

A FRAMEWORK FOR ROBUSTNESS EVALUATION IN ULTRA-DENSE IOT NETWORKS

Viktor Stoynov[✉], Georgi Iliev, Dimitriya Mihaylova

Received on June 11, 2025

Presented by Ch. Roumenin, Member of BAS, on July 29, 2025

Abstract

This paper introduces a framework for evaluating *robustness* as a composite metric tailored for Ultra-Dense IoT (UD-IoT) networks. The evaluation focuses on four core dimensions: operational continuity, resource efficiency, network flexibility, and security. Using theoretical models in conjunction with accurate simulations, this study also examines the impact of critical factors, including the density of devices, network traffic, and environmental disturbances, on system performance. Our simulations confirm the validity of the proposed methodology across three representative deployment scenarios – critical, essential and basic. The results highlight the importance of jointly optimizing operational continuity and resource efficiency to ensure consistently high performance under diverse operating conditions.

Key words: IoT, ultra-dense networks, robustness

Introduction. Network densification is crucial for IoT networks to handle the exponential growth in data traffic and device connectivity driven by the increasing number of connected devices [1]. Modern mobile networks address these demands with higher data rates, reduced latency, and increased capacity using technologies such as Massive MIMO, millimeter-wave communications, and network slicing. The evolution to 6G will further enhance these capabilities, enabling ultra-low latency, ultra-high data rates, and improved energy efficiency for

This study is financed by the European Union – NextGenerationEU, through the National Recovery and Resilience Plan of the Republic of Bulgaria, project No. BG-RRP-2.004-0005.

<https://doi.org/10.7546/CRABS.2025.09.10>

next-generation IoT applications [2, 3]. Since the advent of UD-IoT networks, researchers have proposed solutions for scalability, energy efficiency, and resource optimization. In [4], key metrics like energy efficiency, latency, and throughput are identified, but reliance on static conditions limits adaptability. Collaborative offloading frameworks using NOMA and caching [5] face challenges in high-mobility settings. Machine learning methods [6, 7] improve resource allocation and energy efficiency, but computational overhead and scalability remain concerns. Security approaches [8, 9] focus on multi-layered frameworks and encryption, yet centralized architectures create latency and single points of failure. SDN with network slicing boosts scalability but lacks extreme density validation [10]. Fair resource allocation via NOMA is limited by static assumptions in dynamic UD-IoT environments [11]. In this context, despite significant research, most existing UD-IoT solutions focus on isolated aspects often neglecting their interdependencies. There is a need for a holistic robustness metric that integrates key dimensions like resilience, scalability, adaptability, and reliability. Current methods rarely capture this multi-dimensional nature, often improving one factor at the expense of others.

Robustness evaluation framework. This section presents a novel definition of the robustness metric as a multi-dimensional attribute that encompasses resilience, scalability, reliability, adaptability, and related factors [12]. The evaluation methodology not only addresses these dimensions individually but also considers their interdependencies to achieve a balanced and optimized UD-IoT architecture. Such a framework enables the systematic design of networks that dynamically adapt to changing demands, ensuring sufficient performance and reliability in ultra-dense environments. Below, we introduce four key parameters that collectively define the robustness metric in the context of UD-IoT networks. Each parameter captures a critical aspect of system behaviour, contributing to the overall stability, adaptability, and performance under dynamic conditions.

Operational continuity (OC). In UD-IoT networks, OC is a metric for resilience and reliability, supporting seamless operation and consistent performance despite hardware failures, software bugs, or external disruptions. High interdependence among devices increases cascading failure risk in applications like IoT, smart cities, or healthcare. A well-defined framework is crucial for maintaining operational stability and service quality in uncertain conditions [13]. Equation (1) expresses the OC metric based on these principles:

$$(1) \text{ OC} = \gamma_1 \cdot (1 - \text{MTTR}) + \gamma_2 \cdot \text{FDR} + \gamma_3 \cdot \frac{1}{1 + e^{-k(\text{SAR} - \theta)}} + \gamma_4 \cdot \text{SCP} + \gamma_5 \cdot \text{DRL}^p,$$

where MTTR is the Mean Time to Repair, FDR is the Fault Detection Rate, SAR is the System Availability Ratio, SCI is the Sensor Calibration Index, DRL is the Data Redundancy Level, γ_i is the weighting coefficient, k is a parameter used to control the steepness of the curve, θ is the threshold and p is the power coefficient. These sub-parameters are combined using mathematical transformations –

inverse, sigmoid, and power functions – to reflect real-world impact and account for nonlinearities typical of IoT environments. For example, $1 - \text{MTTR}$ highlights faster recovery, the sigmoid on SAR captures diminishing returns near maximum availability, and power functions for SCI and DRL emphasize the increasing difficulty of marginal improvements at higher levels.

