

Smart Disaster Response Drone for Rapid Relief Operation

Gangule Krushna B¹, Prof. Abhishek Popat Bangar², Prof. S. B. Bhosale³, Dr. A. A. Khatri⁴

Dept. of Computer Engineering, Jaihind College of Engineering, Pune, India¹

Department of Computer Engineering, Jaihind College of Engineering, Kuran, Maharashtra, India^{2,3,4}

Abstract- Disasters such as floods, earthquakes, landslides and large-scale accidents can damage roads, power systems and communication infrastructure, delaying search, assessment and relief delivery. Unmanned aerial vehicles (UAVs) can provide rapid aerial observation, survivor-search support, delivery of lightweight emergency supplies and temporary communication coverage. This review synthesizes three supplied papers: a global review of UAVs for search and rescue, a YOLO-based radio-frequency (RF) spectrogram detector, and a lightweight authentication protocol for emergency UAVs. The search-and-rescue literature emphasizes sensor integration, multi-UAV coordination, communication recovery and the persistent constraints of battery endurance and payload. The RF detection study compares YOLOv8n and YOLOv9t, reporting mAP50–95 values around 0.80–0.85 and inference times of 1.6 ms and 3.0 ms, respectively, in its experimental setting. The authentication study addresses mutual authentication and session-key establishment among an operational drone, ground station and rescue drones, using formal protocol analysis. These contributions are relevant but do not individually demonstrate a complete end-to-end disaster-relief platform. This review proposes a conceptual architecture combining multisensor reconnaissance, edge-based AI, task allocation across multiple UAVs, secure communications and human-supervised relief decisions. Major gaps include limited field validation, uncertain performance under severe weather and radio interference, battery and payload trade-offs, and the need to test security and detection jointly in realistic missions.

Keywords— Disaster response, UAV, search and rescue, YOLO, RF spectrogram, lightweight authentication, multi-UAV coordination, emergency communication

I. INTRODUCTION

Disaster response depends on timely information about damaged infrastructure, blocked routes, survivor locations and urgent supply needs. Ground teams may be delayed by flooding, collapsed structures, fire, landslides or inaccessible terrain. Unmanned aerial vehicles (UAVs) can be deployed rapidly and observe areas that are unsafe or difficult for responders to reach. Quero and Martinez-Carranza review UAV roles in surveying affected areas, locating survivors, assessing hazards, delivering essential supplies and providing temporary communication networks [1]. These functions make drones a promising component of rapid relief operations, but sensing, decision support, communication, coordination and security must work together.

The three source papers address different technical layers. Paper [1] surveys UAV platforms, sensors, coordination and challenges in search-and-rescue (SAR). Slimeni, Delleji and Siala [2] evaluate YOLOv8n and YOLOv9t for identifying UAV-related RF spectrogram patterns. Jan et al. [3] propose a lightweight authentication and key-agreement protocol for emergency UAV participants. The RF detector in [2] concerns drone-related radio signals and should not be interpreted as a validated human-survivor detector. Similarly, the security protocol in [3] is a communication-security mechanism, not a full mission-management system.

This review connects these contributions under the theme of a smart disaster-response drone for rapid relief operations. It compares what each source demonstrates, identifies how the technologies could complement one another, and outlines research

needed before an integrated system can be considered field-ready.

II. REVIEW APPROACH AND SCOPE

This focused narrative review is based on the three supplied papers: the SAR review [1], the RF-spectrogram UAV-detection study [2], and the emergency-UAV authentication protocol [3]. The papers were examined for their objectives, technical approaches, reported findings and limitations. This is a thematic synthesis rather than a systematic review: no independent database search, meta-analysis or new experimental validation was conducted. Numerical results are attributed to the source studies and should be interpreted within their own experimental settings.

III. SMART DRONES IN DISASTER RELIEF

A smart disaster-response system can support several operational stages. During initial reconnaissance, cameras and thermal sensors can map damage, identify possible human presence and flag hazards. During search and rescue, aerial imagery and other sensor signals can help responders prioritize locations for ground inspection. For logistics, drones may carry lightweight first-aid items, medicines or communication devices where payload and safety limits permit. When terrestrial networks fail, UAVs equipped as relays or aerial base stations can help restore communication among survivors and response teams [1].

