telecom

MDPI

Article

A Multi-Dimensional Robustness Evaluation Framework for Ultra-Dense IoT Networks in Smart Cities

Viktor Stoynov * and Dimitriya Mihaylova

Faculty of Telecommunications, Technical University of Sofia, 1756 Sofia, Bulgaria; dam@tu-sofia.bg
* Correspondence: vstoynov@tu-sofia.bg

Abstract

This paper presents a multi-dimensional robustness evaluation framework for ultra-dense Internet of Things (UD-IoT) networks in smart city environments. The framework addresses the need to assess robustness beyond isolated indicators such as latency, throughput, packet loss, or availability by integrating operational continuity (OC), scalable resource efficiency (SRE), network flexibility (NF), and security (SEC) into a unified robustness metric (R). Building on an earlier formulation of the metric, the present study extends its interpretation toward smart city IoT deployments, strengthens the perception layer perspective, and introduces a controlled fifth-generation (5G) connectivity validation procedure. The evaluation is performed in two complementary stages. First, simulation-based analysis is conducted across critical, essential, and basic deployment scenarios to examine the mathematical behavior of the metric under different operational priorities and parameter ranges. Second, a validation setup based on free5GC and UERANSIM is used to transform observable control-plane, user-plane, service-connectivity, and security indicators into comparable robustness components through an explicit normalization and mapping procedure. The results show scenario-dependent robustness degradation across the evaluated smart city IoT conditions, with the strongest degradation in the combined stress scenario where endpoint density, traffic intensity, service recovery stress, and abnormal access conditions occur simultaneously.

Keywords: IoT; ultra-dense IoT networks; smart cities; robustness; operational continuity; scalable resource efficiency; network flexibility; security; 5G connectivity; validation environment

1. Introduction

The Internet of Things (IoT) has reshaped interactions between physical environments and digital systems, enabling communication among devices, services, and applications [1]. This technological shift supports improved efficiency, automation, and data-driven decision-making in domains including smart cities, healthcare, transportation, and industrial automation [2]. The impact of IoT extends beyond basic connectivity to applications such as predictive maintenance, remote monitoring supported by artificial intelligence and machine learning (AI/ML), and autonomous decision-making. In healthcare, IoT devices enable remote patient monitoring and advanced diagnostic services, while in smart cities they support intelligent traffic management, energy-efficient building automation, and environmental monitoring [3]. These capabilities make IoT a key enabling technology for data-driven cyber-physical services and Industry 4.0.

Check for updates

Academic Editor: George Tsoulos

Received: 1 July 2026
Revised: 17 August 2026
Accepted: 28 August 2026
Published: 3 September 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Network densification is increasingly important for supporting growing IoT traffic and device-connectivity requirements [4]. This requires resource allocation mechanisms capable of sustaining higher traffic volumes while maintaining an acceptable quality of service (QoS) [5]. Fifth-generation (5G) mobile networks provide technologies such as massive multiple-input multiple-output (MIMO), millimeter-wave communications, and network slicing that can support dense IoT environments [6,7]. Future sixth-generation (6G) networks are expected to extend these capabilities through higher capacity, lower latency, improved energy efficiency, and tighter integration of communication and sensing [8]. Potential applications include augmented reality (AR), virtual reality (VR), ultra-reliable industrial automation, and connected transportation [9]. Integrated sensing and communication (ISAC) are also expected to support systems that jointly communicate, sense their environment, and adapt their operation accordingly [10].

AI and ML are increasingly used in IoT networks for prediction, anomaly detection, and resource optimization. Edge computing complements these methods by processing data close to the source, which reduces latency and traffic to centralized cloud infrastructure. Together, edge processing and learning-based control support more responsive and scalable IoT operation [9,10].

Security constitutes another fundamental requirement for IoT development, particularly in ultra-dense environments. The large number of connected devices expands the attack surface and requires robust security mechanisms to protect sensitive data and preserve system integrity. Encryption, secure key management, tamper detection, and rapid incident response are therefore essential for mitigating risks in IoT deployments. As IoT networks increasingly support critical applications such as autonomous transportation, smart grids, and public safety services, their reliability and availability become decisive for preventing severe service disruption. Consequently, UD-IoT networks require stable and scalable architectures that provide reliable communication, efficient resource management, security, and sufficient adaptability to cope with the dynamic and heterogeneous nature of future IoT applications [8,9]. Motivated by these challenges, this paper investigates robustness modeling and evaluation in UD-IoT ecosystems as a basis for reliable and scalable IoT-based automation.

1.1. Related Work

Research on UD-IoT networks has focused primarily on scalability, energy efficiency, reliability, and resource management in dense deployments. This section reviews representative contributions and positions the proposed robustness framework against quantitative resilience and operational assessment methods.

Research on dense IoT networks has addressed several complementary performance and architectural problems. Reference [11] provides a taxonomy of ultra-dense networks and associated KPIs, establishing a broad basis for characterizing density, capacity, latency, and efficiency. Reference [12] studies secure collaborative computation offloading and resource allocation in cache-assisted ultra-dense IoT networks, with emphasis on energy, delay, computing resources, and security constraints. Reference [13] surveys massive machine-type communications in ultra-dense cellular IoT networks, including radio access network (RAN) congestion, access mechanisms, QoS issues, and machine-learning-assisted solutions such as Q-learning. Reference [14] proposes cooperative micro-caching through network functions virtualization (NFV) and fuzzy inference to reduce network traffic and service latency. The information-freshness problem is addressed in [15] through Age of Information (AoI) analysis for computation-intensive IoT, while ref. [16] considers data aggregation as a means of reducing transmission overhead and improving efficiency in ultra-dense wireless networks. Reference [17] formulates AoI-aware resource allocation

with interference avoidance for ultra-dense industrial IoT, and ref. [18] analyzes cellular ultra-dense IoT performance under wireless backhaul constraints. At the architectural and resource-management levels, ref. [19] proposes software-defined networking (SDN)-based network slicing for dense and ultra-dense IoT networks, whereas ref. [20] addresses fairness and resource efficiency in multi-access edge computing (MEC)-enabled ultra-dense IoT using non-orthogonal multiple access (NOMA). These studies provide important solutions for access congestion, information freshness, caching, interference, backhaul, slicing, and resource allocation, but they do not provide a common operational robustness score that preserves continuity, resource efficiency, adaptability, and security as separately interpretable dimensions.

These studies establish the performance and architectural context for UD-IoT, while the resilience-focused works in [21–30] provide the closest basis for comparison with the proposed evaluation framework.

Studies [21–30] represent several complementary views of resilience and operational assessment. Nooraei Abadeh and Mirzaie [21] quantify IoT process-chain resilience from changes in performance and availability following disruption. Abbas et al. [22] evaluate the robustness of scale-free IoT topologies under node and link attacks, while Sebestyen and Kopjak [23] define a stability factor for mesh sensor data collection with redundant paths. Wang et al. [24] combine connectivity, communication efficiency, and information entropy to assess industrial Internet of Things (IIoT) topology resilience under heterogeneous attacks. Berger et al. [25] provide a broader taxonomy of IoT resilience mechanisms, and Abadia et al. [26] survey architectural frameworks for smart city IoT. Houichi et al. [27] focus on smart city cybersecurity and intrusion detection. At the 5G infrastructure level, Zieba et al. [28] address cloud-enabled 5G core deployment and analytics, Barbosa et al. [29] evaluate open-source 5G core platforms and performance, and Giambartolomei et al. [30] examine security testing of 5G core web technologies.

Taken together, these studies provide complementary perspectives on quantitative resilience, structural robustness, architectural organization, cybersecurity, and 5G implementation. However, these aspects are generally evaluated separately and are not combined through a common operational procedure. To clarify this gap, Table 1 compares the studies most closely related to the present work. The distinguishing contribution of the proposed framework is the integration of heterogeneous operational indicators into the interpretable dimensions OC, SRE, NF, and SEC, together with an aggregate R value, while linking the evaluation procedure to both simulated UD-IoT behavior and measurable 5G service indicators.

Table 1. Comparative positioning of related IoT resilience, smart city IoT, cybersecurity, and 5G validation approaches.

Study	Main Focus	Methodological Distinction/Limitation
Nooraei Abadeh and Mirzaie [21]	Quantitative resilience of IoT process chains	Measures resilience from performance and availability before and after disruption and uses structural activity metrics. The study focuses on process-chain resilience.
Abbas et al. [22]	Topology robustness of scale-free IoT networks	Quantifies robustness under node and link attacks and evaluates topology rewiring. The study focuses on structural connectivity under attacks.
Sebestyen and Kopjak [23]	Stability factor for mesh sensor data collection	Quantifies data-collection stability from path redundancy and tolerated failures. The study focuses on a specific mesh routing and collection mechanism.
Wang et al. [24]	IIoT topology resilience under heterogeneous attacks	Uses connectivity, communication efficiency, and information entropy to assess topology reconfiguration. The study focuses on attack-driven structural resilience.

Table 1. *Cont.*

Study	Main Focus	Methodological Distinction/Limitation
Berger et al. [25]	IoT resilience taxonomy and mechanisms	Provides conceptual resilience categories but does not operationalize them into a measurable multi-domain evaluation procedure.
Abadia et al. [26]	Smart city IoT framework layers	Focuses on architectural layering and smart city IoT organization but does not quantify cross-layer degradation under dense deployments.
Houichi et al. [27]	Smart city cybersecurity and intrusion detection	Addresses cyber-threat detection, but does not jointly evaluate operational continuity, scalability, flexibility, and service recovery.
Zieba et al. [28]	Cloud-enabled 5G core deployment	Provides deployment-oriented 5G core insights but remains focused on implementation feasibility and does not provide an IoT robustness assessment.
Barbosa et al. [29]	Open source 5GC platform performance	Evaluates 5G core performance indicators but does not relate them to perception layer IoT reliability, adaptability, or security behavior.
Giambartolomei et al. [30]	5G core web-security testing	Focuses on security testing of 5G core components, but does not include scalability, recovery, or multidimensional service robustness.
Proposed framework	Operational UD-IoT robustness assessment with explicit normalization, nonlinear transformations, dimensional grouping, and 5G connectivity validation	Preserves the OC, SRE, NF, and SEC decomposition, maps measurable indicators to engineering dimensions, and produces an interpretable aggregate R value.

The proposed framework extends beyond a simple weighted sum of independent KPIs. Entropy-based complexity measures summarize uncertainty, heterogeneity, or state dispersion and are useful for describing global system complexity. Here, the engineering objective is different. Each indicator is assigned an operational direction, normalized to a common scale, transformed when inverse behavior, thresholds, saturation, or diminishing effects are relevant, and grouped according to its physical meaning within OC, SRE, NF, or SEC. Aggregation is performed only after these steps, preserving the engineering meaning of the indicators and the source of robustness degradation.

1.2. Motivation

UD-IoT robustness extends beyond conventional reliability because dense deployments combine interference, energy constraints, rapidly changing traffic, and cyber-physical threats. A robust network must preserve service under failures and attacks while adapting to changes in traffic, topology, and operating conditions. These requirements are particularly stringent in smart-city and industrial settings, where service interruption can affect monitoring or control functions. This motivates a multidimensional evaluation that captures operational continuity, resource pressure, adaptability, and security within a common framework.

UD-IoT architecture design involves conflicting objectives: increasing system resilience while preserving scalability and energy efficiency. High-density deployments naturally strain resources, creating bottlenecks in data transmission, processing, and storage. Consequently, an approach that strengthens one UD-IoT component may weaken another. For example, solutions that prioritize scalability may lack security consideration, making

networks susceptible to attacks. Conversely, highly secure frameworks may introduce latency or inefficiencies that are prohibitive for real-time applications.

To account for these challenges, this study defines robustness as a multi-dimensional attribute derived from the dominant failure modes of UD-IoT networks. Service interruption and delayed recovery are represented through operational continuity (OC). Resource saturation and inefficient scaling are captured by scalable resource efficiency (SRE). Topology, protocol, and traffic variability are addressed through network flexibility (NF), while unauthorized access, tampering, and incident response are represented through security (SEC). These four dimensions are therefore selected because they correspond to the main sources of degradation in dense IoT deployments and jointly describe the ability of the network to remain operational, scalable, adaptable, and protected under stress. The goal is to develop an evaluation methodology that addresses these dimensions individually while also considering their interdependencies to support balanced and optimized UD-IoT architectures in the context of smart city deployments.

This article addresses two main research questions. The first concerns how robustness in UD-IoT networks can be defined and measured in a structured way. By integrating measures that represent practical challenges, including device density, fault tolerance, and dynamic adaptability, the study provides a definition and assessment framework for robustness. The second concerns how the robustness framework responds to different deployment classes and operational stress conditions. In this regard, the paper evaluates trade-offs across deployment scenarios and examines how changes in continuity, scalability, flexibility, and security are reflected in the resulting scores.

Equations (1)–(5), the four robustness dimensions, and the original simulation scenarios were introduced in [31] and are reused here as the mathematical baseline. The contribution of this study is their operationalization for smart-city UD-IoT environments through a detailed perception-layer interpretation, an explicit normalization and indicator-mapping procedure, a controlled 5G connectivity validation environment based on free5GC and UERANSIM, and a procedure for deriving OC, SRE, NF, SEC, and R from measurable network and service indicators. The study further develops the engineering interpretation of parameter interactions, weighting, monitoring, limitations, and implementation pathways.

Table 2 distinguishes the elements inherited from [31] from the extensions evaluated in this study.

The main contributions of this paper are summarized as follows:

- The mathematical formulation introduced in [31] is retained, while its interpretation is developed for smart city perception layer infrastructures by linking OC, SRE, NF, and SEC to concrete operational degradation mechanisms.
- An explicit normalization and indicator mapping procedure is introduced to transform measurable control plane, user plane, service connectivity, recovery, and security indicators into OC, SRE, NF, SEC, and the aggregate R metric.
- The operationalized framework is evaluated in a controlled free5GC and UERANSIM 5G connectivity environment, and a practical pathway is defined for continuous monitoring and future validation with physical IoT hardware.

The rest of the paper is organized as follows: Section 2 presents the architecture of UD-IoT networks and their main implementation challenges. Section 3 outlines the proposed robustness evaluation methodology and defines the parameters and sub-parameters used to assess different performance aspects of UD-IoT networks. Section 4 analyzes the behavior of the proposed metrics across diverse deployment scenarios and introduces a 5G connectivity validation environment, where measured core-network and service connectivity indicators are transformed into robustness-related components. Finally, Section 5 discusses the

findings, summarizes the main contributions, and identifies directions for future work on robust UD-IoT networks.

Table 2. Traceability of elements inherited from [31] and extensions evaluated in this study.