Scalable resource efficiency (SRE). SRE is crucial in UD-IoT networks as device numbers grow and efficient resource use becomes vital. It measures how well networks can scale with increasing density while maintaining sustainability and reliability. In urban IoT, SRE highlights the need for dynamic resource and spectrum management to handle interference and coordination among thousands of devices [14]. In agricultural IoT, SRE assesses sustainability through power-aware metrics that minimize energy use. Its parameters reflect the network's ability to adapt to traffic and environmental changes, ensuring efficient and scalable operation. These principles are captured in Equation (2).

$$(2) \text{ SRE} = \beta_1 \cdot \text{SDR}^p + \beta_2 \cdot (1 - \text{ISI}) + \beta_3 \cdot \text{THE} + \beta_4 \cdot \sqrt{\text{SPU}} + \beta_5 \cdot \frac{1}{1 + e^{-k(\text{EA} - \theta)}},$$

where SDR is the Sensor Deployment Ratio, ISI is the Integration Speed Index, THE is the Traffic Handling Efficiency, SPU is the Sustainable Power Utilization, EA is the Expansion Agility, and β_i is the weighting coefficient. The SRE formula integrates the above-mentioned sub-parameters using mathematical transformations that reflect their real-world significance, balancing scalability and efficiency in UD-IoT deployments. For example, SDR is scaled by a power function to emphasize early efficiency and diminishing returns at higher saturation, while SPU uses a square root transformation to capture initial energy gains. At the same time, $1 - \text{ISI}$ penalizes slow integration, THE contributes linearly due to its direct impact on traffic, and EA applies a sigmoid function to model the nonlinear benefits of adaptive expansion near operational thresholds.

Network Flexibility (NF). NF quantifies a UD-IoT network's ability to adapt to dynamic conditions and ensure seamless interoperability among diverse devices and protocols. As IoT ecosystems grow more complex, NF measures how efficiently the network can scale and respond to changing operational requirements without loss of functionality [15]. It captures both adaptability – how devices handle varying traffic, density, and environments – and interoperability across different manufacturers and protocols. In this study, NF is defined by Equation (3):

$$(3) \text{ NF} = \delta_1 \cdot \text{FUR} + \delta_2 \cdot \text{PCS}^p + \delta_3 \cdot (1 - \text{DCI}) + \delta_4 \cdot \frac{1}{1 + e^{-k(\text{TPA} - \theta)}} + \delta_5 \cdot \text{DI},$$

where FUR is the Firmware Update Rate, PCS is the Protocol Compatibility Score, DCI is the Dynamic Configuration Index, TPA is the Traffic Pattern Adaptation, DI is the Device Interoperability, and δ_i is the weighting coefficient. FUR

and DI are treated linearly to reflect their direct impact on adaptability and device integration, respectively; PCS is scaled using a power function to capture diminishing returns in protocol compatibility, $1 - DCI$ penalizes slower reconfiguration times, and a sigmoid function is applied to TPA to emphasize significant improvements in traffic responsiveness near critical thresholds.

Security (SEC). SEC is essential in UD-IoT networks for achieving trust, secure data, and consistent operation in high device density and heterogeneous environments. As device numbers grow, so does the risk of vulnerabilities, with each device as a potential entry point for cyber threats [16]. Devices – sensors, actuators, gateways – must be protected from unauthorized access, data breaches, malware, and DDoS. In smart healthcare, loss of security can compromise privacy-sensitive and life-critical data [17]. In industrial IoT, intrusions may disrupt supply chains or infrastructure, causing major economic and social consequences. In Equation (4) these aspects related to security are quantified:

$$(4) \quad SEC = \varepsilon_1 \cdot EKS + \varepsilon_2 \cdot (1 - TDI) + \varepsilon_3 \cdot FIC^p + \varepsilon_4 \cdot \sqrt{UAD} + \varepsilon_5 \cdot \frac{1}{1 + e^{-k(RIM - \theta)}},$$

where EKS is the Encryption and Key Security, TDI is the Tamper Detection Incidents, FIC is the Firmware Integrity Check Frequency, UAD is the Unauthorized Access Detection and Response, RIM is the Response to Security Incidents, and ε_i is the weighting coefficient. EKS and RIM are modelled linearly and sigmoidally, respectively, to capture their foundational role in encryption and response effectiveness; $1 - TDI$ negatively weights frequent tampering incidents, FIC is scaled with a power function to highlight diminishing gains in firmware protection, and UAD uses a square root transformation to balance sensitivity and stability in intrusion detection.

