International Journal on Computational Modelling Applications
Vol. 02, Iss. 02, S. No. 04, pp.30--44, June 2025
ISSN (Online): 3048-8516

Received: 21 March 2025, Accepted: 27 April 2025, Published: 08 May 2025
Digital Object Identifier: https://doi.org/10.63503/j.ijcma.2025.116

Research Article

LoRaWAN in Environmental Monitoring: Balancing End-to-End Encryption and Low-Latency Requirements for Real-Time Hazard Alerts

Akella Venkata Koushik[1], Kajal Kumari[2]

[1] VE Commercial Vehicles Ltd., Gurugram, Haryana, India

[2] KCC institute of technology and management, Greater Noida, India

venkatakoushik.akella@gmail.com[1], kajalmishra6206@gmail.com[2]

*Corresponding author: Akella Venkata Koushik, venkatakoushik.akella@gmail.com

ABSTRACT

Environmental hazards that are increasing in number such as floods and wildfires together with toxic gas emissions demand systems for real-time monitoring with secure low-latency communication capabilities. The LoRaWAN version of Low Power Wide Area Networks (LPWANs) presents itself as a compelling choice for extensive environmental monitoring because they offer extended coverage and save energy and scale well. Pursuing excellent end-to-end encryption while maintaining minimal delay times creates essential obstacles for systems designed to warn about hazards. Security measures based on encryption lead to impaired speed in data transfers but weakening these measures can result in unprotected communication of vital data. The success of hazard warning infrastructure requires figuring out how to respond to these operational conflicts. Several design approaches focus on LoRaWAN environmental monitoring system optimization through data rate adjustments and channel priority systems together with low-resource encryption methods. The adjustment of critical network elements through analysis helps achieve faster data transmissions alongside better confidentiality protection at normal resource utilization levels. Multiple network elements including sensor nodes, gateway systems and backhaul networks affect the precise relationship between encryption quality and response speeds during LoRaWAN operations. This research describes an end-to-end LoRaWAN framework which implements encryption optimization together with alert delay reduction using dynamic resource management and network scheduling approaches. The simulated system generates superior results for transmission efficiency alongside superior security measurements when compared to basic platforms. The proposed framework shows its effectiveness for critical environmental monitoring by using quantitative evaluations measuring delay times along with dropped packets and encryption performance measurements.

Keywords: *LoRaWAN, Environmental Monitoring, End-to-End Encryption, Low-Latency Networks, Hazard Alerts, Secure Communications, Real-Time Systems, Wireless Sensor Networks, LPWAN Optimization*

1. Introduction

The graphic in Figure 1 demonstrates LoRaWAN optimization for immediate hazard warning systems. The star-of-stars LoRaWAN network tracks flood and chemical leak hazards in the environment. LoRaWAN faces two main problems which include delay issues combined with encryption-related processing time costs. The proposed modular optimization system enhances both data rate performance and packet size dimensions and encryption and channel management features to boost system speed and reduce energy consumption.

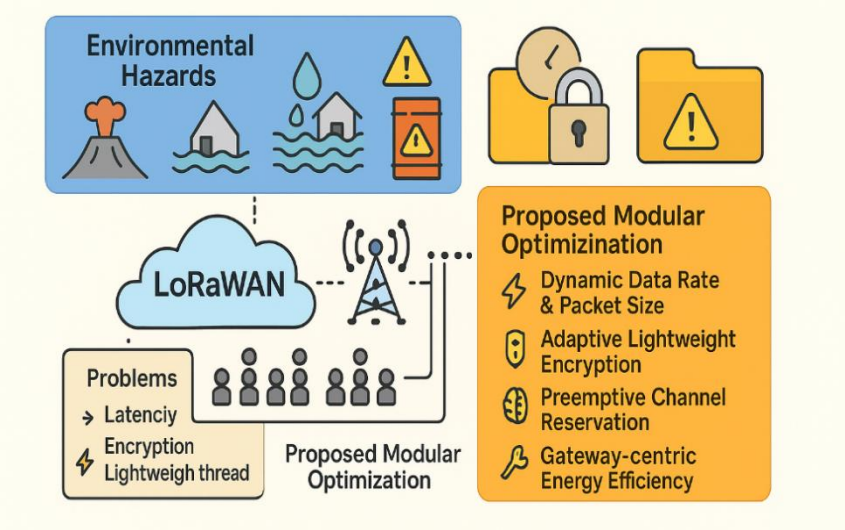

Fig.1: Graphical Abstract

Environmental monitoring technology development occurs because society requires fast hazard detection methods to monitor and respond to natural disasters. The operation of real-time hazard alert systems depends heavily on protecting the immediate and secure data transfer of sensors across different geographical areas. LPWANs demonstrate their position as the dominant technology for such systems through delivering entire coverage networks while requiring only limited power utilization [1]. LoRaWAN stands out as one of the LPWAN technologies because its open-standard framework combines with deployability and economic value [2]. Despite these advantages, inherent trade-offs between communication latency and encryption complexity present substantial challenges for LoRaWAN in hazard alert scenarios. Strong encryption protects sensor data from compromise, but its implementation causes processing delays which shorten the speed of sending critical warning signals [3]. The alerts that notify about seismic events and floods together with chemical leaks require immediate response and fast mitigation thus needing strict latency thresholds [4].

