UDC 004.8 : 004.94 DOI: 10.18372/2073-4751.84.20893

Artem Dremov
https://orcid.org/0009-0005-7214-9458
a.k.dremov@gmail.com
Artem Volokyta
https://orcid.org/0000-0001-9069-5544
artem.volokita@kpi.ua

A METHOD TO DETERMINE THE CRITICALITY OF GATEWAYS IN A LORAWAN NETWORK

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Introduction

Latest years have featured rapid proliferation of Internet of Things (IoT) deployments which has driven widespread adoption of Low-Power Wide-Area Network (LPWAN) technologies. Of these, the LoRaWAN has proven itself as one of the premier long-range, low-power wireless connectivity technologies. A basic LoRaWAN network features a star-of-stars topology with battery powered nodes communicating through one or more gateways with the central network server . This architecture enables kilometer-scale coverage with minimal infrastructure, making LoRaWAN attractive for a variety of IoT applications

However, the structure of LoRaWAN networks introduces a critical vulnerability: gateways serve as single points of aggregation for potentially hundreds of end devices. While the LoRaWAN specification supports multi-gateway reception—where a single packet may be received by multiple gateways to improve reliability—gateway failures can nonetheless cause significant service disruption. However, the gateway placement is often constrained by costs and coverage optimization. As such, select gateways tend to become far more important to the network's reliability than others.

Despite the importance of identifying which gateways are most critical to network function, existing LoRaWAN research has focused predominantly on capacity optimization, interference mitigation, and coverage planning. Current approaches to gateway deployment either treat all gateways as equally important or rely on simple heuristics such as node count or geographic centrality. However, a research avenue exists for developing an algorithmic method for quantifying individual gateway criticality that accounts for the unique characteristics of LoRaWAN networks—including physical layer constraints, adaptive data rate (ADR) mechanisms, and probabilistic connectivity.

This gap is particularly problematic for large-scale LoRaWAN deployments where infrastructure maintenance, redundancy planning, and failure response strategies require prioritization.

This study aims to address this gap by presenting an algorithmic approach to gateway criticality assessment in LoRaWAN networks. The method presented in this study is used to compute a multi-factor criticality score for each gateway based on three key metrics: the number of nodes that can connect to the gateway, the number of nodes that depend exclusively on that gateway, and the traffic volume served by the gateway. Unlike topology-agnostic graph metrics such as betweenness centrality or degree centrality, the approach presented takes into account LoRaWAN-specific factors including received signal strength (RSSI), spreading factor adaptation, and the asymmetric nature of uplink connectivity.

The experimental evaluation presented in this study, conducted using the FLoRa simulator with realistic propagation models and LoRaWAN protocol implementation, demonstrates that the proposed criticality

metric accurately predicts which gateway failures cause the greatest degradation in network-wide packet delivery ratio (PDR). In low scale (up to 7 nodes) and large scale (up to 50 nodes) scenarios, targeting the gateway with the largest criticality score had consistently displayed larger mean PDR drop.

Literature review and problem statement

This paper approaches the problem of identifying critical components in network infrastructure, in particular in LoRaWAN networks. To approach this issue, an overview of existing methodologies from areas of graph theory, network vulnerability analysis, Low-Power Wide-Area Network (LPWAN) is presented in this section.

Graph-theoretic approaches to network criticality

The problem of identifying critical nodes in networked systems has been extensively studied in traditional network analysis. Early work by Albert et al. [1] demonstrated that attacks on scale-free networks that target specific, critical elements, are much more impactful than ones that target network elements at random. Holme et al. [2] extended this work by proposing different attack strategies based on node betweenness centrality. The study conducted had shown that removing high-betweenness nodes causes maximum network fragmentation. Both of these works view networks as graphs, which abstracts many physical properties of said networks and thus, fail to take into account the physical aspect of connections between network elements.

More recent work has adapted network centrality metrics for infrastructure protection. Crucitti et al. [3] used efficiency-based metrics that measure network performance degradation under targeted attacks, demonstrating that centrality metrics described in previous works (degree, betweenness, closeness) correlate with network vulnerability. One of the main findings of the mentioned work, is the combined usage of global and local metrics in order to identify critical nodes. Beygelzimer et al. [4] introduced network robustness measures based on pairwise connectivity, showing that network robustness can be improved for most critical elements by randomizing existing connections and introducing new ones.

Wireless network reliability and transmission mechanisms

Mahmood et al. [5] look into different components of transmission reliability in wireless networks. The components identified by the study are retransmission and network redundancy. This study also reliability improvement strategies, reliability measures and how reliability can be achieved. This lays the theoretical foundations of network reliability that can be applied to LoRaWAN networks. However, these approaches remain topology-centric and fail to take into account the specifics of a wireless domain, such as signal propagation, interference and techniques such as adaptive data rate (ADR).

LoRaWAN network performance and coverage

Research specific to LoRaWAN networks has primarily focused on capacity planning, coverage optimization, and performance modeling rather than criticality assessment. Georgiou and Raza [6] describe the conditions under which an uplink connection may fail in LoRaWAN networks. Bor et al. [7] introduced the LoRaSim simulator and demonstrated that gateway placement significantly impacts network performance, but did not formalize methods for assessing individual gateway importance.

Several studies have addressed gateway placement optimization in LoRaWAN, as well as physical aspects of signal propagation in different environments. Savithi et al. [8] view the issue of gateway placement in LoRaWAN networks as a multi-objective problem based on minimizing total cost while maximizing bitrate performance. Luvisotto et al. [9] introduced and LoRaWAN simulation model and studied the usage of LoRaWAN network in indoor scenarios where interference and

signal propagation are more constrained. Cattani et al. [10] studied signal propagation with different physical settings of LoRa modules, as well as different environmental conditions.

Gateway redundancy and multi-gateway connectivity

We would like to separately mention the work of Xiaofan Yu et al. [11], which concerns the study of LoRaWAN network reliability due to gateway failures. The study in question introduces the concept of m-gateway connectivity which means that every node should be connected to multiple gateways. Several studies, among which we would like to highlight ones done by M. Almuhaya et al. [12], W. Wu et al. [13], look into improving LoRaWAN network transmission reliability by using multiple gateways, such as multi-gateway reception and similar techniques However, the study never explicitly attempts to determine the most critical gateway, reserving to only measuring the impact of gateway failures in sequence. However, such studies also do not analyze the vulnerability of single gateway designs. In the author's opinion, the issue of examining points of failure with a single gateway are an important aspect of network reliability.

