Analyzing LoRaWAN's Challenges and Future Integration for Disaster Management

Wenbo Zhang

{ wenbo.zhang@ucdconnect.ie }

Beijing Dublin International College, Beijing University of Technology, Beijing 100124, China

Abstract. Traditional communication infrastructures are highly susceptible to disruption during disasters, leading to severe communication breakdowns in emergency response operations. Low-Power Wide-Area Networks (LPWANs), particularly LoRaWAN, therefore emerged as a promising alternative due to their long-range connectivity, low-power consumption, and capability for rapid ad-hoc deployment. Nevertheless, LoRaWAN's ALOHA-based medium access introduces a conflict between its best-effort design and the mission-critical reliability demanded in emergency scenarios. This review systematically examines five case studies in industrial monitoring, fire detection, flood surveillance, and search and rescue (SAR) applications to identify the core challenges in practical LoRa deployments. The research results indicate that the reliability of LoRa is highly dependent on non-standard network architecture, optimized physical layer configuration, and environmental conditions. Scalability remains the primary constraint; a mass-alert event can trigger severe packet collisions and network instability. Bandwidth limitations also restrict LoRa to low-rate data, making high-throughput media infeasible. Therefore, Lora can serve as a stable foundation for emergency communications only through integration with 5G core infrastructures to ensure system-level reliability and through AI/ML-driven optimization to enhance energy and network efficiency.

Keywords: LoRaWAN, Emergency Communications, Reliability, Scalability, 5G Integration.

1 Introduction

Traditional communication systems—cellular networks, Wi-Fi, and even specialized industrial links—tend to falter once a large-scale emergency unfolds. As past earthquake and flood events have repeatedly shown, the loss of ground-level power or the collapse of network nodes can occur far sooner than responders expect, and the parts that remain functioning are typically choked by traffic surges [1]. The result is not merely a service interruption but a sudden void in basic situational awareness, during which affected individuals often cannot relay even the simplest distress signals. These recurring observations underscore the need for communication solutions that remain functional without external infrastructure and can operate on minimal power.

ICMEEA 2026, April 24-26, Singapore, Singapore

DOI 10.4108/eai.24-4-2026.2364847

Low-Power Wide-Area Networks (LPWANs) are frequently cited as a workable middle ground: they reach long distances, rely on modest energy budgets, and can support large device populations [2]. Within this family, LoRaWAN has received particular attention. Its CSS modulation is resilient to noise, and its architecture makes small, privately managed deployments feasible—an appealing feature when infrastructure is compromised [3]. Over the past few years, researchers have tested LoRaWAN nodes in different situations ranging from industrial gas facilities to flood-monitoring sites and SAR robots. These trials consistently show that LoRa can deliver essential sensor data when conventional channels fail.

Yet, there is a significant gap between LoRaWAN's "best effort" design and the high reliability required for critical task response. Emergency communication must be predictable even when the channel becomes crowded. In reality, when hundreds of nodes attempt to report simultaneously, collision rates rise sharply, and the system’s throughput would collapse [3]. This conflict forms one of the central barriers to adopting LoRaWAN directly for emergency operations.

This study examines these issues by looking at several practical deployments and their limitations. Then analyze the architectural bottlenecks, focusing on the mismatch between ALOHA-style access and the bursty, high-density alert patterns typical in emergencies [4]. Lastly, an integrated approach combining 5G-core-level reliability mechanisms and AI/ML-based optimization is given to solve the scalability and energy efficiency in practice [5,6].

2 Application Case Studies in Emergency Scenarios

2.1 Case 1: High-Reliability Industrial Gas Leakage Monitoring

In high-risk industrial environments where a gas-leak alarm may need to propagate within fractions of a second, the network’s tolerance for delay or error is practically zero. Tamang et al. approached this constraint by designing a scheduling mechanism that works entirely on the server side. Their idea was to separate life-critical Urgent Packets (UPs) from routine Regular Packets (RPs), allowing UPs to bypass normal queuing. In theory, this design should keep the Packet Loss Rate under 0.1% and the latency below 500 ms, all without requiring firmware changes to the devices in the field [7].