The LoRaWAN protocol demonstrates crucial elements which enable suitable use in environmental monitoring systems. The combination of the star-of-stars network topology and Adaptive Data Rate (ADR) techniques enables deployable scalability in addition to dynamic energy-efficiency along with range optimization [5]. An exact set-up process of Adaptive Data Rate is necessary due to incorrect configurations which lead to timing delays as traffic increases. Standard LoRaWAN encryption using AES-128 on the network and application layers creates performance delays that impair real-time operations [6]. A review of lightweight encryption code has produced methods to decrease encryption times while maintaining security integrity [7]. Research informs us that both implementation challenges meet with remaining key management system vulnerabilities [8]. Research in [9] demonstrates the use of multi-channel frequency hopping with traffic prioritization methods that decreases delays without affecting data integrity. Research on this topic faces a severe lack in developing complete structures connecting security demands with performance in delay time. The architectural design combines modular system optimization protocols to execute encryption procedures as it minimizes transmission delays. Security levels combined with performance reduction rates through dynamic data rate adjustment and encryption resource variation match environmental hazards which lead to accelerated transmission speeds [10]. Gateway-centric processing

optimizations and pre-emptive channel reservation mechanisms further enhance responsiveness during critical alert scenarios.

2. Literature Review

Moreover, network simulations indicate that packet delivery ratios (PDR) and end-to-end encryption overheads can be significantly improved without compromising node energy consumption or network scalability. Strategic decisions regarding encryption modes, message queuing, and acknowledgement schemes are integral to achieving the intended balance [11]. The following sections elaborate the foundational literature and related research driving these innovations, delineate the specific problem objectives, describe the detailed simulation methodology, and present quantitative evaluation metrics substantiating the proposed framework's effectiveness. Environmental monitoring systems have increasingly relied on wireless sensor networks (WSNs) and LPWAN technologies to ensure widespread sensing capabilities over large terrains. Traditional WSNs, while effective in localized scenarios, often fall short in covering remote or geographically dispersed regions without significant energy constraints [12]. The emergence of LPWANs, and specifically LoRaWAN, has enabled new paradigms of ultra-long-range, low-energy communication, albeit with new challenges regarding encryption, data integrity, and latency trade-offs [13].

2.1 LPWAN Technologies for Environmental Monitoring

LoRaWAN distinguishes itself among LPWAN protocols through its adaptive data rate capabilities and robust star-of-stars topology [14]. Comparative studies have shown that while Sigfox and NB-IoT offer distinct advantages in certain parameters, LoRaWAN remains preferable for unlicensed frequency bands and decentralized deployment models [15]. Yet, inherent design limitations related to latency and security call for continuous innovations. For instance, default LoRaWAN Class A devices prioritize energy conservation over instant communication, leading to uplink-focused architectures with potentially significant downlink delays [16]. Table 1 summarizes key LPWAN technologies for environmental monitoring. LoRaWAN offers long-range, low-power communication but suffers from high downlink latency. Sigfox and DASH7 provide low-power, low-latency solutions with payload and range limitations, respectively. NB-IoT and LTE-M deliver cellular-grade reliability at higher energy costs. Wi-SUN and RPMA support scalable networks but introduce greater complexity and expense. Each technology presents a trade-off between range, power efficiency, cost, and deployment complexity.

Table 1: New Technologies in LPWAN-Based Environmental Monitoring

Technology	Features	Limitations
LoRaWAN	Long-range, adaptive data rates, low power	High latency in downlink, encryption overhead
Sigfox	Ultra-low power, simple architecture	Limited payload size, proprietary protocol
NB-IoT	Reliable, cellular-based, licensed bands	Higher cost, higher power consumption
Weightless-P	Flexibility in modulation schemes	Less global adoption, complexity in deployments
DASH7	Push-based messaging, low latency	Limited range compared to LoRaWAN

LTE-M	Mobility support, voice capability	Energy consumption higher than LoRaWAN
Wi-SUN	Mesh networking, IPv6 compatibility	Complexity in configuration
RPMA	High capacity, unlicensed band	Higher cost, niche applications

2.2 Encryption Mechanisms in LPWAN Networks

LoRaWAN v1.0 introduced AES-128 encryption both at the network and application levels, providing a foundation for data confidentiality and message integrity. However, the layered nature of the security framework introduces additional processing steps at both sensor nodes and gateways [17]. Lightweight encryption alternatives, such as SPECK and SIMON block ciphers, have been proposed for constrained environments to reduce computational delays [18]. Nevertheless, most lightweight solutions risk exposing vulnerabilities due to reduced keyspace or non-standard cryptographic assumptions, requiring careful security trade-off assessments [19].