Element	Relation to [31]	Role in This Study
Equations (1)–(5)	Introduced in [31]	Reused as the common mathematical core. No new algebraic formulation is claimed.
OC, SRE, NF, SEC and their original subparameters	Introduced in [31]	Core definitions retained. Engineering interpretation and measurement pathway expanded.
Critical, Essential, and Basic deployment simulation	Introduced in [31]	Reused as the simulation stage and linked to the broader validation workflow.
Component-level CDF and PDF analysis (OC, SRE, NF, and SEC)	Not present in [31]	New component-level CDF and PDF analysis for OC, SRE, NF, and SEC.
Overall robustness distribution analysis	Corresponds to the robustness distribution analysis in [31]	Adapted from [31], with additional interpretation in this study.
Stress-scenario time-series analysis, simulation setup, and summary statistics	Stress scenario analysis originates from [31]	Stress-scenario evidence from [31], with the aggregation and smoothing procedure documented and the event-intensity limitation stated explicitly.
5G connectivity validation setup, KPI mapping, normalization, scenario results, weighting, and baseline comparison	Not present in [31]	5G connectivity mapping, scenario measurements, normalization, weighting documentation, and baseline comparison.
Smart city implementation pathway and limitations	Not present in [31]	Operational interpretation, monitoring pathway, limitations, and deployment discussion.

2. UD-IoT Networks Architecture and Implementation Challenges

As highlighted earlier, UD-IoT networks are recognized for their ability to integrate a vast number of devices within a limited area. These networks address the growing need for considerable IoT connectivity by significantly improving both capacity and efficiency. UD-IoT architecture is designed to support very high device densities, potentially reaching thousands of devices per square kilometer depending on the access technology, spectrum, traffic model, and deployment conditions. This density objective does not by itself guarantee seamless connectivity and creates significant interference and resource management challenges. Their architecture is optimized to process large volumes of data efficiently, providing fast and responsive communication with minimal delays. To achieve this, these networks are outfitted with advanced methods and algorithms for adaptive resource allocation, interference mitigation, and overall system optimization, enabling them to maintain high performance despite the challenges of extreme device density. This makes the UD-IoT concept particularly suitable for smart city environments, where a large number of sensors, meters, cameras, access-control devices, and mobile or static monitoring nodes must operate within geographically limited urban areas while supporting low-latency, reliable, and context-aware services.

Both ultra-dense and massive IoT networks are designed to support large numbers of connected devices, but they differ in deployment objectives and operational implications. UD-IoT networks focus on very high device densities within spatially constrained areas such as smart cities, industrial zones, and stadiums, where reliable communication and interference management are critical [18]. Massive IoT networks, by contrast, address

large numbers of heterogeneous devices distributed over wider geographical areas, as in smart agriculture and energy grids, where scalability and coverage become dominant requirements [15]. UD-IoT therefore emphasizes interference management, low-latency delivery, and high-capacity connectivity, whereas massive IoT places greater emphasis on simple, energy-efficient, wide-area operation. Low-power wide-area network (LPWAN) technologies and Narrowband IoT (NB-IoT) are particularly relevant to the latter class. The main distinctions are summarized in Table 3.

Table 3. Comparison between UD-IoT and massive IoT networks.

Aspect	UD-IoT	Massive IoT
Focus	Spatial density	Quantity of devices
Geographical area	Small	Wide
Device density	Very high	Moderate
Communication efficiency	High	Moderate
Latency requirements	Low latency required	Moderate latency acceptable
Data rate	High	Moderate
Energy efficiency	Less emphasis	High emphasis
Application scenarios	Smart buildings, stadiums, urban areas	Agricultural fields, utility grids, transportation networks

This study focuses on UD-IoT because dense urban and industrial deployments combine high endpoint concurrency with low-latency and high-throughput requirements. Representative use cases include autonomous transportation, smart-city sensing, and precision manufacturing. These environments expose practical challenges in interference management, resource allocation, scalability, and service continuity.

A UD-IoT network builds on conventional IoT architecture while increasing the density of connected devices and access points. The architecture can be organized into several layers with distinct roles. This study focuses primarily on the perception layer (PL), which connects physical sensing and actuation to the digital network. The PL includes sensor nodes, actuators, wearables, smart appliances, cameras, unmanned aerial vehicles (UAVs), connected vehicles, visible light communication (VLC) light-emitting diodes (LEDs), low-earth-orbit (LEO) satellites, smart meters, healthcare devices, and smart tags (Table 4). In UD-IoT deployments, the high spatial density of these devices enables granular and timely data collection but also increases traffic, interference, resource pressure, and exposure to failures or attacks.

Table 4. Comprehensive classification of devices and communication media in UD-IoT networks.

Category	Sub-Category	Brief Description
End Devices	IoT sensor nodes	Environmental sensors, smart meters, wearable health trackers
	Machine-type communication (MTC) devices	Industrial IoT machines, autonomous robots
	Consumer electronics	Smartphones, smart appliances, etc.
	Aerial Systems	Drones and low-earth-orbit satellites
	Extended reality (XR) equipment	AR, VR, and mixed reality (MR) devices
	Intelligent wearables	Smartwatches, fitness trackers, healthcare monitoring devices

Table 4. *Cont.*

Category	Sub-Category	Brief Description
	Body Implants	Biomedical IoT devices for healthcare
Network Infrastructure	Static Access Points	Concentrators, Gateways, Small cell base stations, macro base stations, antennas
	Dynamic access points	Unmanned aerial vehicles (UAVs) or drones serving as mobile base stations
	Backhaul Systems	Fiber optics, millimeter-wave gateways
	Edge gateways	IoT gateways with processing and data aggregation capabilities at the edge
Communication Media	Radio-frequency (RF) technologies	LoRa, Sigfox, Zigbee, NB-IoT, 5G/6G
	VLC	Light-emitting diode (LED) arrays for high-density communication
	Acoustic Systems	Underwater IoT nodes
	Quantum Communication Nodes	Future-proof secure communications
	Terahertz Communication	High-bandwidth communication in terahertz spectrum for ultra-fast data transfer
	Backscatter Communication	Passive communication using reflected signals for low-power IoT devices

Higher spatial and temporal sensing density can improve monitoring granularity and environmental awareness, but it also increases traffic volume and may increase latency, interference, and resource pressure if the network is not provisioned appropriately. These trade-offs make robustness in the perception layer a central evaluation problem, as summarized in Table 5. The perception layer must remain adaptable across heterogeneous operating environments. End devices may operate under harsh physical and communication conditions, including extreme weather, vibration, interference, and tampering risks, while many devices also depend on batteries or energy-harvesting sources with constrained energy budgets.

Edge computing processes dense IoT data close to the source, reducing response time and the volume of traffic sent to centralized cloud infrastructure. Edge servers can perform filtering, local analytics, and ML-assisted decisions before forwarding selected data upstream. At the perception layer, scalability, security, and interoperability remain essential. New devices must be integrated without excessive performance loss, sensitive data must be protected against unauthorized access and tampering, and heterogeneous devices must interoperate across vendors and communication technologies. Because perception-layer failures directly affect sensing, actuation, and data delivery, the robustness of this layer has a direct impact on end-to-end UD-IoT reliability.

For UD-IoT architectures to support robust operation, they must be accompanied by evaluation metrics capable of characterizing resilience against failures, performance under high-load conditions, scalability, adaptability, and security behavior. This paper therefore emphasizes the perception layer while maintaining the proposed robustness model as extensible to other layers of the UD-IoT architecture. Future extensions can examine the Network Layer, where transmission protocols must provide scalability, security, and fault tolerance, as well as the Middleware and Application Layers, where data processing, service delivery, and security policies influence end-to-end robustness. A systematic evaluation of these parameters across all layers can support the development of resilient, sustainable, and scalable IoT architectures.

Table 5. Key vulnerabilities and challenges of the perception layer in UD-IoT networks.

Category	Vulnerabilities and Challenges	Description
Interference and Noise	Device-to-Device Interference	High device density leads to radio frequency interference, degrading communication quality.
	Environmental Noise	Environmental factors such as industrial noise or urban signal pollution can disrupt data collection and accuracy.
Energy Constraints	Limited Battery Life	Many devices are battery-operated, creating challenges for long-term operation in high-density deployments.
	Energy Harvesting Limitations	Energy harvesting systems struggle to provide sufficient power for densely deployed devices.
Data Fidelity	Data Collision and Loss	High density increases the likelihood of data packet collisions, leading to loss or corruption of information.
	Sensor Calibration Drift	Continuous operation in harsh environments can cause sensors to lose accuracy over time.
Security Risks	Unauthorized Access	Devices may lack robust authentication, making them vulnerable to unauthorized access or data breaches.
	Tampering and Physical Attacks	Physical access to sensors can result in tampering, compromising data integrity and device functionality.
	Man-in-the-Middle Attacks	Data transmitted between devices is susceptible to interception and manipulation.
Interoperability Issues	Heterogeneous Devices	Diverse device types and manufacturers can cause compatibility problems.
	Protocol Incompatibility	Differing communication protocols can disrupt data exchange and system functionality.
Latency and Bandwidth	High Latency in Dense Deployments	Data transmission delays increase due to congestion and limited bandwidth.
	Bandwidth Saturation	The high volume of data traffic can overwhelm communication channels.

3. Robustness Evaluation Methodology

In IoT architecture and design, robustness denotes the ability of a system to tolerate perturbations, failures, and hostile conditions while maintaining stable functionality. This property is particularly important in UD-IoT networks, where numerous interconnected devices operate within confined spaces and generate high operational loads. Robustness, in its general sense, includes the ability to withstand both internal and external disturbances, including hardware failures, environmental stressors, cyberattacks, and data leakage. Robust systems anticipate and mitigate such risks, thereby preserving service continuity and quality. This study focuses on the robustness of the perception layer as a system-level property, and not as an isolated property of individual processes such as topology design or resource configuration [32].

The four robustness dimensions defined below follow the formulation in [31]. The measurement mapping used to populate them from observable network and service indicators is presented in Section 4.3.

3.1. Key Characteristics of Robust Architectures

Robust UD-IoT operation requires architectures that maintain stable service under high density, failures, variable load, and security threats. The main characteristics considered in this study are:

- Adaptability to network stress—the ability of the network to perform well in a variety of difficult scenarios, such as traffic spikes or external disruptions.
- Failure resilience—the ability to recover and operate through failure with minimal disruption to services.
- Efficiency under varying load—the ability to optimize the usage of network resources, like energy, bandwidth, and computation in order to handle varying demands without degrading system performance.
- Security and privacy—the ability of the network to be adequately resistant to various types of attacks or unauthorized access, while preserving sensitive information and maintaining trustworthiness.
- Scalability—it is defined as the capacity to expand the network environment and to cater to the growing number of devices and connections seamlessly without affecting system performance or resilience.
- Interoperability—the ability to integrate and communicate seamlessly with different devices, technologies, and protocols, ensuring a flexible and connected ecosystem.

These features are represented within the four main parameters of the proposed robustness metric, providing an integrated evaluation mechanism for UD-IoT performance and resilience.

3.1.1. Operational Continuity—OC

In UD-IoT networks, OC characterizes resilience and reliability in support of seamless operation and consistent performance. It reflects the ability of the network to withstand events such as hardware failures, software errors, and external disruptions. In connected environments such as IIoT systems, smart cities, and healthcare applications, the strong coupling between devices creates a risk of cascading failures. Under dynamic and uncertain operating conditions, a well-defined framework for maintaining operational functionality is crucial for achieving service stability and quality.

Early detection of anomalies and failures is an essential aspect of OC. By using real-time analytics and machine learning, advanced monitoring systems support preemptive detection and isolation of affected network components, thereby minimizing downtime. This shifts network operation from reactive maintenance toward proactive reliability management. Rapid recovery mechanisms, including redundant architectures and failover protocols, ensure continuity of critical functions during localized failures. In scenarios such as smart energy grids, these features are vital for preventing localized faults from escalating into system-wide outages. Moreover, data redundancy provides essential protection for data integrity under failure conditions through mechanisms such as synchronized backups or distributed ledgers. For example, in high-stakes environments such as healthcare IoT, these measures are essential for preserving system functionality and integrity, both of which depend on the continuous availability of accurate and reliable data. Based on these principles, Equation (1) represents the OC metric.

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

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, and DRL is the Data Redundancy Level.

The OC metric is designed to capture the essential elements of system resilience and reliability in UD-IoT networks. MTTR represents the time it takes to restore functionality following a failure, with lower values indicating quicker recovery and fewer service interruptions. FDR reflects the system's ability to detect faults proactively, where higher values point to more advanced detection mechanisms. SAR measures how consistently the system operates without failure, acting as a foundational indicator of reliability. SCI assesses the proportion of sensors maintained within their recommended calibration schedules, offering a clear picture of the network's ability to preserve accuracy and precision over time. Finally, DRL quantifies data redundancy, ensuring that information remains accessible even during system faults—a critical factor in maintaining integrity in demanding environments.

The OC formula combines these sub-parameters using mathematical transformations that reflect their operational relevance while accounting for IoT constraints. For example, the term $(1 - \text{MTTR})$ emphasizes the improvement in operational continuity as recovery times are reduced. The FDR term is directly weighted, reflecting its proportional impact on OC. The sigmoid function applied to SAR scales its contribution, emphasizing significant performance shifts near the threshold parameter θ and diminishing returns beyond this range. The SCI and DRL terms are raised to a power p to account for their nonlinear impact on system performance, reflecting increasing challenges in achieving marginal improvements at higher levels. Weighted coefficients provide flexibility, allowing the formula to adapt to varying operational contexts, such as critical infrastructure or urban environments. This formulation enables scenario-dependent evaluation of OC under different operational priorities.

3.1.2. Scalable Resource Efficiency—SRE

SRE plays an important role in UD-IoT networks because device density increases rapidly while spectrum, energy, bandwidth, and computational resources remain limited. With the growing adoption of IoT, networks must support scalable operation without compromising performance or sustainability. SRE therefore characterizes the ability of the network to sustain increasing device densities while limiting resource saturation and preserving operational reliability. This requirement is particularly important in ultra-dense deployments, where interference, limited bandwidth, and the coordination of thousands of devices create substantial resource-management challenges. In urban IoT scenarios, dynamic resource allocation and efficient spectrum utilization are therefore necessary for stable service operation, while in resource-constrained deployments, energy-aware communication protocols support long-term system sustainability.

SRE is supported by both hardware- and software-level mechanisms. Hardware-level optimizations include energy-efficient sensors, advanced battery technologies, and power-management systems, whereas software-level mechanisms include intelligent resource allocation, traffic optimization, and data compression. Together, these mechanisms support scalable and energy-aware operation in dense IoT deployments. This dual focus on performance and sustainability enables SRE to support long-term IoT operation across smart cities, industrial automation, and remote agricultural systems. Based on these characteristics, Equation (2) is used to represent the SRE metric.

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

where SDR is the Sensor Deployment Ratio, ITI is the Integration Time Index, THE is the Traffic Handling Efficiency, SPU is the Sustainable Power Utilization, and EA is the Expansion Agility.

The SRE metric addresses the challenges of dense IoT deployment and resource utilization. SDR characterizes the ratio of deployed sensors to system demands and highlights the need for efficient resource allocation as network scale increases. ITI reflects the system's ability to integrate new devices quickly, with lower values indicating faster and smoother integration processes. THE measures the ability of the network to manage traffic efficiently, ensuring that increased data traffic can be processed without compromising performance. SPU measures the power efficiency of the network, which is particularly important for power-constrained devices. Finally, EA assesses the system's ability to adapt to changes in scale or demand, ensuring flexible and responsive operation under dynamic conditions.