Adaptive data rate and dynamic link behavior

The concept of Adaptive Data Rate (ADR) in LoRaWAN introduces dynamic link adaptation that complicates criticality assessment. Slabicki et al. [14] studied and tested different approaches to ADR and how it enables nodes to adjust transmission parameters based on link quality. This means that the connectivity between LoRaWAN gateways and nodes is not static and that criticality cannot be determined solely from initial topology—it must account for the network's adaptive behavior. To our knowledge, no prior work has developed a criticality metric that incorporates ADR dynamics and considers single gateway exclusive nodes, that cannot reach any other gateway. In addition, the article in question introduces "flora" framework as a module for OMNeT++ simulation library used extensively in this paper.

Advanced modeling and machine learning approaches

Recent work on network digital twins and 3D modelling of practical environments offers relevant methodologies for runtime criticality assessment. A. Ruz-Nieto et al. [15] use a develop a 3D framework alongside ray tracing techniques for reconstruction of urban environments to more accurately model shadowing and propagation changes induced by various obstacles compared to more traditional mathematical models.

Determining the criticality of network nodes to network reliability algorithmically is not a new concept in literature. For example, study conducted by S. Munikoti et al. [16] employs machine learning algorithms in order to predict the most critical nodes in a network modelled by a graph based on a subset of nodes used for training. However the author's couldn't find extensive works that apply the concept of quantifying node criticality to LoRaWAN networks.

Positioning of contributions presented in this paper

While existing research provides valuable foundations in network vulnerability analysis, graph-theoretic criticality metrics, and LoRaWAN performance modeling, significant gaps remain:

1. Lack of LoRaWAN-specific criticality metrics: Prior work either uses generic graph metrics (degree, betweenness) that ignore physical layer dynamics, or focuses on coverage optimization without quantifying individual gateway importance.

2. Neglect of adaptive behavior: Existing approaches assume static connectivity, whereas LoRaWAN's ADR mechanism enables dynamic link adaptation. Criticality assessment must account for both current and potential connectivity.

3. Absence of exclusive node consideration: Prior works, generally, do no explicitly study cases, where a single

gateway in a network handles multiple nodes exclusive to this gateway — a critical factor in determining failure impact.

Aims of the study

To develop and validate a quantitative metric for assessing gateway criticality in LoRaWAN networks that accurately predicts the impact of gateway failures on network performance.

Metric Development

- Design a criticality scoring function specifically tailored to LoRaWAN network characteristics
- Incorporate LoRaWAN-specific factors (ADR, SF, uncertain connectivity)
- Ensure metric is computationally efficient for real-time deployment

Experimental Validation

- Evaluate metric performance across diverse network topologies and scales
- Measure correlation between predicted criticality and observed failure impact

Problem statement

LoRaWAN's architecture employs a star-of-stars topology where battery-powered end devices transmit to fixed gateways, which forward packets to a central network server. This design, while energy-efficient for devices, creates infrastructure dependencies: gateway availability directly determines network coverage and capacity.

Network operators lack a principled method to identify which gateways are most critical to network operation.

Current approaches suffer from three fundamental limitations:

1. Generic metrics don't apply

- Degree centrality: Counts connections but ignores exclusive dependencies
- Betweenness centrality: Assumes multi-hop routing (absent in LoRaWAN)
- Closeness centrality: Measures path length (uniformly 1-hop in star topology)
- These metrics, designed for general graphs, fail to capture LoRaWAN-specific behavior

2. Adaptive mechanisms ignored

- Existing approaches treat connectivity as binary (connected/disconnected)
- LoRaWAN's ADR dynamically adjusts spreading factors (SF7-SF12)
- A node currently using SF7 may be instructed to switch to SF10 or SF12 when its gateway fails
- This latent redundancy is invisible to traditional graph metrics

3. Operational impact unknown

- It is difficult for operators to predict failure consequences before they occur
- No quantitative basis for prioritizing maintenance or redundancy investments

Research questions

Question 1: Can a single metric accurately predict the operational impact of gateway failures in LoRaWAN networks?

Question 2: Which factors (connected nodes, exclusive nodes, traffic volume) contribute most to gateway criticality?

Question 3: Does the metric generalize across different network scales (small vs. large) and topologies (symmetric vs. asymmetric coverage)?

Question 4: How does ADR adaptation affect criticality assessment compared to static connectivity models?

LoRaWAN network architecture

For the purposes of this study, a standard LoRaWAN network is considered, consisting of three layers: end devices (nodes), gateways, and a network server. Let $N=\{n_1,n_2,\ldots,n_N\}$ denote the set of N end devices and $G=\{g_1,g_2,\ldots,g_M\}$ denote the set of M gateways, as well as, generally, one network server (NS). End devices transmit uplink packets using LoRa modulation with configurable transmission parameters including spreading factor (SF), bandwidth (BW), and coding rate (CR). Gateways operate as transparent packet forwarders, receiving LoRa transmissions and relaying them to the network server via backhaul connectivity (typically IP-based).

The network server performs three critical functions: (1) deduplication of packets received by multiple gateways, (2) downlink scheduling and gateway selection

for acknowledgments and commands, and (3) adaptive data rate (ADR) control to optimize transmission parameters for each device. For this work, the focus is on uplink communication, as it constitutes the majority of traffic in typical LoRaWAN deployments and is directly impacted by gateway availability.

Physical layer model

LoRa employs Chirp Spread Spectrum (CSS) modulation with spreading factors ranging from SF7 (shortest range, highest data rate) to SF12 (longest range, lowest data rate). The relationship between spreading factor, time-on-air, and communication range creates a fundamental tradeoff: higher spreading factors enable longer-range communication but reduce data rate and increase airtime, limiting network capacity. For the purposes of this study, it is assumed the antenna gain and cable loss of LoRa transmitters to be negligible.

The received signal strength at gateway g_j from node n_i is modeled as:

$$RSSI_{ij} = P_{tx} - PL(d_{i,j}) \quad (1)$$

Where P_{tx} - transmission power (typically 14 dBm), $PL(d_{i,j})$ - path loss at distance $d_{i,j}$ between the 2 elements

Path loss is calculated as follows:

$$PL(d) = PL(d_0) + 10\,n \log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \quad (2)$$

Where $PL(d_0)$ - path loss at reference distance d_0 = 40m (typically 127.41 ddB), n - path loss exponent (assumed 2.08 for urban environment) and X_σ - log-normal shadowing loss with standard deviation of σ, typically around 3-4 dB.

The signal is considered received when the $RSSI_{ij} \geq S_{min}$, where S_{min} is the receiver's sensitivity (typically -137 dBm at SF12 and -123 dBm at SF7 at 125 kHz bandwidth)

Connectivity decision representation

This study also distinguishes current connectivity ($E_{current}$) and potential connectivity ($E_{potential}$). Based on current and maximum SF values.