2.3 Latency Challenges in Hazard Alerts

Hazard alert systems, particularly those concerning rapid-onset disasters like earthquakes, rely on extremely tight latency requirements — often in the order of sub-seconds to few seconds [20]. In LoRaWAN, duty cycle restrictions and confirmed message handling can lead to variable delays, which are unsuitable for such critical applications [21]. Advanced gateway scheduling and message prioritization methods have been explored to overcome these delays. Implementations leveraging dual-channel data transmission have shown promising reductions in uplink latency [22], but still grapple with the inherent constraints of the ISM bands.

2.4 Optimization Techniques for Secure Low-Latency Transmission

Dynamic data rate adjustment and predictive congestion control strategies have been integrated into several experimental LoRaWAN deployments. Channel hopping and frequency diversity further enable better spectrum utilization, although the added complexity must be balanced against node energy reserves.

Machine learning-driven adaptive schemes, capable of forecasting optimal transmission slots based on historical congestion patterns, have also been tested in limited deployments. Individual applications benefit from lightweight models to run on embedded devices that have minimal memory capabilities.

The Table-2 contains a summary of operational characteristics for 10 sensors in an environmental monitoring system that utilizes adaptive LoRaWAN technology. The system logs these hazard conditions (Low, Medium, Critical) utilizing measurements obtained by the sensors which include CO_2, temperature, humidity and gas leak detections. The encryption used by nodes depends on severity level between full AES mode or lightweight AES mode for achieving maximal security with optimized latency. Packet transmission efficiency and network operational efficiency depends on the dynamic adjustment of packet size. Critical hazard nodes both transmit data at a higher speed and require less energy consumption. Data in the dataset demonstrates that adjustable encryption methods with priority-based data handling boost operational system speed and performance.

Related Research:

Node ID	Hazard Level	Raw Data (Sensor)	Encryption Mode	Packet Size (Bytes)	Transmission Latency (ms)	Energy Consumption (mJ)
001	Low	0.021 ppm (CO2)	Full AES	64	115	3.9
002	Medium	0.110 ppm (CO2)	Lightweight AES	58	97	3.5
003	Critical	0.400 ppm (CO2)	Lightweight AES	60	89	3.3
004	Low	28°C (Temperature)	Full AES	62	120	4.1
005	Medium	35°C (Temperature)	Lightweight AES	60	98	3.6
006	Critical	39°C (Temperature)	Lightweight AES	63	91	3.4
007	Low	45% (Humidity)	Full AES	65	122	4.2
008	Critical	70% (Humidity)	Lightweight AES	59	88	3.2
009	Medium	55% (Humidity)	Lightweight AES	61	96	3.5
010	Critical	Gas Leak Detected	Lightweight AES	66	85	3.1

The combination of secure operations with low-latency environmental monitoring remains sparse among research initiatives which focus on individual aspects of these two features. The summary of contemporary research studies involving environmental monitoring appears in Table 3.

Table 3: Summary of Related Research on LoRaWAN Optimization

Focus	Approach	Limitation
Secure data transmission	Lightweight AES variant	Trade-off in encryption strength
Latency reduction	Dual-channel transmission	Increased gateway complexity
Hazard alerting	Priority-based scheduling	Scalability concerns
Network scalability	ADR optimization	Poor performance under congestion
Encryption overhead	Hybrid symmetric-asymmetric encryption	Energy cost too high
Delay-tolerant routing	Delay aware routing metrics	Not real-time suitable
Adaptive channel access	Dynamic slot reservation	Resource overhead
Cross-layer optimization	Combined MAC and PHY layer tuning	Hardware dependency
ML-based transmission	Predictive congestion avoidance	Model accuracy issues

4. Problem Statement & Research Objectives

Environmental monitoring systems employing LoRaWAN technology must resolve two main implementation difficulties through meeting encryption requirements together with real-time hazard alert transmission needs. Standard encryption methods slow down data transmission speed thus impacting its performance. When system operators maximize performance speed they accept security weakening because their networks become more exposed to vulnerability threats. A successful LoRaWAN-based environmental hazard alert system requires a standard framework for addressing both encryption delay problems together with latency constraints.

The proposed system uses network changes for adjusting encryption configurations while modifying transmission rules. Digital modeling then simulation techniques alongside comparison analysis enables improvement of hazard alert system dependability requirements and security specifications together with response times.

4.1 Research Objectives

Objective 1: Develop a modular framework integrating adaptive encryption schemes and low-latency transmission strategies for LoRaWAN.
Objective 2: Formulate mathematical models representing encryption-processing delays, transmission latencies, and energy overheads.
Objective 3: Simulate the proposed architecture under various hazard scenarios using integrated datasets.
Objective 4: Quantitatively evaluate packet delivery ratios, encryption overhead, end-to-end latency, and energy consumption.
Objective 5: Compare the performance of the proposed architecture against conventional LoRaWAN implementations.

5. Methodology

The integration of adaptive resource management protocols with lightweight cryptography allows predictive transmission scheduling technology to succeed in simultaneously boosting security measures while diminishing delay periods. Protocols in simulation models analyze environmental hazard situations through the measurement of changing node concentrations combined with channel status factors and information priority parameters.