Overall, the weighting coefficients – γ_i , β_i , δ_i , ε_i , in all formulas are designed to balance the contribution of individual parameters within each respective metric, ensuring they align with the specific priorities of the system being analyzed.

Robustness (R). The overall robustness, R, represents an aggregate measure derived from the four parameters previously described utilizing a weighting coefficient α_i :

$$(5) \quad R = \alpha_1 \cdot OC + \alpha_2 \cdot SRE + \alpha_3 \cdot NF + \alpha_4 \cdot SEC.$$

The formula provides a structured and integrative mathematical representation of system robustness by combining the four key performance factors already presented. The coefficients for the overall robustness metric, α_i , offer flexibility to emphasize OC, SRE, NF, or SEC depending on the deployment scenario or application requirements. Importantly, R is designed to account for natural correlations between sub-parameters for a realistic assessment of system performance. These correlations reflect how certain parameters inherently influence each other in practical UD-IoT scenarios, guiding adjustments during computation.

Simulation setup. In this study, the performance of UD-IoT networks is examined in three deployment scenarios – Critical, Essential, and Basic Deployment – to assess the robustness framework under different operational requirements. Each scenario applies specific parameter ranges reflecting its priorities and challenges. Simulations in GNU Octave generated 10 000 parameter sets per scenario, with calculations repeated across 100 weighting coefficient combinations from a Dirichlet distribution. The focus is on the overall robustness metric, using power scaling ($p = 0.7$) and sigmoid scaling ($k = 10$, θ variable). Normalized PDFs were used to present the parameter distributions.

Analysis of simulation results. The normalized PDFs of the robustness metric (R) for each deployment scenario are shown in Fig. 1, illustrating different distributions across scenarios. For Critical Deployment (blue), the distribution is compact and sharply peaked, reflecting robust, stable, and reliable designs typical of critical environments with stringent requirements. The Essential Deployment scenario (green) shows a broader distribution and higher variance, indicating a more elastic trade-off between stability and flexibility. The Basic Deployment scenario (red) is the most widespread, with robustness values spread out and concentrated at lower levels, which is common for non-critical systems where cost and functional diversity may outweigh strict robustness. Overall, the distributions are symmetric, showing stability in the metric, and the progression from Basic to Critical Deployment demonstrates a shift toward tighter and higher robustness values as the environment becomes more mission-critical.

The robustness threshold in Fig. 1 for each deployment scenario is defined as the minimum value above which the system is considered stable with a chosen probability (e.g., 80%), based on the empirical distribution of robustness values.

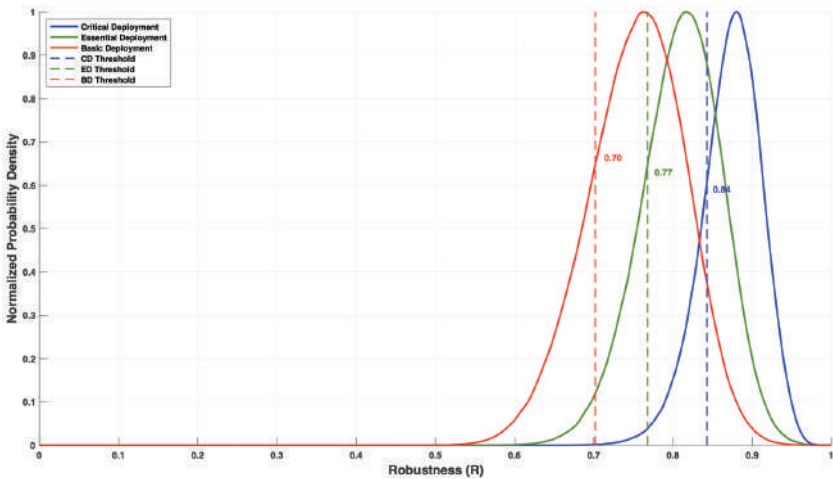


Fig. 1. PDF of robustness metric R with thresholds

This probabilistic approach aligns the threshold with real deployment characteristics, reflecting stricter stability requirements for more critical scenarios. Thresholds are calculated by optimizing the cumulative probability to match the desired stability level, ensuring context-aware and statistically grounded robustness limits.