This distinction is critical for LoRaWAN because ADR dynamically adjusts spreading factors based on link quality. A node currently using SF7 may be able to reach an additional gateway by being instructed to increase to SF10 or SF12, providing latent redundancy that becomes accessible during gateway failures.

As such, the criticality metric presented in this study uses the following properties to measure the gateway criticality:

- Number of total connected nodes, where if gateway g_j has more connected nodes than gateway g_i, then, all else being equal, g_j will have a higher score
- Number of connected exclusive nodes where if gateway g_j has more connected exclusive nodes than gateway g_i, then, all else being equal, g_j will have a higher score
- Traffic volume, where if gateway g_j has higher potential traffic volume than gateway g_i, then, all else being equal, g_j will have a higher score

Failure model

The gateway failures are modelled as complete, instantaneous outages where the failed gateway becomes unable to receive or forward any packets. This represents scenarios such as power failure, hardware malfunction, or complete backhaul connectivity loss. Partial degradation (e.g., reduced sensitivity) is not considered in this work.

When gateway g_j fails at time t_f, the following should be observed:

- Nodes exclusive to gateway g_j become isolated
- Nodes shared between multiple gateways lose one redundancy path
- Due to differences in shared node connectivity to different gateways, ADR may trigger and cause the SF to increase for such nodes

The failure impact is measured through three primary metrics:

- Packet Delivery Ratio (PDR): Fraction of transmitted packets successfully received by the network server

- Node Isolation Count: Number of nodes unable to reach any gateway
- Gateway Reception Redundancy**:** Average number of gateways receiving each successfully delivered packet

Assumptions and scope

This work operates under the following assumptions:

1. Static Node Placement: Nodes do not move during the analysis period. While LoRaWAN supports mobile applications, most deployments involve stationary sensors.
2. Uplink-Focused: We analyze uplink communication, as it dominates LoRaWAN traffic.
3. Known Topology: The network server has knowledge of node locations or RSSI measurements sufficient to construct the connectivity graph.
4. ADR Enabled: NS can instruct nodes to adjust their SF to improve connection reliability
5. Single Failure: This study analyzes single gateway failures rather than simultaneous multiple failures, as single failures are far more common in practice.

These assumptions reflect typical LoRaWAN deployment scenarios and allow this study to focus on the core problem of criticality assessment without unnecessary complexity.

Design rationale

Traditional network centrality metrics such as degree centrality, betweenness centrality, and closeness centrality were developed for general graphs and do not capture the unique characteristics of LoRaWAN networks. Degree centrality simply counts connections, ignoring whether nodes have alternative paths. Betweenness centrality assumes multi-hop routing, which does not occur in LoRaWAN's star topology. Closeness centrality measures average path length, which is uniformly one hop for all node-gateway pairs in LoRaWAN.

The criticality metric presented in this study addresses these limitations by incorporating three LoRaWAN-specific factors:

1. Connected Nodes: The total number of nodes that can reach the gateway, reflecting its coverage contribution to the network.
2. Exclusive Nodes: The number of nodes for which this gateway is the only reachable option, representing single points of failure.
3. Traffic Volume: The aggregate data traffic served by the gateway, accounting for application-level importance and resource utilization.

Criticality score formulation

The factors described before are combined using a weighted linear model. For each gateway $g_j \in G$ the criticality score is calculated as:

$$C(g_j) = \omega_c \frac{|N_c(g_j)|}{N} + \omega_e \frac{|N_e(g_j)|}{N} + \omega_t \frac{T(g_j)}{T_{total}} \quad (3)$$

Where:

$N_c(g_j) = \{n_i \in N : (n_i, g_j) \in E_{potential}\}$ - a set of nodes that can reach the gateway g_j with ADR (if necessary).

$N_e(g_j) = \{n_i \in N : G_e(n_i) = \{g_j\}\}$ - a set of nodes exclusive to gateway g_j

$T(g_j) = \sum(n_i \in N_c(g_j))r_i$ - total potential traffic from connected nodes, where r_i - transmission rate of node i

$\omega_c, \omega_e, \omega_t$ - non-negative weights such that $\omega_c + \omega_e + \omega_t = 1$

Each term is normalized by the maximum possible value so that $C(g_j) \in [0,1]$

Weight selection for weights $(\omega_c, \omega_e, \omega_t)$ are selected as (0.3, 0.5, 0.2) based on the following logic:

- Exclusive node (ω_e = 0.5) due to unavoidable impact due to lack of redundancy for these nodes
- Connected nodes (ω_c = 0.3) due to existing redundancies limiting potential impact
- Traffic volume (ω_t = 0.2) to help differentiate gateways with similar node counts

Connectivity pre-computation

Computing exclusive and connected node sets requires determining which nodes can reach which gateways. In this study, the analysis is performed in two stages:

Connectivity is computed in 2 stages:

- Current connectivity based on $G_{current}(n_i) = RSSI_{ij} \geq S_{min}(SF_i)$ from gateway g_j to node n_i based on current spreading factor of the node
- Potential connectivity based on $G_{potential}(n_i) = RSSI_{ij} \geq S_{min}(SF_{12})$ from gateway g_j to node n_i based on maximum possible spreading factor SF12

This accounts for LoRaWAN's ability to adaptively increase spreading factor to maintain connectivity when a gateway fails. Nodes operating at SF7 may be instructed to switch to SF10 or SF12 to reach a previously unusable gateway, providing latent redundancy.

Algorithm details

The pseudo algorithm is as follows:

1. initialize data structures
2. for each node n_i:
   a. compute current connectivity $G_{current}(n_i)$ and potential connectivity $G_{potential}(n_i)$
   b. if $g_j \in G_{potential}(n_i)$ or $g_j \in G_{current}(n_i)$, then: add n_i to $N_c(g_j)$ and increment $T(g_j)$ by r_i
   c. if $|G_{potential}(n_i)| = 1$, then: node is exclusive to this gateway, add n_i to $N_e(g_j)$
3. compute total traffic: $T_{total} = \sum_{i=1}^{N} r_i$
4. for each gateway: compute criticality score as described before

The expected time complexity of the metric calculation is O(NM) where N is number of nodes and M is number of gateways. The expected space complexity is O(NM) for storing the RSSI values for each node – gateway pair and O(M) for gateway scores.

