Service Assurance and Network Protection in Fifth-Generation (5G) Networks

Position Paper

See. Control. Secure.

Contents

See. Control. Secure.

Service Assurance and Network Protection in Fifth-Generation Networks

Fifth Generation (5G) networks are more than just higher capacity versions of 4G/LTE—they represent a radical evolution in many ways. Mobile networks were born to augment wireline networks with mobile telephony and then with data. With 5G, mobile networks are positioned to be a viable replacement for wireline networks and support accelerated growth of connected devices and the IoT. 5G is a service-based network, capable of supporting multiple services with very specific performance requirements by dynamically allocating shared infrastructure resources. 5G takes into consideration current and future services, application diversity, endpoint massification, and throughput growth.

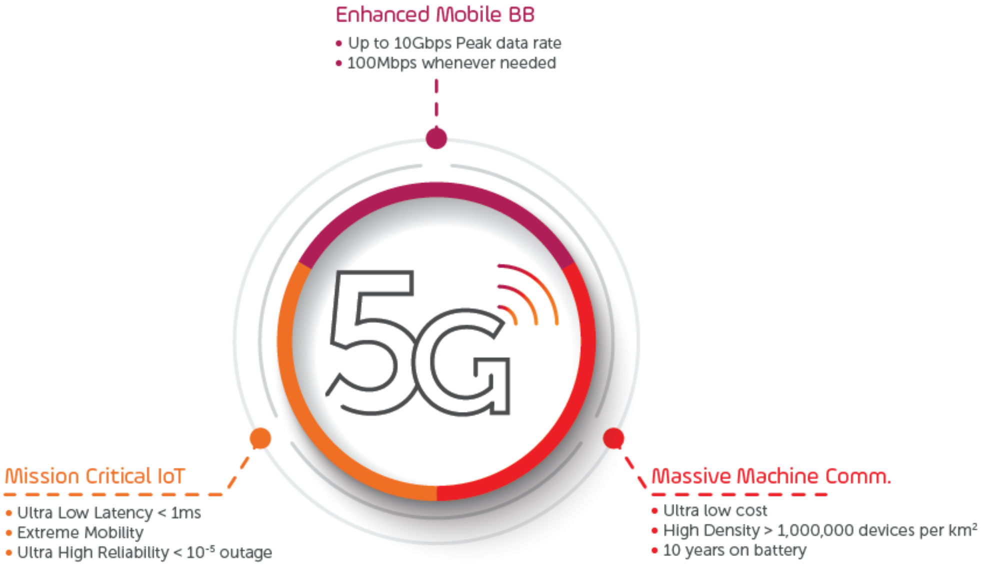
Enhanced Mobile BB
• Up to 10Gbps Peak data rate
• 100Mbps whenever needed
5G
Mission Critical IoT
• Ultra Low Latency < 1ms
• Extreme Mobility
• Ultra High Reliability < 10^{-5} outage
Massive Machine Comm.
• Ultra low cost
• High Density > 1,000,000 devices per km^2
• 10 years on battery

Figure 1. 5G Use Cases

The three main use cases for 5G are **Extreme Mobile Broadband**, **Massive Machine Communication**, and **Critical Machine Communication**. These three services demonstrate the versatility of 5G networks on the vectors of scale, throughput, and latency. 5G drives fixed-mobile convergence and the massive growth of endpoint connectivity.

For example, a single 5G network is capable of supporting 8K video streaming, gaming, and virtual reality in addition to ultra-reliable, low latency, low bandwidth, V2X collision avoidance systems and other machine-to-machine communications, on a massive scale.

Supporting multiple services with such disparate performance objectives on one monolithic network would be extremely cost prohibitive. 5G addresses this with end-to-end network slicing, ensuring that each network slice can support a service and its specific performance objectives.

