engineering proceedings

MDPI

Proceeding Paper

Communication Failures in UAV-Based Wildfire Monitoring: Causes, Cascading Effects, and Resilience Strategies †

Filip Tsvetanov [1,*] and Ivan Ivanov [2]

[1] Department of Communication and Computer Engineering and Technologies, South-West University, 2700 Blagoevgrad, Bulgaria
[2] Department of Information Technology, University of Telecommunications and Post, 1700 Sofia, Bulgaria; idivanov2016@gmail.com
* Correspondence: ftsvetanov@swu.bg
† Presented at the International Conference on Electronics, Engineering Physics and Earth Science (EEPES2026), Bandirma, Turkey, 24–27 June 2026.

Abstract

Unmanned aerial vehicles (UAVs) are increasingly used for wildfire and disaster monitoring, enabling rapid data collection in hazardous, inaccessible areas. Secure and reliable communication is a major challenge in wildfire monitoring, as heat, smoke, terrain obstacles, and electromagnetic interference can degrade or interrupt data transmission. This paper analyzes communication failures in drone-based wildfire-monitoring systems, examining their causes, evolution, and operational implications. A multi-layered analytical framework integrating physical, technical, network, and security aspects is proposed. The study highlights cascading failure processes and supports the design of more resilient UAV communication architectures for dynamic wildfire environments.

Keywords: UAV; drones; wildfire monitoring; communication failures; resilience; mesh networks

1. Introduction

Wildfires are among the most dynamic and difficult-to-manage crisis environments, in which the timely collection and transmission of information are critical to limiting damage and ensuring team safety.

Over the last decade, unmanned aerial vehicles (UAVs), commonly known as drones, have evolved from experimental platforms into important components of early warning and monitoring systems for forest and field fires. Their ability to access difficult and hazardous terrain, together with the integration of multispectral sensors, has made them a valuable tool for fire services and civil protection agencies. With global climate change and the increasing number of extreme fires, drones offer speed, flexibility, and a high level of situational awareness, which are essential for the early or most critical phases of incidents.

However, the overall effectiveness of these systems depends not only on the quality of the sensors used to build them, which is not the main factor in UAV systems, but also on the level of flight autonomy, the reliability of the communication architecture, and the use of various communication standards. Research on FANETs shows that the high mobility of nodes, frequent changes in network topology, limited energy resources, and the instability of multi-hop communication pose serious challenges to the sustainable transmission of data [1,2].

Check for updates

Academic Editors: Teodor Iliev, Ivaylo Stoyanov, Grigor Mihaylov and Selahattin Kosunalp

Published: 3 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

With the increasing number and intensity of wildfires worldwide, drones are emerging as a key technology for observation, assessment, and disaster management, allowing real-time data collection, access to difficult areas, and improved situational awareness. However, the effectiveness of UAV systems is strongly dependent on the reliability of communication links. In disasters, including fires, communication infrastructure is often damaged or destroyed, requiring the use of drones as temporary communication nodes [1]. Despite their indisputable operational advantages, albeit with some disadvantages, there is a fundamental mismatch between the drone's technological potential to "see" the danger and its ability to "transmit" what it sees to the ground operator or crisis headquarters. In fire monitoring, these problems become more severe due to smoke, turbulence, unpredictable terrain, long distances, and the need to transmit data nearly in real time. In the case of drones for fires, the problem is not simply "is there a connection?" but "does communication remain reliable in a highly dynamic, noisy, and infrastructure-limited environment?"

The reliability of the Command-and-Control Link (C2) is the Achilles' heel of these systems. Whereas in a controlled urban environment, connectivity can usually be taken for granted, in environments with limited communication resources, such as mountainous areas or near an active fire, the traditional telecommunications infrastructure is often compromised or completely absent. Research on networks such as FANETs and UAV networks shows that the critical challenges stem from high mobility, frequent topology changes, disruptions in device connectivity, packet loss, delays, energy limitations, and vulnerability to attacks [2]. Additionally, studies on wildfire monitoring indicate that in order to achieve effective monitoring, it is necessary to simultaneously maintain network connectivity, energy efficiency, and rapid response, which turns communication reliability into a central factor for the success of these aerial vehicles and their assistance in localization, detection, and early warning at an early stage of an incident or in dealing with other anomalies related to dynamic changes in processes, their monitoring, and the sending of notifications, ensuring the awareness of the teams and their subsequent response [3].

Failures in communication systems of firefighting drones should not be treated as isolated technical incidents but rather as a systemic risk that directly affects the quality of monitoring, coordination between nodes, and the reliability of decision-making devices. There is a lack of comprehensive analysis integrating the causes, types, and consequences of communication failures in wildfire response operations.

This paper focuses on filling this gap by providing a detailed analysis of communication failures in drones used for wildfire monitoring and proposing a multi-layer analytical framework that integrates physical, technical, network, and security-related causes of communication degradation. This framework can support operations by identifying failure types, causal factors, operational consequences, and technical strategies for risk mitigation and by systematizing current engineering approaches to enhance link resilience and improve the reliability of communication systems. The novelty of this work lies in the framework's ability to explain how failures can propagate across layers and lead to cascading communication degradation in UAV-based wildfire-monitoring systems.

To clarify the position of the proposed approach, Table 1 compares representative related studies with the framework developed in this paper. As shown in Table 1, most related studies address important aspects of UAV communication, FANET routing, topology control, or emergency communication support. However, fewer works explicitly connect physical-layer degradation, technical constraints, network instability, and security threats into a unified cross-layer model of cascading communication failures. The proposed framework addresses this gap by linking causes of failure to operational, informational, and systemic consequences in UAV-based wildfire monitoring.

https://doi.org/10.3390/engproc2026154032

Table 1. Comparative positioning of the proposed framework with respect to related studies.

Study	Main Research Focus	UAV/FANET Communication	Disaster/Wildfire Context	Cross-Layer Perspective	Cascading Failure Analysis	Positioning of the Proposed Framework
Khan et al. [2]	FANET routing schemes	Yes	Partial	Limited	No	It presents a comprehensive review of FANET routing approaches, and the current work focuses on communication outages in forest fire-monitoring scenarios and the propagation of communication failures in wildfire-monitoring scenarios.
Abbas et al. [3]	UAVs and FANETs in disaster management	Yes	Yes	Partial	No	It discusses UAV/FANET applications and challenges in disaster management, while the present work systematizes the causes, consequences, and cascading effects of communication failures.
Chandran and Vipin [4,5]	Multi-UAV networks for disaster monitoring	Yes	Yes	Partial	Limited	It focuses on network-level challenges and opportunities in multi-UAV disaster monitoring and introduces a structured physical–technical–network–security framework.
López-Villegas et al. [6]	UAV-assisted emergency communications	Yes	Yes	Partial	Limited	It reviews UAV-assisted emergency communication systems, while the present work analyzes degradation chains and failure propagation in wildfire environments.
Alam et al. [7]	Topology control in multi-UAV networks	Yes	Partial	Network-oriented	No	It focuses on topology control and connectivity maintenance, while the present work links topology instability with operational, informational, and systemic consequences.
Trinh et al. [8]	UAV networking algorithms and AI-based approaches	Yes	Partial	Partial	No	It reviews communication, control, and AI-based UAV networking approaches, while the present work focuses specifically on failure mechanisms, cascading effects, and resilience strategies.
Proposed framework	Communication failures in UAV-based wildfire monitoring	Yes	Yes	Yes	Yes	It integrates physical, technical, network, and security factors into a unified cross-layer framework for cascading failure analysis and resilience planning.