Dynamic re-computation

In operational deployments, network topology changes due to node additions/removals, gateway maintenance, or environmental changes affecting propagation. This methods supports two re-computation triggers:

1. Periodic Analysis: Scheduled criticality updates (e.g., daily) to capture gradual changes in network state.
2. Event-Driven Analysis: Immediate re-computation when new nodes join or leave the network or gateway failures or recoveries occur

The lightweight computational requirements enable frequent updates without impacting network server performance.

Handling uncertain connectivity

Log-normal shadowing introduces randomness in RSSI measurements, meaning connectivity is probabilistic rather than deterministic. This is adressed address this through conservative connectivity estimation:

For each node-gateway pair the link is considered “reachable” if the mean RSSI exceeds the sensitivity threshold by a margin Δ (a value of 3dB is used in this study) to account for unfavorable and favorable shadowing conditions, that is the node is reachable if $RSSI_{mean} - S_{min} \geq \Delta$. This helps to more accurately identify exclusive nodes.

This conservative approach ensures that nodes classified as "exclusive" truly depend on a single gateway under typical propagation conditions, reducing false positives in criticality assessment.

Simulation environment

The criticality metric presented is evaluated using the FLoRa (Framework for LoRa) simulator, an OMNeT++-based tool specifically designed for LoRaWAN network simulation. FLoRa implements the complete LoRaWAN MAC protocol including join procedures, adaptive data rate (ADR), and multi-gateway packet deduplication at the network server. Unlike abstract network simulators, FLoRa models physical layer characteristics including LoRa modulation, spreading factor orthogonality, and realistic propagation effects.

Simulator Configuration:

- OMNeT++ version: 6.0
- FLoRa version: 2.0 (modified to integrate CriticalGatewayAnalyzer)
- Network server: ChirpStack-compatible implementation with ADR support
- Simulation duration: 14400 seconds (4 hours) per run
- Number of independent seeds: 30 per test scenario

The normal FLoRa framework is extended with a CriticalGatewayAnalyzer module that:

1. Computes gateway criticality scores at regular intervals
2. Triggers controlled gateway failures at predetermined times
3. Records network-wide metrics during pre-failure, failure, and recovery phases
4. Outputs per-node and per-gateway statistics for offline analysis

Propagation model

Accurate propagation modeling is essential for realistic connectivity assessment. A log-normal shadowing model is used with parameters derived from urban LoRaWAN measurement campaigns:

LoRa physical layer parameters:

- Frequency: 868 MHz
- Bandwidth: 125 kHz
- Spreading factors: SF7-SF12
- Coding rate: 4/5
- Transmission power: 14 dBm (max for EU regulations)
- Receiver sensitivity: −137 dBm (SF12), −123 dBm (SF7)

This model creates realistic probabilistic connectivity where nodes at similar distances may experience different link qualities due to shadowing, requiring the ADR mechanism to adapt spreading factors appropriately.

Test network topologies

To validate the criticality metric across diverse scenarios, ten test networks spanning three categories were designed:

Test case 1: single gateway

- Nodes: 12, gateways: 1, area: 3000m × 3000m
- Gateway: GW0 at (1500, 1500, 15m) - Central position
- Node layout: 3 concentric rings around gateway at 50m, 400m, and 600m radii
- Purpose: baseline total-failure scenario, establish worst-case scenario

Test case 2 - 3: asymmetric dual gateway

- Nodes: 7, gateways: 2, area: 3000m × 3000m
- Gateways: GW0 at (500, 1500, 15m), GW1 at (2500, 1500, 15m) - 2000m separation
- Node distribution: 4 nodes exclusive to GW0 (close cluster), 2 nodes exclusive to GW1 (close cluster), 1 marginally connected node at 1100m midpoint
- Failed gateway: GW0 (TC2), GW1 (TC3)
- Purpose: demonstrate criticality differentiation in asymmetric topology

Test case 4 - 5: symmetric dual gateway

- Nodes: 10, gateways: 2, Area: 3000m × 3000m
- Gateways: GW0 at (1000, 1500, 15m), GW1 at (2000, 1500, 15m) - 1000m separation
- Node distribution: 3 nodes exclusive to each gateway, 4 shared nodes in center zone (around 500m to each gateway)
- Failed gateway: GW0 (TC4), GW1 (TC5)

- Purpose: Validate equal criticality yields equal impact

Test case 6 - 10: large-scale urban

- Nodes: 50, gateways: 5, area: 4000m × 4000m
- Gateway layout: central hub + 4 corners pattern
- Gateways: GW0 at (1600, 1600, 15m) central, GW1-4 at corners (400,400), (2800,400), (400,2800), (2800,2800), 1700m – 2900m separation
- Node distribution: 19 nodes exclusive to GW0 (150-180m rings), 4 exclusive to GW1, 5 to GW2, 6 to GW3, 8 to GW4, 8 shared nodes (2 each between GW0 and corner gateways)
- Failed gateway: GW0 (TC6), GW1 (TC7), GW2 (TC8), GW3 (TC9), GW4 (TC10)
- Purpose: evaluate scalability, realistic urban deployment

Experiment structure

Each test scenario follows a standardized three-phase protocol:

Phase 1: Pre-Failure (0-7200s)

- All gateways operational
- Network reaches steady state
- ADR converges to optimal spreading factors
- Metrics recorded: baseline PDR, isolated nodes

Phase 2: Gateway Failure (7200-10800s)

- Target gateway fails at t=7200s (instantaneous complete outage)
- ADR attempts to adapt spreading factors for affected nodes
- Metrics recorded: degraded PDR, newly isolated nodes

Phase 3: Recovery (10800-14400s)

- Failed gateway recovers at t=10800s
- ADR re-optimizes spreading factors
- 30 minute observation period to verify full recovery
- Metrics recorded: recovered PDR, persistent isolated nodes

Timing Rationale:

- 120 minutes pre-failure: allow simulation time to converge, ADR convergence, etc. This simulates failure after extended use
- 60 minutes failure duration: long enough to observe sustained impact
- 30 minutes recovery: accounts for ADR hysteresis and delayed re-optimization

Performance metrics

The network performance is measured through seven key metrics:

Packet delivery ratio:

$$PDR = \frac{\text{Packets received by the Network Server}}{\text{Packets transmitted by nodes}} \times 100\% \quad (4)$$

Packets received at NS level already deduplicate data from different gateways that can receive from the same node.

PDR delta:

$$\Delta PDR = PDR_{pre} - PDR_{failure} \quad (5)$$

Relative PDR degradation:

$$\Delta PDR_{rel} = \frac{PDR_{pre} - PDR_{failure}}{PDR_{pre}} \times 100\% \quad (6)$$

Isolation ratio:

$$R_{iso} = \frac{N_{isolated}}{N_{total}} \times 100\% \quad (7)$$

Coefficient of variation (CV)

$$CV = \frac{\sigma}{\mu} \times 100\% \quad (8)$$

Where σ - standard deviation, μ - mean value.

