From Network Measurements to Robustness Assessment: A Multi-Dimensional Perspective

Assist. Prof. Viktor Stoynov, PhD
Faculty of Telecommunications, Technical University of Sofia

Internet Measurement Day Sofia · Technical University of Sofia · 18 June 2026

Research Motivation

Modern communication networks are evaluated through many individual indicators: latency, throughput, packet loss, availability, recovery time, security events, and resource utilization. These indicators are essential, but they often describe only isolated fragments of system behavior.

The central methodological problem is that a network may appear acceptable according to one KPI while being vulnerable or unstable from another perspective.
A system with high throughput may still be fragile under recovery stress; a highly secure configuration may introduce latency or operational inefficiency; a scalable deployment may become weak if detection and response mechanisms are underdeveloped.

The proposed robustness metric addresses this by transforming heterogeneous observations into a unified, multi-dimensional interpretation of how well a communication infrastructure remains operational, scalable, adaptable, and protected under stress.

Network robustness requires integrated interpretation

Metric Structure - Four Robustness Dimensions

$$R = \alpha_1.OC + \alpha_2 SRE + \alpha_3 NF + \alpha_4 SEC, \quad \Sigma\alpha_i = 1$$

Dimension	Interpretation in communication networks	Typical degradation represented
Operational Continuity (OC)	Ability to preserve service reachability, registration, sessions, forwarding, and recovery after failures.	Service interruption, delayed repair, reduced availability, loss of reliable data continuity.
Scalable Resource Efficiency (SRE)	Ability to handle increasing endpoint density, traffic intensity, and resource demand without collapse.	Traffic overload, resource saturation, inefficient scaling, excessive energy or compute consumption.
Network Flexibility (NF)	Ability to reconfigure, interoperate, update, and adapt to changing topology, protocol, and traffic conditions.	Slow configuration, protocol mismatch, limited interoperability, poor adaptation to traffic variation.
Security (SEC)	Ability to prevent, detect, and respond to abnormal access, tampering, firmware compromise, and incident escalation.	Unauthorized access, weak key management, tamper exposure, delayed incident response.

Component-Level Computation and Observable Indicators

Component	Sub-parameters	What is captured
OC	MTTR, FDR, SAR, SCI, DRL	Recovery speed, fault detection, availability, data accuracy, and redundancy.
SRE	SDR, ISI, THE, SPU, EA	Deployment density, integration speed, traffic handling, sustainable power/resource use, and expansion agility.
NF	FUR, PCS, DCI, TPA, DI	Firmware evolution, protocol compatibility, dynamic reconfiguration, traffic adaptation, and interoperability.
SEC	EKS, TDI, FIC, UAD, RIM	Encryption/key security, tamper resistance, firmware integrity, unauthorized access detection, and incident response.

Mathematical behavior

Linear terms are used when an indicator contributes approximately proportionally to robustness.

Inverse terms are applied for delay-, failure-, or incident-related quantities where lower values are better.

Power, square-root, and sigmoid transformations represent early gains, diminishing returns, and threshold effects.

