# Assuring Latency, Reliability and Connectivity in 5G networks for IoT services

High speed, high reliability and low latency are the key benefits that CSPs (Communication Service Providers) expect from 5G. While high speed helps to upload and download video-based content faster and in larger volumes, high reliability supports mission-critical services such as connected robotic factories, and low latency makes delay-critical services such as driverless cars a reality.

These network benefits were the prime reason behind 5G development: high speed (targeted at 10 Gbps) reducing latency down to less than a millisecond, and increasing reliability (to the tune of 100%). And fully justify the use of 5G networks for life-critical services like remote surgery and autonomous driverless cars. With IoT opening up a new world of differentiated services including connected homes, automated factories and a massive build-up of small devices, there will be tremendous business opportunities for the IoT service providers as well as the CSPs.

ITU has categorised 5G services essentially as eMBB (enhanced mobile broadband), uRLLC (ultra-reliable and low-latency communications) or mMTC (massive machine-type communications) services. Each of these categories has varying needs for latency, reliability and connectivity, with the success of uRLLC services being the most dependent on these 3 parameters. With its ultra-reliable, low latency characteristics, uRLLC becomes the category of choice for new services like the autonomous car, industrial automation and augmented reality.

To achieve the required latency and reliability, the RAN and air interface pose challenges, which despite the virtualization of the 5G core, still remain a hurdle because of the physical entities involved. For this reason, the Cloud RAN of 5G is being designed to reduce latency, and transmission and propagation times are being reduced to a minimum.

However, despite these measures, the onus is on the CSP to assure latency, reliability and connectivity on a 24*7 basis to prevent any degradation of these critical parameters. uRLLC based 5G/IoT services will expect high quality and its users will demand stringent SLAs. And if these are not guaranteed, many of the much touted uRLLC-based 5G/IoT services will buckle under their SLAs and land the IoT service providers in serious commercial problems.

As data generated by uRLLC services such as autonomous cars and connected factories traverses 5G networks, it needs to be monitored in real-time for key network KPIs: capacity, throughput and bandwidth allocation. However, as mentioned above, the more critical measurements would be guaranteeing latency, reliability and connectivity. Here are some solutions for better managing these key parameters.

**Latency** requirements for uRLLC can range from 1-10 ms depending on the IoT services, and varying levels of these parameters require 5G network functions (RAN and Core) to be sliced so that appropriate manoeuvring, i.e., scaling-in, scaling out of resources can be carried out. Assurance systems are needed to extend assurance to 5G slices and sub-slices, not just the entire network.

**Reliability** can be improved through a secure and always-available network with built-in redundancy. To get a feel of the low tolerance to error in 5G, here are some comparative

values: LTE tolerates Block Error Ratio of 0.01, and the BLER for 5G is expected to be 0.00001 in a 1 ms period. The CSP would require an assurance system to assure such high levels of reliability at all points of time, e.g., under massive IoT load conditions, and in dynamic resource allocation situations.

**Connectivity** can be defined as the ability to connect to the network and offer continuity of services, especially when data sessions are handed over between 5G RAN, LTE and WiFi networks. Assuring mobility continuity, coordination and availability throughout an uRLLC session is critical.

To achieve all of the above, many CSP operational processes will require upgrading to be ready for 5G, including integrated proactive closed-loop automation, service assurance and service orchestration. Open APIs including TMF APIs are an effective solution for such complex ecosystem integrations.

The IoT service providers and the 5G CSPs understand that life-critical and delay-critical services are highly dependent on the 5G network quality and the management of its slices. It will require renewed effort on the 5G operator's part to analyse and action network/service data quickly to keep latency, reliability and connectivity under strict control and offer proactive remediation. Through the use of key assurance techniques such as predictive models, automated root cause analysis, closed-loop automation, service orchestration and policy-driven service quality management 5G CSP can be armed to deliver on the promise of IoT services.

Author:

Sandeep Raina

Product Marketing Director
MYCOM OSI
sandeep.raina@mycom-osi.com
info@mycom-osi.com