2. Communication Architectures of Systems for Unmanned Aerial Vehicles (UAVs)

UAV communication systems rely on well-defined architectural paradigms that can easily manage data exchange between aerial platforms and ground control infrastructure, helping ensure scalability, reliability, and resilience in the presence of disturbances. Selecting an appropriate communication topology and applying it effectively are critical factors in the design of UAV systems, especially in mission-critical applications such as wildfire monitoring and emergency response, where environmental dynamics and signal degradation can significantly affect overall system performance.

Communication architectures or, more precisely, topologies used by unmanned aerial vehicles (UAVs), such as drones, can be classified into several main groups. The most commonly used star topology is used not only in UAVs but also in computer networks; this topology is typically used in scenarios with a small number of devices and a limited range. The multi-hop relay topology (for long distances), the mesh topology (most used

in sensor networks), the self-organizing network, and hybrid approaches that combine elements of two or more architectures are also used. Each of these architectures has different capabilities for communication reliability, latency (which is very important in most drone cases), and scalability, depending on the network's complexity and the system's operational requirements. In practice, communication scenarios of these architectures occur in isolated areas; various methods are applied to integrate and combine them depending on the specific mission requirements (Figure 1). Each topology has its own advantages and limitations, which are influenced by terrain, environmental conditions, and the type of hardware used on the aerial platforms [4–6]. Recent studies highlight that UAV communication architectures are highly adaptive and should be dynamically selected based on mission requirements, environmental conditions, and network state [7,8]. In disaster response scenarios, multi-UAV communication architectures are designed to overcome non-line-of-sight (NLOS) conditions and to provide reliable connectivity through multi-hop and mesh paradigms [4].

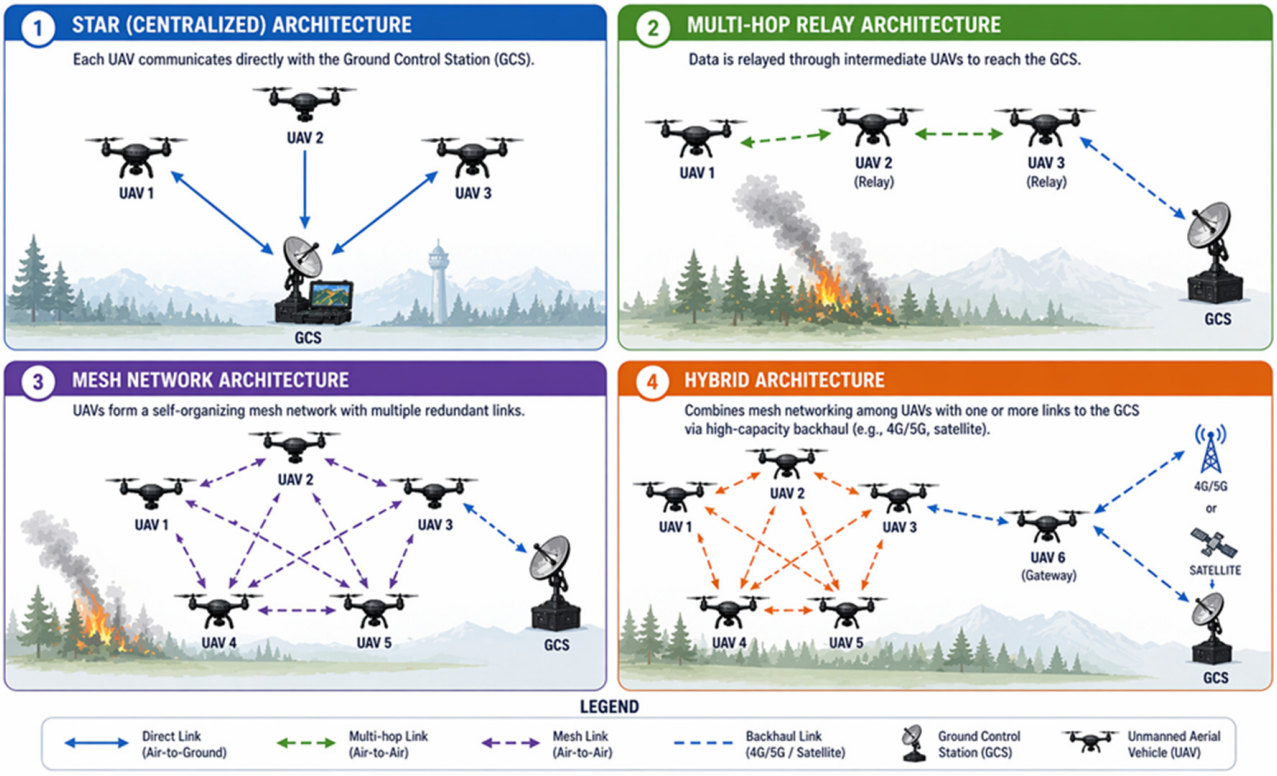


Figure 1. Basic communication architectures of drones for forest fire and emergency monitoring.

The choice of communication architecture (topology) is of primary importance for the network, as it affects its susceptibility to different types of interference and failures. In architectures or topologies based on the star topology, reliance on a single direct main link, for example, a single direct link between the UAV and the ground control station (GCS), creates a single critical point that is vulnerable to failure. Any degradation in signal quality caused by interference, terrain, forests, rock obstacles, smoke, or temperature can lead to immediate or complete loss of communication with the aerial platform. The next topology is the so-called multi-hop relay architecture, which mitigates this limitation by extending connectivity beyond direct line-of-sight conditions. However, they may introduce chains of dependencies. If a node in the network used as an intermediate communication point fails, the entire communication path to the remaining devices will likely be disrupted. Mesh network architectures further increase

resilience by allowing multiple redundant communication paths and enabling so-called self-healing capabilities. Finally, hybrid topologies (architectures), the most commonly used today, aim to balance the compromise between the different approaches. However, their complexity introduces additional considerations regarding failures, coordination, protocol overhead, and the use of heterogeneous communication nodes. The observations in this study indicate that communication failures in UAV systems cannot be attributed to a single factor or layer of system design, such as hardware, topology, or software. Instead, they arise from complex interactions among environmental conditions, system constraints, network dynamics (including the addition and removal of nodes), and, last but not least, security threats. Therefore, a holistic, structured approach is required not only for analysis but also for classification of these failures. To address this need for failures, the following section presents a systematic analysis using a multi-layer framework that captures the interdependencies among physical, technical, network, and security-related factors.