Sensor selection depends on the mission. Visible-light cameras document structural damage and terrain, while thermal imaging may help identify heat signatures under suitable conditions. Radar and other sensing modalities can offer complementary information when visibility is poor, although each adds cost, weight and processing demands. Aerial sensing should be treated as decision support: occlusion, smoke, rain, heat sources and debris can produce missed detections or false alarms. Responders should verify critical findings before dispatching teams or making life-safety decisions.

Single-UAV deployment may suit a localized incident, but large or evolving disasters can require several drones. A coordinated fleet can divide a search area, assign different sensors or payloads to different tasks, and provide redundancy if one aircraft must return for charging. This benefit depends on reliable task allocation, collision avoidance, shared situational awareness and a communication plan that remains useful when infrastructure is damaged. The SAR review [1] highlights multi-UAV collaboration while also identifying energy, payload, autonomy and communication as continuing challenges.

IV. AI-BASED UAV DETECTION AND SITUATIONAL AWARENESS

Slimeni et al. [2] describe an RF-based drone-detection framework using a USRP X310 software-defined radio to capture remote-control, Wi-Fi and Bluetooth signals. Captured signals are represented as spectrogram images and processed using YOLO object-detection architectures. Their comparison reports mAP50–95 values around 0.80–0.85 for both models. YOLOv8n achieved a reported inference time of 1.6 ms, compared with 3.0 ms for YOLOv9t, while YOLOv9t had a smaller parameter footprint. The authors also report better distribution-focal-loss performance for YOLOv8n in their test setting [2].

These results suggest a speed–model-size trade-off. Lower latency can be useful when a detection pipeline must react quickly, whereas a compact model may be attractive when memory or compute resources are limited. However, this was a controlled RF-detection study rather than an end-to-end disaster mission. The paper identifies testing with multiple simultaneous UAVs and complex electromagnetic environments as future work; urban multipath effects and adversarial jamming also require investigation [2]. Its reported performance cannot be assumed to hold unchanged around damaged infrastructure, emergency radios, dense Wi-Fi networks or severe interference.

For a relief drone, AI has at least two distinct roles. Onboard perception can analyze visual or thermal data to flag possible survivors, damaged buildings,

blocked roads and hazards. Separately, RF analysis can detect or classify radio-frequency activity associated with UAVs and other emitters. RF detection may help monitor airspace or radio conditions, but it does not by itself locate survivors. A practical system should evaluate each model against task-specific datasets and report precision, recall, false-alarm rates, latency and power consumption under representative field conditions.

V. SECURE COMMUNICATION AND AUTHENTICATION

Disaster operations depend on the authenticity and integrity of exchanged information. If an attacker impersonates a drone, replays old commands or interferes with mission messages, responders could receive false location reports or lose coordination. Jan et al. [3] present a lightweight authentication and key-agreement protocol for emergency UAV settings involving an operational drone, a ground station and rescue drones. The protocol aims to authenticate participating entities and establish a fresh shared session key. Its analysis includes formal reasoning using GNY logic and verification with ProVerif, together with comparisons of computational and communication overhead [3].

The source reports a total communication cost of 3744 bits for the proposed exchange in its stated protocol design and argues that it offers lower computational and communication complexity than several compared schemes [3]. These are protocol-level findings; they do not establish resilience to every real-world failure, including prolonged jamming, compromised hardware, loss of the ground station or poor connectivity. Formal verification is valuable, but field implementation must also test key storage, device capture, recovery after disconnection and the operational cost of re-authentication.

For rapid relief, security should be lightweight enough for battery-powered platforms and fast enough not to delay urgent coordination. Authentication should be combined with encrypted channels, access control, secure software updates, key revocation and a safe degraded mode for

temporary network loss. A drone should not accept a mission-critical command solely because it arrives quickly; its source and integrity must also be checked. Security procedures must also permit safe contingency operations when a central service is unavailable.

