

Simulation-Based Evaluation of Reliability and Data Continuity in IoT-Based Environmental Quality Monitoring Under Traffic and Failure Scenarios

Andicho Haryus Wirasapta^{1*}, Merisa Rahma Mawaddah², Muhammad Damas Fatih³, Tiara Deta Pamungkas⁴, Octo Gabriel Lumban Tobing⁵, Zeeshan Hamid Malik⁶

^{1,3,5}*Department of Electrical Engineering and Informatics, Faculty of Science and Technology, Universitas Jambi*

²*Department of Mathematics and Natural Sciences, Faculty of Science and Technology, Universitas Jambi*

⁴*Department of Nursing, Politeknik Kesehatan Kementerian Kesehatan Jambi*

⁶*Department of Naval and Industrial Engineering, Ferrol School of Industrial Engineering, University of A Coruña*

*andicho@unja.ac.id

ABSTRACT

Data continuity problems in environmental monitoring systems caused by communication traffic congestion, wireless interference, and component failures make it difficult to maintain accurate and reliable environmental assessment. This paper proposes a simulation framework for evaluating the reliability and data continuity of a distributed IoT-based environmental quality monitoring system under different traffic intensities, wireless interference levels, and component failures. The performance measures are the data delivery ratio (DDR), packet loss ratio (PLR), transmission delay, system availability, mean monitoring interruption duration, and data continuity ratio (DCR), each defined mathematically and reported numerically. Under baseline operation the system achieves DDR = 0.971, PLR = 0.029, and DCR = 0.971. High traffic intensity reduces DDR to 0.71 (DCR = 0.734) and raises the mean transmission delay from about 12 ms to about 99 ms. Combined high traffic and high interference reduce DDR to 0.42 (PLR = 0.58). Gateway failure lowers DCR to 0.612, compared with 0.891 for sensor failure, and the mean interruption lasts 183.5 s versus 48.2 s. Under combined high traffic, high interference, and component failure, DCR falls to 0.487, a 49.8% reduction from the baseline. A sensitivity analysis shows that the failure rate and the gateway recovery rate have the strongest influence on availability, while packet error probability and traffic load have comparable influence on DDR. These results indicate that gateway resilience and communication efficiency are the main determinants of the reliability of IoT-enabled environmental monitoring systems.

Keywords: Environmental Monitoring, IoT Reliability, Data Continuity, Wireless Communication Interference, Failure Modeling.

1. INTRODUCTION

Continuous monitoring of the environment has been found to be very significant in environmental protection, pollution control, and management of resources. Environmental monitoring systems have been utilized to collect various

environmental parameters including the quality of water, air quality, temperature, among others [1]. Continuous and accurate environmental monitoring information has been necessary in the detection of environmental degradation and pollution incidents for environmental management purposes [2]. The increasing application of the Internet of Things (IoT) for environmental monitoring has also increased the need for continuous data collection [3].

With recent advancements in IoT technology, there is now the capability to create environmental monitoring systems that are able to collect data on the environment at different locations in real-time [4]. Environmental monitoring systems based on IoT technology typically comprise of distributed sensors, wireless communications, and a monitoring platform that enables the continuous monitoring and collection of environmental data [5]. [6] found out that methods that incorporate the use of wireless sensor networks together with IoT technology are capable of producing an effective system for monitoring the quality of water. However, this system still faces challenges when it comes to real-time data collection.

Despite all the benefits brought about by IoT technology, there is still the issue of disruptions that may affect the performance of environmental monitoring systems and affect the continuity of data monitoring and collection. Issues such as congestion in communication networks, interference in wireless communications, failure in transmitting packets, and failures within components could greatly affect the capability of the monitoring system in producing timely and accurate data [7].

Reliability is very critical for environmental monitoring systems due to their dependency on constant communication among sensing devices and a centralized environmental monitoring platform [8]. Intensive environmental monitoring will trigger heavy communications between the nodes which result in packet congestion, delay, and losses [9]. In addition, poor wireless communication network environments can pose disturbances during transmissions, impacting monitoring performance as found in simulations of LPWAN and LoRa IoT networks [10].

Apart from communication issues, hardware and infrastructure failure can also cause interruptions in environmental monitoring activities. According to [11] it is very normal for IoT environmental monitoring systems to fail due to hardware malfunctioning, power fluctuations, and environmental conditions, and as a result, there should be a very high availability in systems to be considered efficient. Centralized monitoring infrastructure failures can negatively impact environmental monitoring operations [12].

Several previous studies have investigated IoT-based environmental monitoring systems and wireless sensor network performance under various operational conditions [6], [13], [14], [15], [16]. Nevertheless, existing research efforts tend to address either communication reliability or sensor deployment without examining the reliability of monitoring when subjected to traffic and failure situations. Besides, there have not been sufficient considerations concerning the effect of the connection between communication reliability and the continuation of environmental monitoring.

The novelty of the present work is best read against these approaches. Communication-oriented studies, such as field assessments and simulator comparisons of LoRa-based IoT networks, primarily examine delivery performance as a function of propagation conditions, node density, and interference, without modeling component failure and recovery [9], [10]. Reliability-oriented studies analyze sensor networks mainly through component-level or link-level reliability

models and do not couple them with application-level traffic load or with a metric of monitoring data continuity [15], [17]. Fault-tolerance studies propose redundancy, gateway-layer mesh, load-balancing, or digital-twin schemes to preserve operation after a failure, and generally evaluate the architecture rather than the continuity of the monitoring data [12], [18], [19], [20], [21], [22]. In contrast, the framework proposed here (i) couples a parameterized traffic model, a probabilistic interference model, and a two-state failure and recovery model for both sensing units and the gateway in a single simulation; (ii) introduces the data continuity ratio (DCR), which is measured against the sampling schedule of the monitoring application instead of against transmitted packets only, so that outages of nodes or of the gateway count as lost observations; and (iii) quantifies both the individual and the combined effect of the three disturbance types, supported by closed-form availability expressions and a sensitivity analysis.

Thus, the present study develops a simulation-based analysis framework to examine the reliability and data continuity of IoT-enabled environmental monitoring systems under different traffic levels, communication interference conditions, and component failures. The framework incorporates communication traffic models, communication interference models, and failure and recovery models, and evaluates them through explicitly defined metrics so that the results can be reproduced and compared under realistic operating situations.

Key contributions:

1. A simulation-based approach to assess monitoring reliability under changing traffic conditions, interference levels, and component failures within a single framework.
2. A formal mathematical description of the performance and reliability metrics (DDR, PLR, delay, availability, interruption duration, and DCR) and of how the input parameters (N , T_s , P_e , λ , μ) determine them.
3. Quantitative results for individual and combined disturbances, a sensitivity analysis of the main parameters, and an analytical verification of the failure and recovery sub-model.
4. Engineering implications for gateway redundancy, buffering, and adaptive sampling in environmental monitoring deployments.

The contribution of the current study lies in the understanding of limitations that environmental monitoring systems may face in actual use. It is expected to contribute toward designing robust environmental monitoring infrastructures.

2. MATERIAL AND METHODS

2.1 SYSTEM ARCHITECTURE

In the current research, we focus on a distributed environmental quality monitoring system that can provide constant surveillance and timely recognition of pollution events. The structure of such a monitoring system will include three main components, namely, sensing nodes, a data collection gateway, and a central monitoring system.

The sensing nodes comprise a set of distributed monitoring points positioned in the observed environment. Each sensing unit periodically collects environmental

parameters such as water quality indicators, including pH, turbidity, and temperature. These parameters are selected as representative indicators of environmental quality commonly used to assess changes in environmental conditions [23]. [24] demonstrated a similar distributed WSN-based sensing approach for municipal drinking water quality monitoring, while [25] applied connected IIoT sensor networks to enable real-time water quality observation across multiple monitoring points. The sensing units operate autonomously and generate data at predefined sampling intervals, enabling continuous monitoring over time.

The data aggregation gateway functions as an intermediate node that receives data from multiple sensing units. In addition to aggregating incoming data, the gateway performs temporary buffering to handle variations in incoming traffic and prevent immediate data loss during transient communication disturbances. As a key component involved in data collection and transmission, the gateway is an important link in the process where any possible disruption may greatly affect monitoring continuity [12].

A monitoring platform is required for storing, analyzing, and displaying collected data. Data are analyzed to make sure that environmental assessment and trend monitoring can be conducted effectively. Through such analysis, abnormal patterns or threshold violations that may imply pollution and environmental damage can be detected. Continuous data collection is important for conducting proper environmental monitoring and taking action in time [2].