The time-series plots for R under five realistic operation scenarios – Normal Conditions, High Event Intensity, High Traffic Load, Network Congestion, and High Load with Low Sensor Reliability – are shown in Fig. 2. These results demonstrate how key operational challenges such as event intensity, traffic load, and sensor reliability impact overall system stability. The simulations were conducted over 750 time steps and 10 000 time units, with 100 to 2500 devices, using LOESS smoothing (factor 0.1) and base values of 0.85 for robustness components

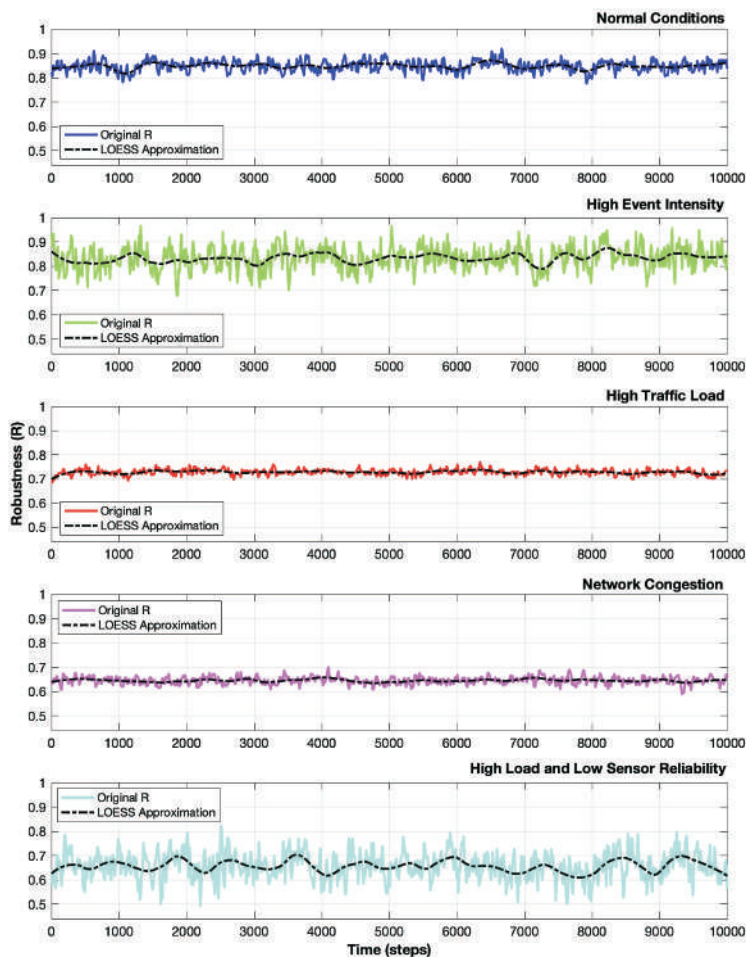


Fig. 2. PDF for robustness metric R across five different scenarios

(OC, SRE, NF, SEC). Scenario-specific variables included event intensity, failure factor, and load factor, capturing stress conditions like high traffic, congestion, or sensor unreliability.

Under Normal Conditions, the system maintains high robustness with minimal fluctuations, indicating efficient operation. High event intensity introduces greater variability and vulnerability to performance drops. With high traffic load, robustness steadily declines due to congestion and limited resources, highlighting the need for effective traffic management. Network congestion causes moderate, but noticeable, decline, while high load combined with low sensor reliability leads to erratic behaviour and large fluctuations – underscoring the importance of sensor accuracy. These trends emphasize the need for adaptive, resilient network architectures and real-time optimization in ultra-dense IoT environments.

Conclusion. Based on our research, two conclusions can be drawn. First, the robustness metric for UD-IoT networks is highly sensitive to event intensity and traffic load –robustness degrades under high event intensity due to increased contention and limited resources, challenging the network’s ability to adapt dynamically and highlighting the need for intelligent traffic management and load balancing. Second, OC alone is not sufficient for a full robustness assessment; it must be integrated with resource efficiency to address high-density environments with limited computational power, energy, and bandwidth. While scalable resource allocation helps networks adapt to changing demand, maintaining high OC alongside optimized resource use in real time remains a challenge. Future studies will use real data from operational IoT networks to further test and refine the robustness methodology, enabling more accurate evaluation and validation of the metric in ultra-dense, dynamic scenarios.