VI. COMPARATIVE ANALYSIS

The three papers are complementary but evaluate different system layers. The SAR review [1] provides broad operational context; the YOLO study [2] provides measured RF-detection results; and the authentication paper [3] analyzes a security protocol. Their outcomes are not directly comparable because they use different methods, evaluation measures and objectives.

VII. PROPOSED CONCEPTUAL ARCHITECTURE

Based on the reviewed sources, a smart relief architecture can be organized into six cooperating layers. (1) Mission planning: an incident commander defines priority zones, no-fly constraints, payload needs and search objectives. (2) Aerial sensing: UAVs capture visible, thermal, RF, location and environmental data according to the assigned mission. (3) Edge intelligence: onboard or nearby edge computers run perception and anomaly-detection models, attach confidence scores and flag uncertain cases for human review. (4) Secure networking: authenticated UAV-to-ground and UAV-to-UAV links carry telemetry, maps, task updates and alerts. (5) Fleet coordination: a mission manager allocates search sectors, schedules battery swaps, tracks aircraft health and reassigns work when a drone fails or loses connectivity. (6) Relief decision support: verified detections and damage maps are shown to rescue coordinators, who prioritize dispatch, supply delivery and further inspection.

An important design principle is graceful degradation. If cloud access fails, local detection and essential alerts should continue where safe; if one UAV loses power, the fleet should redistribute its

assigned region; if communication is unreliable, drones should follow pre-approved return, loiter or landing procedures. Security checks, flight-safety constraints and human oversight must remain part of the design rather than being added after AI development. This architecture is a synthesis proposed by this review, not a system experimentally demonstrated by the three source papers.

VIII. RESEARCH GAPS AND FUTURE DIRECTIONS

First, the gap between controlled evaluation and field performance is substantial. RF detection requires testing with diverse drone models, overlapping signals, non-drone emitters, multipath propagation and intentional interference. Visual survivor-detection systems require testing under smoke, darkness, rain, occlusion and varied terrain. Second, endurance remains a system-level constraint: extra sensors, compute hardware and communication payloads increase mass and power demand. Future studies should report flight time and energy use alongside AI accuracy.

Third, multi-UAV coordination needs real trials. Studies should measure search coverage, time to first detection, mission completion, collision avoidance, handoff success and performance when links or individual drones fail. Fourth, security evaluations should include realistic deployment conditions such as intermittent connectivity, device capture, replay attempts, compromised credentials and recovery after network partition. Fifth, datasets and evaluation procedures should be documented, with independent test locations and task-specific metrics to reduce the risk of overestimating performance. Finally, emergency agencies and communities should be involved in testing privacy, safe flight procedures, payload priorities and integration with existing command structures.

IX. CONCLUSION

Smart UAVs can strengthen rapid disaster relief by combining aerial reconnaissance, AI-supported analysis, coordinated fleet operations and secure