An overview of the proposed environmental quality monitoring system architecture is shown in Figure 1.

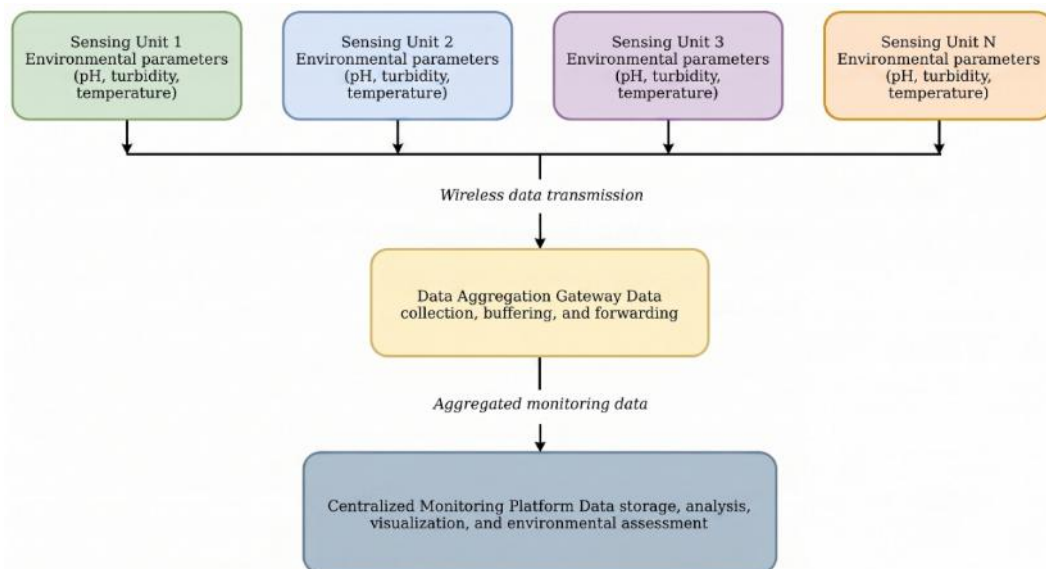


FIGURE 1. Architecture of the Environmental Quality Monitoring System Showing Sensing

2.2 COMMUNICATION AND TRAFFIC MODEL

In the suggested system architecture, each sensor node continuously produces environmental monitoring packets based on a predetermined sampling period. These

monitoring packets contain the environment parameters that have been gathered in a continuous manner from different monitoring points. In view of the fact that sensing nodes are operated concurrently, the total communication load in the proposed system is influenced by the number of active sensing nodes as well as the sampling rate [26].

The entire communication protocol has been modeled based on an uplink periodic transmission from sensing nodes to the gateway where the data contains information about the parameters of the environment, such as pH value, turbidity, and temperature.

The traffic intensity of the monitoring system is regulated through altering the sampling period of the sensing devices. Decreasing the sampling period leads to an increased rate of data packets being generated, hence resulting in more communication traffic [9]. On the other hand, increasing the sampling period reduces the network workload but might affect the resolution of the monitoring process in terms of its reaction time to sudden changes in the environment. To analyze the performance of the system at varying monitoring intensities, three traffic scenarios have been proposed for this experiment. The traffic scenario configurations are summarized in Table 1.

For N active sensing units, each generating one packet of P bytes every sampling interval T_s , the aggregate offered load at the gateway is

$$G = \frac{N}{T_s}, \quad G_b = \frac{8NP}{T_s} \quad (1)$$

Table 1 therefore lists, for each traffic scenario, the number of sensing units, the sampling interval, and the resulting offered load, which increases fifty-fold from 1 to 50 packets/s between the low and the high traffic scenario. Because N and T_s are changed together, each scenario represents a combined change in node count and sampling rate, that we can see the limitations in Section 3.8.

TABLE 1.
Traffic Scenario Configuration

Traffic Scenario	N	T_s (s)	Offered load G (packets/s)	Monitoring Characteristic
Low Traffic	10	10	1	Routine monitoring
Medium Traffic	30	5	6	Periodic intensive monitoring
High Traffic	50	1	50	Real-time intensive monitoring

2.3 INTERFERENCE MODELING

The environmental quality monitoring system using wireless communication is susceptible to several types of communication interferences that could impair data transmission reliability and sustainability of the monitoring process. Interference could come from signal weakening, overlapping wireless communications, physical barriers, electromagnetic interference, and unstable communication environment [27]. These factors could negatively affect the quality of communication and increase the chances of failing to deliver data.

Communication interferences are accounted for in the simulations by implementing packet errors and losses due to probabilistic failures in transmitting packets of monitoring data from sensing nodes to the data aggregation gateway: each transmission fails independently with the packet error probability P_e . The

communication link is expected to have fluctuating interferences affecting the successful delivery of data packets. Routing protocols for air-pollution monitoring WSNs, such as the energy-efficient stable election protocol of [28], are designed to sustain data delivery over unreliable wireless links, which underlines the need to model channel impairments explicitly when evaluating monitoring systems. Three interference conditions are adopted to simulate different communication environments, including low, medium, and high interferences, as shown in Table 2.

TABLE 2.
Interference Scenario Configuration

Interference Level	Packet Error Probability	Communication Condition
Low Interference	0.01	Stable communication
Medium Interference	0.10	Moderate degradation
High Interference	0.30	Severe disturbance

2.4 FAILURE AND RECOVERY MODEL

Alongside the effect of communication disruptions on environmental monitoring systems, such systems could also suffer from component failures that might disrupt monitoring activities and lower data continuity. Sensing unit, communication, and data aggregation components are likely to fail owing to hardware malfunctions, power instabilities, and environmental exposure [11]. These failures can potentially affect the environment observation system and hinder the detection of environmental conditions.

In order to determine the robustness of the system in terms of operational disturbances, this paper presents the failure and recovery processes in the model setting. The failure probability in the sensing unit and gateway data aggregator for the proposed model is considered in the model setting. The failures in the sensing unit result in temporary disruption in collecting environmental information from particular sites, while the failures in the gateway have more severe consequences since the gateway serves as the primary data aggregation and transmission point for the entire system [12].

Each monitored element (a sensing unit or the gateway) is described by a two-state continuous-time Markov model in which the element is either operational or failed. The failure rate λ (s^{-1}) is the transition rate from the operational to the failed state, and the recovery rate μ (s^{-1}) is the transition rate from the failed back to the operational state, so that the mean time to failure is $MTTF = 1/\lambda$ and the mean time to repair is $MTTR = 1/\mu$. The failure and recovery rates used in this paper are presented in Table 3. A sensing-unit failure removes only the affected node from the delivery of observations, whereas a gateway failure interrupts the forwarding of all packets. The availability curves in Figure 4(a) correspond to the representative recovery rates $\mu_s = 0.05 s^{-1}$ and $\mu_g = 0.02 s^{-1}$, which lie within the ranges of Table 3.

TABLE 3.
Failure and Recovery Parameters

Parameter	Symbol	Value range	Unit	Description
Sensor failure rate	λ_s	0.001–0.01	s^{-1}	Operational-to-failed transition rate of a sensing unit
Gateway failure rate	λ_g	0.001–0.010	s^{-1}	Operational-to-failed transition rate of the gateway
Sensor recovery rate	μ_s	0.01–0.10	s^{-1}	Failed-to-operational transition rate of a sensing unit
Gateway recovery rate	μ_g	0.005–0.05	s^{-1}	Failed-to-operational transition rate of the gateway

2.5 SIMULATION SETUP

The suggested environmental quality monitoring system is analyzed using the simulation-based approach in order to study the system reliability and monitoring continuity in changing traffic, interference, and failures. The approach of analyzing systems through simulations prior to their implementation has gained popularity for evaluating IoT and LPWAN-based communications, such as that demonstrated by [29] during their comparative analysis of LoRa and Sigfox performance. In this simulation approach, a distributed environment where environmental monitoring occurs is simulated, consisting of multiple sensing units, a gateway for aggregating data, and a centralized monitoring system. This is explained in detail in the System Architecture part of this paper.

The following operational parameters will be considered within the simulation: the number of sensing units, interval of generating packets, packet size, transmission delay, interference level, and the probability of failure of individual components. Changing these parameters enables studying how the monitoring system works in various environmental monitoring scenarios. A full configuration of the simulation parameters is shown in Table 4.