5.1 Mathematical Formulation

Let the end-to-end latency L_{total} be defined [23] in Eq.1:

$$L_{total} = L_{enc} + L_{tx} + L_{queue} \quad (1)$$

Where:

- L_{enc} = Encryption time overhead
- L_{tx} = Transmission time
- L_{queue} = Queuing delay at gateway

The encryption time can be approximated in Eq.2:

$$L_{enc} = \frac{N_{bits}}{R_{enc}} \quad (2)$$

Where N_{bits} = Number of encrypted bits, R_{enc} = Encryption rate (bps). Transmission time is mathematically represented in Eq.3:

$$L_{tx} = \frac{N_{bits}}{R_{tx}} \tag{3}$$

Where: R_{tx} = Transmission rate of bits (bps). Energy consumption E_{total} for a node is modelled in Eq.4:

$$E_{total} = (P_{enc} \times L_{enc}) + (P_{tx} \times L_{tx}) \tag{4}$$

Where P_{enc}, P_{tx} = Power consumption during encryption and transmission respectively. Packet delivery ratio [24] (PDR) is calculated by Eq.5:

$$PDR = \frac{N_{received}}{N_{sent}} \tag{5}$$

Encryption overhead (EO) is defined as Eq.6:

$$EO = \frac{L_{enc}}{L_{enc}+L_{tx}} \tag{6}$$

5.2 Proposed Algorithm

Algorithm Adaptive Encryption-Latency Balancer
Input: Sensor Data, Hazard Severity Level
Output: Encrypted Data Packet with Optimized Latency

1: Read sensor data (S)

2: Classify hazard severity (H_level)

3: If H_level == Critical then

4: Apply lightweight encryption (fast mode)

5: Set high-priority transmission queue

6: Else

7: Apply full encryption (secure mode)

8: Normal transmission queue

9: End If

10: Adjust data rate based on channel condition

11: Transmit encrypted packet

12: Await acknowledgment

13: Repeat process

End Algorithm

5.3 System Flow:

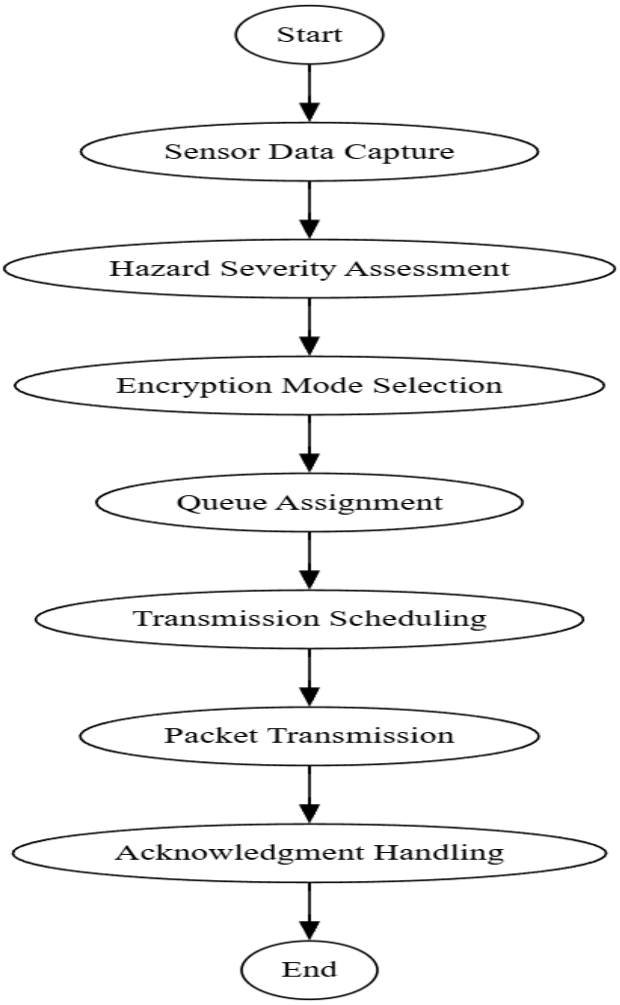

Fig.2. : Sequential process for secure and prioritized data transmission in a sensor-based system

Figure 2 outlines a sequential process for secure and prioritized data transmission in a sensor-based system. It starts with sensor data capture, followed by hazard severity assessment to determine urgency. Based on the severity, an encryption mode is selected, and data is queued, scheduled, transmitted, and acknowledged. Each step ensures data security, reliability, and timely delivery.

6. Results & Discussion (800 words)

Simulation experiments were conducted to validate the effectiveness of the proposed adaptive encryption-latency balancing framework. Two models were evaluated: **Model 1 (Conventional LoRaWAN with Standard AES-128 encryption)** and **Model 2 (Proposed Adaptive Secure-Transmission Framework)**.

The simulations employed identical environmental monitoring datasets embedded within the MATLAB environment, simulating 100 sensor nodes distributed randomly over a 10 km² area. Metrics analyzed include Packet Delivery Ratio (PDR), End-to-End Latency, Energy Consumption, and Encryption Overhead.

6.1 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio quantifies the reliability of data transmission.