However, the experimental results revealed a more fundamental issue with the single gateway setup. Due to the gateway operating in half-duplex mode, incoming UP cannot be heard at any time when transmitting downlink control messages. This results in a surprisingly high PLR - about 3.66% - far exceeding the acceptable threshold for FMAR alerts. Researchers have addressed this issue by introducing a second gateway specifically designed for uplink reception, achieving a PLR well below 0.1%.

This study demonstrates that architectural redundancy can indeed enable LoRaWAN to support high-reliability applications. But it introduces a higher cost, the increased hardware and a more complex deployment. Scalability is also questionable, as the experiment only included eight devices.

2.2 Case 2: Fire Detection: Architectural Fault-Tolerance and Protocol Reliability

Traditional fire alarms depend on local power and Wi-Fi infrastructure that often fails during emergencies. Safi et al. addressed this vulnerability by designing a dual-channel surveillance system that uses Wi-Fi as the primary link and automatically switches to a LoRaWAN backup when Wi-Fi disconnects [8]. This mitigates the single point of failure and validates LoRaWAN's suitability as a fault-tolerant, infrastructure-independent lifeline channel.

However, this approach addresses infrastructure failure but not the inherent reliability of the LoRaWAN protocol itself. In a separate study on forest fire monitoring, Mukhia et al. found that the standard LoRaWAN Packet Delivery Ratio (PDR) was unacceptably low for critical alerts (e.g., 73% for SF10) [9]. They also noted that LoRaWAN's standard confirmed transmission mode was unreliable, as the end-device's weaker sensitivity often fails to receive the downlink acknowledgment (ACK) from the more sensitive gateway. To solve this, they implemented a custom application-layer retransmission mechanism. End-nodes only delete sensor data after receiving a software-level ACK from the server, successfully raising the end-to-end Data Completeness Ratio (DCR) to over 91.5% despite the poor underlying PDR.

The physical environment's impact is equally critical. Safi et al. noted that latency surged by 39% in enclosed indoor spaces [8]. Mukhia et al. made a more interesting discovery: maintaining a clear line-of-sight (LOS) was more important than distance [9]. In their tests, a 9.34 km node with LOS actually outperformed an obstructed 4.9 km node.

2.3 Case 3: Flood Monitoring and Link Quality Analysis

Flood warning systems depend on reliable data from remote, power-constrained sensors. While building a solar-powered monitoring platform, Zakaria et al. empirically compared two key LoRaWAN configurations: high-speed SF7 and long-range SF12[10].

The field experiments revealed a clear trade-off. The SF7 configuration performed perfectly within 600 m, achieving a 100% Packet Delivery Ratio (PDR), positive SNR, and a delay under 0.5 s. Conversely, the SF12configuration struggled beyond 500 m, where its SNR dropped below zero, PDR fell to 80%, and delays were high, ranging from 2.5 to 3.75 s.

For regional flood monitoring, SF7 provides the optimal balance of reliability, latency, and energy efficiency. This study also confirmed that SNR is the true factor of link reliability, not RSSI. This study was a single-node test, neglecting the network scalability and collision management. Furthermore, its reliance on the less-secure Activation by Personalization (ABP) method makes it unsuitable for large-scale deployment without additional security measures.

2.4 Case 4: Infrastructure-Independent Search and Rescue Robotics

To address total infrastructure failure in post-disaster environments, Manuel et al. developed an integrated search and rescue (SAR) system that deliberately bypasses the standard LoRaWAN protocol [1]. Instead, the system utilizes LoRa's physical layer for direct peer-to-peer (P2P) and broadcast communication, forming an ad-hoc network entirely independent of central servers. The design supports a complete SAR workflow, incorporating GPS beacon transmission from victims (EMERG), robot control commands (RoboMaC), and low-bitrate voice communication (RoboTalkie).

The simulations demonstrated that autonomous robots were able to navigate to target GPS coordinates and establish duplex voice connections, which confirms the functionality of LoRa P2P as a robust, gateway-free system for essential lifeline data transmission

The primary limitation of this architecture lies in its extremely restricted bandwidth, which prevents real-time video streaming and generates delays. Moreover, its reliability under complex non-line-of-sight (NLOS) conditions remains unverified, as the experiment was conducted only within a university campus [1].

3 The Conditional Potential and Challenges of LoRa in Emergency Communications

Analysis of the case studies demonstrates that LoRa's potential for high-reliability communication is not inherent but strictly conditional. This chapter examines the challenges in detail, focusing on internal limitations and structural contradictions between LoRa's technical design and the operational requirements of emergency communications.