TABLE 4.
Simulation Parameters

Parameter	Symbol	Value	Description
Number of sensing units	N	10–50	Distributed monitoring points
Sampling interval	T_s	1–10 s	Monitoring data generation interval
Packet size	P	64–256 bytes	Monitoring data payload
Communication delay	D	10–100 ms	Transmission delay
Packet error probability	P_e	0.01–0.30	Communication interference level
Sensor failure rate	λ_s	0.001–0.01 s^{-1}	Sensing unit failure rate
Gateway failure rate	λ_g	0.001–0.010 s^{-1}	Gateway failure rate
Recovery rate	μ	0.01–0.10 s^{-1}	Component recovery rate (Table 3)
Simulation duration	T_{sim}	1000–10 000 s	Total simulation time

The simulation follows a discrete-event procedure in which packet generation [30], failure, and recovery events are processed in time order, as shown in the flowchart in Figure 2. Discrete-event simulation is widely used to evaluate IoT and LoRa-based networks before deployment [10], [29]. The time-resolved results in Figure 6 cover $T_{sim} = 10.000$ s, and the error bars in Figure 5(b) indicate the variability of the mean interruption duration. The implementation details, namely the software platform, the number of independent replications, and the random seeds, were not recorded for this study. The reported values are therefore representative point estimates, and no confidence intervals are given, that we can see in Section 3.8. The simulation code and parameter files can be obtained from the corresponding author upon reasonable request.

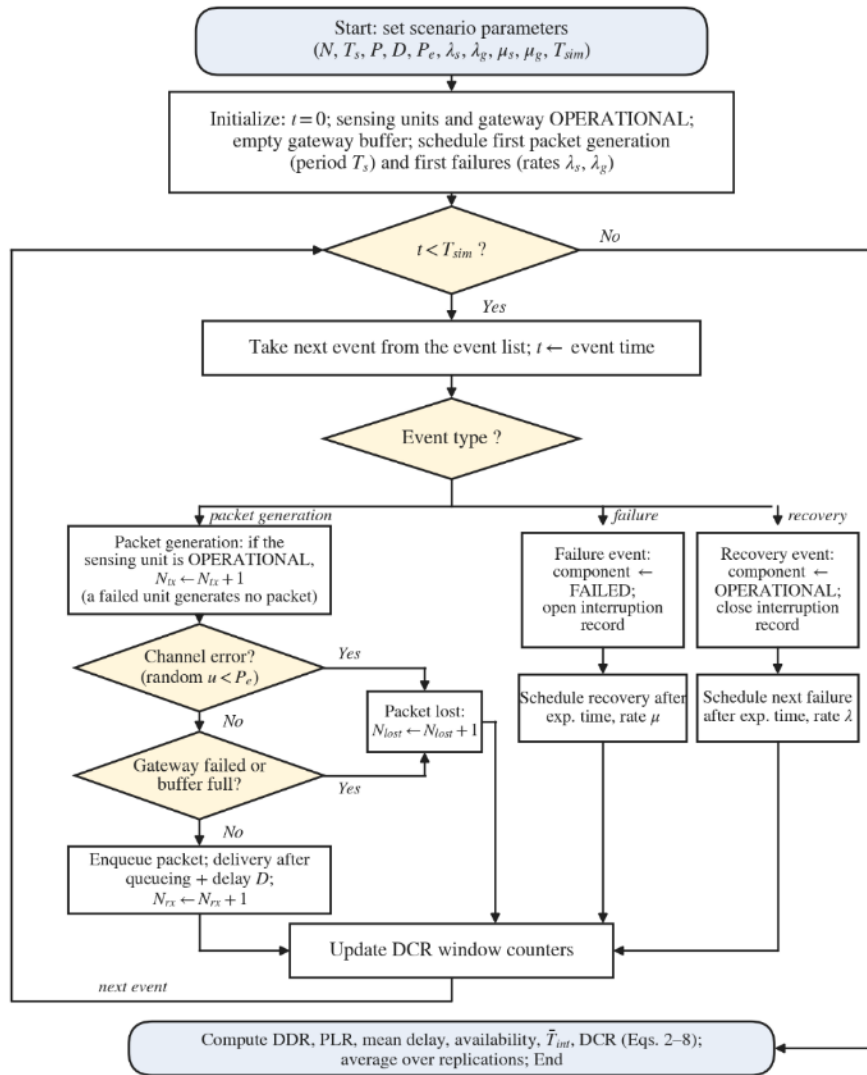


FIGURE 2. Flowchart of the Simulation Procedure

2.6 PERFORMANCE METRICS AND MATHEMATICAL FORMULATION

The system is evaluated with six indicators: the data delivery ratio (DDR), the packet loss ratio (PLR), the mean transmission delay, the system availability, the mean

monitoring interruption duration, and the data continuity ratio (DCR). Numeric indicators of data reliability are an important aspect of IoT monitoring applications [31]. This section defines them mathematically and shows how the input parameters of Table 4 determine them.

Let N_{tx} be the number of packets transmitted by operational sensing units during T_{sim} and N_{rx} the number received by the monitoring platform. Then

$$DDR = \frac{N_{rx}}{N_{tx}}, \quad PLR = 1 - DDR = \frac{N_{lost}}{N_{tx}} \quad (2)$$

A packet is lost either through a channel error, which occurs with probability P_e (Table 2), or through congestion at the gateway (buffer overflow or an unavailable gateway), which occurs with probability P_c . If the two mechanisms act independently,

$$PLR = 1 - (1 - P_c)(1 - P_e) \quad (3)$$

P_c is not an input: it is an output of the simulation that grows with the offered load G in Eq. (1) and with the fraction of time during which the gateway is failed. Increasing N or reducing T_s therefore raises P_c , whereas P_e is set directly by the interference level. The mean transmission delay is

$$\bar{D} = \frac{1}{N_{rx}} \sum_{i=1}^{N_{rx}} (t_i^{rx} - t_i^{gen}) \quad (4)$$

where t_i^{gen} and t_i^{rx} are the generation and reception times of packet i . The delay of a packet comprises the link delay D (Table 4) and the waiting time in the gateway buffer, which grows with G . For a component $i \in \{s, g\}$ (sensing unit or gateway) with failure rate λ_i and recovery rate μ_i , the steady-state availability of the two-state model is

$$A_i = \frac{MTTF}{MTTF + MTTR} = \frac{\mu_i}{\lambda_i + \mu_i}, \quad i \in \{s, g\} \quad (5)$$

with $MTTF = 1/\lambda_i$ and $MTTR = 1/\mu_i$. Because every observation must pass through both a sensing unit and the gateway, the two components act in series and the system availability is

$$A_{sys} = A_s A_g \quad (6)$$

Eqs. (5) and (6) show how λ and μ are translated into availability: availability decreases with λ and increases with μ , and the gateway term has the larger effect because a gateway failure affects all N sensing units at once, whereas a sensing-unit failure affects only one. A monitoring interruption is a contiguous interval in which the affected observations do not reach the monitoring platform. With K interruption events that start at t_k^{start} and end at t_k^{end} , the mean interruption duration is

$$\bar{T}_{int} = \frac{1}{K} \sum_{k=1}^K (t_k^{end} - t_k^{start}) \quad (7)$$

The data continuity ratio compares the observations actually received with those expected from the sampling schedule. Over a window of length Δ ending at time t , $N\Delta/T_s$ observations are expected, so

$$DCR(t) = \frac{N_{rx}(t-\Delta, t]}{N \Delta / T_s} \quad (8)$$

The summary DCR of a scenario uses $\Delta = T_{sim}$. In contrast to DDR, whose denominator counts only packets that were actually transmitted, the denominator of

DCR is fixed by the schedule, so observations that were never generated because a sensing unit was failed, or never forwarded because the gateway was failed, reduce DCR. A DCR of 0.70 is used as the minimum acceptable continuity level in the analysis (dashed line in Figure 6). Finally, the sensitivity of an output M to an input x is measured by its absolute and relative change over the tested range of x , with all other inputs at their reference values:

$$\Delta M_x = M(x_{max}) - M(x_{min}), \quad \delta M_x = \frac{\Delta M_x}{M(x_{min})} \times 100\% \quad (9)$$

2.7 MODEL VERIFICATION AND VALIDATION APPROACH

Verification and validation are carried out at two levels. First, the failure and recovery sub-model is verified analytically by comparing the simulated availability with the closed-form expressions in Eqs. (5) and (6) (Section 3.7). Second, the behavior of the simulated metrics is compared with empirical and simulation findings reported in previous studies, namely the effect of node density and error probability on delivery, the role of the gateway as a single point of failure, and the effect of concurrent failures [10], [12], [17], [21]. A hardware testbed has not been used in this work, and the consequences of this are discussed in Section 3.8.