Per-Node Transmission Statistics: Individual packet data for each node, enabling identification of most-affected devices.

Per-Gateway Reception Counts: Traffic distribution across gateways, validating criticality-based traffic predictions.

Statistical analysis

To ensure validity of presented results, the following process is used:

1. Multi-Seed Validation: Each test scenario runs with 30 independent random seeds, providing statistical confidence in results. This study reports mean ± standard deviation for all metrics.

2. Coefficient of Variation (CV) Analysis (as presented in formula 8).

4. This study verifies CV < 15% for critical metrics (PDR pre/during/post), ensuring low variance suitable for scientific conclusions.

3. Correlation Analysis: Spearman rank correlation (ρ) and Pearson correlation (r) between criticality scores and PDR drop impact are computed across all test scenarios. Statistical significance is assessed at α = 0.05 level.

The results of the experiments are presented in fig. 1 through fig. 5

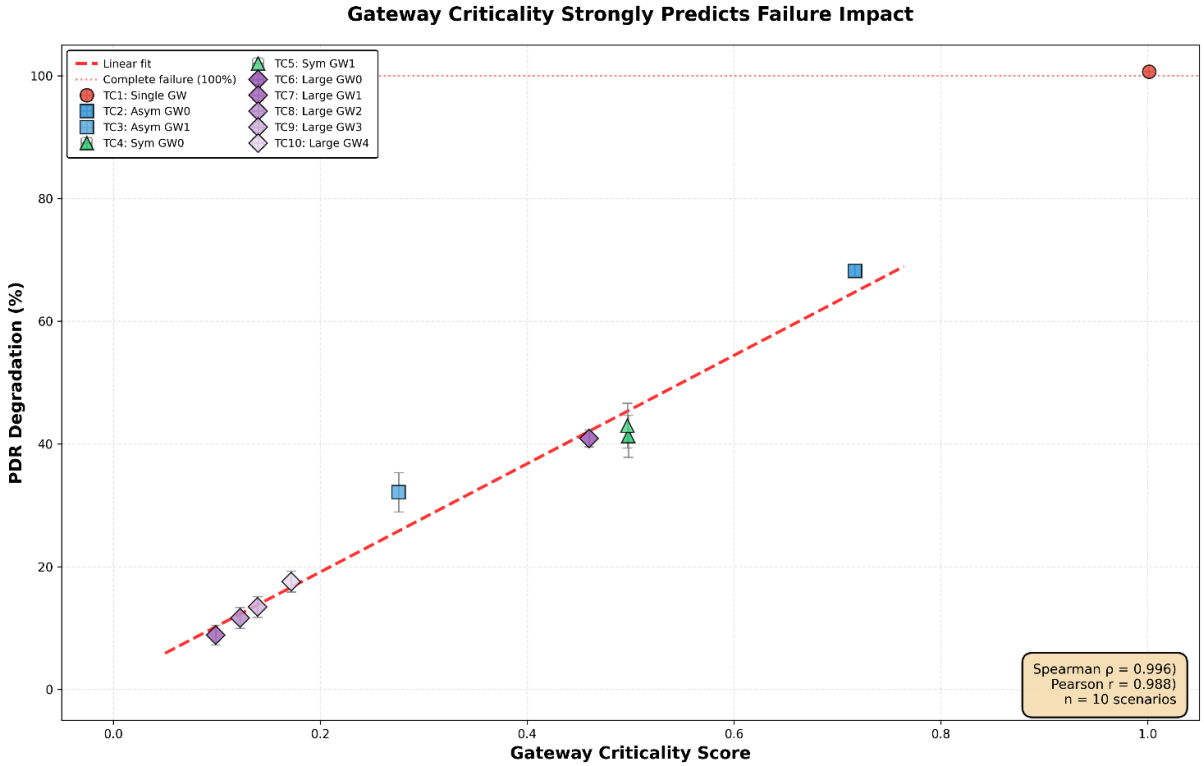

Fig. 1. Gateway criticality to PDR degradation correlation

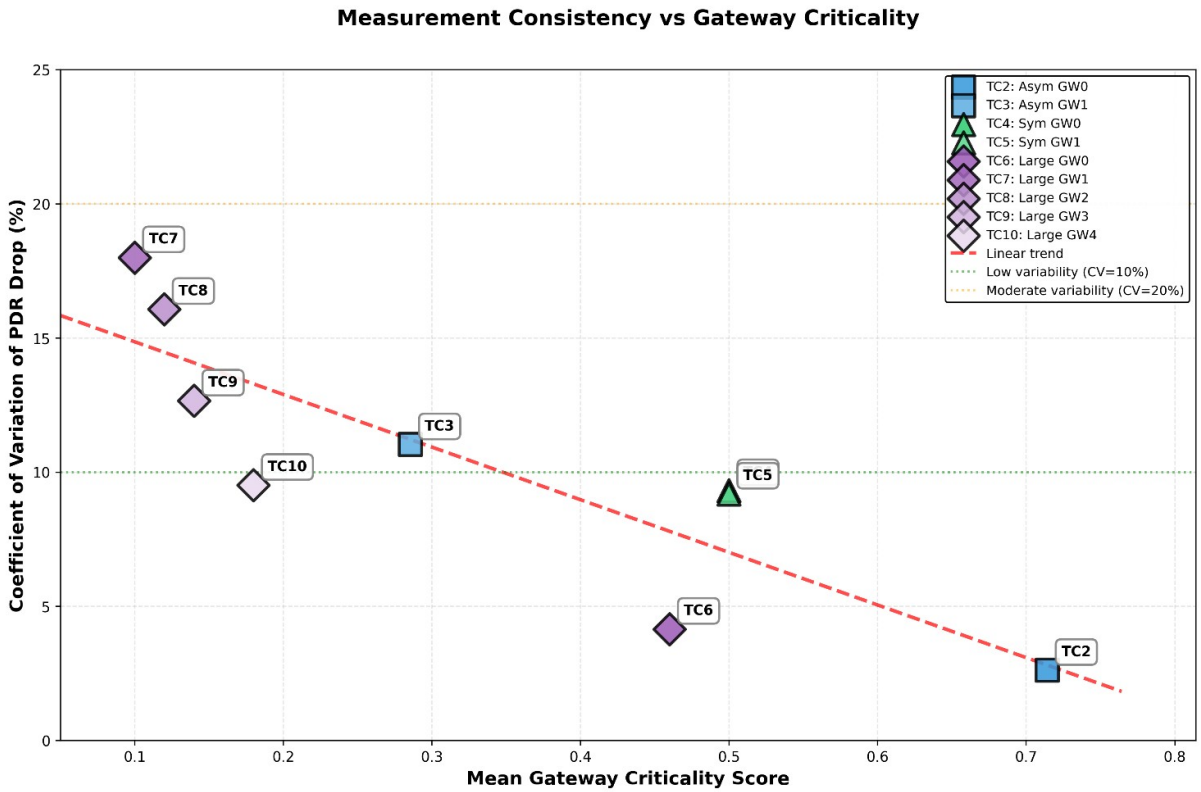

Fig. 2. CV of PDR decrease against mean criticality score

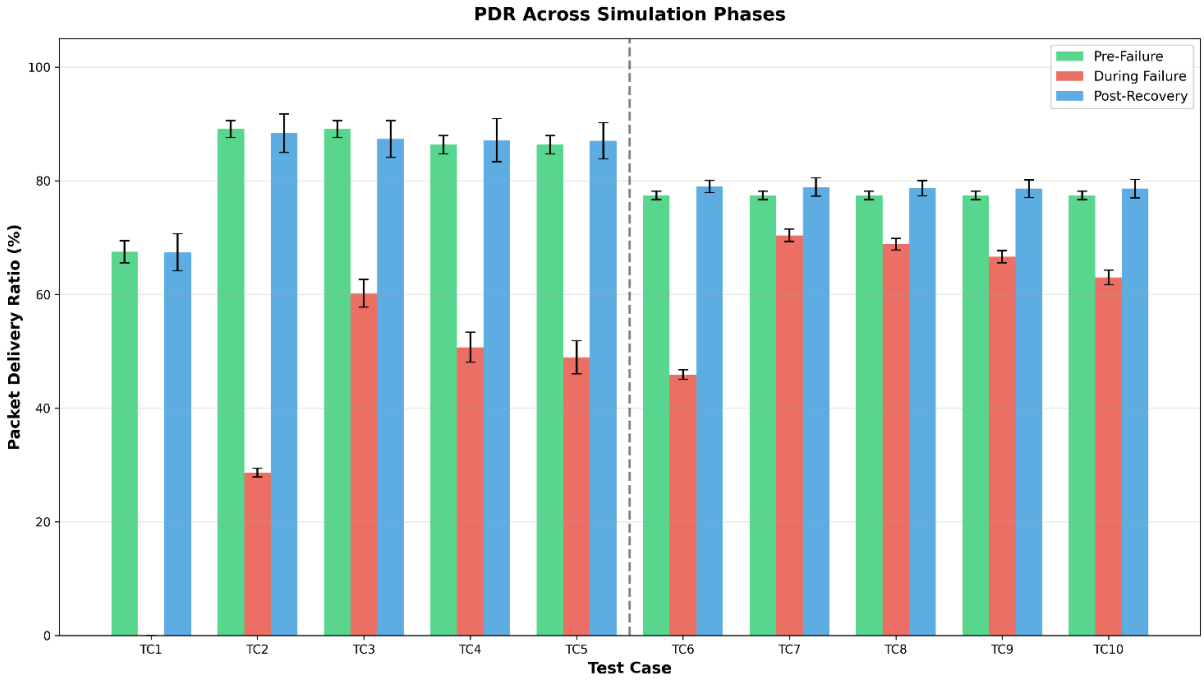

Fig. 3. PDR statistics comparison per test case

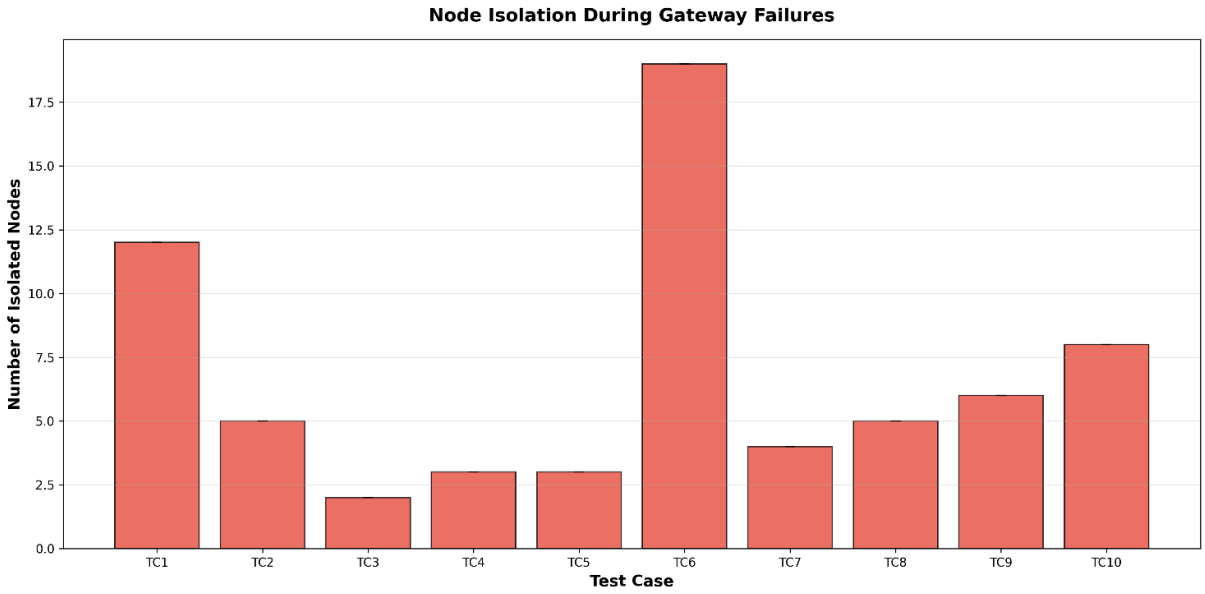

Fig. 4. Isolated node count per test case

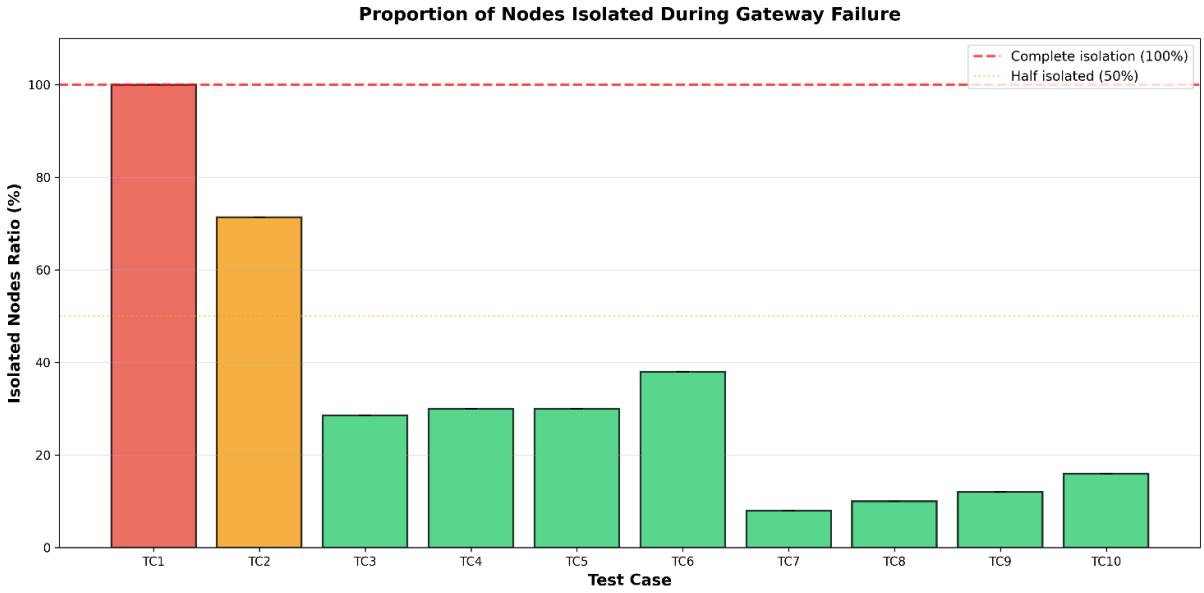

Fig. 5. Ratio of isolated nodes to total network capacity per test case

Analysis of obtained results

As seen in fig. 1, 2 and 3, the criticality metrics shows strong correlation with simulated PDR drop and medium to low variance against mean of criticality score, especially when criticality is high. Note that test case 1 with a single GW is a sanity check and therefore is excluded from the correlation consideration.

There is an outlier representing test case 3.