3.1 Internal Challenges: The Prerequisites of LoRa Performance

The industrial gas monitoring case study illustrates the architectural challenge of achieving reliability with LoRa [7]. Under a stringent reliability standard (packet loss rate below 0.1%, latency under 500 ms), the single-gateway LoRaWAN configuration failed to meet the target. The half-duplex operation of the gateway caused a critical conflict: when transmitting Downlink Control Packets (DCPs), the gateway was unable to receive UPs, resulting in an unacceptable packet loss rate of 3.66%. This limitation was overcome only by introducing architectural redundancy through a second, dedicated gateway for receiving UPs, which enabled the system to satisfy the reliability requirement. A similar approach was observed in the smart building fire detection case, where LoRa served as a Wi-Fi backup to ensure fault tolerance. These findings confirm that standard LoRaWAN architecture is insufficient to meet high reliability requirements without adopting redundant or hybrid configurations [8].

The flood monitoring case study demonstrates that LoRa's performance is highly sensitive to parameter configuration [10]. A frequent misconception is that the most robust spreading factor (SF12) always ensures optimal performance. Field measurements summarized in Table 1 show that this assumption is incorrect. Although SF12 achieved slightly stronger RSSI, its SNR dropped into negative values at 500 m, resulting in an 80% packet delivery rate (PDR). In contrast, SF7 maintained full reliability (100% PDR) with a positive SNR. Moreover, SF12 exhibited a latency of approximately 3.75 seconds—over seven times longer than SF7's sub-0.5-second delay [10]. These results indicate that careful parameter optimization is essential for efficient and reliable network performance. A suboptimal configuration not only degrades data integrity but also shortens battery life and reduces network capacity.

Table 1. LoRaWAN Link Quality Comparison (SF7 vs SF12) [10]

Distance (m)	RSSI SF7 (dBm)	RSSI SF12 (dBm)	SNR SF7 (dB)	SNR SF12 (dB)	PDR SF7 (%)	PDR SF12 (%)	Delay SF7 (s)	Delay SF12 (s)
100	-83	-81	9	8	100	100	~2.5	~3.5
200	-88	-85	8	6	100	100	~2.5	~3.5
300	-92	-90	6	4	100	100	~2.4	~3.5
400	-96	-95	4	2	100	100	~2.25	~3.6
500	-100	-99	2	-2	100	80	~2.25	~3.7

600	-102	-102	1	-6	100	100	~2.4	~3.75

Environmental factors play a decisive role in LoRa performance. The fire detection study compared open and closed indoor conditions, revealing that at a fixed distance of 600 m [8], latency in enclosed environments was 39% higher than in open ones (570 ms versus 409 ms). This finding quantitatively demonstrates the severe signal attenuation caused by walls and other obstacles. The forest fire deployment further reinforces this conclusion, showing that a clear line-of-sight (LOS) exerts greater influence on communication quality than distance itself: a 9.34 km LOS node outperformed an obstructed node at 4.9 km [9]. These results indicate that LoRa performs optimally only under near-ideal, unobstructed conditions, which are rarely achievable in smoke-filled buildings or urban rubble environments. Table 2 is a performance comparison in open vs. closed environments [8].

Table 2. Performance Comparison in Open vs. Closed Environments [8]

Environment	Distance(m)	Sensor Height	RSSI (dBm)	Network Delay (ms)	Response Time (ms)
Open	100	2 m	-96.48	226	626
Open	300	2 m	-111.18	287	687
Open	600	2 m	-124.28	409	809
Closed	100	1st Floor	-99.24	281	660
Closed	300	1st Floor	-111.6	398	687
Closed	600	1st Floor	-123	570	842

3.2 The Scalability Challenge: The "Mass Alert" Contradiction

Scalability has repeatedly surfaced as a weak point for LoRa when it is pushed into emergency-response roles. In situations where many devices attempt to send alerts at roughly the same moment, the ALOHA-based channel access offers little protection against collisions. Even small-scale tests illustrate the issue: in the gas-monitoring experiment, two nodes sharing a spreading factor already produced close to a 30% loss rate—a surprisingly high figure given the simplicity of the setup [7]. Predictably, the problem becomes far more pronounced once the network scales. In the large-scale simulation conducted by Lopes et al., which modeled disaster-monitoring deployments with thousands of nodes, the Data Extraction Rate fell sharply as node density and reporting frequency increased [4]. These observations indicate that LoRaWAN's uncoordinated medium access poses a fundamental bottleneck to scalability during high-traffic emergency scenarios. Table 3 is a two-node collision test in a factory scenario.