3. RESULTS AND DISCUSSION

3.1. BASELINE SYSTEM PERFORMANCE

First, the baseline scenario was tested for the evaluation of the normal operation of the proposed environmental quality monitoring system with stable communication without any interference or component failure. Under the baseline scenario, sensors operated with the low-traffic approach where there were minimal packet losses during their operation, and all system components were working correctly.

Simulation findings show that the proposed monitoring model is capable of stable communication and environmental observation under normal operation. Under the baseline scenario, DDR was 0.971 and PLR was 0.029, meaning that 97.1% of the monitoring packets reached the monitoring platform, with a mean transmission delay of about 12 ms (Figure 3(a)). The remaining 2.9% loss reflects the residual channel error of the stable-communication setting ($P_e = 0.01$) and minor buffering effects at the gateway, and no component failure occurred. Such findings are similar to those presented by [2], who found that stable IoT-based environmental monitoring systems are capable of sustaining high acquisition of environmental data even when operating normally. [13] confirmed that the IoT-based environment monitoring system operates successfully under tropical climate conditions.

System availability was 1.000 because no component failure events were injected in this scenario, so monitoring continued without interruption during the entire simulation time and DCR equaled 0.971. The baseline performance indicators are summarized in Table 5, and each value can be traced to Figure 3(b) and Figure 6(b).

TABLE 5.
Baseline System Performance

Performance indicator	Symbol	Value
Data delivery ratio	DDR	0.971
Packet loss ratio	PLR	0.029
Mean transmission delay	$\bar{D}$	≈ 12 ms
System availability	A_{sys}	1.000
Mean interruption duration	$\bar{T}_{\text{int}}$	0 s
Data continuity ratio	DCR	0.971

3.2. IMPACT OF TRAFFIC INTENSITY ON MONITORING PERFORMANCE

The influence of communication traffic volume on the efficiency of environmental monitoring processes was assessed by analyzing the system operation under low, moderate, and high traffic volumes. Communication traffic volume was manipulated through the variation of the frequency of sensing unit sampling, where reduced sampling intervals resulted in an increased number of monitoring packets and enhanced communication activities in the network.

According to the simulation results, the growth in communication traffic volume had a significant effect on communication activity and monitoring continuity. Under low traffic ($N = 10$, $T_s = 10$ s, 1 packet/s), the monitoring system operated stably with $DDR = 0.97$, $PLR = 0.03$, and a mean delay of about 12 ms, and no sign of congestion was observed at the gateway, which supports the findings of [6] who concluded that WSN-IoT systems operate effectively when experiencing light communication traffic loads. [10] showed in simulation experiments for LoRa IoT networks that growing node density increases collision and packet error probabilities, which is consistent with the trend observed here at higher N .

Under medium traffic ($N = 30$, $T_s = 5$ s, 6 packets/s), the gateway workload increased: DDR fell to 0.88 ($PLR = 0.12$), the mean delay rose to about 25 ms, and DCR was 0.882, so the monitoring process remained continuous but packet buffering became evident. The worst performance occurred under high traffic ($N = 50$, $T_s = 1$ s, 50 packets/s), where constant packet generation by many sensors congested the gateway: DDR dropped to 0.71 ($PLR = 0.29$), the mean delay reached about 99 ms, roughly eight times the low-traffic value, and DCR fell to 0.734, close to the 0.70 threshold. The effect of traffic intensity on performance is shown in Table 6, while Figure 3 shows its effect on transmission delay and DDR .

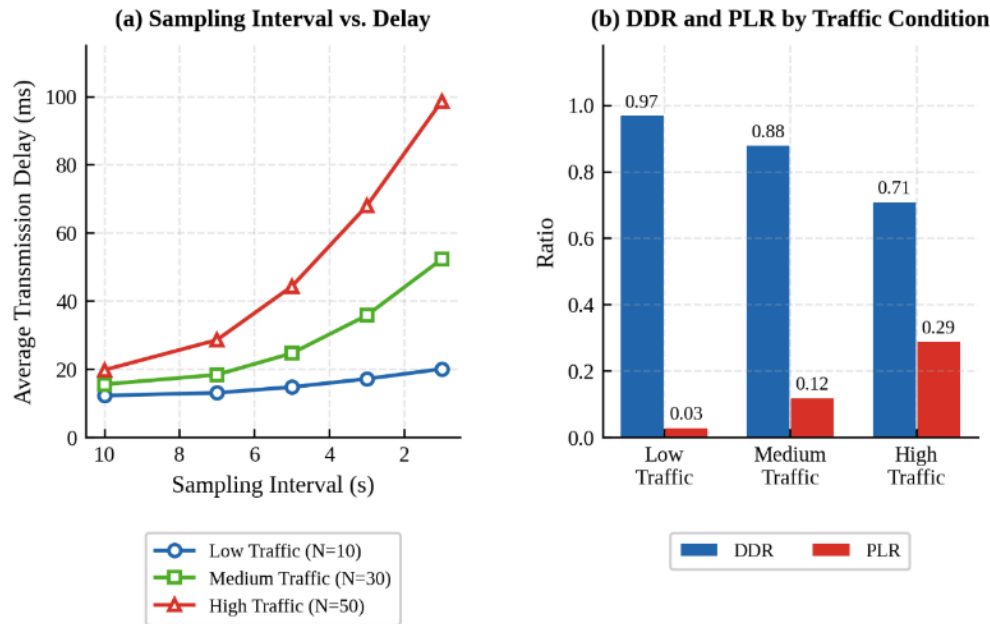


FIGURE 3. (a) Effect of Traffic Intensity on Transmission Delay and (b) Data Delivery Ratio with Packet Loss Rate Within the Environmental Monitoring System

TABLE 6.
Effect of Traffic Intensity on Monitoring Performance

Traffic condition	N	T_s (s)	G (packets/s)	Mean delay (ms)	DDR	PLR	DCR
Low traffic	10	10	1	≈ 12	0.97	0.03	0.956
Medium traffic	30	5	6	≈ 25	0.88	0.12	0.882
High traffic	50	1	50	≈ 99	0.71	0.29	0.734

From the point of view of environmental management, these findings reveal that increased monitoring intensity could harm monitoring effectiveness when the availability of communication resources is limited. While high sampling rates produce better temporal resolution of environmental measurements, they are likely to result in greater communication overhead and decreased system stability [9]. For example, shortening the sampling interval from 5 s to 1 s, together with an increase of the node count from 30 to 50, improved temporal resolution fivefold but cost 0.17 in DDR and about 74 ms in additional delay. This limitation was emphasized further by [16] when discussing environmental monitoring in wireless sensor networks.

3.3. IMPACT OF COMMUNICATION INTERFERENCE

Different communication interference situations were investigated to evaluate the proposed system's performance in terms of the reliability of the monitoring scheme when exposed to poor communication situations. The levels of communication interference were depicted via different levels of probability of packet losses in transmission in cases of low, moderate, and high-interference situations.

In the low-interference case ($P_e = 0.01$), the communication process was hardly affected: DDR was 0.97 under low traffic and DCR was 0.953. In the moderate-interference case ($P_e = 0.10$), performance started to deteriorate: DDR decreased to 0.89 (PLR = 0.11) under low traffic and to 0.76 under medium traffic, and DCR dropped to 0.847.

The most severe degradation occurred under high interference ($P_e = 0.30$). Frequent communication disturbances caused substantial packet loss and unstable data delivery: DDR fell to 0.71 under low traffic, 0.58 under medium traffic, and 0.42 under high traffic, and the single-factor DCR dropped to 0.673, below the 0.70 threshold. This is consistent with findings reported by [32] regarding interference impacts on IoT monitoring systems. [17] further confirmed through Markov-based WSN reliability analysis that increasing error probability significantly reduces component-level and system-level reliability indices. The impact of communication interference on DDR is illustrated in Figure 4, and the numerical results are given in Table 7.