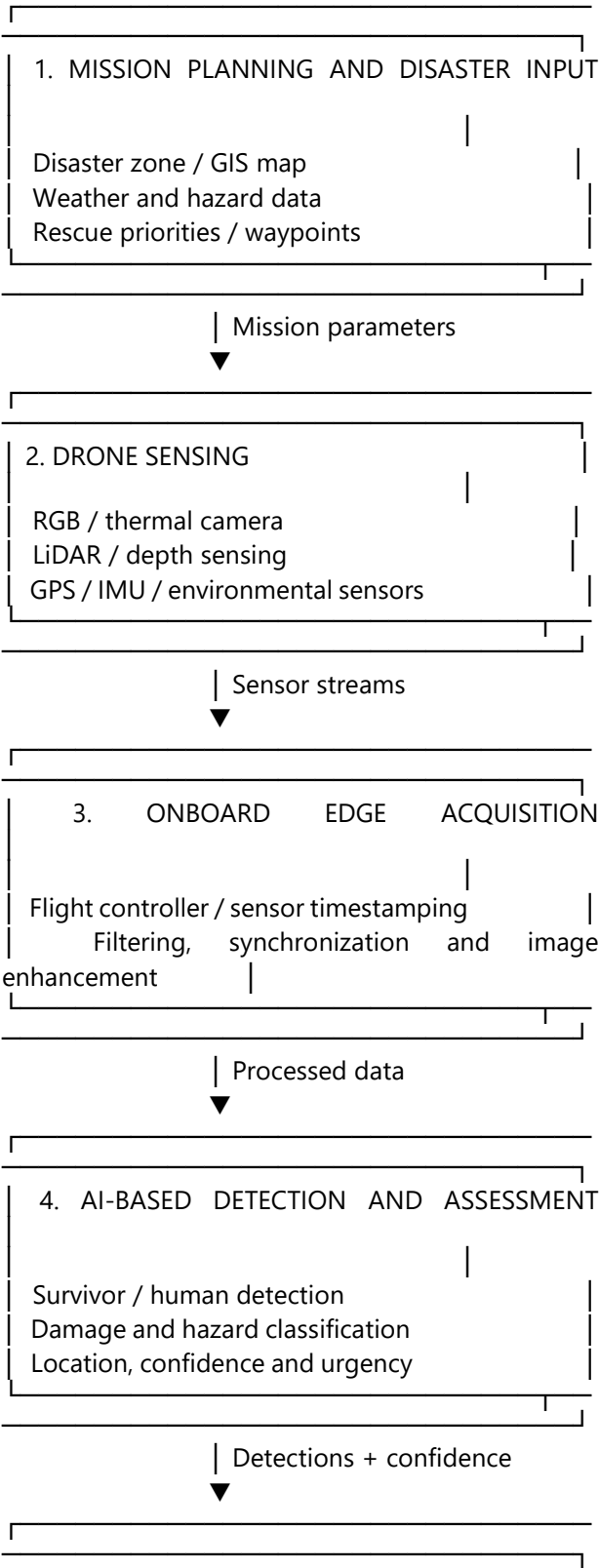
communication. The SAR paper [1] describes the breadth of UAV applications and the continuing challenges of endurance, payload and connectivity. The RF-spectrogram study [2] reports promising detection performance for YOLOv8n and YOLOv9t, with YOLOv8n faster in the tested configuration, while acknowledging that multi-UAV and complex electromagnetic validation remains incomplete. The authentication study [3] contributes a lightweight protocol intended to protect emergency UAV communications, but protocol analysis alone cannot guarantee complete operational resilience.

The main conclusion is that no single model or protocol constitutes a complete disaster-response solution. A dependable platform must integrate sensors, edge AI, secure networking, fleet coordination and human-supervised decisions, and must be evaluated in realistic disaster-like conditions. Future work should prioritize joint field trials that measure safety, latency, energy use, detection reliability and recovery from communication failure. Such validation is necessary before the proposed integrated architecture can be treated as operationally ready.

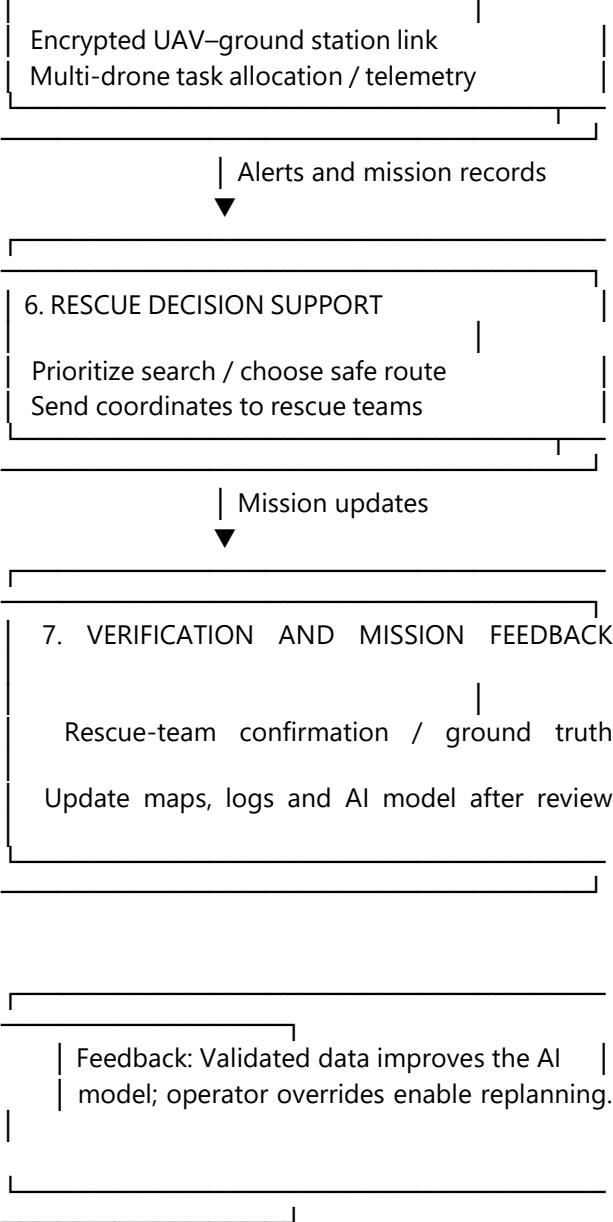
Table 1. Comparison of the Three Source Papers