The SRE formula integrates these sub-parameters using mathematical transformations that reflect their operational significance while balancing scalability and efficiency. For instance, the SDR term is scaled using a power function, highlighting diminishing returns as efficiency approaches its upper limit while prioritizing early gains. Similarly, a square-root transformation is applied to SPU, emphasizing its impact while accounting for diminishing marginal improvements. The $(1 - \text{ITI})$ term inversely penalizes slower integration times that could hinder network growth. THE is treated linearly to reflect its direct contribution to maintaining reliable service under increasing traffic loads. The sigmoid function applied to EA captures the nonlinear relationship between adaptability and system efficiency, emphasizing significant changes near the threshold θ and diminishing effects beyond that point. Weighted coefficients provide flexibility, allowing the formula to align with specific operational goals, such as energy conservation in remote IoT deployments or dynamic scalability in urban environments. This formulation supports the evaluation of scalability and resource efficiency across diverse IoT application scenarios.

3.1.3. Network Flexibility—NF

NF represents the ability of a UD-IoT network to adapt to changing operational conditions while preserving interoperability among heterogeneous devices and communication protocols. As IoT ecosystems become increasingly complex, they must integrate diverse device types, communication standards, traffic patterns, and service requirements. In this context, NF captures both adaptability, reflected in the network response to changes in traffic load, topology, and environmental conditions, and interoperability, reflected in the ability of devices from different manufacturers and protocol families to communicate reliably.

In healthcare IoT, for instance, NF enables the seamless integration of new technologies such as wearable sensors or diagnostic equipment into existing systems, even as patient needs and workloads shift. Similarly, industrial IoT (IIoT) deployments rely on NF to accommodate machinery upgrades or changes in communication protocols without disrupting production processes. Smart city applications, including adaptive traffic management and real-time environmental monitoring, also depend on highly flexible networks to handle diverse devices, variable data streams, and mobility patterns. By supporting dynamic configuration, such as automatic routing adjustments or bandwidth prioritization, and ensuring protocol compatibility across communication standards, NF enables IoT networks to remain responsive and resilient in a variety of scenarios. This adaptability, combined with the ability to harmonize interactions between heterogeneous devices, positions NF as a foundational enabler of scalable and robust IoT systems. In this study, NF is calculated using Equation (3):

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

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

The NF metric integrates sub-parameters that characterize the adaptability and interoperability of UD-IoT networks, both of which are critical in dynamic and heterogeneous environments. FUR measures how often firmware updates are released, directly influencing adaptability by keeping devices updated with new features and security patches. PCS quantifies compatibility across different communication protocols and facilitates interaction between devices operating across diverse protocol families. DCI indicates the normalized time required for a network to reconfigure after a change in topology or operating state. TPA evaluates the network's ability to respond to varying traffic patterns, ensuring consistent performance under fluctuating loads. Finally, DI represents the ease with which new devices can be integrated, reflecting network scalability and integration capability.

The NF formula combines these parameters using mathematical transformations that represent their operational impact. FUR is treated linearly, highlighting its direct contribution to adaptability and fault tolerance. PCS is scaled using a power function, reflecting diminishing returns as interoperability improves and prioritizing early gains. The term $(1 - \text{DCI})$ inversely captures the impact of slower reconfigurations, emphasizing the importance of rapid adaptability under dynamic conditions. The sigmoid function applied to TPA represents its nonlinear influence, rewarding networks that handle diverse traffic efficiently while moderating diminishing returns as adaptability reaches a threshold θ. DI is included linearly, emphasizing its role in seamless device integration, which is essential for scalability in complex IoT ecosystems. Weighted coefficients allow the formula to prioritize specific parameters based on deployment needs, such as rapid adaptability in industrial IoT or enhanced interoperability in smart city applications. This formulation supports the evaluation of NF under heterogeneous and dynamic UD-IoT conditions.

3.1.4. Security—SEC

SEC is a core requirement for preserving trust, data confidentiality, and consistent operation in high-density and heterogeneous UD-IoT environments. As the number of connected devices increases in these networks, the probability of exploitable vulnerabilities also increases, with each device acting as a potential entry point for cyber threats. These devices range from sensors and actuators to gateways and must be protected against threats such as unauthorized access, data breaches, malware, and distributed denial of service (DDoS). In applications such as smart healthcare, a security compromise may expose privacy-sensitive and potentially life-critical information or services. Likewise, in industrial IoT contexts such as manufacturing and energy grids, an intrusion may disrupt supply chains or affect critical infrastructure, with potentially severe economic and social consequences.

To address these challenges, a responsive security framework combining proactive and reactive mechanisms is required. Proactive mechanisms include encryption of transmitted data, multi-factor authentication for preventing unauthorized access, and secure boot procedures for preserving device integrity from startup. Reactive mechanisms reduce the impact of incidents through real-time monitoring, intrusion detection systems (IDS), and automated mitigation procedures. Because UD-IoT networks are highly dynamic and devices are regularly added or reconfigured, temporary vulnerabilities must be detected and mitigated before they can be exploited. Compliance with industry regulations is also important, particularly in verticals such as healthcare and finance. By satisfying these

requirements, the network reduces legal and operational risks while improving user trust. Equation (4) quantifies these security-related aspects:

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

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 Rate, and RIM is the Response to Security Incidents.

The SEC metric aggregates important sub-parameters to assess the resilience of UD-IoT networks against various types of attacks. EKS captures effective encryption and key management and represents the primary line of defense for data confidentiality, ensuring that sensitive information cannot be disclosed to or accessed by unauthorized entities. UAD measures the system's ability to detect unauthorized access attempts, enhancing overall security by identifying potential breaches before they escalate. TDI represents the frequency of tamper-related incidents. Lower values indicate stronger tamper protection and reduced physical attack risk. FIC reflects the frequency of firmware integrity checks, preventing unauthorized changes to device firmware. Finally, RIM characterizes the effectiveness of identifying and resolving security events, indicating whether the network can continue to operate reliably under threat conditions.

The SEC formula balances the contribution of these parameters through mathematical transformations. EKS is modeled linearly to emphasize its role in security management across diverse IoT applications. The $(1 - \mathrm{TDI})$ term inversely represents tamper-related incident occurrence, so lower normalized TDI values contribute positively to security robustness. FIC is scaled using a power function to represent diminishing returns as firmware integrity improves. The square root transformation applied to UAD moderates the effect of very high detection rates while preserving meaningful contributions across the normalized range. The sigmoid function applied to RIM captures the nonlinear benefit of improved incident response near the threshold parameter θ and diminishing effects beyond that region. Weighted coefficients provide flexibility to align the metric with deployment priorities, such as stronger physical protection and firmware integrity in industrial IoT or access security in smart city services.

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

OC, SRE, NF, and SEC should be interpreted as conceptual robustness dimensions and not as immutable numerical categories. This interpretation emphasizes their role as fundamental building blocks for UD-IoT architecture design. The specific measurable sub-parameters associated with each dimension may evolve as monitoring technologies and deployment requirements change. However, the conceptual structure provides a stable basis for evaluating robust, scalable, and adaptable IoT systems.

Together, Equations (1)–(4) provide the four-dimension scores used in the aggregate robustness metric defined next.

3.2. Robustness

The overall robustness, R, represents an aggregate measure derived from the four parameters previously described:

$$\mathrm{R} = \alpha_1 \cdot \mathrm{OC} + \alpha_2 \cdot \mathrm{SRE} + \alpha_3 \cdot \mathrm{NF} + \alpha_4 \cdot \mathrm{Sec}, \quad (5)$$

The formula provides a structured and integrative mathematical representation of system robustness by combining the four key performance factors presented above. The

coefficients of the overall robustness metric provide flexibility to emphasize OC, SRE, NF, and SEC according to the deployment scenario or application requirements.

Because the weighting coefficients within each main parameter sum to one, each component contributes proportionally to the corresponding robustness dimension. This normalization provides a consistent basis for comparing metric behavior across the defined deployment scenarios while keeping the component scales comparable. All subparameters and their brief descriptions are presented in Table 6. To prevent the model from being interpreted as an arbitrary weighted aggregation, the selected subparameters and nonlinear transformations are associated explicitly with their operational meaning. Each subparameter corresponds to a degradation mechanism considered relevant to dense smart-city IoT deployments, including service interruption, delayed recovery, resource saturation, traffic overload, limited adaptability, interoperability degradation, and security exposure. Linear terms are applied where contribution is modeled proportionally, inverse terms where lower delay or incident values are favorable, power and square-root transformations where diminishing effects are intended, and sigmoid functions where threshold behavior is represented. The weighting coefficients are deployment-dependent policy parameters and are not treated as universal constants.

For practical deployment, the weights are obtained through a reproducible multi-criteria decision procedure instead of ad hoc selection. The Analytic Hierarchy Process (AHP) is used as the practical calibration workflow. At each aggregation level, the operator defines criteria from service objectives and service-level agreement (SLA) requirements and constructs a reciprocal pairwise priority matrix $A = [a_{ij}]$, with $a_{ii} = 1$ and $a_{ji} = 1/a_{ij}$. The unnormalized priority for criterion i is calculated from the row geometric mean $g_i = (\text{product over j of } a_{ij})^{\wedge 1/n}$), and the normalized coefficient is $w_i = g_i/\text{sum}(g_k)$. The procedure can be applied first to OC, SRE, NF, and SEC and then to the five subparameters within each dimension. Consistency is checked from lambda_max = mean$[(A_w)i/w_i]$, CI = (lambda_max $-$ n)/(n $-$ 1), and CR = CI/RI. A consistency ratio below 0.10 is used as the acceptance criterion. The Dirichlet procedure in Section 4.1 is used only for stochastic sensitivity assessment and is not the operational weight-selection method.

For the reference connectivity policy used in the connectivity-validation stage, the pairwise comparison matrix for [OC, SRE, NF, SEC] is A = [[1, 1, 2, 1], [1, 1, 1, 1], [1/2, 1, 1, 1], [1, 1, 1, 1]]. Applying the geometric-mean AHP procedure gives the normalized weight vector alpha = (0.2951, 0.2481, 0.2087, 0.2481). Using this vector, lambda_max = 4.0604, CI = 0.0201, and CR = 0.0224 for RI = 0.90 and $n = 4$. The consistency ratio is therefore below the 0.10 acceptance threshold. These coefficients are used for the final aggregation in the connectivity-validation stage and reproduce the displayed R values after rounding.

Within the connectivity-validation mapping, the five conceptual subparameters of each robustness dimension use equal base coefficients of 0.20 as a neutral reference before measurement availability is considered. A subparameter enters the connectivity score only when it is directly observable or when an explicit connectivity proxy is defined in the validation mapping. Hardware-dependent quantities without an available measurement or an explicit proxy are not assigned synthetic values. If AD denotes the active subparameter set for dimension D, the active coefficients are renormalized as w_tilde_i = wi/sum (wj for j in AD). This availability-aware rule preserves unit-sum weighting within each dimension and prevents unmeasured quantities from influencing the score. Deployment-specific implementations can replace the neutral base coefficients with AHP-derived subparameter priorities when the required measurements are available.

Table 6. List of sub-parameters and their brief description.

Sub-Parameter	Full Name	Brief Description
MTTR	Mean Time to Repair	The average time required to recover after a failure, a key indicator of network resilience.
FDR	Fault Detection Rate	The frequency of error detection, measuring the system's efficiency in identifying issues.
SAR	System Availability Ratio	The percentage of time the system operates correctly without interruptions.
SCI	Sensor Calibration Index	A measure of sensor calibration quality, reflecting network reliability over time.
DRL	Data Redundancy Level	The degree of redundant data availability or delivery preservation during failures, supporting continuity when individual data paths or copies are lost.
SDR	Sensor Deployment Ratio	The proportion of deployed sensors relative to the system's total capacity.
ITI	Integration Time Index	The normalized time required to integrate and activate new devices or sensors. Lower values indicate faster integration.
THE	Traffic Handling Efficiency	The network's efficiency in managing and routing data traffic.
SPU	Sustainable Power Utilization	A measure of energy efficiency in IoT device operation, critical for scalability.
EA	Expansion Agility	The network's ability to adapt to increases in scale or changes in structure.
FUR	Firmware Update Rate	The frequency of firmware updates, essential for network adaptability.
PCS	Protocol Compatibility Score	A score assessing compatibility between various network protocols.
DCI	Dynamic Configuration Index	The time for dynamic reconfiguration of the network in response to topology changes.
TPA	Traffic Pattern Adaptability	The network's adaptability to different traffic patterns.
DI	Device Interoperability Level	The ability of the devices to work seamlessly together, ensuring smooth integration and communication.
EKS	Encryption and Key Security	A normalized measure of encryption and key protection for valid communications and service access.
UAD	Unauthorized Access Detection Rate	The frequency of detecting unauthorized access, crucial for security.
TDI	Tamper Detection Incidents	The frequency of detected attempts to tamper with hardware or software.
FIC	Firmware Integrity Check Frequency	The frequency of firmware integrity checks, ensuring protection against vulnerabilities.
RIM	Response to Security Incidents	The effectiveness and speed of identifying, isolating, and responding to security-related incidents.

4. Simulation-Based Evaluation and 5G Connectivity Validation

This section evaluates the proposed robustness framework through two complementary stages. First, a simulation analysis is performed for the Critical, Essential, and Basic deployment scenarios to examine the mathematical behavior of OC, SRE, NF, SEC, and

R under controlled parameter ranges and varying operational priorities. These scenarios represent different trade-offs among reliability, scalability, flexibility, and security. Second, the framework is evaluated in a 5G connectivity environment, where observable network indicators are mapped to the proposed robustness dimensions. This stage demonstrates the operational use of the metric with measurable connectivity and service indicators. Full perception-layer validation with constrained physical IoT hardware remains outside the scope of this environment.

4.1. Simulation Setup

For the three deployment scenarios, broad stochastic sampling was used to examine the behavior of the framework across the parameter ranges in Table 7. The ranges represent different operational priorities. For example, the Critical Deployment scenario requires low MTTR and high FDR to represent fast recovery and strong fault detection, whereas the Basic Deployment scenario permits wider operating ranges consistent with less stringent service requirements. For each repetition, 10,000 parameter realizations were generated. A total of 100 repetitions were performed, with new normalized weights generated in every repetition. The weights were sampled from a symmetric Dirichlet distribution with equal concentration parameters, so no component is privileged by its identity during the sensitivity sampling. The parameter p used for power scaling of SCI, DRL, SDR, PCS, and FIC was set to 0.7. The sigmoid slope k was fixed at 10, with θ values of 0.97 for SAR, 0.8 for EA, 0.8 for TPA, and 0.85 for RIM. These values define the operating sensitivity of the nonlinear transformations used in the inherited formulation. Normalized probability density functions (PDFs) describe the distribution of the simulated metric values. The vertical axis therefore represents probability density, not probability. The simulation stage builds on the scenario formulation reported in [31] and is used here as the mathematical component of the broader operational validation workflow.

Table 7. List of sub-parameters' values range according to different deployment scenarios.