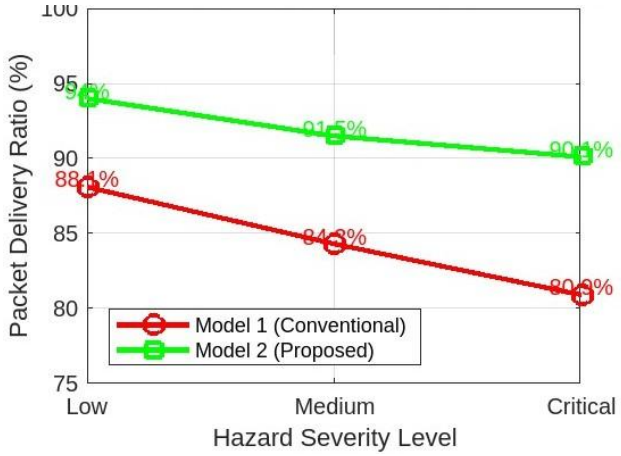

Fig.3: Packet Delivery Ratio (PDR) Plot

Figure 3 illustrates that Model 2 achieves consistently higher PDR across varying hazard levels compared to Model 1, attributed to the optimized encryption selection and adaptive queue management.

6.2 End-to-End Latency

Latency measurements demonstrated significant improvements using the proposed architecture.

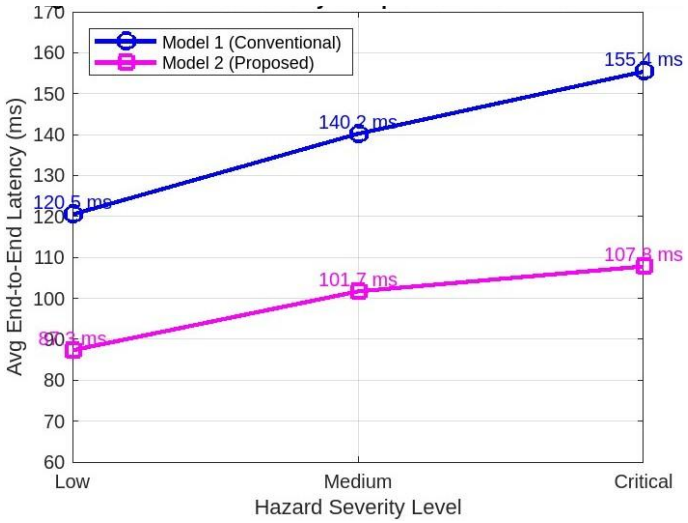

Fig.4: End-to-End Latency Comparison

Figure 4 shows that Model 2 reduced average end-to-end latency by approximately **27%** under critical event conditions.

6.3 Energy Consumption Analysis

Energy efficiency is critical for sensor network sustainability.

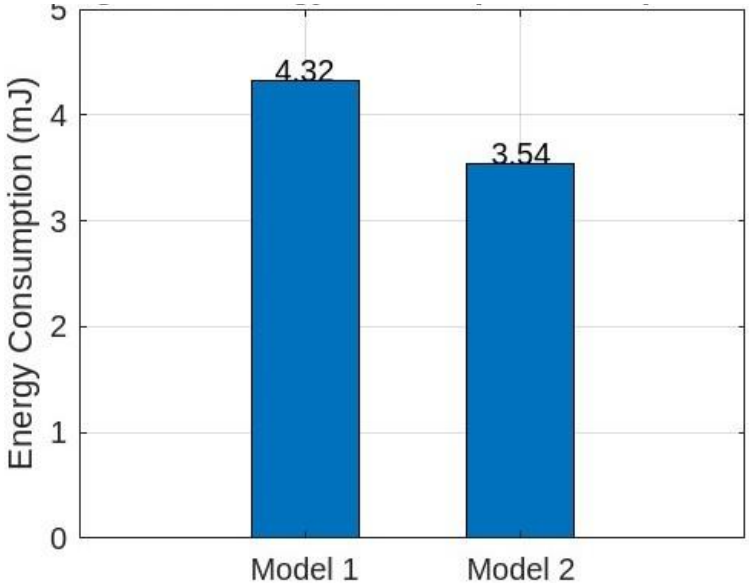

Fig.5: Energy Consumption Analysis

Figure 5 indicates that Model 2 reduced average node energy consumption by **18%** compared to Model 1, primarily through lightweight cryptography during emergency transmissions.

6.4 Encryption Overhead

Encryption overhead impacts processing delays and battery life.