Source	Focus	Contribution	Limitation
Quero & Martine z-Carranza [1]	SAR and disaster operations	Reviews sensors, multi-UAV use, communications and relief applications	Broad review; performance varies across cited studies
Slimeni et al. [2]	RF spectrogram detection	YOLOv8n: 1.6 ms; YOLOv9t: 3.0 ms; mAP50–95 around 0.80–0.85	Controlled setting; multi-UAV and complex RF conditions need testing
Jan et al. [3]	Emergency UAV authentication	Authentication and session-key agreement with formal analysis	Protocol analysis does not replace field testing

I. PROPOSED CONCEPTUAL ARCHITECTURE



5. SECURE COMMUNICATION AND COORDINATION



II.

Research Gaps and Future Directions

Gaps supported by the reviewed evidence. (i) Limited real-world validation: AI-based drone detection and search-and-rescue methods require further evaluation under diverse disaster conditions, including smoke, dust, poor lighting and obstructed views [1]. (ii) Sensor and environmental limitations: camera-based detection can be affected by visibility, while thermal and other sensing modalities require

additional validation across different operational environments [1]. (iii) Limited edge-processing capability: lightweight AI models offer faster inference, but balancing detection accuracy, computational cost and onboard resource constraints remains a challenge [2]. (iv) Incomplete multi-drone evaluation: simultaneous UAV operation, complex environments and coordination under changing mission conditions require further testing [2]. (v) Security and authentication overhead: emergency UAVs need lightweight authentication and secure key establishment, while their performance and scalability must be assessed under practical communication and energy constraints [3]. (vi) Communication reliability: disaster environments may have damaged infrastructure or intermittent connectivity, making dependable data exchange and local decision-making important challenges.

X. CONCLUSION

Ai-Enabled Disaster Response Drones Have Progressed Toward Integrating Aerial Sensing, Computer Vision, Lightweight Ai Inference, Secure Communication And Multi-Drone Coordination For Rapid Relief Operations. These Technologies Offer Potential Benefits For Survivor Detection, Damage Assessment, Hazard Identification And The Delivery Of Timely Information To Rescue Teams. However, The Reviewed Evidence Highlights Continuing Challenges In Real-World Validation, Environmental Robustness, Onboard Computational Efficiency, Communication Reliability And Secure Uav Authentication. Lightweight Ai Architectures Can Reduce Inference Latency, While Secure Authentication Mechanisms Can Support Safer Communication Between Drones And Ground Stations; Nevertheless, Their Performance Must Be Evaluated Under Realistic Disaster Conditions. Reliable Deployment Will Require Diverse Field Datasets, Multi-Sensor Fusion, Energy-Efficient Onboard Processing, Resilient Communication, Rigorous Performance Evaluation And Human-Supervised Decision-Making, As Reflected In The Proposed Conceptual Architecture. These Improvements Can Help Establish More Reliable And

Scalable Drone-Assisted Systems For Rapid Disaster Response And Emergency Relief.