Parameter	Critical Deployment	Essential Deployment	Basic Deployment
MTTR	0.01–0.2	0.2–0.5	0.5–0.8
FDR	0.8–1.0	0.6–0.9	0.4–0.7
SAR	0.95–1.0	0.85–0.95	0.7–0.85
SCI	0.9–1.0	0.7–0.9	0.5–0.7
DRL	0.8–1.0	0.6–0.9	0.3–0.6
SDR	0.8–1.0	0.6–0.9	0.4–0.7
ITI	0.01–0.2	0.2–0.5	0.5–0.8
THE	0.8–1.0	0.6–0.9	0.4–0.7
SPU	0.9–1.0	0.7–0.9	0.5–0.7
EA	0.8–1.0	0.6–0.9	0.4–0.7
FUR	0.8–1.0	0.6–0.9	0.4–0.7
PCS	0.9–1.0	0.7–0.9	0.5–0.7
DCI	0.01–0.2	0.2–0.5	0.5–0.8
TPA	0.8–1.0	0.6–0.9	0.4–0.7
DI	0.9–1.0	0.7–0.9	0.5–0.7
EKS	0.9–1.0	0.7–0.9	0.5–0.7

Table 7. *Cont.*

Parameter	Critical Deployment	Essential Deployment	Basic Deployment
UAD	0.8–1.0	0.6–0.9	0.4–0.7
TDI	0.01–0.2	0.2–0.5	0.5–0.8
FIC	0.9–1.0	0.7–0.9	0.5–0.7
RIM	0.8–1.0	0.6–0.9	0.4–0.7

Because the weights are resampled across all 100 repetitions, this procedure also serves as a stochastic sensitivity assessment of the weighting scheme. For each robustness dimension, the five-element coefficient vector is sampled independently from the symmetric distribution Dirichlet (1, 1, 1, 1, 1), so every subparameter has the same prior concentration and no component is privileged by identity. The resulting OC, SRE, NF, SEC, and R distributions retain the same qualitative ordering of the Critical, Essential, and Basic deployment scenarios across the sampled weighting configurations. This indicates that the principal conclusions are not determined by one manually selected within-dimension weight vector.

The coefficients also have a direct engineering interpretation. Within each robustness dimension, they express the relative importance of the associated indicators, while the coefficients of the aggregate metric express the service priority assigned to OC, SRE, NF, and SEC. The Dirichlet sampling used in the simulation explores a broad weight space without fixing a preferred operating policy. In an operational deployment, the coefficients can be calibrated from service-level targets, service criticality, historical incident data, operator policy, and structured expert assessment. For example, critical infrastructure can assign greater importance to OC and SEC, while large-scale telemetry services can place greater emphasis on SRE and NF. The coefficients are normalized so that their sum within each aggregation stage equals one and the resulting robustness values remain comparable.

4.2. Analysis of Simulation Results

Figures 1 and 2 present the distributions of OC and SRE, respectively, and show clear separation among the Critical, Essential, and Basic deployment scenarios under the selected parameter ranges. The cumulative distribution function (CDF) and probability density function (PDF) curves place the Critical scenario at higher OC and SRE values with narrower dispersion, the Essential scenario in an intermediate region, and the Basic scenario at lower values with broader dispersion. These differences reflect the scenario assumptions imposed in Table 7 and should not be interpreted as an empirical ranking of real deployments. The slight change in shape visible in the OC density is consistent with the mixed input distributions used in the simulation, including the distinct treatment of MTTR relative to the other sampled parameters.

Similarly, the NF (Figure 3) and SEC (Figure 4) distributions show the same scenario ordering under the selected parameter ranges, with the Critical Deployment scenario concentrated at higher NF and SEC values. Essential and Basic Deployment exhibit broader distributions, with Basic Deployment showing the largest dispersion. These plots demonstrate the behavior of the mathematical formulation under the imposed scenario assumptions. They do not constitute independent empirical evidence that one deployment class is intrinsically superior outside those assumptions.

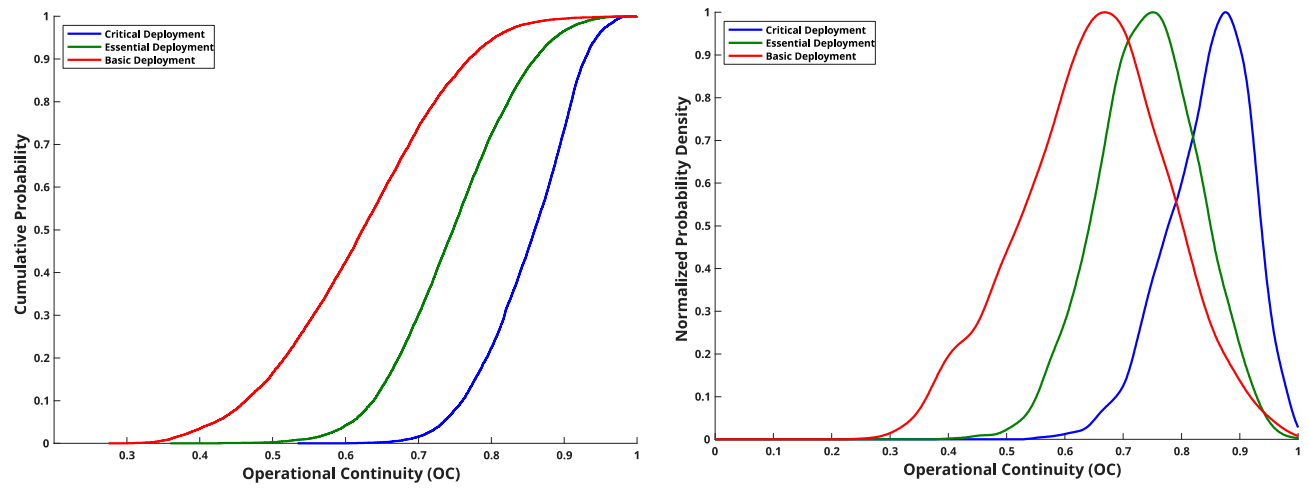


Figure 1. (**a**) CDF for OC across different deployment scenarios. Critical Deployment shows the highest levels of continuity, followed by Essential Deployment and Basic Deployment. (**b**) PDF for OC across the same scenarios, highlighting the relative densities of OC values. The sharper peak in Critical Deployment indicates more concentrated and higher values of OC compared to the broader distributions for Essential and Basic Deployments.

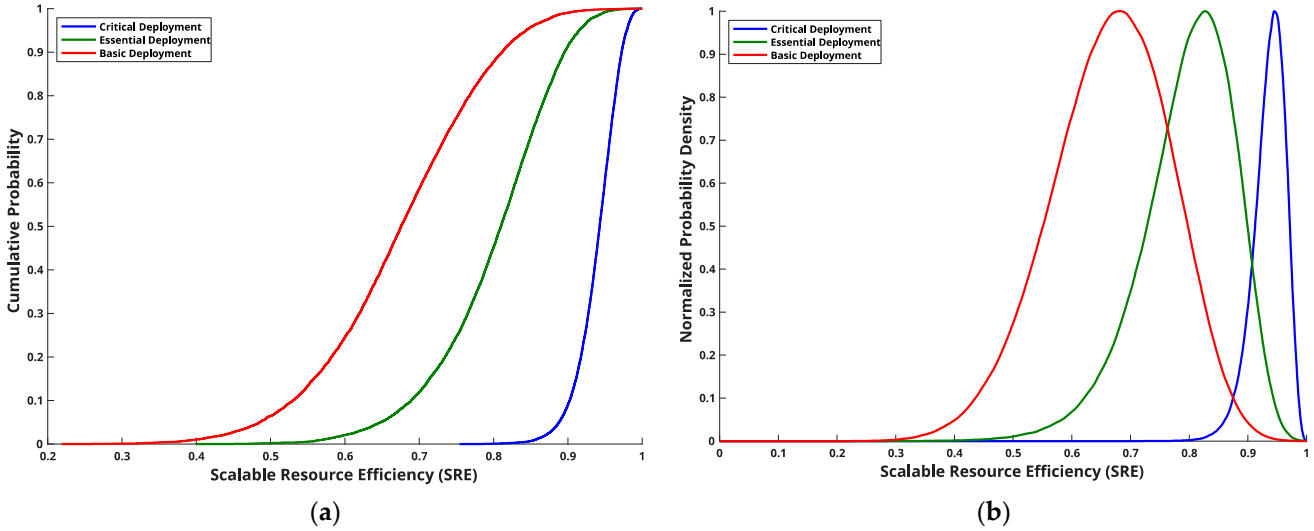
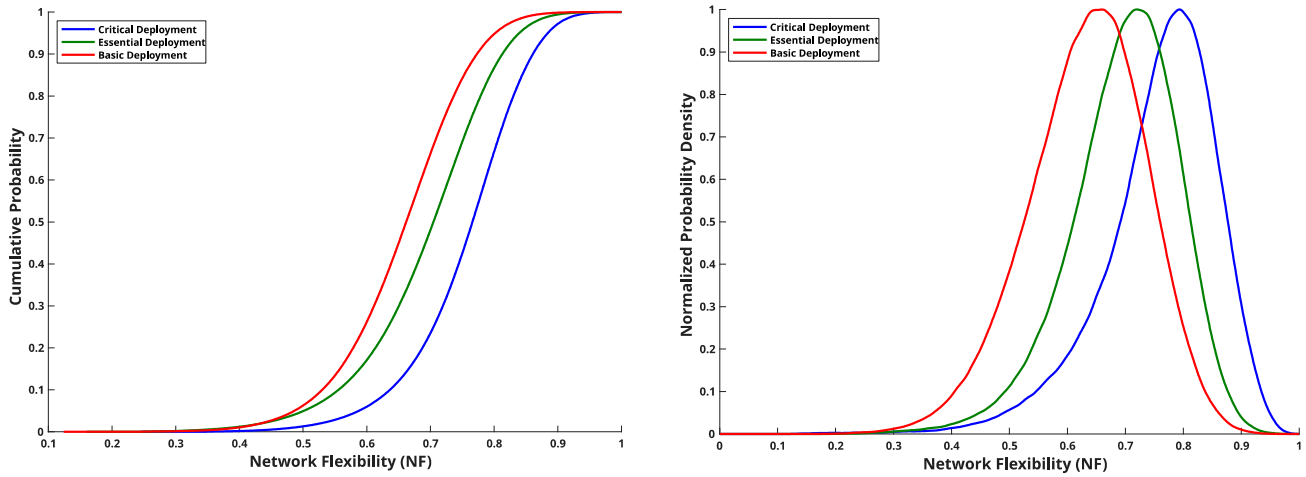


Figure 2. (**a**) CDF for SRE across different deployment scenarios. Critical Deployment shows the highest levels of resource efficiency, followed by Essential Deployment and Basic Deployment. (**b**) PDF for SRE across the same scenarios, illustrating the relative densities of SRE values. The sharper peak in Critical Deployment reflects more concentrated and higher values of SRE, while Essential and Basic Deployments show broader and more varied distributions.

These patterns illustrate the trade-offs produced by the selected deployment ranges. Under the simulation assumptions, Critical Deployment yields the highest and most concentrated OC, SRE, NF, and SEC values. Essential Deployment occupies an intermediate region, while Basic Deployment exhibits broader and generally lower distributions. The result is interpreted as scenario separation within the model, not as a universal ranking of real deployments. The CDF curves do not start at zero on the x-axis because several input parameters have strictly positive lower bounds, which shifts the distributions toward the operating ranges defined for each scenario.

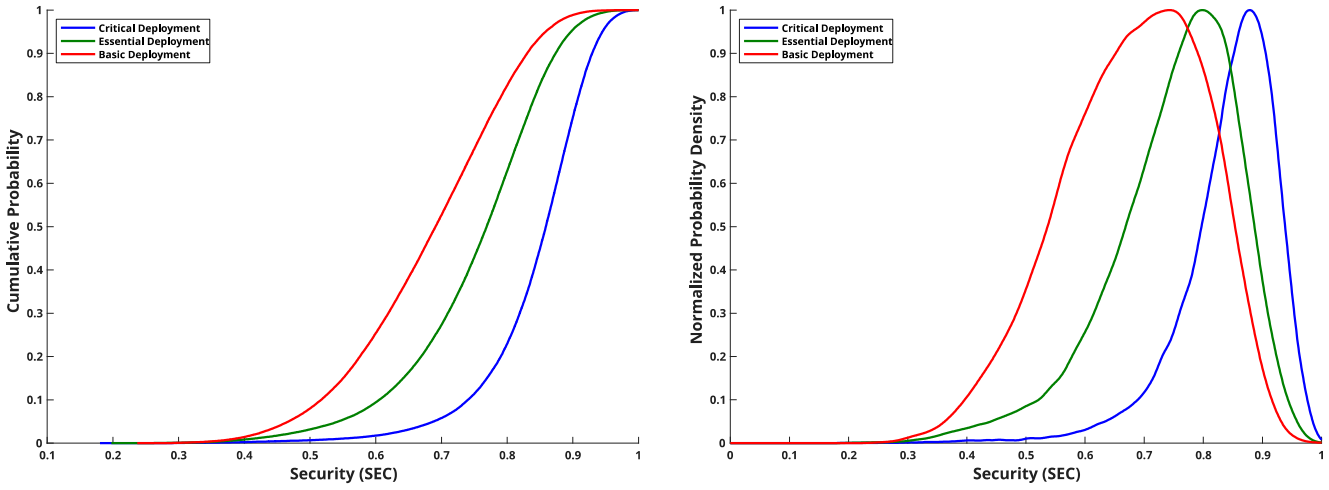
The simulation results show that the four parameter formulations respond consistently to the imposed value ranges and produce coherent differences across the simulated

deployment conditions. This demonstrates the internal consistency of the mathematical formulation under the selected assumptions. Empirical validation of complete perception-layer and physical IoT behavior requires direct hardware measurements.



(**a**) (**b**)

Figure 3. (**a**) CDF for NF across different deployment scenarios. Critical Deployment achieves the highest levels of flexibility, followed by Essential Deployment and Basic Deployment. (**b**) PDF for NF across the same scenarios, highlighting the relative densities of NF values. The sharper peak in Critical Deployment reflects more concentrated and higher NF values, while Essential and Basic Deployments exhibit broader and more varied distributions.



(**a**) (**b**)

Figure 4. (**a**) CDF for SEC across different deployment scenarios. Critical Deployment achieves the highest levels of security, followed by Essential Deployment and Basic Deployment. (**b**) PDF for SEC across the same scenarios, showing the relative densities of SEC values. The sharper peak in Critical Deployment indicates more concentrated and higher SEC values, whereas Essential and Basic Deployments demonstrate broader and more varied distributions.

Table 8 summarizes expected engineering relationships among selected subparameters and is used as a consistency check during weight elicitation. These relationships do not introduce an additional numerical term into R in the reported experiments.

Table 8. Expected engineering relationships among selected subparameters used as weight elicitation guidance.