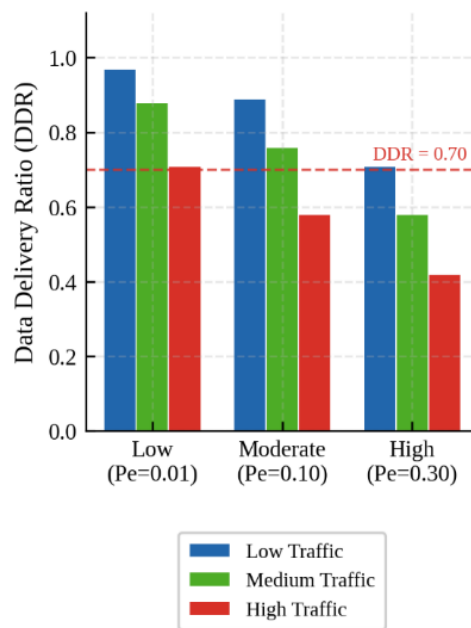


FIGURE 4. Data Delivery Ratio (DDR) under Combined Traffic and Interference Scenarios

TABLE 7.
Effect of Communication Interference on Monitoring Reliability

Interference level	P_e	DDR (low traffic)	DDR (medium traffic)	DDR (high traffic)	DCR (single factor)	DCR vs. 0.70
Low	0.01	0.97	0.88	0.71	0.953	Above
Moderate	0.10	0.89	0.76	0.58	0.847	Above
High	0.30	0.71	0.58	0.42	0.673	Below

Note: PLR = 1 - DDR (Eq. 2); DDR values are read from Figure 4.

The results also indicate that communication interference amplifies the impact of high traffic intensity. Under combined high-traffic and high-interference conditions the communication channel experienced both congestion and transmission instability: DDR reached 0.42 and PLR 0.58, a reduction of 0.55 in DDR relative to the baseline. This reduction slightly exceeds the sum of the individual reductions (0.26 for traffic and 0.26 for interference), so the two disturbances interact rather than act independently. This study emphasizes the significance of data quality control in IoT surveillance systems, as shown in [33], who found that deterioration in the quality of IoT data can adversely affect the performance of environmental models. Similarly, [34] stated that the reliability of sensor data plays an important role in IoT-based air quality surveillance systems.

3.4. IMPACT OF COMPONENT FAILURES

The impact of component failures on monitoring reliability was studied by simulating failures of sensing units and of the data aggregation gateway. The results show that the impact is highly significant, especially for the key aggregation component: DCR fell to 0.891 under sensor failure and to 0.612 under gateway failure, compared with 0.971 in the baseline.

Failures of sensing units led to localized problems because the affected units could not collect environmental information. The other sensors remained operational, so data collection was incomplete only at the missing monitoring points, and the mean interruption lasted 48.2 s. Gateway failures had a larger effect because the gateway is the aggregation point and the forwarding point toward the monitoring platform: the transmission of data from all sensing units stopped, producing a system-wide interruption with a mean duration of 183.5 s, about 3.8 times longer than for sensor failure. This finding corroborates the research of [12], which showed that gateways of IoT systems are prone to becoming single points of failure that can leave the entire system inoperable. Several remedies have been proposed: [18] presented a dual base station model that maintains IoT fault tolerance, [19] proposed triplicated IoT devices with software-based digital twins to tolerate sensor-level faults, and deep learning-based techniques have been considered to improve fault tolerance at the gateway layer [35].

Concurrent failures arising from communication disruption and individual component failures caused the greatest impact on the system, with a mean interruption of 247.8 s and a DCR of 0.487. These effects on system availability and monitoring interruptions are illustrated in Figure 5, and the numerical results are given in Table 8. System availability, calculated with Eqs. (5) and (6), decreased from 0.98 to 0.83 for sensor failure, from 0.95 to 0.67 for gateway failure, and from 0.93 to 0.56 for combined failure as the failure rate λ increased from 0.001 to 0.010 s⁻¹. [21] found that concurrent failures between nodes and links in IoT-based metering systems lead to longer service disruptions than single-node failures, which is in line with the longer interruption observed here for the combined case.

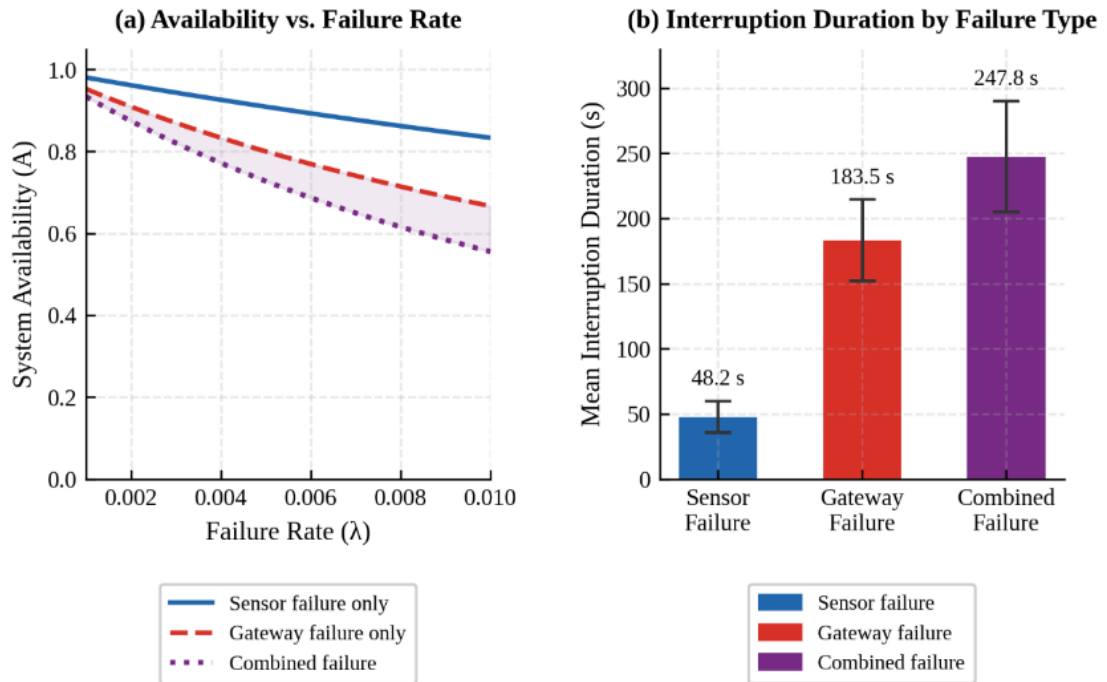


FIGURE 5. (a) Effect of Component Failures on System Availability as a Function of Failure Rate and (b) Mean Monitoring Interruption Duration by Failure Type

TABLE 8.
Effect of Component Failures on Monitoring Reliability

Failure scenario	System availability ($\lambda = 0.001\text{-}0.010\text{ s}^{-1}$)	Mean interruption duration (s)	DCR
Sensor failure	0.98-0.83	48.2	0.891
Gateway failure	0.95-0.67	183.5	0.612
Combined failure	0.93-0.56	247.8	0.487

3.5. OVERALL RELIABILITY ANALYSIS AND ENVIRONMENTAL IMPLICATIONS

The general outcome of the simulation shows that reliability in monitoring is largely dependent on the level of traffic, communication disturbances, and failure of components. As monitoring traffic levels rise, there will be an increase in the number of observations made in the environment, but this will also create more communication traffic. The interference in communication contributes to reducing monitoring reliability due to packet losses and transmission errors [9]. [15] observed similar trends in the reliability assessment of WSNs.

Table 9 consolidates the numerical results of all scenarios, and the values quoted in the abstract are taken directly from this table.

TABLE 9.
Summary of Numerical Results for All Scenarios

Scenario	Configuration	DDR	PLR	DCR
Baseline	$N = 10, T_s = 10 \text{ s}, P_e = 0.01$, no failure	0.971	0.029	0.971
Low traffic	$N = 10, T_s = 10 \text{ s}$	0.97	0.03	0.956
Medium traffic	$N = 30, T_s = 5 \text{ s}$	0.88	0.12	0.882
High traffic	$N = 50, T_s = 1 \text{ s}$	0.71	0.29	0.734
Low interference	$P_e = 0.01$	0.97	0.03	0.953
Moderate interference	$P_e = 0.10$	0.89	0.11	0.847
High interference	$P_e = 0.30$	0.71	0.29	0.673
High traffic + high interference	$N = 50, T_s = 1 \text{ s}, P_e = 0.30$	0.42	0.58	-
Sensor failure	λ_s only	-	-	0.891
Gateway failure	λ_g only	-	-	0.612
Combined (high traffic + high interference + failure)	$N = 50, T_s = 1 \text{ s}, P_e = 0.30$, failures	-	-	0.487

Note: - = not available from the simulation output; the failure scenarios were evaluated through DCR and interruption duration.