3. Systematic Analysis of Communication Failure Causes: Multi-Layered Framework

To provide a comprehensive analysis and understanding of the causes of communication problems, a problem-decomposition approach is applied. Communication failures in firefighting drones are rarely the result of a single factor; rather, they are the cumulative effect of limitations introduced during the design phase and extreme external influences in the operational environment. The analysis is conducted across four main dimensions, based on the OSI model and adapted to the physical conditions of wildfire environments, as illustrated in Figure 2.

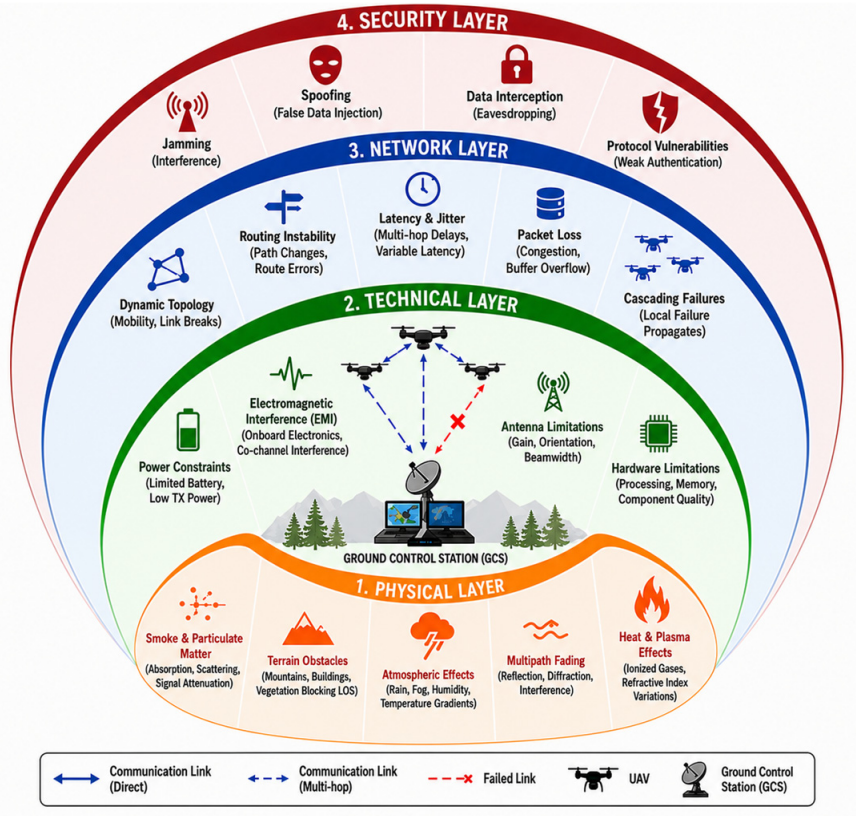


Figure 2. A multi-layered framework for the causes of communication failures in drone-based wildfire monitoring.

3.1. Fundamental Limitations at the Physical Layer

The physical layer represents the fundamental level at which communication takes place. As is well known, it is closely related to environmental conditions, especially in areas affected by wildfires. In such scenarios, there is a high density of smoke, the release of particulate matter from combustion, terrain obstacles, and rising high temperatures in the atmosphere, accompanied by atmospheric disturbances. Dense smoke, soot, and other particles in wildfires cause significant signal attenuation, especially at the higher frequencies commonly used for communication between a drone and base station (e.g., 2.4 GHz and 5.8 GHz), leading to only one result, degradation of the signal-to-noise ratio (SNR), when the thermal gradients from ionized gases generated by flames further affect the propagation of electromagnetic waves through absorption, and scattering processes lower the signal strength. Another important factor to always consider is the terrain itself and the fact that key terrain-related factors affecting UAV communication are the need for line-of-sight (LOS) conditions, the impact of terrain characteristics, reflection, diffraction, and scattering effects, as well as the frequency range and flight altitude, which create non-line-of-sight conditions and shadowing, which degrade signal propagation and weaken overall communication. These effects significantly reduce the reliability of the communication link and may result in poor radio connectivity or complete loss of communication between devices in the network [4]. It is important to note that many of these problems arise even before the drone takes off, but their actual impact becomes evident when the system operates under load.

3.2. Technical-Layer Factors

The technical layer includes limitations related to the hardware of unmanned aerial vehicles, including communication systems that use different standards, varying power constraints, electromagnetic interference (EMI) and potential shielding, thermal effects on components, and limitations in processing the generated data. The type of battery and its capacity are crucial to any drone's performance, not only for transmission power and the communication range but also for installed electronics, which can be damaged or affected by EMI, degrading signal quality or even causing failure. Elevated temperatures in a fire environment can negatively affect the performance of communication modules. Hardware limitations in processing and memory can further affect the efficiency of data encoding, compression, and transmission, and these limitations directly contribute to increased error rates in transmitted packets and, consequently, those received by both sides of a communication [7,8].

3.3. Network-Layer Factors

At the network layer, communication failures are primarily triggered by the dynamics of topology shifts, routing inefficiencies, and the compounding effects of latency and packet loss. These communication problems become significantly more severe in multi-UAV configurations that rely more often on mesh- or relay-based architectures, because the native mobility of individual nodes is always subject to environmental interference, necessitating frequent topology reconfigurations to switch between types and directly compromising the stability of data exchange pathways. When using multi-hop, the delay at each intermediate node is compounded by the fact that this delay accumulates at the next neighboring node, resulting in excessive end-to-end latency and jeopardizing the real-time processing of mission-critical data, including live video, sensor data, and other valuable streams that support mission success. Moreover, buffer saturation, electromagnetic noise, or link volatility can often cause data packet depletion. This spread of a point of failure,

which starts with link volatility and packet loss, threatens the integrity of all nodes and can lead to the total failure of the network infrastructure [6,9].

3.4. Security-Layer Factors

The security layer also responds to vulnerabilities that are caused by deliberate interference as well as cyber-attacks, such as jamming, spoofing, and data interception. Jamming attacks cause significant interference, disrupting communication channels, and spoofing attacks compromise system integrity by introducing false data or impersonating legitimate nodes. Interception of data compromises the confidentiality and integrity of missions, especially over unsecured communication channels. Such threats may cause significant increases in both physical- and network-layer vulnerabilities in firefighting UAV systems, potentially affecting operational reliability [10].

3.5. Cross-Layer Interactions and Failure Cascades

One of the most important conclusions from the proposed framework is that communication failures rarely remain confined to a single layer; they propagate across layers, creating cascades of failures. For example, various types of degradations at the physical layer (e.g., SNR reduction due to smoke) can cause retransmissions at the network layer, increasing latency and packet loss, triggering fault tolerance systems such as Return-to-Home (RTH) and aborting the mission. Similarly, network instability can highlight areas of vulnerability that security threats can exploit. Such interactions, as in this example, underscore the need to view the system as a whole and to develop holistic solutions that reduce the risk of failure at every stage, considering the multitude of layers that extend beyond communication.