Test case 3 features and asymmetrical topology with 2 gateways and non critical gateway being failed. The impact is higher than expected, however this can be explained by the considerable distance between nodes and the secondary gateway (1500m to 2000m). This means that with unfavorable shadowing, the nodes that used to transmit to the failed gateway, now can only transmit packets to secondary gateway at most at about 25% success rate. Alongside this, reception collisions at a more heavily used secondary gateway are theorized to be the reason for observed PDR drop.

Otherwise, experiments conducted show that the developed criticality metric shows a strong correlation with expected PDR drop across several scenarios and is able to predict with a degree of certainty which gateway's failure will cause the highest impact.

A curious case can be seen when examining the PDR percentages per simulation phase. That is, after gateway recovers, the packet delivery ratio on average is higher that before failure, especially in highly distributed scenarios with higher ratio of shared nodes. It is suspected, that due to gateway failure, the NS instructs nodes to increase the SF so they can reach secondary gateways. This may improve the reception statistics increasing overall PDR.

As can be seen from fig. 3, 4 and 5, the isolation ratio features a high correlation with PDR drop.

Conclusions and discussion

This study successfully developed and demonstrated a way to algorithmically determine the most critical gateway in a LoRaWAN network. This study has presented a metric that can quantify the criticality of a gateway in a LoRaWAN network and presented an algorithm that utilizes said metric for an analysis of a LoRaWAN network. This study also used FLoRa and OMNeT++ simulation environments to test the developed metric against several distinct scenarios and measure the metric's correlation with simulated network impact.

The results of this study indicate, that the metric is highly corelative with network impact in a variety of scenarios, however the algorithm still needs adjustment for specific cases in order to handle highly redundant scenarios, as well as scenarios with very marginally connected nodes.

References

1. *Albert R., Jeong H., Barabási A.-L.* Error and attack tolerance of complex networks. *Nature*. 2000. Vol. 406, no. 6794. P. 378–382. URL: https://doi.org/10.1038/35019019 (date of access: 11.02.2026).