Sub-Parameters Relationship	Expected Relationship Type	Explanation
MTTR–FDR	Inverse	Lower recovery time may coincide with stronger fault detection and diagnostic capability. The relationship is used only as engineering consistency guidance.
SAR–SCI	Direct	Higher service availability can be associated with better-maintained sensing quality, but no empirical correlation is estimated in this study.
DRL–SAR	Direct	Greater data redundancy can support availability during failures by preserving access to data when an individual path or copy is lost.
SDR–SPU	Inverse	Higher sensor density can increase resource and energy pressure, potentially reducing sustainable power efficiency.
ITI–EA	Inverse	Lower integration time is expected to support greater expansion agility.
THE–SPU	Direct	Efficient traffic handling can reduce unnecessary resource use and may support more sustainable operation.
FUR–PCS	Direct	Successful update capability can support protocol compatibility when software changes are required across heterogeneous devices.
TPA–DI	Direct	Stable adaptation to different traffic profiles can support interoperable operation across heterogeneous endpoint classes.
EKS–UAD	Direct	Strong encryption and key management can complement unauthorized access detection and rejection controls.
TDI–RIM	Inverse	A lower residual tamper-related incident level is expected to coincide with more effective incident response and protection.

The reported values of OC, SRE, NF, SEC, and R are calculated only from Equations (1)–(5), the stated nonlinear transformations, and the stated weighting procedure. Table 8 provides engineering guidance for avoiding redundant emphasis when weights are calibrated. No separate correlation penalty or reward is applied to the numerical results reported here.

A deployment may later introduce an explicit dependency correction if field data demonstrate a stable statistical relationship between two subparameters. Such a correction would require a separately defined and validated computational term and is not part of the present evaluation.

The nonlinear behavior used in the present framework is fully represented by the inverse, power, square root, and sigmoid transformations already defined in Equations (1)–(4). No additional hidden dynamic scaling operation is applied during calculation of R.

Accordingly, the reproducible calculation path consists of normalization, the explicit transformations in Equations (1)–(4), calibrated or sensitivity-sampled weights, and the final aggregation in Equation (5).

The normalized PDFs of the robustness metric (R) for each deployment scenario are shown in Figure 5, indicating that robustness is distributed differently across the scenarios. For the Critical Deployment scenario, the distribution is more compact and sharply peaked than in the other scenarios. This indicates a narrower dispersion of robustness values around a central region associated with stable and reliable system behavior. Such a distribution is expected for highly critical environments, where robustness must consistently satisfy stringent requirements. For the Essential Deployment scenario, the distribution is broader and slightly shifted toward lower robustness values, reflecting moderate system variability and less stringent operational requirements. For the Basic Deployment scenario, the distri-

bution is the widest, indicating greater variability and lower robustness consistency under less demanding deployment assumptions.

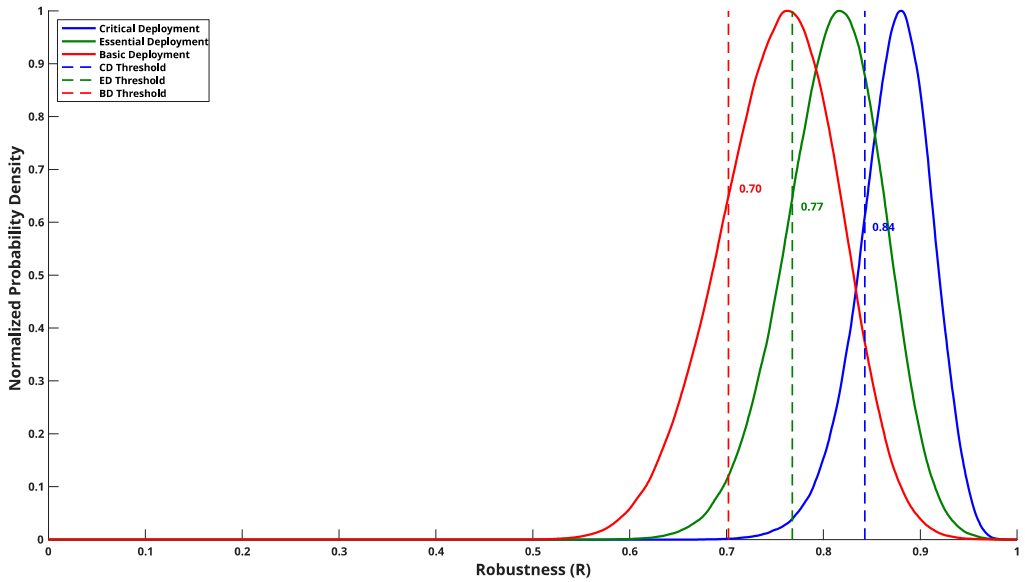


Figure 5. PDF of robustness metric R with thresholds. Adapted from [31].

The transition from Basic to Essential to finally Critical Deployment scenarios shows a clear pattern of tighter robustness value distributions, as well as a movement to higher robustness regions. This progression emphasizes the need for stability and reliability as the deployment scenario moves to a more mission-critical setting.

A scenario-specific robustness threshold T is derived from the simulated distribution by selecting a target exceedance probability. The procedure identifies the value of T for which the proportion of simulated R values at or above T is closest to the selected target, for example 80%. The threshold is derived solely from the simulated distribution and represents a scenario-specific decision boundary, not an empirical probability of physical system stability. It is obtained from the simulated cumulative distribution and is mathematically formalized as:

$$T = \arg\min_{T \in [0,1]} \left| P(R \geq T) - P_{\text{desired}} \right|, \quad (6)$$

where $P\ (R \geq T)$ denotes the proportion of simulated robustness values greater than or equal to T, and Pdesired denotes the selected target exceedance probability. The procedure adjusts T so that $1 - \text{FR(T)}$, where FR(T) is the cumulative distribution function of R, approaches Pdesired. Values above and below T can therefore be interpreted as higher robustness and lower robustness regions relative to the selected scenario threshold. The threshold is a configurable decision boundary derived from the simulated distribution. It does not by itself demonstrate a physically stable or unstable state.

From a deployment perspective, the CDF and PDF curves summarize both the level and dispersion of the simulated robustness values. A narrow distribution concentrated at high R values indicates greater consistency within the selected parameter ranges, while a broader distribution or a shift toward lower R values indicates greater variability or lower modeled robustness. These patterns can inform design choices such as redundancy, recovery mechanisms, access control, and resource allocation, but they remain conditional on the simulation assumptions and selected threshold policy.

Tables 9 and 10 summarize the parameters reported for the reproduced stress-scenario analysis. Table 9 specifies the common setup: 750 time steps, 10,000 total time units, 100–2500 devices, a LOESS factor of 0.1, and an initial value of 0.85 for OC, SRE, NF, and

SEC. Table 10 lists the scenario-specific event-intensity bounds, failure factors, and load factors. Reference [31] reports these quantities as scenario descriptors but does not define a separate equation that maps each descriptor to the OC, SRE, NF, or SEC trajectories. The descriptors are therefore used only to distinguish the stress scenarios, and Figure 6 is used for descriptive comparison without attributing causal sensitivity to individual descriptors.

Table 9. List of basic simulation parameters' values.

Parameter	Value
Time steps	750
Total Time Units	10,000
Number of Devices	100–2500
Smoothing Factor for LOESS Approximation	0.1
Base Value for Robustness Parameters	0.85

Table 10. Parameter values across different deployment scenarios.

Parameter/ Scenario	Minimum Event Intensity	Maximum Event Intensity	Failure Factor	Load Factor
Normal Conditions	0.1	0.2	0.05	0.1
High Event Intensity	0.5	0.8	0.2	0.5
High Traffic Load	0.6	0.7	0.3	0.7
Network Congestion	0.4	0.7	0.3	0.6
High load and Low Sensor Reliability	0.5	0.7	0.5	0.9

Figure 6 reproduces the five stress scenarios reported in [31]: Normal Conditions, High Event Intensity, High Traffic Load, Network Congestion, and High Load and Low Sensor Reliability. The analysis applies the reported aggregation and one-step smoothing procedure described below. Event-intensity bounds, failure factors, and load factors remain scenario descriptors because [31] does not specify separate equations linking them to the four component trajectories. Figure 6 consequently compares the overall scenario behavior without estimating the isolated effect of an individual descriptor.

Moreover, Figure 6 shows distinct trajectories across the five operating scenarios. Normal Conditions remains comparatively stable. High Event Intensity exhibits greater variability. High Traffic Load and Network Congestion produce lower robustness levels, while High Load and Low Sensor Reliability shows the widest fluctuation. These trajectories characterize overall scenario behavior and do not isolate sensitivity to individual stress parameters. Locally estimated scatterplot smoothing (LOESS) is applied only to improve visualization of the trajectories.

The time-series analysis in Figure 6 and the summary values in Table 11 reproduce the analysis in [31]. The four dynamic dimension values are combined at each step as $R_{raw}(t) = 0.30\ OC(t) + 0.20\ SRE(t) + 0.30\ NF(t) + 0.20\ SEC(t)$. For $t > 1$, one-step smoothing is applied as $R(t) = [R_{raw}(t) + R(t-1)]/2$, after which R is constrained to the interval [0, 1]. The scenarios use the common initial component value 0.85, 750 time steps, 10,000 total time units, and the descriptors listed in Tables 9 and 10. LOESS with factor 0.1 is used only to display the trend. Figure 6 and Table 11 compare the reported stress scenarios at the aggregate level. Reference [31] does not specify explicit equations linking event intensity, failure factor, load factor, or sensor reliability to the individual robustness components, so these results do not isolate parameter-specific effects.

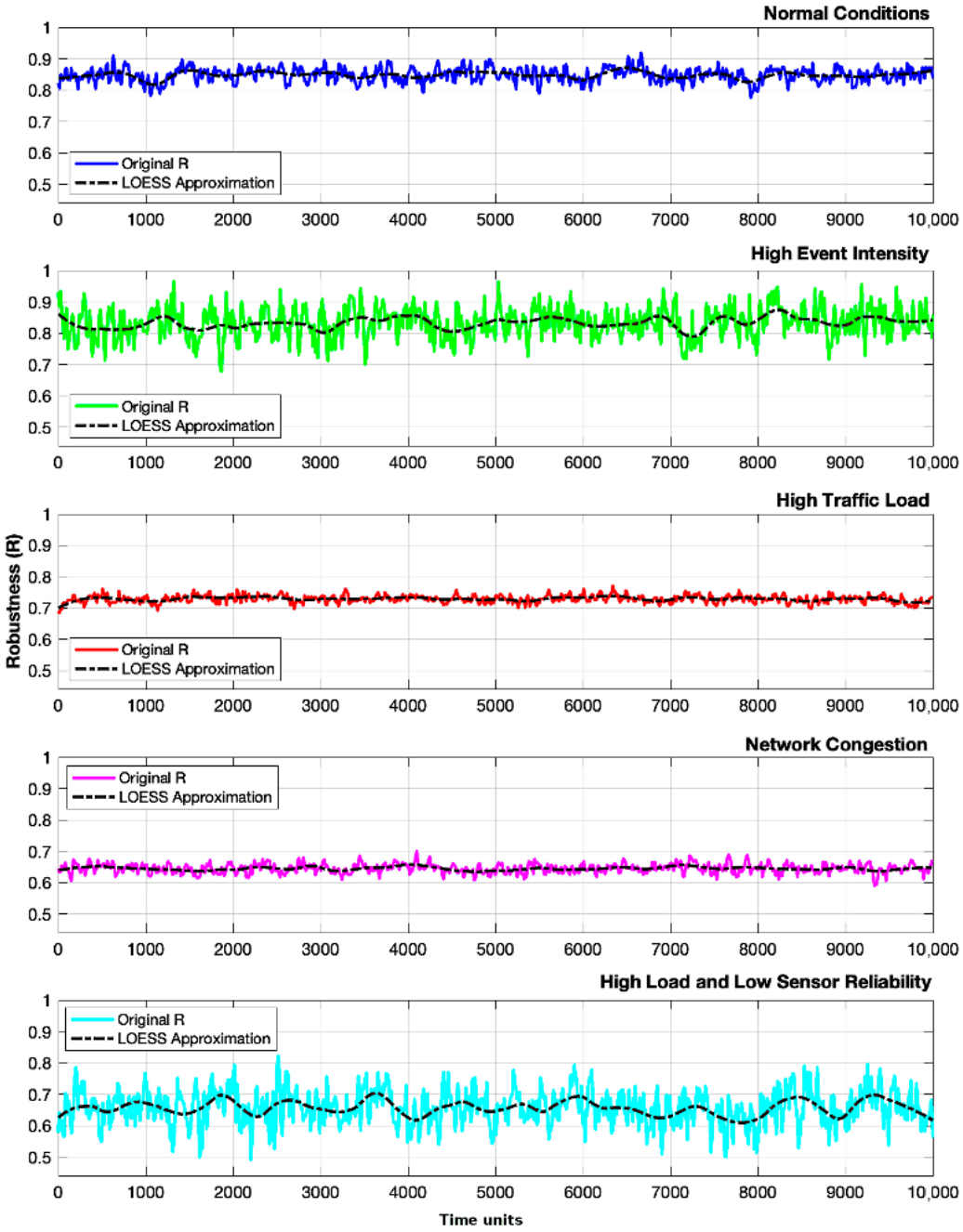


Figure 6. Time-series behavior of the robustness metric R across five operational stress scenarios with LOESS-smoothed trajectories. Adapted from [31].

Table 11 is consistent with the trajectories in Figure 6. Normal Conditions has the highest mean R (0.8467) and a relatively narrow range (0.1307). High Event Intensity has a similar mean (0.8363) but greater dispersion, with a range of 0.2870 and standard deviation of 0.0520. High Traffic Load has mean R = 0.7292 with the narrowest range (0.0613), while Network Congestion has the lowest mean R (0.6456). High Load and Low Sensor Reliability has the largest range (0.3524) and the highest standard deviation (0.0524). These statistics summarize the reproduced stress trajectories and characterize the differences among the modeled scenarios without isolating the effects of individual stress factors.

It is important to mention that the Threshold R column in Table 11 is a robustness decision level associated with the selected exceedance criterion. It represents neither a stabilization time nor an independently measured probability of physical stability. Its

value is evaluated relative to the corresponding scenario distribution and the procedure in Equation (6).

The reproduced simulation results from [31] show distinct robustness distributions and trajectories under the modeled operating conditions. In the present study, they are used to examine the internal behavior of the metric and provide context for the subsequent connectivity validation. No adaptive control mechanism is included in this simulation stage.

Table 11. Performance metrics of R under different deployment scenarios.

Scenario	Min R	Max R	Mean R	Std R	Threshold R	Range of R
Normal Conditions	0.7748	0.9173	0.8467	0.0213	0.8500	0.1307
High Event Intensity	0.6977	1.0000	0.8363	0.0520	0.8526	0.2870
High Traffic Load	0.6954	0.7659	0.7292	0.0118	0.7254	0.0613
Network Congestion	0.6004	0.6957	0.6456	0.0142	0.6417	0.1218
High Load and Low Sensor Reliability	0.4871	0.8345	0.6523	0.0524	0.6456	0.3524

4.3. Validation in a 5G Connectivity Environment

The connectivity-validation stage evaluates whether observable control-plane, user-plane, service-connectivity, and security indicators can be transformed into the same robustness dimensions used in the simulation analysis. The environment combines a standalone 5G core with an emulated radio access network, while the endpoints model IoT-oriented 5G devices generating periodic sensing traffic, alarm-driven bursts, actuator-like downlink control, and abnormal access behavior.