The multi-layer framework provides a rational basis for researching communication failures of unmanned air systems in complex fire settings. By determining the interdependencies among layers, one can make more accurate predictions about the system's behavior under stress and implement more resilient communication architectures. Also, the framework facilitates the understanding of operational implications, including slow response times.

3.6. Formalization of Failure Propagation

To better capture the dynamics of communication degradation in UAV systems, the failure process can be expressed through a simplified cross-layer causal chain:

$$SNR \downarrow \Rightarrow \ BER \uparrow \Rightarrow \ Packet\ Loss \uparrow \Rightarrow \ Retransmissions \uparrow \Rightarrow \ Latency \uparrow \Rightarrow \ Throughput \ \downarrow \quad (1)$$

where SNR—signal-to-noise ratio; BER—bit error rate.

This degradation chain is especially important in a fire environment, where physical-layer perturbations (e.g., smoke and thermal effects) directly impact higher-layer behavior. Latency in multi-hop UAV networks: In multi-hop UAV networks, the latency can be estimated as follows:

$$T_{total} = \sum_{i=1}^{n} (T_{tx,i} + T_{queue,i} + T_{proc,i}) \quad (2)$$

where n—number of hops; T_{tx}—transmission delay; T_{queue}—queuing delay; T_{proc}—processing delay.

This correlation reveals that multi-hop architectures improve connectivity but can also introduce cumulative delays that impact real-time decision-making [7,8]. A summary of communication metrics, such as SNR, BER, packet loss, latency, throughput, link availability, and recovery time, is presented in Table 2.

Table 2. Communication metrics relevant to UAV-based wildfire monitoring.

Metric	Meaning in UAV Wildfire Monitoring	Relation to Failure Propagation	Operational Impact
SNR	Indicates the quality of the received signal under smoke, terrain obstruction, and interference conditions	Low SNR increases the probability of bit errors and unstable links	May trigger video degradation, retransmissions, or loss of control link
BER	Measures the probability of incorrectly received bits	High BER results from poor signal quality and increases packet corruption	Reduces the reliability of telemetry, sensor data, and command transmission
Packet loss	Represents missing or dropped packets during data transmission	May occur due to congestion, interference, or unstable routing	Leads to incomplete video, missing sensor data, and reduced situational awareness
Latency	Describes the end-to-end delay of data delivery	Accumulates in multi-hop and relay-based architectures	Delays fire-front assessment, decision-making, and operator response
Throughput	Represents the useful data rate available for transmission	Decreases under link degradation, retransmissions, and congestion	Limits real-time video, thermal imagery, and multispectral data transfer
Link availability	Indicates the percentage of time during which the communication link remains usable	Reduced by NLOS conditions, terrain, smoke, jamming, or node mobility	Determines whether the UAV can maintain continuous mission support
Recovery time	Time required to restore communication after a disruption	Depends on routing adaptation, fail-safe mechanisms, and network redundancy	Affects mission continuity and the ability to regain tactical awareness

These metrics are interdependent and provide a measurable basis for evaluating cascading communication failures in UAV-based wildfire-monitoring systems.

3.7. Comparative Analysis of Failure Factors Across Layers

Table 3 summarizes the main failure causes across the physical, technical, network, and security layers, together with their communication effects, mission impact, and typical mitigation approaches.

Table 3. Comparative analysis of failure factors across layers.

Layer	Key Causes	Effects on Communication	Impact on Mission	Typical Mitigation
Physical	Smoke, soot, obstacles, thermal gradients	SNR degradation, attenuation, multipath fading	Link instability, signal loss	Frequency selection, adaptive power control
Technical	Power constraints, EMI, thermal stress, hardware limits	Reduced transmission range, increased errors	Reduced reliability, intermittent links	Shielding, energy optimization, robust hardware
Network	Dynamic topology, routing instability, congestion	Packet loss, latency, jitter	Delayed response, loss of situational awareness	Mesh routing, redundancy, QoS mechanisms
Security	Jamming, spoofing, interception	Signal disruption, false data injection	Incorrect decisions, system compromise	Encryption, authentication, anti-jamming techniques

3.8. Integrated Cross-Layer Perspective

Recent research highlights that cross-layer design should be used to address communication problems in UAVs, in which information from multiple layers is used collectively to make adaptive decisions [4]. For example:

- Adaptive modulation and coding schemes can be activated by physical-layer degradation (low SNR);

- Dynamic routing can help to reduce network-layer congestion;
- Anomaly-based monitoring can be used to detect security threats.

This combined vision is especially essential in firefighting, where the environment rapidly changes and demands real-time system modifications.

4. The Implications of Failed Communication

A technical failure in fire-detection drones is rarely isolated. Signal loss or degradation can trigger a ripple effect across the interdependencies among control, navigation, and communication systems. This affects the overall performance of the firefighting operation. These consequences are classified in this section into three main types, namely, operational consequences, informational consequences, and systemic consequences (see Figure 3).