REFERENCES

1. M. Deruyck, J. Wyckmans, W. Joseph, and L. Martens, "Designing UAV-aided emergency networks for large-scale disaster scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, pp. 1–12, Dec. 2018.
2. N. Zhao et al., "UAV-assisted emergency networks in disasters," *IEEE Wireless Communications*, vol. 26, no. 1, pp. 45–51, Feb. 2019.
3. K. G. Panda, S. Das, D. Sen, and W. Arif, "Design and deployment of UAV-aided post-disaster emergency network," *IEEE Access*, vol. 7, pp. 102985–102999, 2019.
4. J. Sanchez-García, D. G. Reina, and S. L. Toral, "A distributed PSO-based exploration algorithm for a UAV network assisting a disaster scenario," *Future Generation Computer Systems*, vol. 90, pp. 129–148, Jan. 2019.
5. M. Y. Arafat and S. Moh, "Localization and clustering based on swarm intelligence in UAV networks for emergency communications," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8958–8976, Oct. 2019.
6. I. Chandran and K. Vipin, "Multi-UAV networks for disaster monitoring: Challenges and opportunities from a network perspective," *Drone Systems and Applications*, vol. 12, pp. 1–28, Jan. 2024.
7. M. Erdelj, M. Krol, and E. Natalizio, "Wireless sensor networks and multi-UAV systems for natural disaster management," *Computer Networks*, vol. 124, pp. 72–86, Sep. 2017.
8. S. Ogunbunmi, Y. Chen, E. Blasch, and G. Chen, "A survey on reputation systems for UAV networks," *Drones*, vol. 8, no. 6, Art. no. 253, Jun. 2024.
9. J. Sanchez-García, J. M. García-Campos, S. L. Toral, D. G. Reina, and F. Barrero, "An intelligent strategy for tactical movements of UAVs in disaster scenarios," *International Journal of Distributed Sensor Networks*, vol. 12, no. 3, Mar. 2016, Art. no. 8132812.

10. K. Illyass, Z. Baig, and N. Syed, "Robust and lightweight mutual authentication scheme for drone swarm networks," *Journal of Network and Computer Applications*, vol. 242, Oct. 2025, Art. no. 104264.
11. Z. Zhao, C. Hsu, L. Harn, Z. Xia, X. Jiang, and L. Liu, "Lightweight ring-neighbor-based user authentication and group-key agreement for Internet of Drones," *Cybersecurity*, vol. 7, no. 1, Art. no. 50, Aug. 2024.
12. L. Zhang, J. Xu, M. S. Obaidat, X. Li, and P. Vijayakumar, "A PUF-based lightweight authentication and key agreement protocol for smart UAV networks," *IET Communications*, vol. 16, no. 10, pp. 1142–1159, Jun. 2022.
13. Z. He, Y. Zheng, S. Chen, Z. Du, S. Liu, and K. Zhang, "Security-enhanced lightweight authentication key-agreement protocol for unmanned aerial vehicle communication," *Applied Sciences*, vol. 15, no. 9, Art. no. 4680, Apr. 2025.
14. L. Teng et al., "Lightweight security authentication mechanism towards UAV networks," in *Proceedings of the International Conference on Networking and Network Applications (NaNA)*, Oct. 2019, pp. 379–384.
15. M. Adil, H. Abulkasim, A. Farouk, and H. Song, "R3ACWU: A lightweight, trustworthy authentication scheme for UAV-assisted IoT applications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, pp. 6161–6172, Jun. 2024.
16. J. Zhu, J. Peng, and L. Wang, "A lightweight and trustworthy authentication protocol for UAV networks based on PUF," in *Proceedings of the 14th International Conference on Communication and Network Security*, Dec. 2024, pp. 71–77.
17. S. U. Jan, F. Qayum, and H. U. Khan, "Design and analysis of lightweight authentication protocol for securing IoD," *IEEE Access*, vol. 9, pp. 69287–69306, 2021.