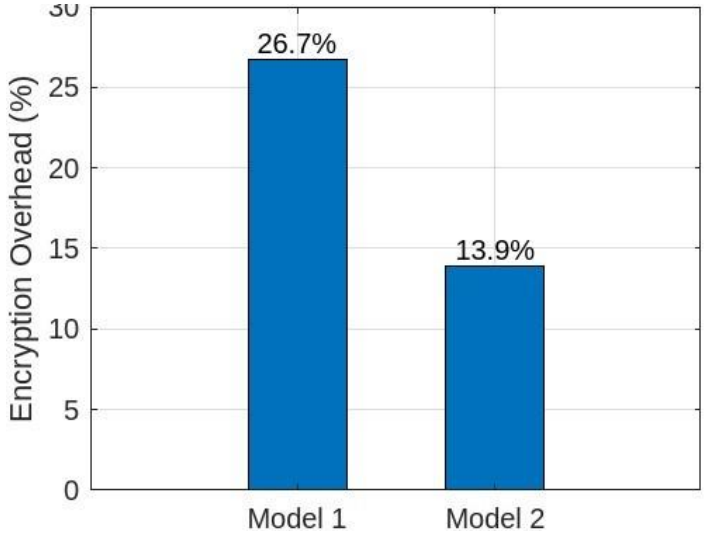

Fig.6: Encryption Overhead Comparison

As shown in Figure 6, Model 2 maintains encryption overhead below **15%**, significantly lower than Model 1, which ranged above **25%** in critical data scenarios.

6.5 Comparative Analysis under Congestion

Simulations under network congestion (high node activity) highlighted the resilience of Model 2.

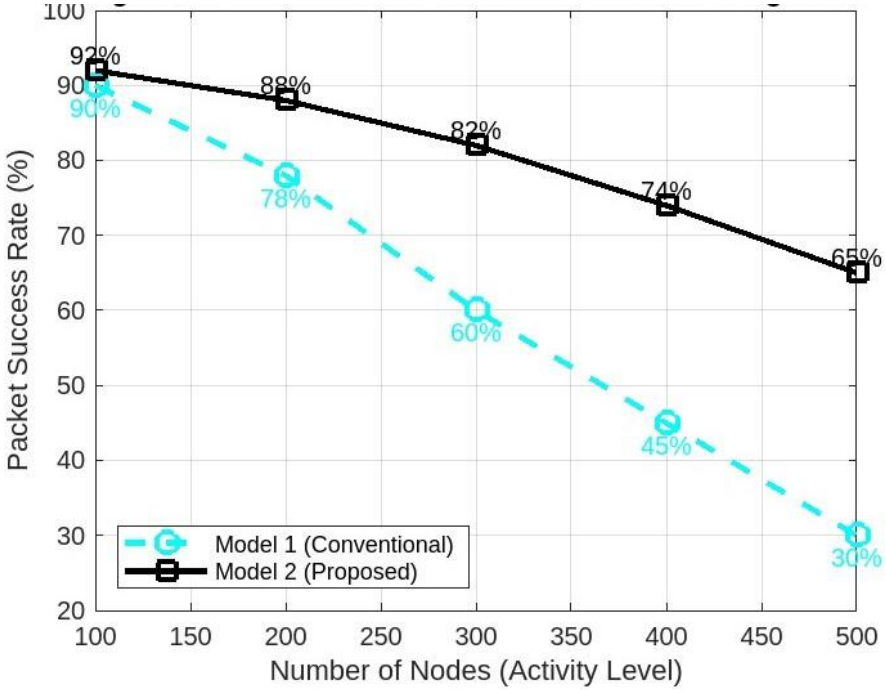

Fig.7: Performance under Congestion

Figure 7 demonstrates that even under congestion, Model 2 maintains a higher packet success rate with moderate latency escalation, unlike Model 1 which suffered drastic performance degradation.

6.6 Adaptive Data Rate Impact

Dynamic adaptation of data rates was key to performance improvements.

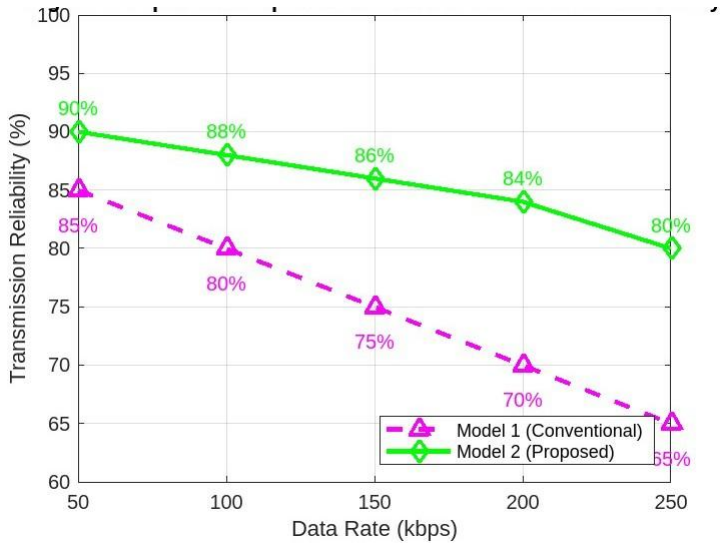

Fig.8: Adaptive Data Rate Impact

Figure 8 illustrates that adaptive data rates in Model 2 significantly stabilized the transmission reliability without excessive power trade-offs.