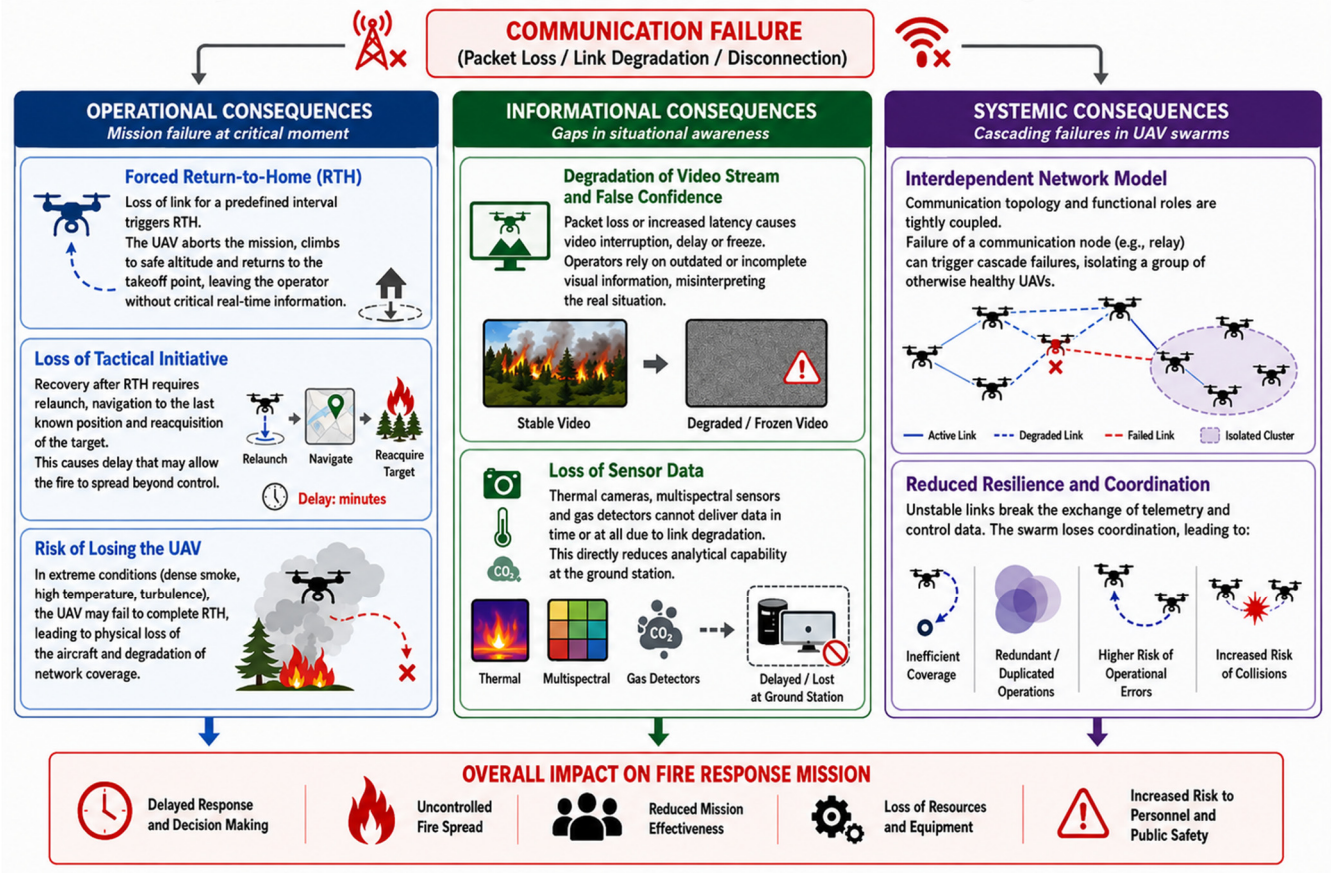


Figure 3. Communication problems in drone fire-monitoring missions.

4.1. Operational Consequences—Mission Failure at Critical Junctures

The most immediate repercussion of a communication breakdown is the triggering of automated safety protocols. While these are essential for safeguarding the aircraft, they often result in the abrupt termination of the operational task.

- *Mandatory Return-to-Home (RTH—Return-to-Home).* The onboard flight controller triggers RTH functionality when a connection to the ground station is lost, usually after a predetermined time interval (a few seconds). When activated, the drone abandons its mission, enters a fail-safe flight mode, and flies back to its starting point. In a situation of firefighting operations, this implies that the UAV may leave a high-value-information area at a critical point in surveillance, leaving the operator without critical situational awareness. Figure 4 shows the cause-and-effect chain by which

signal degradation (SNR reduction) in a challenging environment triggers a reaction, including Return-to-Home (RTH) activation or video stream degradation.

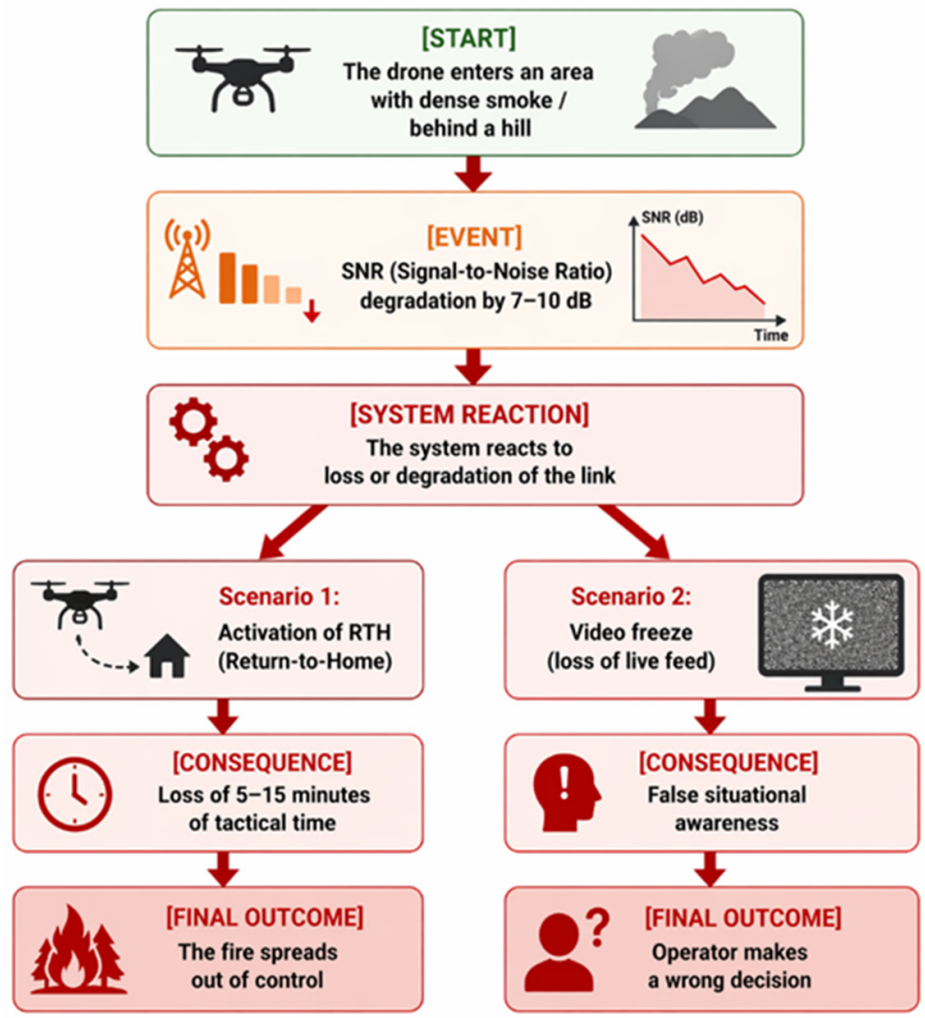


Figure 4. Cascade model of communication failure in UAV fire-monitoring operations.

- The cascade model in Figure 4 shows and explains the sequential propagation of communication failures in UAV-based fire-monitoring systems. It also explains and highlights how a low-level communication issue escalates into a high-impact issue with operational consequences. This process begins to occur when the UAV enters an extremely difficult environment characterized by dense smoke or terrain obstructions, leading to degradation of the signal-to-noise ratio (SNR). This interferes with the physical layer and directly affects the quality of the communication, which triggers system-level responses designed to preserve the platform, like fail-safe mechanisms or adaptive communication strategies. Two main scenarios of system operation have been identified. In the first scenario, the system activates a Return-to-Home (RTH) procedure, resulting in mission interruption and loss of critical observation time. In the second scenario, the operator cannot assess the exact situation due to deteriorating communication, which, in turn, disrupts the video stream, leading to freezing, delays, or worse. Ultimately, communication failure leads to high-level operational consequences in both scenarios. The loss of real-time situational awareness may lead to delayed or incorrect decision-making. Mission interruptions may allow the fire to spread beyond the control of the fire teams, making it unstoppable, unpredictable, and hard to monitor and making it difficult to gather

information on its spread. This model demonstrates how failures in communication in UAV systems are serious and should not be treated as isolated technical issues but rather as a likely cascading process that propagates across system layers and directly affects mission effectiveness.