2. Attack vulnerability of complex networks / *P. Holme* et al. *Physical review E*. 2002. Vol. 65, no. 5. URL: https://doi.org/10.1103/physreve.65.056109 (date of access: 11.02.2026).

3. Efficiency of scale-free networks: error and attack tolerance / *P. Crucitti* et al. *Physica A: statistical mechanics and its applications*. 2003. Vol. 320. P. 622–642. URL: https://doi.org/10.1016/s0378-4371(02)01545-5 (date of access: 12.02.2026).

4. Improving network robustness by edge modification / *A. Beygelzimer* et al. *Physica A: statistical mechanics and its applications*. 2005. Vol. 357, no. 3-4. P. 593–612. URL: https://doi.org/10.1016/j.physa.2005.03.040 (date of access: 12.02.2026).

5. *Mahmood M. A., Seah W. K. G., Welch I.* Reliability in wireless sensor networks: a survey and challenges ahead. *Computer networks*. 2015. Vol. 79. P. 166–187. URL: https://doi.org/10.1016/j.comnet.2014.12.016 (date of access: 12.02.2026).

6. *Georgiou O., Raza U.* Low power wide area network analysis: can lora scale?. *IEEE wireless communications letters*. 2017. Vol. 6, no. 2. P. 162–165. URL: https://doi.org/10.1109/lwc.2016.2647247 (date of access: 12.02.2026).

7. Do LoRa Low-Power Wide-Area Networks Scale? / *M. C. Bor* et al. *MSWiM '16: 19th ACM international conference on modeling, analysis and simulation of wireless and mobile systems*, Malta Malta. New York, NY, USA, 2016. URL: https://doi.org/10.1145/2988287.2989163 (date of access: 12.02.2026).

8. *Savithi C., Kaewta C.* Multi-Objective optimization of gateway location selection in long-range wide area networks: a tradeoff analysis between system costs and bitrate maximization. *Journal of sensor and actuator networks*. 2024. Vol. 13, no. 1. P. 3.

URL: https://doi.org/10.3390/jsan13010003 (date of access: 12.02.2026).

9. On the use of lorawan for indoor industrial iot applications / *M. Luvisotto* et al. *Wireless communications and mobile computing*. 2018. Vol. 2018. P. 1–11.
URL: https://doi.org/10.1155/2018/3982646 (date of access: 12.02.2026).