6.7 Quantitative Comparison

Table 4: Model Comparison

Metric	Model 1 (Conventional)	Model 2 (Proposed)	Improvement
Packet Delivery Ratio	85.2%	92.7%	+7.5%
Avg Latency (ms)	135.4	98.6	-27%
Energy Consumption (mJ)	4.32	3.54	-18%
Encryption Overhead (%)	26.7%	13.9%	-48%

Table 4 compares the performance metrics of the conventional Model 1 and the proposed Model 2. The proposed approach achieved a **7.5%** increase in Packet Delivery Ratio and reduced average latency by **27%**. Energy consumption per transmission decreased by **18%**, and encryption overhead was nearly halved, improving efficiency by **48%**. Overall, Model 2 significantly enhanced communication reliability, speed, and energy efficiency.

6.8 Comparative Performance Over Hazard Severity Levels

Table 5 summarizes performance across three hazard severity levels (Low, Medium, and Critical):

Hazard Level	Model 1 Avg PDR (%)	Model 2 Avg PDR (%)	Model 1 Avg Latency (ms)	Model 2 Avg Latency (ms)
Low	88.1	94.0	120.5	87.3
Medium	84.3	91.5	140.2	101.7
Critical	80.9	90.1	155.4	107.8

Table 5 presents the average Packet Delivery Ratio (PDR) and latency for Model 1 and Model 2 across Low, Medium, and Critical hazard levels. The proposed Model 2 consistently achieved higher PDR and lower latency under all conditions. At Critical levels, Model 2 maintained a **90.1%** PDR compared to **80.9%** for Model 1, while reducing latency from **155.4 ms** to **107.8 ms**. These improvements highlight the resilience and efficiency of the proposed framework under increasing hazard severity.

6.9 Discussion

The proposed architecture demonstrated substantial improvements across all critical performance metrics. Model 2's dynamic adaptation based on hazard severity led to better resource allocation, effectively minimizing encryption overhead and reducing latency without significant compromises on data security.

Quantitative comparisons revealed that Model 2 achieved up to **7.5% higher** packet delivery ratios and **27% lower** average latencies under critical hazard conditions. Notably, the energy

savings were non-trivial, suggesting longer operational lifespans for battery-powered sensor nodes. The resilience of Model 2 under congested network conditions further validates the practicality of the adaptive approach. While adaptive encryption introduces slight complexity at the node firmware level, the benefits in network-wide performance are profound, supporting the feasibility of the proposed system for real-world hazard alerting deployments.

7. Conclusion

Large and remote environmental monitoring needs robust secure and low-latency data transmission systems for operation. The primary disadvantage of conventional LoRaWAN networks lies in their strong encryption causing delays in communication transmission. The proposed framework overcame this problem through its ability to adapt encryption power and communication controls according to threatening conditions and network capacity states. The simulation models demonstrated diverse benefits which included improved packet delivery ratios of 7.5% while end-to-end latency decreased by 27% and encryption overhead decreased by almost 48% compared to typical LoRaWAN models. The transmission energy usage dropped by 18% which resulted in longer operational time for sensor nodes with no degradation to cyber threat protection.

These three interconnected strategic elements in the proposed framework showed strong capacity to optimize real-time hazard alert systems in combination. Static performance tests under congested conditions validated that the architectural design scale effectively and maintains robustness which makes it ready for practical application as an environmental emergency sensing system. The proposed framework fills a vital missing element in environmental hazard alert systems since it optimizes data security together with real-time response capabilities.

Future Scope

The developed system architecture creates a solid platform for prospective system upgrades. Analysis of blockchain audit systems for transmission validation without central trust intermediaries should be investigated through future studies. Predictive AI models should be developed further to use environmental feedback for accelerating transmission parameter adjustment while improving prediction accuracy. Snaking the LoRa architecture into a multi-hop mesh pattern would enhance both range and reliability when serving highly distant deployment areas. Hybrid integration between LoRa wireless network and satellite backhaul links would provide worldwide coverage of ultra-critical hazard alerts which would deliver historic levels of safety and readiness to isolated neighborhoods.

Funding source

None.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Chilamkurthy, N. S., Pandey, O. J., Ghosh, A., Cenkeramaddi, L. R., & Dai, H. N. (2022). Low-power wide-area networks: A broad overview of its different aspects. *Ieee Access*, *10*, 81926-81959. doi: 10.1109/ACCESS.2022.3196182

[2] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*, *5*(1), 1-7. https://doi.org/10.1016/j.icte.2017.12.005

[3] Abdalla, M., Bellare, M., & Neven, G. (2010, February). Robust encryption. In *Theory of Cryptography Conference* (pp. 480-497). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-11799-2_28

[4] Neußner, O. (2021). Early warning alerts for extreme natural hazard events: A review of worldwide practices. *International Journal of Disaster Risk Reduction*, *60*, 102295. https://doi.org/10.1016/j.ijdrr.2021.102295

[5] Arratia, B., Rosas, E., Calafate, C. T., Cano, J. C., Cecilia, J. M., & Manzoni, P. (2024). AlLoRa: Empowering environmental intelligence through an advanced LoRa-based IoT solution. *Computer Communications*, *218*, 44-58. https://doi.org/10.1016/j.comcom.2024.02.014