- *Loss of Tactical Initiative.* The process of mission recovery following an RTH activation entails a series of time-consuming steps: re-launching the aircraft, transiting back to the last known coordinates, and re-establishing either visual or sensory contact with the target area. This introduces a significant tactical lag, the impact of which depends on the operational environment. In the specific case of rapidly evolving wildfires, such a delay can be catastrophic, allowing the fire front to propagate unimpeded beyond the window of effective containment.
- *Risk of Asset Attrition*. Operation under extreme conditions is a hard task for anyone. Specifically, when navigating through dense smoke plumes, intense thermal radiation, and turbulent updrafts, there is a small, even tiny, probability that the UAV may fail to execute its recovery sequence effectively. Even outside these scenarios, a brief loss of communication can also escalate into a loss of physical network contact with the aircraft or drone. Events of this type not only result in hardware loss. Several instances of degradation of overall network coverage put the reliability of the remaining communication infrastructure at risk.

4.2. Informational Repercussions and Eroded Situational Awareness

Even in cases of partial link degradation where a total connection loss has not yet occurred, the integrity and consistency of the incoming data stream are significantly compromised. This leads to the following critical issues:

- *Video stream deterioration and false confidence*. Packet loss and jitter often result in video feeds that are intermittent, delayed, or "frozen." Such distortions introduce a dangerous risk of misinterpretation; the operator may inadvertently base tactical decisions on outdated or fragmented visual cues while the fire's actual dynamics continue to shift rapidly.
- *Sensor data loss*. Modern fire-surveillance UAVs are equipped with sophisticated arrays, including thermal imaging, multispectral sensors, and gas detectors. When there is degradation of the communication channel, telemetry fails to reach ground-based analytical systems or arrives with an unacceptable delay, resulting in latency. [11]. This is particularly detrimental, as drones frequently serve as aerial communication gateways, bridging the gap between the physical and network layers. Any disruption to this bridging function results in a direct collapse of the team's overall analytical capacity.

4.3. Systemic Consequences and Cascading Failures in Drone Swarms

When deploying multiple UAVs to cover expansive areas, communication issues can have a multiplicative effect due to the inherent interdependencies between individual units [6].

- *Interdependent network model*. Modern research has introduced the framework of interdependent information–communication networks, in which the communication topology and the functional roles of drones are highly connected [12]. A failure within the communication layer of a single drone does not simply remove it from the network; it can trigger a communication failure between devices, which can cascade throughout the entire network. In such a scenario, the loss of a pivotal relay node results in the stochastic isolation of an entire subgroup of drones, regardless of their individual physical integrity [13].

- *Degraded swarm resilience and coordination*. Under unstable link conditions, the swarm loses its capacity for emergent coordinated behavior. The algorithms that handle task distribution, such as collision avoidance and synchronization, are fundamentally dependent on these continuous occurrences in some situations and on high-level telemetry accuracy. Any disruption to this data flow degrades the swarm's collective intelligence. Therefore, this breakdown results in inefficient spatial coverage, operational redundancy, and a high risk of catastrophic errors, one of which is mid-air collision.

5. Modern Risk Mitigation Approaches and Resilience Assurance

In response to the identified causes and their severe repercussions, the research and engineering communities have pioneered multi-layered strategies designed to bolster communication resilience. These methodologies are categorized based on their application level, ranging from physical-layer enhancements to comprehensive system-level architectures (see Figure 5).

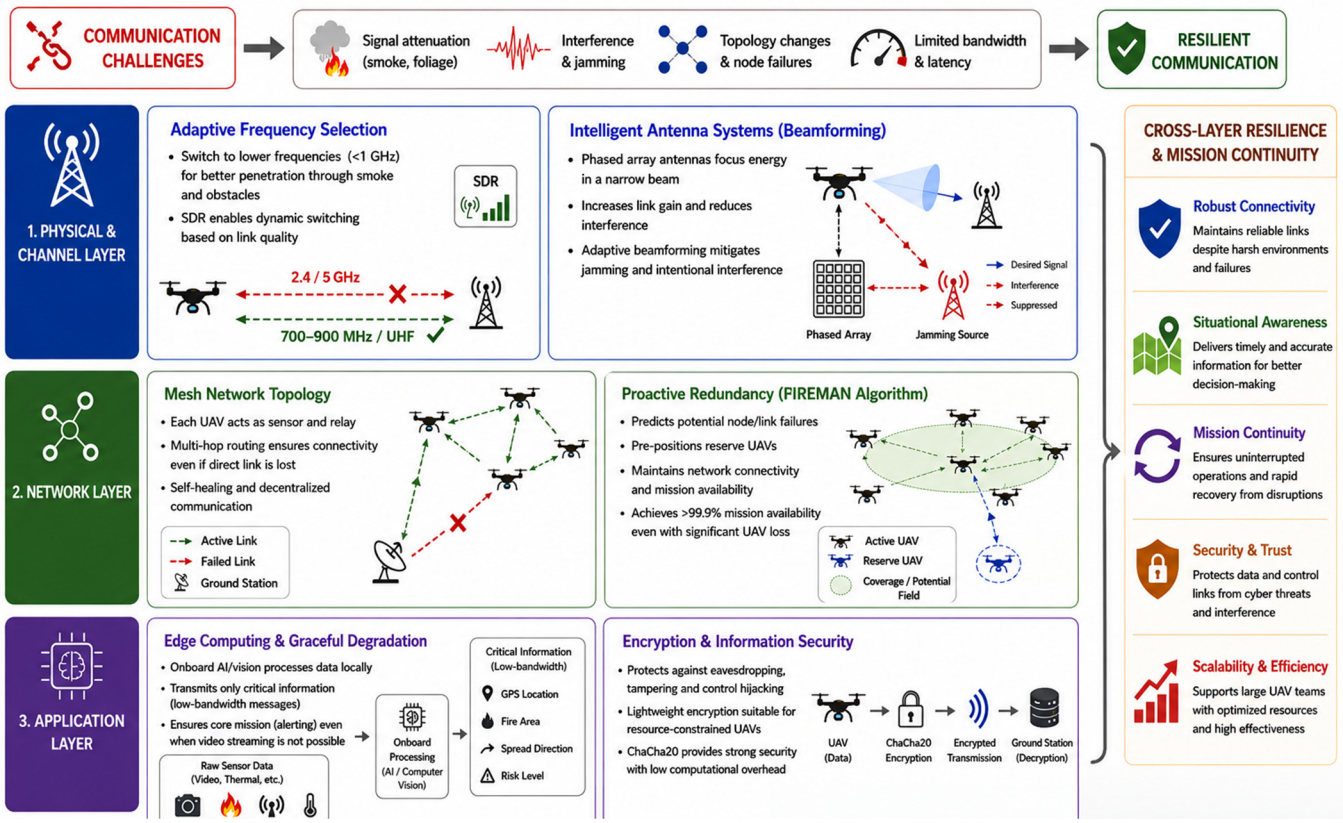


Figure 5. Modern approaches to risk mitigation and communication resilience in drone systems.