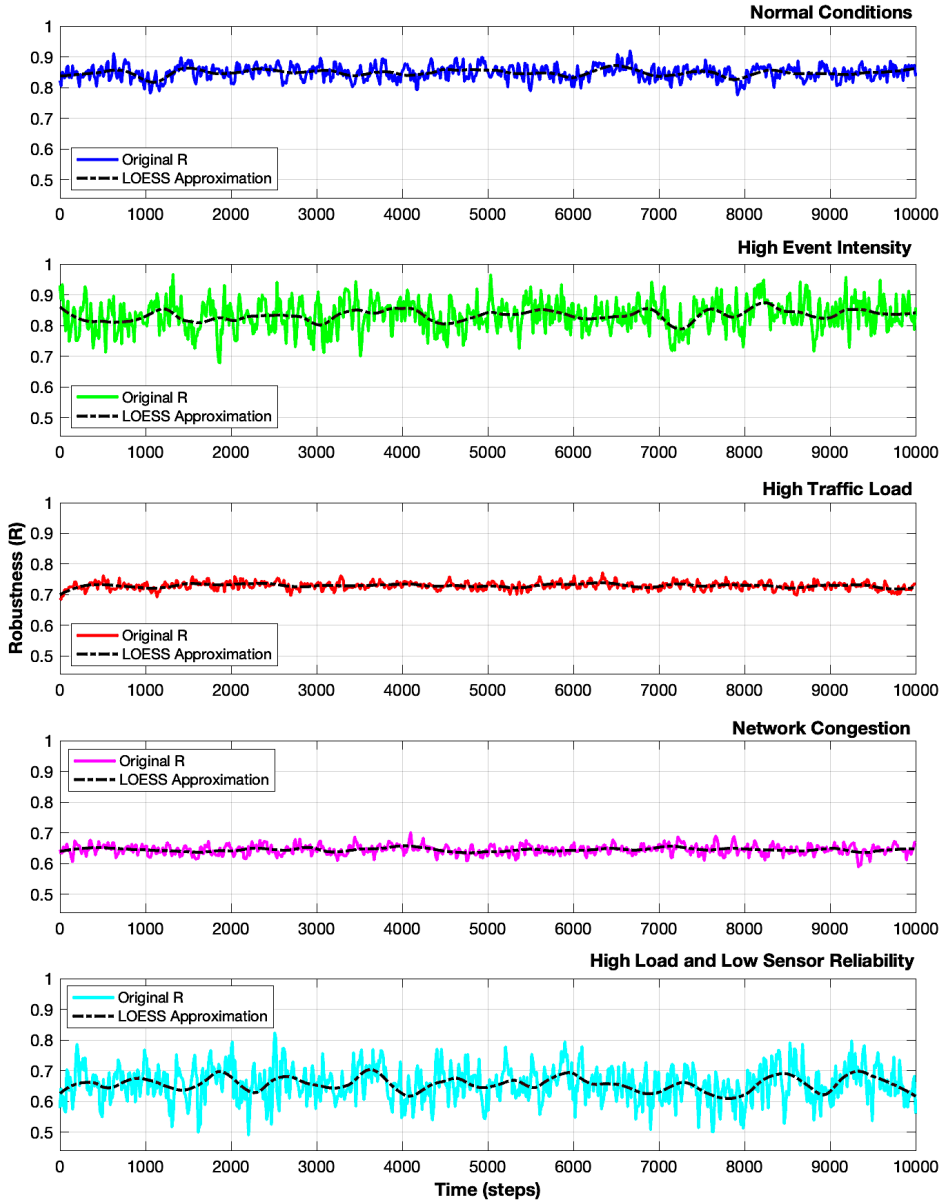
Evaluation design

Simulation stage: 10 000 samples per repetition and 100 repetitions with normalized weights.

Scenarios: normal conditions, high event intensity, high traffic load, congestion, and combined stress.

Validation: free5GC and UERANSIM indicators mapped to OC, SRE, NF, SEC, and R.