Table 3. Two-Node Collision Test in Factory Scenario [7]

Scenario	Node	Spreading Factor	Packet Loss Rate (PLR %)
Transmission on Same SF	ED1	SF 7	94.3
	ED2	SF 7	35
	Both (Combined Loss)	SF 7	29.66
	ED1	SF 7	4.7

Transmission on Different SFs	ED2	SF 8	3.23
	Both (Combined Loss)	SF 7 & SF 8	0.12

3.3 The Inherent Bandwidth Challenge: Defining LoRa's Role

Bandwidth is the most defining constraint for LoRa-based emergency systems. A search and rescue (SAR) case study highlights this limitation. Researchers implemented a peer-to-peer (P2P) LoRa system for infrastructure independence, which successfully transmitted lifeline data such as GPS coordinates, SOS signals, and voice messages. However, the extremely limited bandwidth made real-time video transmission infeasible. This forced rescuers to wait until robots returned to base to access visual data [1]. The finding confirms that while LoRa is suited for essential alerts, it cannot support high-throughput applications like live video. Its proper function in emergency response is therefore as a low-power, long-range perception layer, not a comprehensive communication solution.

3.4 Design Trade-offs for Emergency Communications

The analysis above highlights that using LoRa in emergency communication systems involves navigating several inherent trade-offs. High reliability can only be achieved through tailored, often costly solutions that go beyond default settings, such as deploying multiple gateways or implementing retransmission mechanisms at the application layer [7][9]. When enhancing scalability, a more advanced scheduling strategies are indispensable to prevent network failure during large-scale alerts, the simplicity of LoRaWAN becomes a limitation [7]. The robustness in balancing energy efficiency calls for careful tuning of parameters, previous research suggests the more conservative SF12 can compromise overall network performance and significantly increase latency. The complexity of the real environment makes deployment more complicated. Though LoRa performs well in open environments, its effectiveness diminishes remarkedly in confined or obstructed spaces [10]. Moreover, there is a clear trade-off between system capability and operational independence. LoRa allows communication without relying on infrastructure, which also limits data throughput [1].

These considerations define the feasible scope of LoRa in emergency scenarios. Its main advantage lies in providing critical, low-rate communication under challenging conditions. However, realizing this potential requires careful architectural choices, protocol adjustments, and adaptation to environmental constraints. LoRa's suitability for emergency communication is conditional rather than absolute.

4 Future Research Outlook

4.1 Architectural Innovation: Seamless 5G–LoRaWAN Integration

From the previous studies, four critical barriers are concluded, including half-duplex conflicts, mass-alert instability, static configurations, and limited bandwidth. To make lora/LoRaWAN realistic in real world environment, its strengths of long range and low power are not enough.

The main obstacle to reliability lies in the standard LoRaWAN architecture. As shown in the industrial gas-monitoring case, the use of downlink control packets caused gateway conflicts, producing a 3.66% packet loss rate—far exceeding the <0.1% reliability target [7]. Scalability studies further confirm that the ALOHA-based MAC protocol collapses under large-scale, simultaneous transmissions typical of emergency mass alerts [4].

A promising solution is integrating LoRaWAN within the 5G Core. Jradi et al. proposed an Adaptation Function (AF) module that enables LoRaWAN to communicate with 5G's Access and Session Management Functions (AMF and SMF) [5]. This hybrid architecture directly addresses LoRa's weaknesses. The Service-Based Architecture (SBA) of 5G provides reliable, centralized coordination to eliminate gateway conflicts [7]; its massive machine-type communication (mMTC) capability allows handling of large-scale alert bursts [5]; and the dual-network framework alleviates bandwidth limitations by offering a 5G path without requiring changes to LoRa end devices [6].

Such 5G–LoRaWAN integration preserves LoRa's low-power, long-range benefits while introducing high reliability and scalability through 5G's backbone. Future work should focus on lightweight AF implementation, latency optimization between the two cores, and standardized APIs to ensure interoperability across heterogeneous network operators.