10. *Cattani M., Boano C. A., Romer K.* An experimental evaluation of the reliability of lora long-range low-power wireless communication. *Journal of sensor and actuator networks*. 2017. Vol. 6, no. 2. P. 7.
URL: https://doi.org/10.3390/jsan6020007 (d ate of access: 12.02.2026).

11. Automating reliable and fault-tolerant design of lora-based iot networks / *X. Yu* et al. *2021 17th international conference on network and service management (CNSM)*, Izmir, Turkey, 25–29 October 2021. 2021.
URL: https://doi.org/10.23919/cnsm52442.2021.9615512 (date of access: 12.02.2026).

12. ZBMG-LoRa: a novel zone-based multi-gateway approach towards scalable lorawans for internet of things / *M. Almuhaya* et al. *Sensors*. 2025. Vol. 25, no. 17. P. 5457.
URL: https://doi.org/10.3390/s25175457 (dat e of access: 12.02.2026).

13. *Wu W., Wang H., Cheng Z.* ReLoRaWAN: Reliable data delivery in LoRaWAN networks with multiple gateways. *Ad hoc networks*. 2023. P. 103203.
URL: https://doi.org/10.1016/j.adhoc.2023.103203 (date of access: 12.02.2026).

14. *Slabicki M., Premsankar G., Di Francesco M.* Adaptive configuration of lora networks for dense IoT deployments. *NOMS 2018 - 2018 IEEE/IFIP network operations and management symposium*, Taipei, Taiwan, 23–27 April 2018. 2018.
URL: https://doi.org/10.1109/noms.2018.8406255 (date of access: 12.02.2026).

15. A 3D simulation framework with ray-tracing propagation for LoRaWAN communication / *A. Ruz-Nieto* et al. *Internet of things*. 2023. P. 100964.
URL: https://doi.org/10.1016/j.iot.2023.100964 (date of access: 12.02.2026).

16. *Munikoti S., Das L., Natarajan B.* Scalable graph neural network-based framework for identifying critical nodes and links in complex networks. *Neurocomputing*. 2022. Vol. 468. P. 211–221.
URL: https://doi.org/10.1016/j.neucom.2021.10.031 (date of access: 12.02.2026).

Dremov A. K., Volokyta A. M.

A METHOD TO DETERMINE THE CRITICALITY OF GATEWAYS IN A LORAWAN NETWORK

LoRaWAN networks rely on gateways to relay packets from resource-constrained end devices to the network server, creating a potential single point of failure in network infrastructure. While traditional graph centrality metrics exist for general networks, they fail to capture LoRaWAN-specific characteristics such as adaptive data rate (ADR) mechanisms, spreading factor orthogonality, and asymmetric node-gateway connectivity patterns. This paper introduces a gateway criticality metric specifically designed for LoRaWAN networks, as well as an algorithm that employs this metric in an analysis task in order to identify and prioritize critical infrastructure components before failures occur.

The metric for gateways presented in this study combines three LoRaWAN-specific factors: connected node count (coverage contribution), exclusive node count (single points of failure), and served traffic volume (application-level importance). Unlike traditional centrality measures, the algorithm presented accounts for ADR's ability to adaptively increase spreading factors when gateways fail, recognizing latent redundancy that becomes accessible during outages. The exclusive nodes are weighted most heavily (50% contribution), as their isolation has immediate, unavoidable impact on network availability.

The metric is validated through 300 simulations across diverse network topologies spanning 7 to 50 nodes and 1 to 5 gateways. Results demonstrate strong correlation between criticality scores and measured failure impact. High-criticality gateway failures ($C \geq 0.7$) caused packet delivery ratio (PDR) drops of around 60%, while low-criticality failures ($C < 0.3$) produced up to 25% drops. The metric generalizes across reviewed network scales and topologies, from simple dual-gateway deployments to complex scenarios with 50 nodes and 5 gateways.

Key words: *LoRaWAN, Gateway Criticality, Network Reliability, Internet of Things, Adaptive Data Rate*

Дремов А. К., Волокита А. М.

СПОСІБ ВИЗНАЧЕННЯ КРИТИЧНОСТІ ШЛЮЗІВ В LORAWAN МЕРЕЖІ

Мережі LoRaWAN покладаються на мережеві шлюзи для ретрансляції пакетів від кінцевих пристроїв з обмеженими ресурсами до мережевого сервера, створюючи потенційну єдину точку відмови в мережевій інфраструктурі. Хоч і існують традиційні метрики центральності графів для загальних мереж, вони не враховують властивості, специфічні для LoRaWAN, такі як механізми адаптивної швидкості передачі даних (ADR), ортогональність коефіцієнта розповсюдження та асиметричні шаблони зв'язку вузлів та шлюзів. У цій статті представлено метрику для визначення критичності шлюзів, спеціально розроблену для мереж LoRaWAN, а також алгоритм, який використовує цю метрику в завданні аналізу для виявлення та визначення пріоритетів критичних компонентів інфраструктури до виникнення збоїв.

Метрика для шлюзів, представлена в цьому дослідженні, поєднує три специфічні для LoRaWAN фактори: кількість підключених вузлів (внесок у покриття), кількість вузлів підключених виключно (єдині точки відмови) та обсяг обслуговуваного трафіку (важливість на прикладному рівні). На відміну від традиційних показників центральності, представлений алгоритм враховує здатність ADR адаптивно збільшувати коефіцієнти розповсюдження, коли шлюзи виходять з ладу,

розпізнаючи приховану надлишковість, яка стає доступною під час перебоїв. Вузли підключені виключно до одного шлюзу, мають найбільшу вагу (внесок 50%), оскільки їхня ізоляція має негайний, неминучий вплив на доступність мережі.

Метрику перевірено за допомогою 300 симуляцій у різних мережевих топологіях, що охоплюють від 7 до 50 вузлів та від 1 до 5 шлюзів. Результати демонструють сильну кореляцію між показниками критичності та виміряним впливом збоїв. Збої шлюзів з високою критичністю (C ≥ 0,7) призвели до падіння коефіцієнта доставки пакетів (PDR) приблизно на 60%, тоді як збої з низькою критичністю (C < 0,3) призвели до падіння до 25%. Метрика узагальнюється для розглянутих мережевих масштабів та топологій, від простих розгортань з двома шлюзами до складних сценаріїв з 50 вузлами та 5 шлюзами.

Ключові слова: *LoRaWAN, критичність шлюзів, надійність мережі, інтернет речей, адаптивна швидкість передачі даних.*

Стаття подана до редакції: 03/12/2025
Стаття прийнята до опублікування: 16/12/2025
Стаття опублікована: 30/12/2025