Gateway faults were found to generate the most significant impact on monitoring continuity among all other considered scenarios since the gateway is the key component for communication and data integration purposes. This observation corroborates the findings of previous studies examining fault tolerance in IoT architectures, in which centralized gateway components were identified as major vulnerabilities requiring proper recovery mechanisms [22]. The significance of recovery design in ensuring reliable operation of IoT systems was also noted in general IoT architecture reliability investigations [36]. In addition, the results of the simulations revealed that recovery mechanisms are vital for ensuring continuity of operations, as fast recovery capacity contributes significantly to increased availability and reduced monitoring downtime periods. [35] demonstrated that load balancing of computational resources in IoT networks using microcontroller networking techniques could alleviate single point recovery constraints and enhance resilience of IoT systems.

In terms of environmental monitoring, the need to collect continuous data is necessary to ensure accurate environmental evaluation and the early detection of any pollution incidents. The lack of information about the environment due to communication issues or equipment breakdowns can limit the accuracy of environmental management decisions and affect monitoring efforts [33]. It is especially true in water quality monitoring where continuous data collection is crucial for identifying environmental change and supplying safe water [37]. Figure 5 illustrates monitoring DCR over simulation time and all assessed scenarios.

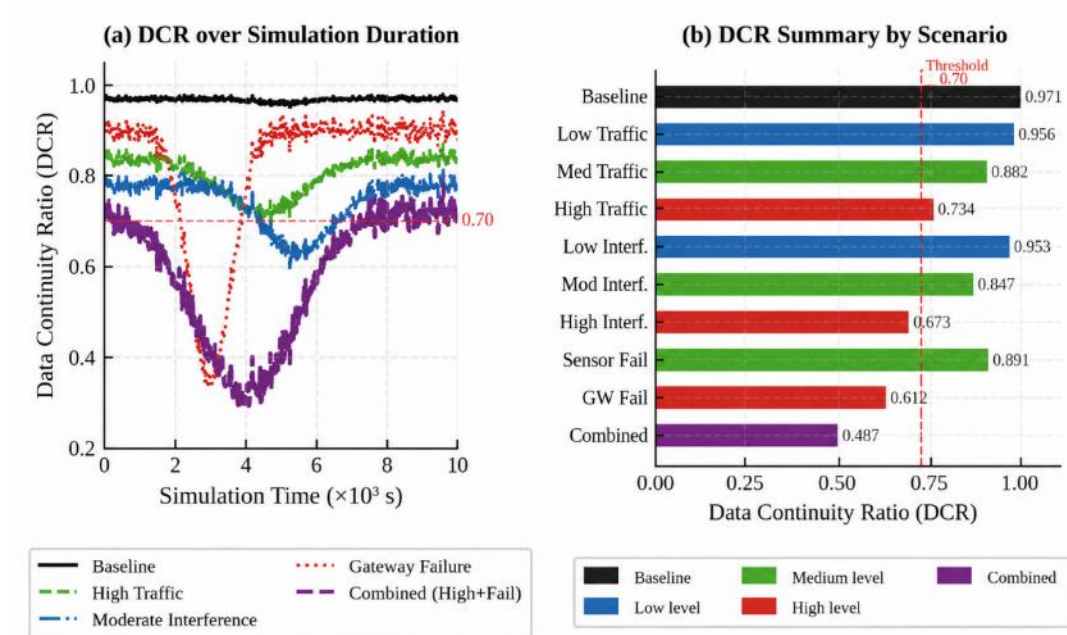


FIGURE 6. (a) Monitoring Data Continuity Ratio (DCR) over Simulation Duration under Different Operational Scenarios and (b) DCR Summary Comparison across All Evaluated Scenarios

The baseline scenario had the highest DCR (0.971) since the communication environment was stable and there were no operational disruptions, as illustrated in Figure 6. High traffic gave the lowest DCR among the traffic scenarios (0.734) because the communication environment was busy with packet buffering. Communication interference caused further drops (0.847 at moderate and 0.673 at high interference) because of packet transmission failures and failed data deliveries. Gateway failure reduced DCR to 0.612, and the worst case, the joint effect of high traffic, high interference, and component failure, reduced DCR to 0.487, which is 49.8% below the baseline and severely interrupted the environmental monitoring process.

The simulation model sheds light on the operational challenges and vulnerability factors involved in distributed monitoring systems in the context of real-world disturbances. Generally, it is important to note that distributed environmental monitoring systems provide the key basis for implementing environmentally sustainable strategies and programs aimed at controlling and detecting environmental hazards [2]. Edge computing integration with an IoT-based monitoring system has also proven to increase robustness and reduce latency in operation [14].

3.6. SENSITIVITY ANALYSIS

A one-at-a-time sensitivity analysis was carried out over the parameter ranges of Tables 1-4, with all other parameters held at their reference values. Table 10 reports the change in each output between the lowest and the highest tested value of the parameter (Eq. 9). The traffic and interference rows are taken from the simulation

results in Figures 3 and 4, and the availability rows are obtained from Eqs. (5) and (6), which reproduce Figure 5(a) (Section 3.7).

TABLE 10.
Sensitivity of the Main Outputs to the Input Parameters

Parameter varied	Output M	$M(x_{\min})$	$M(x_{\max})$	ΔM	δM
Traffic load (N, T_s): low $\rightarrow$ high	DDR	0.97	0.71	-0.26	-26.8%
Traffic load (N, T_s): low $\rightarrow$ high	Mean delay (ms)	≈ 12	≈ 99	+87	$\times 8$
P_e : 0.01 $\rightarrow$ 0.30 (low traffic)	DDR	0.97	0.71	-0.26	-26.8%
P_e : 0.01 $\rightarrow$ 0.30 (medium traffic)	DDR	0.88	0.58	-0.30	-34.1%
P_e : 0.01 $\rightarrow$ 0.30 (high traffic)	DDR	0.71	0.42	-0.29	-40.8%
λ_s : 0.001 $\rightarrow$ 0.010 s^{-1} (sensor)	Availability	0.98	0.83	-0.15	-15.0%
λ_g : 0.001 $\rightarrow$ 0.010 s^{-1} (gateway)	Availability	0.95	0.67	-0.29	-30.0%
λ : 0.001 $\rightarrow$ 0.010 s^{-1} (combined)	Availability	0.93	0.56	-0.38	-40.5%

Note: the failure-rate rows use $\mu_s = 0.05 s^{-1}$ and $\mu_g = 0.02 s^{-1}$.

Three observations follow. First, availability is the most sensitive output: raising λ from 0.001 to 0.010 s^{-1} reduces the availability of the combined system by 0.38 (-40.5%), that of the gateway alone by 0.29, and that of the sensing units by only 0.15, so the gateway failure rate is the most influential single parameter. Second, delivery is sensitive to load and to channel quality to a similar extent: increasing P_e from 0.01 to 0.30 lowers DDR by 0.26-0.30 in absolute terms, and the relative loss grows with traffic (-27% at low traffic against -41% at high traffic), which confirms the interaction between traffic and interference. Third, the recovery rate is as influential as the failure rate. Table 11 shows that raising μ_g from 0.005 to 0.05 s^{-1} at $\lambda_g = 0.005 s^{-1}$ lifts the gateway availability from 0.50 to 0.91, so a tenfold faster recovery more than offsets a fivefold higher failure rate ($A_g = 0.91$ at $\lambda_g = 0.005$ and $\mu_g = 0.05$, against 0.83 at $\lambda_g = 0.001$ and $\mu_g = 0.005$). This quantifies why recovery mechanisms contribute strongly to the availability of the system.

TABLE 11.
Gateway Availability A_g as a Function of Failure and Recovery Rates (Eq. 5)

$\lambda_g (s^{-1})$	$\mu_g = 0.005$	$\mu_g = 0.010$	$\mu_g = 0.020$	$\mu_g = 0.050$
0.001	0.833	0.909	0.952	0.980
0.003	0.625	0.769	0.870	0.943
0.005	0.500	0.667	0.800	0.909

Note: values are analytical (Eq. 5). One-at-a-time variation ignores interactions other than traffic and interference, and N and T_s were varied together (Table 1).

3.7. MODEL VERIFICATION AND COMPARISON WITH PREVIOUS STUDIES

The failure and recovery sub-model were verified against its analytical solution. With $\mu_s = 0.05 s^{-1}$ and $\mu_g = 0.02 s^{-1}$, Eqs. (5) and (6) give availabilities of 0.98, 0.95, and 0.93 at $\lambda = 0.001 s^{-1}$ and 0.83, 0.67, and 0.56 at $\lambda = 0.010 s^{-1}$ for sensor, gateway,

and combined failure, respectively. These values coincide with the simulated curves in Figure 5(a) to within the resolution of the plot (about ± 0.01), which confirms that the simulated outages follow the intended exponential failure and repair process.