The objective of this validation phase is to provide a measurable bridge between conventional network KPIs and the proposed OC, SRE, NF, SEC, and R metrics without replacing the perception-layer model. For practical integration into existing network infrastructures, the conceptual parameters must be mapped to indicators that can be observed in contemporary communication systems, such as registration success, protocol data unit (PDU) session establishment, latency, packet loss, throughput, recovery time, and access-control outcomes. This mapping provides a connectivity-level operationalization while leaving hardware-dependent perception-layer quantities for subsequent physical validation.

4.3.1. Validation Architecture and IoT Endpoint Abstraction

The validation architecture is built around free5GC [33], which provides the main 5G core functions: Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), Authentication Server Function (AUSF), Unified Data Management (UDM), Unified Data Repository (UDR), Network Repository Function (NRF), Policy Control Function (PCF), and Network Slice Selection Function (NSSF). UERANSIM [34] is used to emulate the next-generation Node B (gNB) and multiple user equipment (UE) instances (Table 12). In this study, each emulated UE represents either a single 5G-capable IoT device or an aggregated IoT access endpoint associated with a group of constrained sensing devices. This abstraction enables evaluation of dense IoT connectivity patterns while preserving the signaling and service behavior of a 5G IoT access environment.

The logical topology follows the standard 5G service path. The emulated IoT endpoints attach to the UERANSIM gNB, which exchanges N2 signaling with the AMF and forwards user-plane traffic over N3 toward the UPF. The UPF provides connectivity to a local data network (DN) over N6, where traffic sinks, monitoring tools, and application-layer services are deployed. Control-plane behavior is observed through free5GC and UERANSIM

logs, while user-plane and service behavior is characterized using packet captures on the N3 and N6 interfaces, active round-trip time (RTT) probes, iperf3 measurements, User Datagram Protocol (UDP) traffic, Message Queuing Telemetry Transport (MQTT)-like traffic generation, and host-resource counters. The traffic model includes low-volume periodic uplink telemetry, synchronized event-driven bursts, downlink control messages, and abnormal registration attempts.

Table 12. Validation configuration for UD-IoT evaluation in a 5G connectivity environment.

Component	Configuration	Role in Robustness Evaluation
5G core platform	free5GC v3.4.0 standalone 5G core with AMF, SMF, UPF, AUSF, UDM, UDR, NRF, PCF, and NSSF	Provides control plane registration, session management, policy control, authentication, and user plane forwarding
RAN and UE emulation	UERANSIM v3.2.8 gNB and multiple UERANSIM UE instances	Represents 5G access and IoT-oriented endpoints under increasing endpoint count and signaling load
IoT endpoint model	Periodic telemetry, event-driven bursts, actuator-like downlink traffic, and abnormal access attempts	Introduces UD-IoT service behavior at the traffic, session, and access-control levels
Data network	Local data network (DN) connected through the UPF N6 interface	Hosts traffic sinks, monitoring tools, and application layer endpoints
Traffic generation	iperf3 v3.9 TCP/UDP load, Python 3.10.12 UDP telemetry and MQTT-like traffic generators, and active latency probes	Produces heterogeneous IoT flows for evaluating THE, TPA, and user plane stability
Observability	AMF/SMF/UPF/UERANSIM logs, N3/N6 packet captures with tcpdump v4.99.1, latency probes, throughput measurements, and host CPU/RAM counters	Provides measurable inputs for transformation into OC, SRE, NF, SEC, and R
Failure injection	UE process termination, gNB restart, UPF restart, and traffic overload	Evaluates recovery time, availability degradation, packet loss, and session restoration
Security stress	Invalid credentials, unauthorized subscription permanent identifier (SUPI) attempts, and abnormal registration bursts	Evaluates unauthorized access detection, rejection behavior, and signaling robustness

The validation environment was deployed on Ubuntu 22.04.4 LTS (64-bit) on a workstation equipped with an Intel Core i7-12700H processor (14 cores, 20 threads) and 32 GB of RAM. The validation processes were allocated 8 CPU cores and 16 GB of RAM. The 5G core used free5GC v3.4.0, while UERANSIM v3.2.8 provided the gNB and UE emulation. Traffic was generated with iperf3 v3.9 for TCP/UDP load and with Python 3.10.12-based generators for periodic UDP telemetry and MQTT-like application traffic. Packet captures were collected with tcpdump v4.99.1 and analyzed with Wireshark, while free5GC/UERANSIM logs and host CPU and memory counters were recorded during each run.

Each scenario was executed for 300 s after a 30 s initialization period and was independently repeated 10 times. The reported scenario-level values are arithmetic means across the 10 runs. Run-to-run variability is reported using the sample standard deviation (SD), and two-sided 95% confidence intervals (CIs) for the mean are calculated using the Student t distribution with 9 degrees of freedom.

The largest evaluated scenario contains 1500 emulated endpoints. These endpoints represent concurrent software processes, not a spatial density expressed in devices per square kilometer. The environment does not model radio propagation, multipath fading,

urban clutter, device mobility, antenna effects, or battery-constrained hardware operation. The validation therefore characterizes control-plane, user-plane, service-continuity, and security behavior at the connectivity level. Physical-layer scalability remains outside the scope of this validation.

4.3.2. Transformation of Observable KPIs into Robustness Metrics

The transformation from validation measurements to the proposed robustness dimensions is performed through a normalization layer (Table 13). The normalization rule is selected according to the semantic direction of the target subparameter and the transformation already present in Equations (1)–(4). Positive score variables are normalized so that larger values indicate better behavior. For adverse variables that are explicitly inverted in the equations, including MTTR, ITI, DCI, and TDI, larger raw adverse values are mapped to larger normalized adverse values and the corresponding $1 - x$ term performs the inversion. For a positive score derived from an adverse raw measurement, such as RIM derived from incident response time, inverse normalization is used so that the resulting score increases as response time decreases. This convention avoids applying the same inversion twice.

Table 13. Operational interpretation of robustness subparameters in the 5G connectivity validation context.

Robustness Dimension	Sub-Parameter	Testbed Observable	Normalization Direction	Interpretation
OC	MTTR	Service recovery time after UE, gNB, or UPF interruption	Adverse and inverted in the equation	Shorter recovery time increases operational continuity
OC	FDR	Detected failed registrations, session drops, and forwarding interruptions	Positive	Higher detection rate improves fault awareness
OC	SAR	Ratio of time with established PDU sessions and reachable DN service	Positive	Higher service availability increases continuity
OC	SCI	Valid telemetry ratio and payload consistency under load	Positive	Higher data validity reflects stable sensing service behavior
OC	DRL	Delivered application messages after disruption and retransmission handling	Positive	Higher delivery preservation improves data resilience
SRE	SDR	Ratio of active IoT endpoints to configured endpoint capacity	Positive	Higher sustained endpoint density improves scalability
SRE	ITI	Time required to register and activate new IoT endpoints	Adverse and inverted in the equation	Lower integration time improves scalable resource efficiency
SRE	THE	Throughput, packet delivery ratio, and forwarding stability	Positive	Efficient traffic handling sustains service performance
SRE	SPU	Host resource or energy efficiency per active endpoint (conceptual proxy that is not directly reported among the principal service-connectivity KPIs).	Positive	Direct device power efficiency is not measured in the present validation. SPU remains a conceptual hardware-dependent quantity.

Table 13. *Cont.*

Robustness Dimension	Sub-Parameter	Testbed Observable	Normalization Direction	Interpretation
SRE	EA	Endpoint scaling response under increasing registration and traffic load	Positive	Higher scaling agility improves expansion capability
NF	FUR	Endpoint or service update and reconfiguration success used as a connectivity proxy for update capability.	Positive	Successful update or reconfiguration supports adaptability. Physical device firmware-update behavior is not directly measured.
NF	PCS	Support for UDP, MQTT-like flows, and control-traffic profiles	Positive	Protocol compatibility improves heterogeneous IoT operation
NF	DCI	Time required for gNB, UPF, or endpoint reconfiguration	Adverse and inverted in the equation	Faster dynamic configuration increases flexibility
NF	TPA	Robustness under periodic, burst, and mixed traffic profiles	Positive	Stable operation across traffic patterns increases adaptability
NF	DI	Successful coexistence of multiple endpoint classes and payload profiles	Positive	Higher interoperability improves flexible integration
SEC	EKS	Non-access stratum (NAS) security establishment and encrypted/accepted valid sessions	Positive	Secure attachment and session establishment increase protection
SEC	TDI	Residual abnormal or tamper-like incident rate in the connectivity context. Physical tampering is not directly measured.	Adverse and inverted in the equation	Lower incident occurrence improves SEC through the inverse term in Equation (4).
SEC	FIC	Integrity of endpoint configuration and core service state	Positive	Higher integrity preservation improves operational security
SEC	UAD	Unauthorized registration rejection and anomaly detection	Positive	Higher rejection and detection rates improve access security
SEC	RIM	Time to identify and isolate security-related signaling events	Inverse	Faster incident response improves security robustness

For positive score indicators, the normalized value increases proportionally between the lower and upper operational bounds. When an adverse raw KPI is mapped to a positive score term, such as RTT mapped to traffic handling performance or response time mapped to RIM, inverse normalization is used. By contrast, an adverse subparameter that is already represented by an explicit inverse term in Equations (1)–(4) retains its adverse direction during normalization. The bounds are defined from the operational envelope of the validation environment across baseline, dense, burst, recovery, and security stress

scenarios. Values outside the envelope are clipped to [0, 1]. This distinction preserves the directionality of the mathematical formulation and prevents double inversion.

The operational bounds used for this transformation are summarized in Table 14. In the normalization expressions, x denotes the measured value, while L and U denote the lower and upper operational bounds. For positive score terms, $(x - L)/(U - L)$ is used. For adverse raw KPIs that must be converted directly into positive score terms, $(U - x)/(U - L)$ is used. However, MTTR is an adverse subparameter that is explicitly inverted in Equation (1). Its raw recovery time is therefore normalized as $(x - L)/(U - L)$, after which the equation applies $1 - \text{MTTR}$. Values outside [L, U] are clipped to [0, 1]. The selected bounds are validation-specific operational limits and are not universal thresholds for all 5G IoT deployments.

Table 14. Normalization bounds used to transform observable 5G connectivity KPIs into robustness sub-parameters.

Observable KPI	Unit	Lower Bound	Upper Bound	Direction	Normalization Formula	Target Sub-Parameter
Registration success rate	%	90	100	Positive	$(x - L)/(U - L)$	SAR
PDU session success rate	%	90	100	Positive	$(x - L)/(U - L)$	SAR
Mean RTT	ms	10	60	Inverse	$(U - x)/(U - L)$	THE, TPA
Packet loss	%	0	5	Inverse	$(U - x)/(U - L)$	DRL, THE
Scenario aggregate throughput	Mbps	5	60	Positive	$(x - L)/(U - L)$	THE
Service recovery time	s	0	15	Adverse and inverted in Equation (1)	$(x - L)/(U - L)$	MTTR
Unauthorized rejection rate	%	95	100	Positive	$(x - L)/(U - L)$	UAD, EKS
Valid telemetry ratio	%	90	100	Positive	$(x - L)/(U - L)$	SCI, DRL
Configuration recovery time	s	0	15	Adverse and inverted in Equation (3)	$(x - L)/(U - L)$	DCI
Security incident response time	s	0	315	Inverse	$(U - x)/(U - L)$	RIM
Protocol compatibility success rate	%	90	100	Positive	$(x - L)/(U - L)$	PCS

Table 13 defines the operational interpretation of the twenty conceptual subparameters, while Table 14 lists the common normalized observables used in the connectivity validation. The subsequent scenario-results table reports the principal service-connectivity KPIs, but it is not the complete source of every contextual input. Additional quantities such as configuration-recovery time, protocol-compatibility success, valid-telemetry ratio, and security-event response time are extracted from the corresponding logs and scenario controls. Shared raw measurements are used only when the event context gives them a distinct engineering meaning. Service restoration after a forwarding interruption represents MTTR, configuration restoration after a gNB or service-configuration change represents DCI, and detection plus isolation time for abnormal signaling represents RIM. PDU-session availability contributes to SAR, while PCS is associated with protocol and session compatibility tests.

When multiple normalized observables are mapped to the same subparameter, their arithmetic mean is used to obtain the corresponding subparameter score. Hardware-dependent quantities such as direct power efficiency and physical tampering are not inferred from throughput or access logs. When a conceptual subparameter has neither a direct observation nor an explicit connectivity proxy, it is excluded and the active within-dimension coefficients are renormalized according to the availability-aware rule in Section 3.2. No missing physical quantity is imputed solely to complete the five-term structure.

The bounds in Table 14 are specific to the validation environment and are not intended as universal limits. For a new deployment, each lower and upper bound should be fixed before robustness evaluation using documented service requirements, SLA limits, or a reference observation window. If empirical calibration is used, robust quantiles such as the 5th and 95th percentiles can define an initial operating envelope, followed by expert review against service requirements. Cross-deployment comparison is meaningful only when the same normalization policy is used or when both deployments are calibrated against a common service specification.

4.3.3. Validation Scenarios and Numerical Results

Six operational scenarios are considered to evaluate the transition from stable IoT operation to dense, burst-driven, failure-prone, and security-stressed states (Table 15). The first scenario, normal periodic monitoring (S1), represents stable operation with a moderate number of IoT endpoints. The second scenario, dense periodic monitoring (S2), increases endpoint density while preserving regular telemetry behavior. The event-driven burst scenario, denoted by S3, introduces synchronized alarm-oriented traffic. The fourth scenario (S4) evaluates service recovery after a UPF disruption. The fifth scenario, unauthorized UE signaling (S5), combines valid IoT operation with abnormal access attempts. Finally, the combined stress condition (S6) jointly incorporates endpoint density, burst traffic, recovery stress, and unauthorized signaling.

Table 15. Operational scenario configuration for the 5G connectivity validation.

ID	Scenario	IoT Endpoints	Traffic Profile
S1	Normal IoT monitoring	200	periodic uplink, 128 B/2 s
S2	Dense periodic monitoring	800	periodic uplink, 128 B/1 s
S3	Event-driven burst	1200	synchronized alarm burst, 256 B/0.2 s
S4	UPF disruption and recovery	800	periodic uplink with UPF restart
S5	Unauthorized UE signaling	800	600 valid and 200 unauthorized endpoints
S6	Combined stress condition	1500	burst, congestion, recovery and unauthorized access

From a smart city perspective, these scenarios correspond to common urban IoT service conditions: normal environmental or metering telemetry, burst traffic caused by incident or alarm reporting, dense periodic sensing under increased endpoint population, core-network disruption affecting edge-to-cloud service continuity, unauthorized access attempts from rogue or misconfigured endpoints, and combined stress during service degradation. This mapping strengthens the interpretation of the validation results as robustness indicators for smart city IoT infrastructures and not only generic 5G connectivity measurements.