4.2 Intelligent Optimization: AI/ML-Driven Efficiency

LoRa's second weakness is its static, environment-insensitive operation. As the flood-monitoring case showed, a suboptimal parameter SF12 caused high latency (~3.75s) and poor delivery (80% PDR), whereas SF7 performed ideally [10]. In a disaster's shifting channel conditions, fixed parameters are insufficient. AI-based adaptive optimization is a solution. For example, González-Palacio et al. used machine learning to enhance ADR, predicting path loss from real-time variables (e.g., temperature, humidity) instead of just historical SNR [6]. This predictive model achieved >99% PDR and 43% energy savings over traditional ADR, translating to longer device life and more stable emergency connectivity.

Future research should explore federated or edge learning for distributed training, maintaining functionality without cloud connectivity. Integrating ML-enhanced ADR with 5G network slicing could also enable priority-based resource allocation, balancing efficiency with reliability.

5 Conclusion

This review identifies a mismatch between LoRa's inherent design and the absolute reliability demanded by emergency response. The analysis of previous practical studies concludes that LoRa's considerable potential, but remains strictly conditional to many settings.

Standard LoRaWAN is significantly limited in terms of reliability, scalability, parameter efficiency, and bandwidth. Therefore, LoRa should not be used as a substitute for the traditional communication infrastructure, but rather as a low-power method in specific applications, transmitting critical data such as critical alarms and sensor updates in circumstances when the main system collapses.

Systematic integration is essential for Lora. On the one hand, LoRa should be integrated with the 5G core network architecture to achieve system-level reliability; On the other hand, utilizing AI-driven optimization to dynamically ensure link efficiency and energy consumption. Only by achieving this integration can LoRa become an indispensable and powerful layer in the future complex emergency communication architecture.

References

[1]. Manuel, M.P., Faied, M., Krishnan, M.: A LoRa-based disaster management system for search and rescue mission. IEEE Internet of Things Journal (2024).

[2]. Chaudhari, B.S., Zennaro, M. and Borkar, S.: LPWAN technologies: Emerging application characteristics, requirements, and design considerations. Future Internet 12(3), 46 (2020).

[3]. Almuhaya, M.A., Jabbar, W.A., Sulaiman, N. and Abdulmalek, S.: A survey on Lorawan technology: Recent trends, opportunities, simulation tools and future directions. Electronics 11(1), 164 (2022).

[4]. Lopes IR, Coelho PR, Pasquini R, Miani RS.: Evaluating the performance of LoRa networks: a study on disaster monitoring scenarios. IoT 6(1), 14(2025).

[5]. Jradi, H., Nouvel, F., Samhat, A.E., Prévotet, J.C., Mroue, M.: A seamless integration solution for LoRaWAN into 5G system. IEEE Internet of Things Journal 10(18), 16238-16252 (2023)

[6]. González-Palacio, M., Tobón-Vallejo, D., Sepúlveda-Cano, L.M., Rúa, S., Le, L.B.: Machine-learning-based combined path loss and shadowing model in LoRaWAN for energy efficiency enhancement. IEEE Internet of Things Journal 10(12), 10725-10739 (2023)

[7]. Tamang, D., Pozzebon, A., Parri, L., Fort, A., Abrardo, A.: Designing a reliable and low-latency LoRaWAN solution for environmental monitoring in factories at major accident risk. Sensors 22(6), 2372 (2022)

[8]. Safi, A., Ahmad, Z., Jehangiri, A.I., Latip, R., Zaman, S.K.U., Khan, M.A., Ghoniem, R.M.: A fault tolerant surveillance system for fire detection and prevention using LoRaWAN in smart buildings. Sensors 22(21), 8411 (2022)

[9]. Mukhia, R., Sarambage Jayarathna, K.G., Lertsinsrubtavee, A.: Performance evaluation of lorawan forest fire monitoring network in the wild. In: Proceedings of the 18th Asian Internet Engineering Conference, pp. 96-104 (2023)

[10]. Zakaria, M.I., Jabbar, W.A., Sulaiman, N.: Development of a smart sensing unit for LoRaWAN-based IoT flood monitoring and warning system in catchment areas. Internet of Things and Cyber-Physical Systems 3, 249-261 (2023)