The behavior of the simulated metrics was then compared with findings reported in previous studies. Table 12 lists the main trends. In every case the direction of the effect agrees with the literature.

TABLE 12.
Comparison of Simulated Trends with Previous Studies

Aspect	Present simulation	Previous studies	Ref.	Agreement
Node density and traffic load	DDR $0.97 \rightarrow 0.71$ and delay $\approx 12 \rightarrow \approx 99$ ms as N rises from 10 to 50	Growing node density increases collisions and packet error probability in LoRa networks	[10]	Same direction
Channel error	DDR falls by 0.26–0.30 as P_e rises from 0.01 to 0.30	Increasing error probability reduces component-level and system-level reliability	[17]	Same direction
Gateway as single point of failure	Gateway failure: DCR 0.612 and 183.5 s outage, against 0.891 and 48.2 s for sensors	Gateways are prone to becoming single points of failure; centralized gateways are major vulnerabilities	[12], [22]	Same direction
Concurrent failures	Combined failure: 247.8 s mean interruption, longer than 183.5 s	Concurrent node and link failures cause longer service disruptions than single-node failures	[21]	Same direction

This agreement supports the qualitative realism of the model, but it is not a quantitative validation. The absolute values of DDR, delay, and DCR depend on the assumed parameters (Table 4) and on the gateway buffering behavior, and they have not been compared with measurements from a physical IoT testbed.

3.8. ENGINEERING IMPLICATIONS AND LIMITATIONS

Gateway redundancy. Gateway failure produced the longest single-component interruption (183.5 s) and the largest availability loss, so the gateway is the first element that should be duplicated. Under the assumption of independent failures, an active pair of identical gateways has an availability of $1 - (1 - A_g)^2$. With $\mu_g = 0.02 \text{ s}^{-1}$, this raises A_g from 0.80 to 0.96 at $\lambda_g = 0.005 \text{ s}^{-1}$ and from 0.952 to 0.998 at $\lambda_g = 0.001 \text{ s}^{-1}$. These are analytical projections rather than simulation results, and they ignore common-cause failures and the failover time. They indicate that a second gateway is far more effective than improving sensor reliability, because the sensing-unit term reduced availability by only 0.15 over the whole range.

Fault-tolerant architecture and buffering. The mean outages of 183.5 s (gateway) and 247.8 s (combined) can be bridged by local buffering with store-and-forward after recovery, which converts lost observations into delayed ones and preserves DCR at the cost of latency. At the generation rates of Table 1, an outage of 183.5 s corresponds to about 184 packets at 1 packet/s, 1101 packets at 6 packets/s, and 9175 packets at 50 packets/s. With payloads of 64–256 bytes (Table 4), the high-traffic case needs

roughly 0.6–2.3 MB of buffer, which exceeds the on-chip RAM of many microcontroller-class gateways, so flash or external memory would be required.

Adaptive sampling. The degradation of DDR doubles between medium and high traffic (-0.09 from low to medium, -0.17 from medium to high), while the delay grows from about 25 ms to about 99 ms. Reducing T_s from 5 s to 1 s is therefore justified only when the environment changes quickly. An adaptive scheme that samples at the long interval by default, shortens it only when a threshold is crossed, and lengthens it again when the gateway reports congestion or a failed state would keep the system near the medium-traffic operating point ($DDR \approx 0.88$) for most of the time. Because DDR falls below 0.70 at high interference even under low traffic, the scheme should also react to a rising packet error rate.

Limitations. All values come from simulation with the parameters of Tables 1-4, and no hardware testbed validation was performed. The number of replications and the random seeds were not recorded, so the results are representative point estimates without confidence intervals. N and T_s were varied together, so their individual effects cannot be separated. The sensitivity analysis is one-at-a-time. The model assumes a single-hop star topology with one gateway, independent failures with the sensing units and the gateway in series, and no correlated (common-cause) failures. Future work should validate the framework on an IoT testbed, extend it to multi-gateway and multi-hop topologies, and include correlated failures.

4. CONCLUSION

The simulation approach proposed in this research can be used to assess the reliability and continuity of data transmission in IoT-enabled environmental monitoring systems under different levels of traffic intensity, communication interference, and component failure. The simulation results show that traffic intensity causes delays and packet accumulation (DDR fell from 0.97 to 0.71 and the delay rose from about 12 ms to about 99 ms), while interference causes packets to be dropped, resulting in irregular delivery of information ($DDR = 0.71, 0.58, \text{ and } 0.42$ at $P_e = 0.30$ under low, medium, and high traffic). In particular, gateway failure had the largest effect on availability and continuity ($DCR = 0.612$, and a mean interruption of 183.5 s) because the gateway plays a pivotal role in collecting and transmitting packets, and the combined disturbance reduced DCR to 0.487, a 49.8% reduction from the baseline. The sensitivity analysis showed that the failure rate and the recovery rate dominate availability, so appropriate recovery strategies and gateway redundancy can minimize interruptions in data transmission. These results imply that the reliability of the monitoring system depends greatly on communication quality and system robustness. In the context of environmental management, reliable and consistent information delivery is vital for detecting abnormalities in the monitored areas, and it is therefore important to design efficient monitoring systems capable of operating consistently for long periods. Future work will validate the framework on an IoT testbed and extend it to multi-gateway topologies and correlated failures.

REFERENCES

- [1] A. Y. Cil, D. Abdurahman, and I. Cil, "Internet of Things enabled real time cold chain monitoring in a container port," *Journal of Shipping and Trade*, vol. 7, no. 1, p. 9, Dec. 2022, doi: 10.1186/s41072-022-00110-z.
- [2] S. Ranjan Laha, B. K. Pattanayak, and S. Pattnaik, "Advancement of Environmental Monitoring System Using IoT and Sensor: A Comprehensive Analysis," *AIMS Environ. Sci.*, vol. 9, no. 6, pp. 771–800, 2022, doi: 10.3934/environsci.2022044.
- [3] A. I. A. Alzahrani, S. H. Chauhdary, and A. A. Alshdadi, "Internet of Things (IoT)-Based Wastewater Management in Smart Cities," *Electronics (Basel)*, vol. 12, no. 12, p. 2590, Jun. 2023, doi: 10.3390/electronics12122590.
- [4] S. L. Ullo and G. R. Sinha, "Advances in Smart Environment Monitoring Systems Using IoT and Sensors," *Sensors*, vol. 20, no. 11, p. 3113, May 2020, doi: 10.3390/s20113113.
- [5] D. R. Ramani, B. Ben Sujitha, and S. Tangade, "Smart Environmental Monitoring Systems," in *Environmental Monitoring Using Artificial Intelligence*, Wiley, 2025, pp. 45–60. doi: 10.1002/9781394270392.ch3.
- [6] Y. Singh and T. Walingo, "Smart Water Quality Monitoring with IoT Wireless Sensor Networks," *Sensors*, vol. 24, no. 9, p. 2871, Apr. 2024, doi: 10.3390/s24092871.
- [7] R. Wiryasaputra, C.-Y. Huang, Y.-J. Lin, and C.-T. Yang, "An IoT Real-Time Potable Water Quality Monitoring and Prediction Model Based on Cloud Computing Architecture," *Sensors*, vol. 24, no. 4, p. 1180, Feb. 2024, doi: 10.3390/s24041180.
- [8] S. Metia, H. A. D. Nguyen, and Q. P. Ha, "IoT-Enabled Wireless Sensor Networks for Air Pollution Monitoring with Extended Fractional-Order Kalman Filtering," *Sensors*, vol. 21, no. 16, p. 5313, Aug. 2021, doi: 10.3390/s21165313.
- [9] A. I. Griva *et al.*, "LoRa-Based IoT Network Assessment in Rural and Urban Scenarios," *Sensors*, vol. 23, no. 3, p. 1695, Feb. 2023, doi: 10.3390/s23031695.
- [10] S. Idris, T. Karunathilake, and A. Förster, "Survey and Comparative Study of LoRa-Enabled Simulators for Internet of Things and Wireless Sensor Networks," *Sensors*, vol. 22, no. 15, p. 5546, Jul. 2022, doi: 10.3390/s22155546.
- [11] J. Liu, W. Gao, J. Dong, N. Wu, and F. Ding, "Low-Power Failure Detection for Environmental Monitoring Based on IoT," *Sensors*, vol. 21, no. 19, p. 6489, Sep. 2021, doi: 10.3390/s21196489.
- [12] B. Chokara and S. K. R. Jammalamadaka, "Hybrid models for computing fault tolerance of IoT networks," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 21, no. 2, p. 333, Apr. 2023, doi: 10.12928/telkomnika.v21i2.22429.
- [13] D. Kairuz-Cabrera, V. Hernandez-Rodriguez, O. Schalm, A. Martinez, P. M. Laso, and D. Alejo-Sánchez, "Development of a Unified IoT Platform for