The results in Table 16 show a gradual deterioration of RTT, packet loss, and recovery behavior as the operational conditions move from periodic IoT monitoring toward combined stress. Under normal monitoring, the validation environment maintains high registration and PDU session success rates, low RTT, and negligible packet loss. Dense periodic monitoring increases throughput demand and endpoint registration pressure, but

the service remains stable. The event-driven burst condition produces a stronger increase in RTT and packet loss because multiple endpoints transmit alarm-oriented payloads in a synchronized manner. The UPF disruption scenario mainly affects OC through increased recovery time and packet loss, while the unauthorized signaling scenario primarily stresses SEC through repeated abnormal access attempts. The combined stress condition produces the lowest service stability and the largest run-to-run variation in RTT, packet loss, throughput, and recovery time because endpoint density, traffic intensity, recovery stress, and abnormal access conditions occur simultaneously.

Table 16. Service-connectivity KPI results across the evaluated validation scenarios. Values are reported as mean ± SD, with the 95% CI shown in parentheses (n = 10).

ID	Registration Success (%)	PDU Session Success (%)	Mean RTT (ms)	Packet Loss (%)	Throughput (Mbps)	Recovery Time (s)	Unauthorized Rejection (%)
S1	99.6 ± 0.2 (99.5–99.7)	99.4 ± 0.3 (99.2–99.6)	11.8 ± 0.8 (11.2–12.4)	0.09 ± 0.03 (0.07–0.11)	6.8 ± 0.4 (6.5–7.1)	0.0 ± 0.0 (0.0–0.0)	99.8 ± 0.1 (99.7–99.9)
S2	98.7 ± 0.4 (98.4–99.0)	98.4 ± 0.4 (98.1–98.7)	17.6 ± 1.2 (16.7–18.5)	0.32 ± 0.08 (0.26–0.38)	18.4 ± 1.1 (17.6–19.2)	0.8 ± 0.2 (0.7–0.9)	99.6 ± 0.2 (99.5–99.7)
S3	96.8 ± 0.6 (96.4–97.2)	96.1 ± 0.7 (95.6–96.6)	31.4 ± 2.6 (29.5–33.3)	1.18 ± 0.22 (1.02–1.34)	42.7 ± 2.8 (40.7–44.7)	2.6 ± 0.4 (2.3–2.9)	99.2 ± 0.3 (99.0–99.4)
S4	98.1 ± 0.5 (97.8–98.4)	97.6 ± 0.6 (97.2–98.0)	25.9 ± 2.1 (24.4–27.4)	3.72 ± 0.40 (3.43–4.01)	16.2 ± 1.4 (15.2–17.2)	8.4 ± 0.9 (7.8–9.0)	99.5 ± 0.2 (99.4–99.6)
S5	98.3 ± 0.4 (98.0–98.6)	97.9 ± 0.5 (97.5–98.3)	20.8 ± 1.7 (19.6–22.0)	0.64 ± 0.12 (0.55–0.73)	14.9 ± 1.2 (14.0–15.8)	1.4 ± 0.3 (1.2–1.6)	98.9 ± 0.4 (98.6–99.2)
S6	94.2 ± 0.9 (93.6–94.8)	93.5 ± 1.0 (92.8–94.2)	47.8 ± 4.2 (44.8–50.8)	4.95 ± 0.55 (4.56–5.34)	55.3 ± 4.5 (52.1–58.5)	13.2 ± 1.4 (12.2–14.2)	96.4 ± 0.6 (96.0–96.8)

Table 17 shows that the normalized dimension scores respond differently across the evaluated scenarios and do not simply reproduce a single conventional KPI. For example, the UPF disruption and recovery scenario is associated with a clear reduction in OC because recovery time and packet loss increase, while SEC remains comparatively high because the security mechanisms are not directly compromised. Conversely, the unauthorized UE signaling scenario preserves a relatively strong SEC score due to the high rejection rate of invalid access attempts, while SRE and NF are moderately affected by the additional signaling load. The combined stress condition produces the lowest R value because all four robustness dimensions are simultaneously affected.

Table 17. Normalized robustness components derived for the 5G connectivity validation scenarios.

ID	Scenario	OC	SRE	NF	SEC	R
S1	Normal IoT monitoring	0.936	0.901	0.889	0.922	0.914
S2	Dense periodic monitoring	0.903	0.857	0.873	0.901	0.885
S3	Event-driven burst	0.837	0.781	0.816	0.879	0.829
S4	UPF disruption and recovery	0.703	0.742	0.758	0.861	0.763
S5	Unauthorized UE signaling	0.861	0.807	0.834	0.934	0.860
S6	Combined stress condition	0.642	0.671	0.704	0.812	0.704

For Table 17, the final aggregation uses the AHP-derived dimension weight vector alpha = (0.2951, 0.2481, 0.2087, 0.2481) for OC, SRE, NF, and SEC, respectively, with coefficients summing to one. Recalculation with this vector reproduces the displayed R

values after rounding to three decimals. The corresponding AHP consistency ratio is 0.0224, as described in Section 3.2. The simulation study in Section 4.1 uses Dirichlet (1, 1, 1, 1, 1) sampling for the within-dimension gamma, beta, delta, and epsilon vectors in each repetition. In the connectivity-validation mapping, the neutral within-dimension base coefficients are 0.20 and are renormalized over the active directly observed or explicitly proxied subparameters. Table 18 summarizes these distinct weighting procedures.

Table 18. Weighting specification used in the simulation and connectivity validation stages.

Aggregation Level	Coefficient Notation	Values or Procedure	Scope
Overall validation metric R	alpha1 to alpha4	AHP: (0.2951, 0.2481, 0.2087, 0.2481) for OC, SRE, NF, SEC. CR = 0.0224.	Section 3.2, Table 17
OC	gamma1 to gamma5	Dirichlet (1, 1, 1, 1, 1), independently resampled in every simulation repetition	Equation (1), Section 4.1
SRE	beta1 to beta5	Dirichlet (1, 1, 1, 1, 1), independently resampled in every simulation repetition	Equation (2), Section 4.1
NF	delta1 to delta5	Dirichlet (1, 1, 1, 1, 1), independently resampled in every simulation repetition	Equation (3), Section 4.1
SEC	epsilon1 to epsilon5	Dirichlet (1, 1, 1, 1, 1), independently resampled in every simulation repetition	Equation (4), Section 4.1
Connectivity within-dimension mapping	Five base coefficients per dimension	Base weights = 0.20 each. Unavailable unproxied subparameters are excluded and active coefficients are renormalized to unit sum.	Section 3.2, Tables 13–17

For the combined stress scenario S6 (Tables 16 and 17), the observed service connectivity indicators show the strongest degradation among the evaluated scenarios. This scenario combines high endpoint density, burst-oriented traffic, recovery disruption, and unauthorized access attempts, which jointly affect the control plane, user plane, recovery, and security behavior of the validation environment. Registration success and PDU session success decrease, while mean RTT, packet loss, and recovery time increase substantially. Although the throughput value is high, it reflects the increased offered load and does not indicate improved robustness. Consequently, S6 produces the lowest R value among the evaluated scenarios, which is consistent with degradation distributed across multiple dimensions and not limited to a single isolated KPI.

Table 18 summarizes the weighting specification used in the simulation and connectivity-validation stages.

To place the proposed aggregation in context using the same validation inputs, Table 19 compares R with three simpler input-compatible robustness baselines.

The equal dimension baseline assigns 0.25 to OC, SRE, NF, and SEC. The weakest dimension baseline uses the minimum of the four dimension scores. For the direct KPI baseline, the seven measured indicators in Table 16 are first converted to higher-is-better performance scores using the operational bounds in Table 14: success, throughput, and rejection rates use direct scaling, while RTT, packet loss, and recovery time use inverse performance scaling. Their unweighted mean produces the values reported in Table 19. This baseline is intentionally independent of the MTTR representation used inside Equation (1).

All four scoring approaches identify the combined stress condition as strongly degraded, while the numerical level depends on the aggregation rule. Because no common external reference for robustness is available, the comparison focuses on the effects of dimensional structure and weighting policy on the resulting robustness scores.

Table 19. Quantitative comparison with simple input-compatible robustness baselines.

ID	Proposed R	Equal Dimension Mean	Weakest Dimension	Direct KPI Mean
S1	0.914	0.912	0.889	0.834
S2	0.885	0.884	0.857	0.801
S3	0.829	0.828	0.781	0.711
S4	0.763	0.766	0.703	0.579
S5	0.860	0.859	0.807	0.735
S6	0.704	0.707	0.642	0.334

The baselines also differ in diagnostic value and deployment effort. The equal-dimension mean preserves the four component scores but removes service-priority weighting. The weakest-dimension baseline highlights the bottleneck but discards compensating behavior in the remaining dimensions. The direct-KPI mean is the simplest to deploy, but it loses the OC, SRE, NF, and SEC attribution that indicates the type of degradation. The proposed aggregation requires an explicit mapping and weight-calibration step, but it retains the four component scores before aggregation and therefore supports more targeted operational interpretation. Its practical benefit lies in diagnostic transparency and policy-aware assessment. Predictive accuracy is not evaluated in this comparison.

4.3.4. Interpretation of the Connectivity Validation Results

Within the evaluated 5G connectivity environment, the robustness metric is populated from measurable network and service indicators. The mapping applies the same OC, SRE, NF, and SEC structure used in the simulations to observable system behavior. A single KPI such as RTT, packet loss, or throughput cannot identify the type of degradation, whereas the four component scores preserve this information before aggregation into R. This interpretation is limited to the scenarios and observables available in the current environment.

These results characterize connectivity-level behavior only. Physical sensor drift, device energy consumption, radio-propagation effects, mobility, and physical tampering are outside the current experiment and are addressed explicitly as validation limitations in Section 5.4.

The connectivity-validation results show that robustness degradation is distributed unevenly across the four evaluated dimensions. OC, SRE, NF, and SEC therefore provide an interpretable engineering decomposition for the scenarios studied here. These results do not test whether the decomposition is unique or mathematically minimal, and its suitability should be reassessed when the framework is transferred to other IoT domains or measurement environments.

5. Discussion and Conclusion

5.1. Main Findings

This paper evaluates a multi-dimensional robustness metric for UD-IoT networks, focusing on operational continuity, scalable resource efficiency, network flexibility, and security. The evaluation combines the simulation stage from [31], used to examine the math-

ematical behavior of the metric, with a connectivity-validation stage based on measurable network and service indicators.

The results support three main conclusions:

- The simulation results show clear and consistent separation among the Critical, Essential, and Basic deployment scenarios across OC, SRE, NF, SEC, and the aggregate robustness metric R. The scenario ordering is preserved under stochastic variations in the weighting coefficients, indicating that the observed robustness patterns are stable across different weighting configurations.
- The 5G connectivity validation demonstrates that measurable control-plane, user-plane, service, recovery, and security indicators can be mapped into differentiated OC, SRE, NF, and SEC responses. The combined stress scenario S6 produces the lowest aggregate R, while the individual dimension scores reveal which aspects of robustness are most affected under each operating condition.
- The comparison with simpler scoring approaches shows the practical value of preserving the four robustness dimensions before calculating the aggregate R. While conventional KPI aggregation provides an overall performance score, the proposed framework retains information about continuity, resource efficiency, flexibility, and security, enabling more interpretable and policy-aware robustness assessment.

5.2. Practical Implementation Pathway for Smart City Robustness Monitoring

The practical value of the proposed robustness metric for smart city deployments lies in its ability to transform heterogeneous technical indicators into a unified decision-support view of urban IoT reliability. In a smart city environment, separate KPIs such as latency, packet loss, availability, recovery time, or unauthorized access attempts are typically monitored independently. However, such isolated indicators do not directly show whether the sensing infrastructure as a whole remains operational, scalable, adaptable, and secure under changing urban conditions. By aggregating these aspects into OC, SRE, NF, SEC, and finally (R), the proposed framework enables city operators to identify whether degradation originates mainly from service interruption, resource saturation, limited adaptability, or security exposure.

The implementation of the framework can follow a structured procedure. First, the target smart city service should be defined, such as traffic monitoring, smart metering, environmental sensing, emergency reporting, or access-security management. Second, observable indicators should be collected from the perception layer and supporting connectivity infrastructure, including endpoint availability, registration behavior, traffic load, packet loss, recovery time, firmware status, interoperability events, and abnormal access attempts. Third, these indicators should be normalized according to their operational direction and mapped to the corresponding OC, SRE, NF, and SEC sub-parameters. Fourth, the robustness value (R) should be calculated periodically or event-triggered and compared with deployment-specific thresholds. Finally, the resulting robustness profile should guide operational actions such as traffic prioritization, edge-resource allocation, sensor maintenance, redundancy activation, access-control adjustment, or incident response.

To make this pathway operational, a reference automation loop is defined. At each monitoring interval, parsers extract the required indicators from core-network logs, packet measurements, service probes, and security events. The indicators are time-aligned, normalized using the active deployment profile, mapped to the available subparameters, and aggregated into OC, SRE, NF, SEC, and R. The resulting component vector is compared with policy thresholds. Low OC can indicate a need for recovery or failover actions. Low SRE can motivate resource scaling. Low NF can identify configuration or interoperability problems, while low SEC can trigger security-oriented investigation or access-control responses. The

output can be exposed to analytics or management functions such as the 5G Network Data Analytics Function (NWDAF). The framework specifies the monitoring and decision pathway, while live NWDAF integration, automated network actuation, and experimentally demonstrated real-time closed-loop control remain outside the current implementation.

The reference pipeline can be implemented as a deterministic eight-step monitoring algorithm: (1) ingest telemetry for the current evaluation interval, (2) validate timestamps and remove incomplete records, (3) compute the required KPI window statistics, (4) normalize the observables using the active bounds in Table 14, (5) apply Table 13 mapping and the availability-aware coefficient renormalization, (6) calculate OC, SRE, NF, SEC, and R, (7) compare the component vector and R with deployment-specific thresholds, and (8) emit a recommendation record containing the timestamp, component scores, aggregate R, dominant degraded dimension, and corresponding operational action. Metric computation is separated from actuation, allowing NWDAF or another management function to consume the output independently of any closed-loop control implementation.

This workflow extends conventional KPI monitoring with a robustness-aware view of service condition. By combining multiple indicators, operators can identify multi-dimensional degradation and target corrective actions before the affected IoT service becomes unreliable.

5.3. Validation Insight

The 5G connectivity evaluation provides evidence that the proposed robustness dimensions can be connected to observable control-plane, user-plane, and service-connectivity measurements. The evaluated scenarios show that registration success, PDU-session stability, packet delivery, recovery time, traffic handling, and unauthorized-access behavior can be organized into differentiated OC, SRE, NF, and SEC responses.

The validation reveals distinct degradation profiles across OC, SRE, NF, and SEC. From S1 to the combined stress scenario S6, OC decreases by 0.294, SRE by 0.230, NF by 0.185, and SEC by 0.110, corresponding to relative reductions of approximately 31.4%, 25.5%, 20.8%, and 11.9%, respectively. These differences show how the decomposition identifies whether degradation is dominated by continuity, resource efficiency, adaptability, or security. The analysis does not test the uniqueness of the four-dimensional structure.