5.1. Physical- and Data-Link-Layer Methodologies

- Adaptive Frequency Selection. Transitioning to lower-frequency bands remains one of the most potent strategies for mitigating signal attenuation caused by smoke and flames. When aircraft use the standard 2.4 GHz and 5 GHz bands, they are highly susceptible to atmospheric absorption and scattering due to the characteristics of these bands. The use of frequencies below 1 GHz (e.g., 700–900 MHz or specialized UHF channels) provides better, and even excellent, penetration through obstacles and ionized environments at lower frequencies. Modern Software-Defined Radio (SDR) modules enable UAVs to dynamically hop between frequency bands based on real-time link quality metrics.

https://doi.org/10.3390/engproc2026154032

- Intelligent Antenna Systems (Beamforming). This technique, which uses smart antennas and spatial filtering, significantly increases signal gain while reducing the impact of external interference. Instead of relying on commonly used omnidirectional radiation patterns, UAVs can be equipped with additional antennas, such as phased antenna arrays that concentrate signal energy into a narrow beam directed toward the ground station or a neighboring node in the swarm. Research in communication security indicates that adaptive beamforming techniques can effectively neutralize even intentional jamming attempts.

5.2. Network-Layer Approaches for Resilient Architectures

- Self-organizing mesh networks (Mesh Networks). The most promising strategy for ensuring robustness in high-risk environments is to implement self-organizing mesh topologies. In this architectural paradigm, every UAV serves as both an active sensor and a relay node, providing additional alternative network paths. Should the direct link between "Drone A" and the base station be severed, the system autonomously reroutes data packets through "Drone B" and "Drone C" to maintain connectivity, keeping all devices communicating at all times and leading to high performance. As researchers emphasize, this decentralized communication framework is indispensable when traditional, centralized infrastructure is compromised.
- Proactive redundancy and spatial coordination (Proactive Redundancy). To mitigate the threat of cascading failures, advanced algorithms for proactive redundancy are being developed. The Adaptive algorithms developed provide information about the positions of devices (nodes) in the network, not only to support but also to enhance coordination between them. The aims of these protocols are to help maintain the swarm's structural robustness, mitigate connectivity gaps, and ensure seamless network cohesion under adverse conditions. For example, the FIREMAN algorithm (Physics-Informed Robust Employment of Multi-Agent Networks) utilizes physics-inspired potential fields to generate a network geometry that preserves structural integrity even after the loss of a significant number of constituent drones [14].

5.3. Application-Layer Approaches for Intelligence and Security

- Edge Computing and Graceful Degradation. To circumvent the reliance on bandwidth-intensive raw video transmission—which is inherently vulnerable to link instability—UAVs can be outfitted with onboard processing units for localized data analysis. When using machine vision algorithms, the drone can detect, identify, and classify potential internal fire hotspots and transmit only high-priority metadata, such as GPS coordinates, burn area dimensions, and likely spread vectors (e.g., wind direction). This "edge computing" strategy significantly minimizes network traffic and enables the system to maintain operational functionality even under severely restricted connectivity [15].
- Encryption and Information Security. Unsecured control channels are susceptible to cyber-attacks that can compromise data integrity or even facilitate unauthorized hijacking of the platform. Therefore, current research focuses on integrating robust security frameworks into UAVs using lightweight cryptographic algorithms designed and suitable for resource-constrained systems. One of the choices is a stream cipher solution, such as ChaCha20, which is highly valued for providing sufficient security with minimal computational overhead, making the proposed solution ideal for securing telemetry and command data in UAV networks. Figure 6 presents a conceptual comparison between a traditional star-based communication architecture and a resilient mesh topology within UAV-based fire-surveillance systems. The illustration high-

lights how communication reliability is significantly enhanced through distributed, multi-hop connectivity.

