*, vol. 4, pp. 83–96, 2023.

[32] X. Qiu, Y. Yang, L. Xu, J. Yin, and Z. Liao, "Maintaining links in the highly dynamic fanet using deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 3, pp. 2804–2818, 2023.

[33] T. Lamenza *et al.*, "Gradys-sim–a omnet++/inet simulation framework for internet of flying things," *arXiv preprint arXiv:2202.08134*, 2022.

[34] S. Manzoor *et al.*, "Which simulator to choose for next generation wireless network simulations? ns-3 or omnet++," *Network*, vol. 46, no. 1, p. 36, 2023.

[35] M. Tropea, C. E. Q. Aldana, E. P. de Freitas, and F. De Rango, "Sfem3: A performance comparative analysis for sdn-based fanet emulation using mininet-wifi and ns-3," *Ad Hoc Networks*, vol. 177, p. 103859, 2025.

[36] J. Jiang, H. Huang, J. Liao, and S. Chen, "Extending dijkstra's shortest path algorithm for software defined networking," in *The 16th Asia-Pacific Network Operations and Management Symposium*, Sep. 2014, pp. 1–4.

[37] D. Rosário, Z. Zhao, C. Silva, E. Cerqueira, and T. Braun, "An omnet++ framework to evaluate video transmission in mobile wireless multimedia sensor networks," in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, ser. SimuTools '13. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 277–284. [Online]. Available: http://dl.acm.org/citation.cfm?id=2512734.2512774

[38] E. M. Belding-Royer and C. E. Perkins, "Evolution and future directions of the ad hoc on-demand distance-vector routing protocol," *Ad Hoc Networks*, vol. 1, no. 1, pp. 125 – 150, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870503000167

[39] C. E. Perkins, E. M. Belding-Royer, and S. R. Das, "Ad hoc on-demand distance vector (aodv) routing," Internet Request for Comments, RFC Editor, RFC 3561, Jul. 2003. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3561

[40] N. Van Tu, J. Hyun, and J. W. Hong, "Towards onos-based sdn monitoring using in-band network telemetry," in *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Sep. 2017, pp. 76–81.