The current validation provides a connectivity-oriented operationalization of the robustness metric. Complete physical-layer and hardware validation requires experiments with constrained IoT nodes that directly capture physical interference, battery depletion, sensor drift, and tampering. The OC, SRE, NF, SEC, and R structure can then be populated with direct hardware measurements in place of connectivity-level proxies where appropriate.

For SCI, SPU, DRL, and other hardware-dependent quantities, the software environment provides connectivity-level proxies. Direct validation of these quantities requires measurements of sensor drift, energy consumption, radio interference, and physical data redundancy. Until such measurements are available, their use is limited to connectivity-level assessment.

5.4. Limitations

The main limitation of the free5GC and UERANSIM setup is that it does not reproduce the complete physical behavior of constrained IoT hardware. The environment captures emulated endpoint behavior, signaling reliability, service connectivity, recovery events, and abnormal access attempts, which can be mapped to OC, SRE, NF, and SEC. Real radio propagation, battery depletion, sensor calibration drift, environmental exposure, mobil-

ity, antenna effects, and physical tampering are not directly measured. Direct hardware experiments are therefore required for the corresponding perception-layer quantities.

A second limitation concerns the scope of statistical replication. The software validation was repeated 10 times per scenario, which allows the mean, SD, and 95% CI to be reported for the service-connectivity KPIs in Table 16. However, this sample size remains limited for characterizing long-term operational variability. The reported intervals describe between-run variation in the controlled free5GC/UERANSIM environment and do not represent uncertainty bounds for physical IoT hardware, radio propagation, mobility, or heterogeneous field deployments. Larger repeated experiments and physical testbeds are therefore required to quantify these additional sources of variability.

Validation with a large physical IoT deployment would provide stronger experimental evidence for the complete perception layer model. In such a deployment, the OC, SRE, NF, SEC, and R structure can be retained, while the current normalized indicators can be complemented or replaced by direct measurements from IoT devices. Relevant measurements include battery depletion, sensor calibration drift, radio interference, device failures, recovery events, and physical tampering. The normalization bounds and weighting parameters should then be calibrated using measurements and operational requirements from the target deployment.

Prediction accuracy is not used as the comparison criterion because R is an evaluation and aggregation metric and does not estimate a labeled target variable. The approaches summarized in Table 1 also use different robustness targets, datasets, and definitions, which prevents a consistent numerical comparison using a common external reference for robustness. The present comparison therefore focuses on multidimensional coverage, interpretability through OC, SRE, NF, and SEC, and derivation of R from measurable network indicators. A future comparative study can evaluate multiple frameworks on the same field dataset and shared robustness reference.

5.5. Future Work

Future work will focus on adaptive, near-real-time robustness evaluation under changing network and environmental conditions. Machine-learning methods can be investigated for adaptive weighting, threshold calibration, and prediction of robustness degradation, while direct hardware measurements are needed to calibrate sensor reliability, energy use, interference, and physical-security indicators. These extensions should also examine integration with operational network-management and monitoring systems.

A concrete next validation stage is a small-scale physical IoT testbed with tens of constrained nodes connected through one or more gateways. A reference protocol would evaluate at least baseline, controlled-interference, and injected-failure conditions with repeated runs per condition and synchronized gateway and device logging. Direct measurements would include sensor validity and calibration drift for SCI, current or energy consumption per delivered payload for SPU, packet preservation or replicated delivery for DRL, device-level recovery events, and physical or enclosure-tampering events where applicable. These measurements can then be compared with the connectivity proxies to quantify proxy error and recalibrate the normalization bounds before larger field deployment.

For weighting, the AHP procedure described in Section 3.2 provides a reproducible initial policy from service priorities. Adaptive learning remains a subsequent extension because the current dataset is too small and environment-specific to justify training a general online weighting model. Once repeated hardware and network telemetry are available, online learning can update the AHP-initialized weights subject to nonnegativity, unit sum, stability, and service-safety constraints.

The mathematical evaluation of the framework is computationally lightweight and can support periodic or near-real-time network monitoring. For one interval with approximately 20 subparameters, the metric requires at most about 20 normalization operations, up to 20 scalar transformations, 20 within-dimension weight multiplications, approximately 16 additions to form the four dimension sums, and four multiplications plus three additions for the final aggregation. The exact count is slightly lower when a subparameter is unavailable and excluded by the availability-aware rule. In asymptotic terms, evaluation of m monitored indicators is O(m), and N independently evaluated services or network entities scale as O(Nm). Telemetry collection, synchronization, parsing, and preprocessing are expected to dominate the operational overhead. Because no dedicated end-to-end runtime benchmark was performed, real-time closed-loop performance remains to be evaluated experimentally.

Author Contributions: Conceptualization, V.S. and D.M.; methodology, V.S.; software, V.S.; validation, V.S. and D.M.; formal analysis, D.M.; investigation, V.S.; resources, V.S.; data curation, V.S. and D.M.; writing—original draft preparation, V.S.; writing—review and editing, V.S. and D.M.; visualization, V.S. and D.M.; supervision, D.M.; project administration, D.M.; funding acquisition, V.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been accomplished with financial support by the European Regional Development Fund within the Operational Programme "Bulgarian national recovery and resilience plan", procedure for direct provision of grants "Establishing of a network of research higher education institutions in Bulgaria", and under Project BG-RRP-2.004-0005 "Improving the research capacity anD quality to achieve intErnAtional recognition and reSilience of TU-Sofia (IDEAS)".

Data Availability Statement: The numerical data reported in the article and the simulation methodology are included in the manuscript. The validation environment, run duration, number of repetitions, and scenario-level summary statistics are reported in Section 4.3.1 and Table 16. Available simulation scripts and validation configuration materials can be provided by the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AHP	Analytic Hierarchy Process
AI	Artificial intelligence
AMF	Access and Mobility Management Function
AoI	Age of information
AR	Augmented reality
AUSF	Authentication Server Function
CDF	Cumulative distribution function
CI	Confidence interval
CPU	Central processing unit
DCI	Dynamic configuration index
DDoS	Distributed denial of service
DI	Device interoperability level
DN	Data network
DRL	Data redundancy level
EA	Expansion agility
EKS	Encryption and key security
FDR	Fault detection rate
FIC	Firmware integrity check frequency
FUR	Firmware update rate

gNB	Next-generation Node B
IDS	Intrusion detection system
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISAC	Integrated sensing and communication
ITI	Integration time index
KPI	Key performance indicator
LED	Light-emitting diode
LEO	Low-earth orbit
LOESS	Locally estimated scatterplot smoothing
LPWAN	Low-power wide-area network
MEC	Multi-access edge computing
MIMO	Multiple-input multiple-output
ML	Machine learning
MQTT	Message Queuing Telemetry Transport
MR	Mixed reality
MTC	Machine-type communication
MTTR	Mean time to repair
NAS	Non-access stratum
NB-IoT	Narrowband IoT
NF	Network flexibility
NFV	Network functions virtualization
NOMA	Non-orthogonal multiple access
NRF	Network Repository Function
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
OC	Operational continuity
PCF	Policy Control Function
PCS	Protocol compatibility score
PDF	Probability density function
PDU	Protocol data unit
PL	Perception layer
QoS	Quality of service
R	Robustness
RAM	Random access memory
RAN	Radio access network
RF	Radio frequency
RIM	Response to security incidents
RTT	Round-trip time
SAR	System availability ratio
SCI	Sensor calibration index
SD	Standard deviation
SDN	Software-defined networking
SDR	Sensor deployment ratio
SEC	Security
SLA	Service-level agreement
SMF	Session Management Function
SPU	Sustainable power utilization
SRE	Scalable resource efficiency
SUPI	Subscription permanent identifier
TDI	Tamper detection incidents
THE	Traffic handling efficiency
TPA	Traffic pattern adaptability
UAD	Unauthorized access detection rate

UAV	Unmanned aerial vehicle
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	Unified Data Repository
UD-IoT	Ultra-dense Internet of Things
UE	User equipment
UERANSIM	5G UE and RAN simulator
UPF	User Plane Function
VLC	Visible light communication
VR	Virtual reality
XR	Extended reality

References

1. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
2. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
3. Cisco Annual Internet Report (2018–2023) White Paper. Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 3 June 2024).
4. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.; Zhang, J.C. What Will 5G Be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082. [CrossRef]
5. Gupta, A.; Jha, R.K. A Survey of 5G Network: Architecture and Emerging Technologies. *IEEE Access* **2015**, *3*, 1206–1232. [CrossRef]
6. Lu, L.; Li, G.Y.; Swindlehurst, A.L.; Ashikhmin, A.; Zhang, R. An Overview of Massive MIMO: Benefits and Challenges. *IEEE J. Sel. Top. Signal Process.* **2014**, *8*, 742–758. [CrossRef]
7. Rappaport, T.S.; Xing, Y.; MacCartney, G.R.; Molisch, A.F.; Mellios, E.; Zhang, J. Overview of Millimeter Wave Communications for Fifth-Generation (5G) Wireless Networks—With a Focus on Propagation Models. *IEEE Trans. Antennas Propag.* **2017**, *65*, 6213–6230. [CrossRef]
8. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.A. The Roadmap to 6G: AI Empowered Wireless Networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
9. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.* **2020**, *34*, 134–142. [CrossRef]
10. Latva-aho, M.; Leppänen, K. Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence. 6G Flagship White Paper. Available online: http://jultika.oulu.fi/files/isbn9789526223544.pdf (accessed on 3 June 2024).
11. Stoynov, V.; Poulkov, V.; Valkova-Jarvis, Z.; Iliev, G.; Koleva, P. Ultra-Dense Networks: Taxonomy and Key Performance Indicators. *Symmetry* **2023**, *15*, 2. [CrossRef]
12. Zhou, T.; Wang, B.; Qin, D.; Nie, X.; Jiang, N.; Li, C. Secure Collaborative Computation Offloading and Resource Allocation in Cache-Assisted Ultradense IoT Networks with Multislope Channels. *IEEE Internet Things J.* **2025**, *12*, 17828–17843. [CrossRef]
13. Sharma, S.K.; Wang, X. Toward Massive Machine Type Communications in Ultra-Dense Cellular IoT Networks: Current Issues and Machine Learning-Assisted Solutions. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 426–471. [CrossRef]
14. Farooq, M.U.; Zeeshan, M.; Jahangir, M.T.; Asif, M. A Novel Cooperative Micro-Caching Algorithm Based on Fuzzy Inference Through NFV in Ultra-Dense IoT Networks. *J. Netw. Syst. Manag.* **2022**, *30*, 20. [CrossRef]
15. Zhou, B.; Saad, W. Age of Information in Ultra-Dense Computation-Intensive Internet of Things (IoT) Systems. In Proceedings of the 2021 19th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), Philadelphia, PA, USA, 18–21 October 2021; pp. 293–300. [CrossRef]
16. Kim, D.Y.; Kim, S. Data Aggregation-Based Transmission Method in Ultra-Dense Wireless Networks. *Intell. Autom. Soft Comput.* **2023**, *35*, 727–737. [CrossRef]
17. Huang, J.; Yu, T.; Yang, F.; Zhang, S.; Jiang, W.; Niyato, D. AoI-Aware Resource Allocation with Interference Avoidance for Ultradense Industrial Internet of Things Networks. *IEEE Internet Things J.* **2024**, *11*, 28787–28797. [CrossRef]
18. Elbayoumi, M.; Ibrahim, M.; Elhoushy, S.; Hamouda, W.; Youssef, A.M. Performance Analysis of Cellular Ultradense IoT Networks with Wireless Backhauls. *IEEE Internet Things J.* **2023**, *10*, 15774–15787. [CrossRef]
19. Theodorou, T.; Mamatas, L. DENIS-SDN: Software-Defined Network Slicing Solution for Dense and Ultra-Dense IoT Networks. *arXiv* **2023**, arXiv:2312.13662. [CrossRef]

20. Wang, Q.; Zhou, F. Fair Resource Allocation in an MEC-Enabled Ultra-Dense IoT Network with NOMA. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019. [CrossRef]
21. Nooraei Abadeh, M.; Mirzaie, M. Resiliency-aware analysis of complex IoT process chains. *Comput. Commun.* **2022**, *192*, 245–255. [CrossRef]
22. Abbas, S.M.; Javaid, N.; Azar, A.T.; Qasim, U.; Khan, Z.A.; Aslam, S. Towards Enhancing the Robustness of Scale-Free IoT Networks by an Intelligent Rewiring Mechanism. *Sensors* **2022**, *22*, 2658. [CrossRef] [PubMed]
23. Sebestyen, G.; Kopjak, J. Stability Analysis through a Stability Factor Metric for IQRF Mesh Sensor Networks Utilizing Merged Data Collection. *Sensors* **2024**, *24*, 4977. [CrossRef] [PubMed]
24. Wang, T.; Li, D.; Zhang, B.; Liu, X.; Shang, W. Resilient Topology Reconfiguration for Industrial Internet of Things: A Feature-Driven Approach Against Heterogeneous Attacks. *Entropy* **2025**, *27*, 503. [CrossRef] [PubMed]
25. Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms. *ACM Comput. Surv.* **2021**, *54*, 147. [CrossRef]
26. Abadia, J.J.P.; Walther, C.; Osman, A.; Smarsly, K. A systematic survey of Internet of Things frameworks for smart city applications. *Sustain. Cities Soc.* **2022**, *83*, 103949. [CrossRef]
27. Houichi, M.; Jaidi, F.; Bouhoula, A. Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach. *Comput. Mater. Contin.* **2024**, *81*, 393–441. [CrossRef]
28. Zieba, M.; Natkaniec, M.; Borylo, P. Cloud-Enabled Deployment of 5G Core Network with Analytics Features. *Appl. Sci.* **2024**, *14*, 7018. [CrossRef]
29. Barbosa, M.; Silva, M.; Cavalcanti, E.; Dias, K. Open-Source 5G Core Platforms: A Low-Cost Solution and Performance Evaluation. In Proceedings of the 2025 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 15–17 January 2025; pp. 99–104. [CrossRef]
30. Giambartolomei, F.; Barcelo, M.; Brighente, A.; Urbieta, A.; Conti, M. Penetration Testing of 5G Core Network Web Technologies. *arXiv* **2024**, arXiv:2403.01871.
31. Stoynov, V.; Iliev, G.; Mihaylova, D. A Framework for Robustness Evaluation in Ultra-Dense IoT Networks. *C. R. Acad. Bulg. Sci.* **2025**, *78*, 1352–1359. [CrossRef]
32. Qiu, T.; Chen, N.; Zhang, S. *Robustness Optimization for IoT Topology*; Springer: Singapore, 2022; pp. 1–214.
33. free5GC. free5GC: Open-Source 5G Core Network. Available online: https://free5gc.org/ (accessed on 2 June 2026).
34. Gör, A.G. UERANSIM: Open-Source 5G UE and gNodeB Simulator. Available online: https://github.com/aligungr/UERANSIM (accessed on 2 June 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.