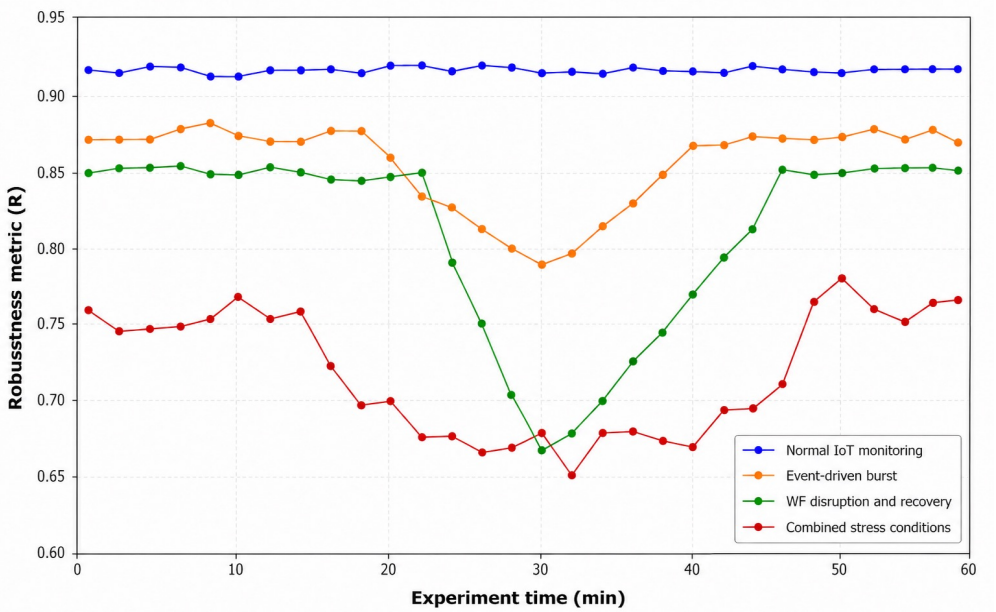
Simulation-based Stress Evaluation

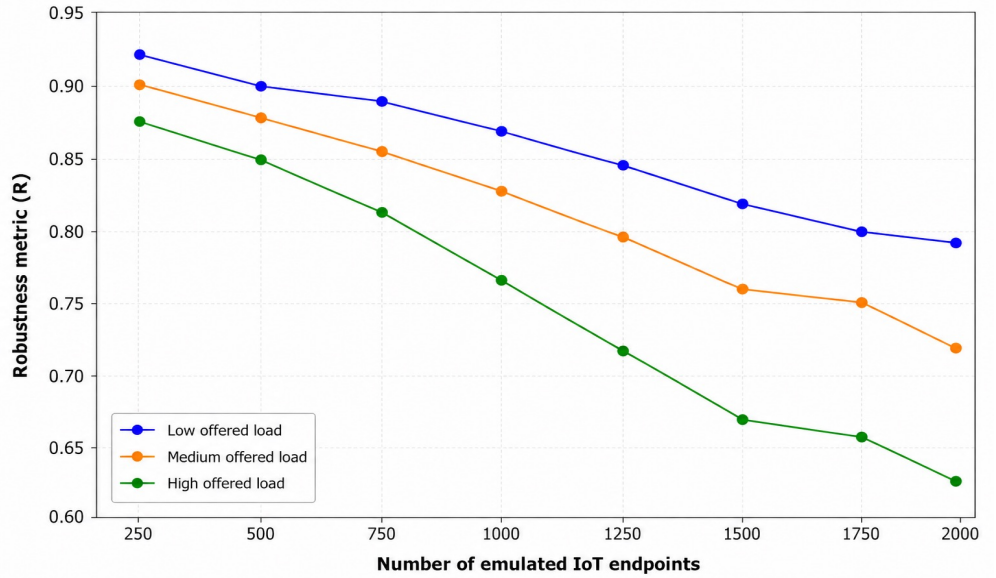


Scenario	Mean R	Threshold R	Range
Normal Conditions	0.8467	0.8500	0.1307
High Event Intensity	0.8363	0.8526	0.2870
High Traffic Load	0.7292	0.7254	0.0613
Network Congestion	0.6456	0.6417	0.1218
High Load + Low Sensor Reliability	0.6523	0.6456	0.3524

- The normal operating scenario maintains the highest stable robustness.
- High traffic load remains relatively bounded, but congestion and combined stress reduce the achievable robustness region.
- The combined-stress scenario has the widest range, indicating high uncertainty and unstable behavior when load, reliability, and disturbance factors interact.

5G-Enabled IoT Testbed Validation





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	0.893	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	0.943	0.860
S6	Combined stress condition	0.642	0.671	0.704	0.812	0.704

- The testbed results confirm the central claim of the metric: robustness loss is multi-dimensional.
- The combined stress scenario produces the lowest R because endpoint density, burst traffic, recovery disruption, and abnormal access behavior jointly degrade OC, SRE, NF, and SEC.

Conclusion

Robustness assessment complements network measurement by translating raw indicators into operational meaning.

- Network measurements become more useful when mapped to continuity, scalability, flexibility, and security.
- Robustness is broader than resilience: it captures recovery, resource efficiency, adaptability, and protection.
- Integrated metrics can support better comparison between deployment scenarios and stress conditions.
- Measurement-driven robustness assessment can help operators, researchers, and infrastructure teams identify where degradation becomes operationally significant.

Reliable infrastructure requires not only visibility, but interpretable robustness indicators.

Thank you!

Viktor Stoynov, PhD
Faculty of Telecommunications
Technical University of Sofia
Sofia, Bulgaria

E-mail: vstoynov@tu-sofia.bg
Research focus: Communication networks, IoT, 5G/6G, network robustness, physical layer security