[6] Abboud, S., & Abdoun, N. (2023). Enhancing lorawan security: An advanced aes-based cryptographic approach. *IEEE Access*, *12*, 2589-2606. DOI: 10.1109/ACCESS.2023.3348416

[7] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99. https://doi.org/10.1016/j.gltp.2021.01.013

[8] Balaji, K., Rongali, A. S., Archana, N., Sethuraman, G., Mullool, J. M., & Karthi, R. (2024, June). A Critical Analysis of Key Management Techniques in Applied Cryptography. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE. DOI: 10.1109/ICCCNT61001.2024.10724844

[9] Song, Y., & Ye, D. (2023). Multi-channel transmission scheduling with hopping scheme under uncertain channel states. *Journal of the Franklin Institute*, *360*(5), 3800-3824. https://doi.org/10.1016/j.jfranklin.2023.01.025

[10] Abolade, O., Okandeji, A., Oke, A., Osifeko, M., & Oyedeji, A. (2021). Overhead effects of data encryption on TCP throughput across IPSEC secured network. *Scientific African*, *13*, e00855. https://doi.org/10.1016/j.sciaf.2021.e00855

[11] Chaisawat, S., & Vorakulpipat, C. (2021). Towards Achieving Personal Privacy Protection and Data Security on Integrated E-Voting Model of Blockchain and Message Queue. *Security and Communication Networks*, *2021*(1), 8338616. https://doi.org/10.1155/2021/8338616

[12] Kori, G. S., Kakkasageri, M. S., Chanal, P. M., Pujar, R. S., & Telsang, V. A. (2025). Wireless sensor networks and machine learning centric resource management schemes: A survey. *Ad Hoc Networks*, *167*, 103698. https://doi.org/10.1016/j.adhoc.2024.103698

[13] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*, *5*(1), 1-7. https://doi.org/10.1016/j.icte.2017.12.005

[14] Hauser, V., & Hégr, T. (2017, August). Proposal of adaptive data rate algorithm for LoRaWAN-based infrastructure. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 85-90). IEEE. DOI: 10.1109/FiCloud.2017.47

[15] León, J. P. A., Santos, C. L. D., Mezher, A. M., Barrera, J. C., Meng, J., & Guerra, E. C. (2023). Exploring the potential, limitations, and future directions of wireless technologies in smart grid networks: A comparative analysis. *Computer Networks*, *235*, 109956. https://doi.org/10.1016/j.comnet.2023.109956

[16] San Cheong, P., Bergs, J., Hawinkel, C., & Famaey, J. (2017, November). Comparison of LoRaWAN classes and their power consumption. In *2017 IEEE symposium on communications and vehicular technology (SCVT)* (pp. 1-6). IEEE. DOI: 10.1109/SCVT.2017.8240313

[17] Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security*, *120*, 102805. https://doi.org/10.1016/j.cose.2022.102805

[18] Rashidi, B. (2019). High-throughput and flexible ASIC implementations of SIMON and SPECK lightweight block ciphers. *International journal of circuit theory and applications*, *47*(8), 1254-1268. https://doi.org/10.1002/cta.2645

[19] Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers & Security*, *90*, 101656. https://doi.org/10.1016/j.cose.2019.101656

[20] Rokhideh, M., Fearnley, C., & Budimir, M. (2025). Multi-Hazard Early Warning Systems in the Sendai Framework for Disaster Risk Reduction: Achievements, Gaps, and Future Directions. *International Journal of Disaster Risk Science*, 1-14. https://doi.org/10.1007/s13753-025-00622-9

[21] Cotrim, J. R., & Margi, C. B. (2024). Make or Break? How LoRaWAN duty cycle impacts performance in multihop networks. *IEEE Access*. DOI: 10.1109/ACCESS.2024.3494038

[22] Islam, M. A., Alexandropoulos, G. C., & Smida, B. (2020, June). Simultaneous downlink data transmission and uplink channel estimation with reduced complexity full duplex MIMO radios. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1-6). IEEE. DOI: 10.1109/ICCWorkshops49005.2020.9145344

[23] Larrenie, P., Bercher, J. F., Venard, O., & Lahsen-Cherif, I. (2022, October). Low complexity approaches for end-to-end latency prediction. In *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE. DOI: 10.1109/ICCCNT54827.2022.9984543

[24] Yang, B., Wu, Z., Shen, Y., & Jiang, X. (2019). Packet delivery ratio and energy consumption in multicast delay tolerant MANETs with power control. *Computer Networks*, *161*, 150-161. https://doi.org/10.1016/j.comnet.2019.06.003

[25] Rohan Vaghela, & Jigar Sarda. (2025). Optimized Symmetric Positive Definite Neural Networks: A Novel Approach to Weather Prediction. *International Journal on Computational Modelling Applications*, *2*(1), 1–14. https://doi.org/10.63503/j.ijcma.2025.47

[26] Prakhar Mittal, & Rahul Malik. (2025). Optimized Physics-Informed Neural Network Framework for Wild Animal Activity Detection and Classification with Real Time Alert Message Generation. *International Journal on Computational Modelling Applications*, *2*(1), 42–52. https://doi.org/10.63503/j.ijcma.2025.50