REFERENCES

- [1] ANDREWS J. G., S. BUZZI, W. CHOI et al. (2014) What will 5G be?, *IEEE J. Sel. Areas Commun.*, **32**(6), 1065–1082.
- [2] SAAD W., M. BENNIS, M. CHEN (2020) A vision of 6G wireless systems: applications, trends, technologies, and open research problems, *IEEE Network*, **34**(3), 134–142.
- [3] LATVA-AHO M., K. LEPPÄNEN (Eds) (2020) Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence, 6G Flagship White Paper, University of Oulu, Available online: <http://jultika.oulu.fi/files/isbn9789526223544.pdf> (accessed on June 3, 2024).
- [4] STOYNOV V., V. POULKOV, Z. VALKOVA-JARVIS et al. (2023) Ultra-dense networks: Taxonomy and key performance indicators, *Symmetry*, **15**(1), 2.
- [5] ZHOU T., B. WANG, D. QIN et al. (2024) Secure collaborative computation offloading and resource allocation in cache-assisted UD-IoT networks, *arXiv preprint*,

Available online: <https://arxiv.org/abs/2410.14142> (accessed on December 4, 2024).

- [6] SHARMA S. K., X. WANG (2022) Towards massive machine type communications in ultra-dense cellular IoT networks, *IEEE Commun. Surveys & Tutorials*, **24**(1), 156–180.
- [7] FAROOQ M. U., M. ZEESHAN, M. ASIF (2023) A novel cooperative micro-caching algorithm based on fuzzy inference through NFV in UD-IoT networks, *J. Netw. Comput. Appl.*, **211**, 102973.
- [8] HUANG J., T. YU, F. YANG et al. (2024) AoI-aware resource allocation with interference avoidance for ultra-dense industrial IoT networks, *IEEE Internet Things J.*, **11**(2), 876–891.
- [9] ELBAYOUMI M., M. IBRAHIM, S. ELHOUSHY (2023) Performance analysis of cellular ultra dense IoT networks with wireless backhauls, *IEEE Trans. Ind. Inform.*, **19**(3), 2487–2502.
- [10] THEODOROU T., L. MAMATAS (2023) DENIS-SDN: Software-defined network slicing solution for dense and ultra-dense IoT networks, arXiv preprint, available online: <https://arxiv.org/abs/2312.13662> (accessed on December 4, 2024).
- [11] WANG Q. (2019) Fair resource allocation in an MEC-enabled UD-IoT network with NOMA, Utah State University Thesis, Logan, UT, USA, Available online: <https://digitalcommons.usu.edu/etd/2023/> (accessed on December 4, 2024).
- [12] QIU T., N. CHEN, S. ZHANG (2022) Robustness Optimization for IoT Topology, Singapore, Springer, ISBN: 978-981-16-9608-4, 214 pp.
- [13] XING L. (2021) Cascading failures in Internet of Things: Review and perspectives on reliability and resilience, *IEEE Internet Things J.*, **8**(1), 44–64.
- [14] ALSHARIF M. H., A. H. KELECHI, A. JAHID et al. (2024) A comprehensive survey of energy-efficient computing to enable sustainable massive IoT networks, *Alexandria Eng. J.*, **91**, 12–29.
- [15] GEORGE A., G. RAMANA MURTHY (Eds) (2023) Towards Wireless Heterogeneity in 6G Networks, Boca Raton, FL, CRC Press.
- [16] QI Q., X. CHEN, C. ZHONG, Z. ZHANG (2020) Physical layer security for massive access in cellular Internet of Things, *Sci. China Inf. Sci.*, **63**, 121301.
- [17] BAKARDJIEVA T., A. IVANOVA, Y. YANKOV, Z. ZHEKOV (2025) Cybersecurity for sustainable Internet of Things implementation in healthcare, *C. R. Acad. Bulg. Sci.*, **78**(4), 562–570.

Faculty of Telecommunications, Technical University of Sofia,

8 Kliment Ohridski Blvd, 1756 Sofia, Bulgaria

e-mails: vstoynov@tu-sofia.bg, gli@tu-sofia.bg, dam@tu-sofia.bg