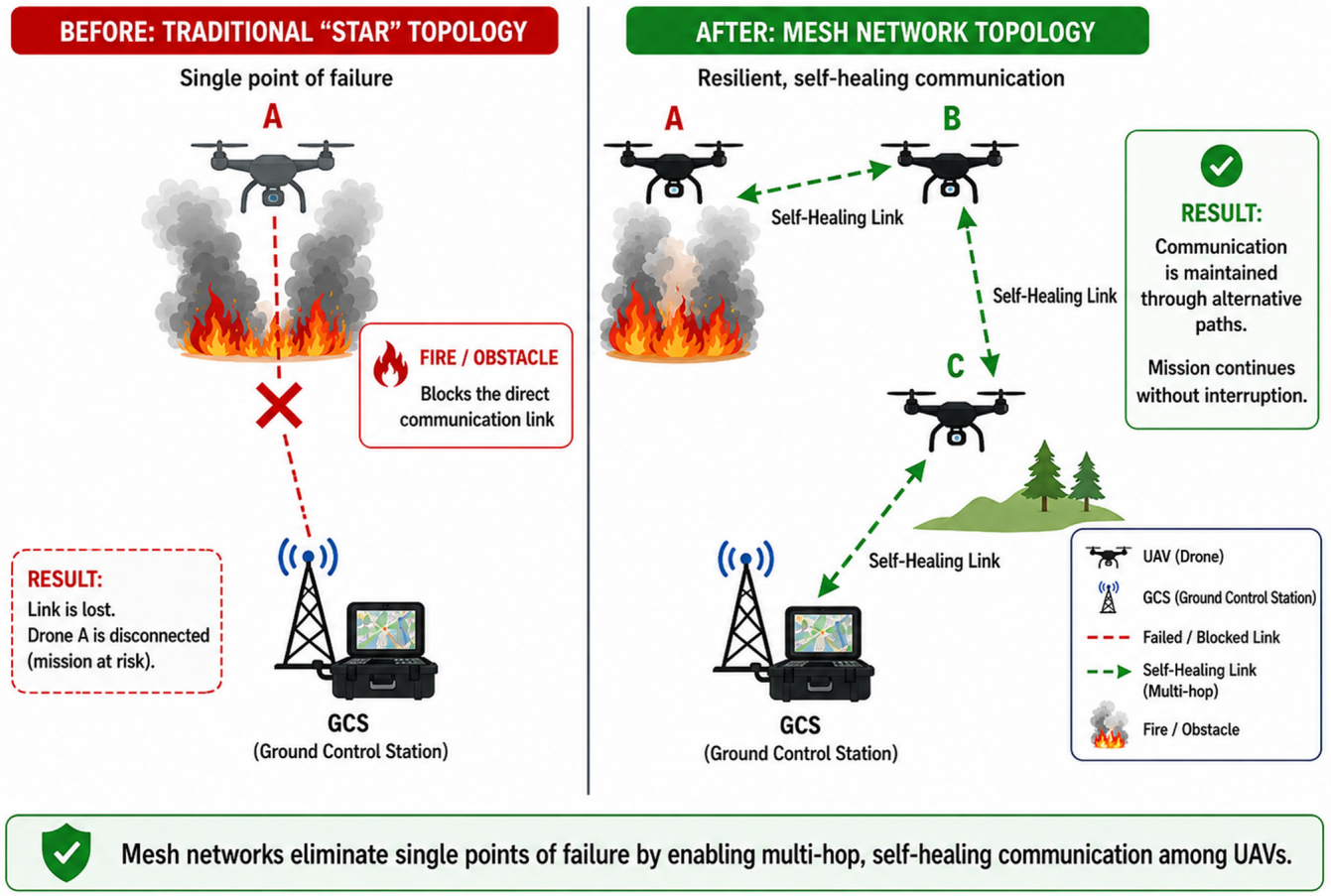


Figure 6. Conceptual comparison between star-based communication and a robust mesh-based architecture for fire surveillance.

6. Conclusions

Communication failures in UAV-based forest fire-monitoring systems are complex, multi-layered phenomena that isolated technological solutions cannot mitigate. The analysis conducted shows that such failures stem from closely related interactions between system-level design constraints—such as EMI, energy limitations, and hardware inefficiencies—and extreme environmental conditions, including signal attenuation, out-of-line propagation (NLOS), and thermally induced interference. All these factors cause chain-stage, or so-called cascading, failure processes that spread across communication layers. As a result, this leads to serious deterioration of operational functions, ranging from mission termination to (network or data transfer) collapse, when multiple UAVs (swarm) are used. In this dynamic field of technology development, recent advances are shifting towards resilient, adaptive communication architectures. In particular, when decentralized network topologies are combined with proactive redundancy and edge-processing mechanisms, they significantly improve system reliability. For example, the system can enable multiple mechanisms for self-healing connectivity and reduce reliance on continuous high-speed connections. These approaches transform drones from passive data transmitters into autonomous, intelligent, context-conscious devices with the capability of maintaining functional performance under degraded communication conditions.

However, critical research gaps remain—the lack of standardized, interoperable communication protocols for emergency and hazardous situations involving the use of unmanned aerial vehicles (UAVs) continues to hinder their large-scale deployment. In addition, most proposed solutions are primarily verified through simulation, necessitating comprehensive experimental validation in real-world conditions. Emerging paradigms, such as Integrated Surveillance and Communications (ISAC), offer promising opportunities for collaborative environmental perception and data transmission. At the same time, the development of lightweight post-quantum cryptographic schemes is essential for ensuring the long-term security of Command-and-Control (C2) connections.

In summary, addressing communication failures in unmanned aerial vehicle (UAV) forest fire scenarios requires a holistic design approach across different levels, integrating physical, network, and application strategies. Such integration is critical to the creation of next-generation UAV systems capable of maintaining reliable, secure, and sustainable operation in highly dynamic and hostile environments.

Author Contributions: Methodology, F.T.; conceptualization, F.T.; resources, F.T. and I.I.; writing, review, and editing, F.T. and I.I.; visualization, F.T.; contributed to the interpretation of the results, All. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are obtained in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mishra, L.J.; Kaabouch, N. Multi-Parameter Optimization Using Metaheuristic Algorithms to Improve Uncrewed Aerial Vehicles' Wireless Communications: A Performance Analysis. *IEEE Access* **2025**, *13*, 98374–98398. [CrossRef]
2. Khan, M.F.; Yau, K.-L.A.; Noor, R.M.; Imran, M.A. Routing Schemes in FANETs: A Survey. *Sensors* **2020**, *20*, 38. [CrossRef] [PubMed]
3. Abbas, S.; Abu Talib, M.; Ahmed, I.; Belal, O. Integration of UAVs and FANETs in Disaster Management: A Review on Applications, Challenges and Future Directions. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e70023. [CrossRef]
4. Chandran, I.; Vipin, K. Multi-UAV Networks for Disaster Monitoring: Challenges and Opportunities from a Network Perspective. *Drone Syst. Appl.* **2024**, *12*, 1–28. [CrossRef]
5. Tsvetanov, F.; Tsvetanov, K.A.; Ivanova, E.; Georgieva, I. Modelling and Simulation of Communication Efficiency in Low-Speed Networks. In Proceedings of the 22nd Telecommunications Forum (TELFOR 2014), Belgrade, Serbia, 25–27 November 2014; pp. 178–182.
6. López-Villegas, I.; Martínez-Ríos, E.A.; Izquierdo-Reyes, J.; Bustamante-Bello, R.; Falcone, F. A Systematic Literature Review of Emergency Communications Assisted by Unmanned Aerial Vehicles. *Ad. Hoc. Netw.* **2025**, *182*, 104063. [CrossRef]
7. Alam, M.M.; Arafat, M.Y.; Moh, S.; Shen, J. Topology Control Algorithms in Multi-Unmanned Aerial Vehicle Networks: An Extensive Survey. *J. Netw. Comput. Appl.* **2022**, *207*, 103495. [CrossRef]
8. Trinh, M.L.; Nguyen, D.T.; Dinh, L.Q.; Nguyen, M.D.; Setiadi, D.R.I.M.; Nguyen, M.T. Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-Based Approaches. *Algorithms* **2025**, *18*, 244. [CrossRef]
9. Tsvetanov, F.A.; Pandurski, M.N. Selection of Protocols for Integration of Sensory Data Networks in Cloud Structures. *Int. J. Online Biomed. Eng.* **2022**, *18*, 29–40. [CrossRef]
10. Visa, S.B.; Sunday, C.G.; Abdulkadir, A. A Novel Clustering-Based Scheme for Wildfire Monitoring in Flying Ad Hoc Networks. *J. Multidiscip. Sci.* **2025**, *3*, 111–124. [CrossRef]
11. Tsvetanov, F. Hardware Challenges in AI Sensors and Innovative Approaches to Overcome Them. *Eng. Proc.* **2025**, *104*, 19. [CrossRef]
12. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic Cascade of Failures in Interdependent Networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef] [PubMed]

13. Bekmezci, I.; Sahingoz, O.K.; Temel, S. Flying Ad-Hoc Networks (FANETs): A Survey. *Ad. Hoc. Netw.* **2013**, *11*, 1254–1270. [CrossRef]
14. Muslimov, T. Particle Swarm Optimization for Target Encirclement by a UAV Formation. *Eng. Proc.* **2023**, *33*, 15. [CrossRef]
15. Alam, M.; Moh, S. AI-Enabled Edge Computing for UAV-Based Remote Sensing. *Remote Sens.* **2023**, *15*, 1873. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.