- Assessing Meteorological and Air Quality Data in a Tropical Environment,” *Sensors*, vol. 24, no. 9, p. 2729, Apr. 2024, doi: 10.3390/s24092729.
- [14] J. Roostaei, Y. Z. Wager, W. Shi, T. Dittrich, C. Miller, and K. Gopalakrishnan, “IoT-based edge computing (IoTEC) for improved environmental monitoring,” *Sustainable Computing: Informatics and Systems*, vol. 38, p. 100870, Apr. 2023, doi: 10.1016/j.suscom.2023.100870.
- [15] M. Catelani, L. Ciani, A. Bartolini, C. Del Rio, G. Guidi, and G. Patrizi, “Reliability Analysis of Wireless Sensor Network for Smart Farming Applications,” *Sensors*, vol. 21, no. 22, p. 7683, Nov. 2021, doi: 10.3390/s21227683.
- [16] A. Rana, K. Kaur, P. Kaur, and E. Bhatti, “Energy-efficient protocols for environmental monitoring in wireless sensor networks: A review,” *J. Ambient Intell. Smart Environ.*, vol. 17, no. 2, pp. 139–163, May 2025, doi: 10.1177/18761364241297221.
- [17] A. Kumar, S. Jadhav, and O. M. Alsalami, “Reliability and Sensitivity Analysis of Wireless Sensor Network Using a Continuous-Time Markov Process,” *Mathematics*, vol. 12, no. 19, p. 3057, Sep. 2024, doi: 10.3390/math12193057.
- [18] J. K. R. Sastry, B. Ch, and R. R. Budaraju, “Implementing Dual Base Stations within an IoT Network for Sustaining the Fault Tolerance of an IoT Network through an Efficient Path Finding Algorithm,” *Sensors*, vol. 23, no. 8, p. 4032, Apr. 2023, doi: 10.3390/s23084032.
- [19] T. Baranwal, S. Varada, S. Das, and M. R. Haider, “Fault-Tolerant IoT System Using Software-Based ‘Digital Twin,’” in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, IEEE, Nov. 2024, pp. 828–833. doi: 10.1109/WF-IoT62078.2024.10811168.
- [20] S. K. R. Jammalamadaka, B. Chokara, S. B. Jammalamadaka, and B. K. Duvvuri, “Using DL Models in the Service Layer to Enhance the Fault Tolerance of IoT Networks,” *Electronics (Basel)*, vol. 13, no. 22, p. 4334, Nov. 2024, doi: 10.3390/electronics13224334.
- [21] H. Mohapatra and A. K. Rath, “A fault tolerant routing scheme for advanced metering infrastructure: an approach towards smart grid,” *Cluster Comput.*, vol. 24, no. 3, pp. 2193–2211, Sep. 2021, doi: 10.1007/s10586-021-03255-x.
- [22] S. K. R. Jammalamadaka, B. Chokara, S. B. Jammalamadaka, B. K. Duvvuri, and R. Budaraju, “Enhancing the Fault Tolerance of a Multi-Layered IoT Network through Rectangular and Interstitial Mesh in the Gateway Layer,” *Journal of Sensor and Actuator Networks*, vol. 12, no. 5, p. 76, Oct. 2023, doi: 10.3390/jsan12050076.
- [23] S. Syafrudin, A. Sarminingsih, H. Juliani, M. A. Budihardjo, A. S. Puspita, and S. Auliya Arlin Mirhan, “Water Quality Monitoring System for Temperature, pH, Turbidity, DO, BOD, and COD Parameters Based on Internet of Things in Garang Watershed,” *Ecological Engineering & Environmental Technology*, vol. 25, no. 2, pp. 1–16, Feb. 2024, doi: 10.12912/27197050/174412.
- [24] E. B. Belachew, M. B. Bekele, and B. A. Birawo, “Intelligent water quality monitoring using WSN and Machine Learning Approaches,” in *2023 the 7th International Conference on Information System and Data Mining (ICISDM)*, New York, NY, USA: ACM, May 2023, pp. 50–55. doi: 10.1145/3603765.3603766.

- [25] S. O. Ajakwe, V. U. Ihekoronye, I. U. Ajakwe, T. Jun, D.-S. Kim, and J. M. Lee, "Connected Intelligence for Smart Water Quality Monitoring System in IIoT," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, Oct. 2022, pp. 2386–2391. doi: 10.1109/ICTC55196.2022.9952785.
- [26] A. H. Wirasapta, T. D. Pamungkas, and S. S. Mishri, "Simulation-Based Analysis of Packet Scheduling Strategies and Traffic Load Effects on Network QoS," *Energy Insights*, vol. 1, no. 2, pp. 49–58, Apr. 2026, doi: 10.59562/ei.v1i2.11311.
- [27] Y. Niu, Z. Wei, L. Wang, H. Wu, and Z. Feng, "Interference Management for Integrated Sensing and Communication Systems: A Survey," *IEEE Internet Things J.*, vol. 12, no. 7, pp. 8110–8134, Apr. 2025, doi: 10.1109/JIOT.2024.3506162.
- [28] E. Dixit and V. Jindal, "IEESEP: an intelligent energy efficient stable election routing protocol in air pollution monitoring WSNs," *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10989–11013, Jul. 2022, doi: 10.1007/s00521-022-07027-5.
- [29] Dr. N. Osman and E. Abbas, "Performance Evaluation of LoRa and Sigfox LPWAN Technologies for IoT," *Academic Journal of Research and Scientific Publishing*, vol. 4, no. 38, pp. 05–24, Jun. 2022, doi: 10.52132/Ajrsp.e.2022.38.1.
- [30] A. H. Wirasapta, P. Nugroho, and S. B. Wibowo, "Designing QPSK Modulator Using LTspice-Based Discrete Components," in *2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*, IEEE, Nov. 2022, pp. 283–288. doi: 10.1109/COMNETSAT56033.2022.9994317.
- [31] S. S. Shafin, G. Karmakar, I. Mareels, V. Balasubramanian, and R. R. Kolluri, "Sensor Self-Declaration of Numeric Data Reliability in Internet of Things," *IEEE Trans. Reliab.*, vol. 74, no. 2, pp. 2751–2765, Jun. 2025, doi: 10.1109/TR.2024.3416967.
- [32] T. L. Narayana *et al.*, "Advances in real time smart monitoring of environmental parameters using IoT and sensors," *Heliyon*, vol. 10, no. 7, p. e28195, Apr. 2024, doi: 10.1016/j.heliyon.2024.e28195.
- [33] J. Buelvas, D. Múnera, D. P. Tobón V., J. Aguirre, and N. Gaviria, "Data Quality in IoT-Based Air Quality Monitoring Systems: a Systematic Mapping Study," *Water Air Soil Pollut.*, vol. 234, no. 4, p. 248, Apr. 2023, doi: 10.1007/s11270-023-06127-9.
- [34] H. Karnati, "IoT-Based Air Quality Monitoring System with Machine Learning for Accurate and Real-time Data Analysis," Jul. 2023.
- [35] S. K. R. Jammalamadaka, B. Chokra, S. B. Jammalamadaka, and B. K. Duvvuri, "Networking Microcontrollers and Balancing the Load on the Service Servers to Enhance the Fault Tolerance of the IoT Networks," *Mathematics*, vol. 12, no. 23, p. 3730, Nov. 2024, doi: 10.3390/math12233730.
- [36] K. Singh, M. Yadav, Y. Singh, D. Barak, A. Saini, and F. Moreira, "Reliability on the Internet of Things with designing approach for exploratory analysis," *Front. Comput. Sci.*, vol. 6, Jun. 2024, doi: 10.3389/fcomp.2024.1382347.

- [37] G. A. López-Ramírez and A. Aragón-Zavala, “Wireless Sensor Networks for Water Quality Monitoring: A Comprehensive Review,” *IEEE Access*, vol. 11, pp. 95120–95142, 2023, doi: 10.1109/ACCESS.2023.3308905.