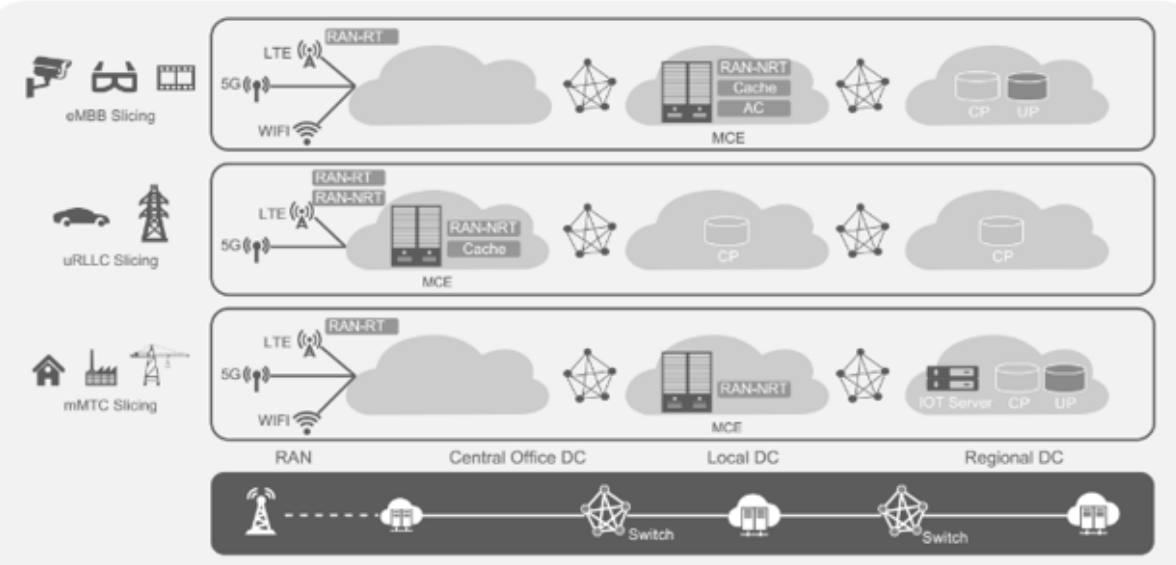

Figure 2. Network Slicing

Network slicing relies on virtualization of physical resources and network functions, and the employment of advanced network management and orchestration systems. The network allocates resources and their placement in the network to meet the performance objectives for each slice and its associated service. The network dynamically scales network function resources up or down to adapt to changing traffic conditions.

Disparate·network·services·are·supported·on·a·shared·infrastructure·with·end-to-end·network·slicing.·The·network·dynamically·allocates·virtual·resources·and·their·optimal·placement·in·the·network·to·meet·the·performance·objectives·of·each·slice·and·service.¶

Control and User Plane Separation enable flexible network deployment and operation, and the independent scaling between control plane and user plane functions.

The building blocks of network resources and function are based on micro services to maximize utilization of physical resources. With 5G and the requirement for network slicing, NFV implementation is mandated together with advanced management and orchestration.

Allot’s Position in 5G Networks

Service Assurance

At the core of the Allot Service Gateway is its capability to virtualize network resources into a hierarchy so that applications, users, communication links, and network entities (such as base stations) can be represented, monitored, and controlled. The Service Gateway already delivers real-time service assurance with automated QoE management for existing network architectures and will do so for 5G as well.

5G network slices are quantified by their allocated resources and dynamic scaling of resources is based on their utilization and technical KPIs[1]. The Allot Service Gateway takes a customer-centric approach, and monitors performance and allocates resources based on Key Quality Indicators (KQIs), such as resolution and stalls when quantifying video quality of experience. QoE monitoring, in addition to technical KPIs, can provide for better-informed resource allocation and service assurance.

The Allot Service Gateway takes a customer centric approach and measures and allocates resources based on the quality of experience of a user, device or application¶

In addition, the Service Gateway provides precise detection and treatment of problems, whether related to a specific application in a Mobile Broadband slice, a given video resolution (this capability also applies to encrypted video) or problems at a specific cell. The Service Gateway can manage the QoE at the device, cell, and customer level for contextual and accurate results.

Service Differentiation

A second benefit is that while a slice is optimized for a specific set of performance requirements, there is, and always will be, a requirement for additional granular (e.g. application specific) control. Within an mBB slice, we may want to differentiate between applications, service providers, users, and locations. For example, video and cloud backup, both applications that would typically run on a Mobile Broadband slice, would benefit from QoE-based traffic management. End-user QoE expectations of these two services are completely different even though they may share the same slice. Stalling, for example, while it has a significant impact on the QoE of video consumption, it is not a big deal for cloud backup.

[1] An Overview of QoE for 5G Networks: http://www.iteejournal.org/Download_dec16_pdf_1.pdf

Network Protection

With increased access rates and massification of connected endpoints, enabled and driven by 5G, there is valid concern that attacks from the radio access network (RAN) can have a significant impact on network performance and resource utilization. IoT-based attacks have proven to have devastating effects in traditional networks. 5G ups the ante.

> *Protect·the·5G·infrastructure:·In-line,·bi-directional·DDoS·detection·and·mitigation·in·addition·to·endpoint·infection·and·weaponization·prevention.¶*

5G infrastructure must be protected from the three steps of a DDoS attack—the compromise or infection of endpoints, the weaponization of the endpoint, and the detection and mitigation of the DDoS traffic.

Allot's approach to protecting 5G networks is based on carrier-class DDoS detection and mitigation that does more. It includes:

- In-line, bi-directional, automated detection and mitigation of DDoS attacks
- Traffic-shaping policies that limit the effects of flash-flood and DDoS traffic on critical network resources
- QoE assurance during DDoS attacks
- Behavioral analysis of host communications to identify and quarantine compromised endpoints
- Network-based malware protection of endpoint devices
- Blocking of botnet command-and-control communications

The solution is fully NFV compliant for automated and dynamic network allocation and scaling. These capabilities also serve as the basis for IoT[2] and user[3] security, value-added services.

Migration to 5G

Today, the service gateway provides granular visibility, control, and service assurance in 4G/LTE networks for applications, users, communication links, and network entities. SLA parameters and QoE objectives can be mapped and carried over to enable a smooth migration from existing networks to 5G.

[2] Please refer to https://www.allot.com/service-providers/iot-secure/ for more information

[3] Please refer to https://www.allot.com/service-providers/security-as-a-service/ for more information

5G Compatibility

AOS, the underlying software that powers every Allot Service Gateway is fully virtualized and NFV compliant. Allot has made significant investments in NFV, including integrations with the leading 5G core and RAN vendors and compatibility with third-party orchestration systems. The architecture of the Service Gateway has Control and User Plane Separation that fits into the 5G architecture with minimal adaptation. The virtual edition of the Service Gateway (SGVE) employs flow balancers to scale up with additional virtual controllers, in keeping with the concept of micro-services.

Summary

Fifth-generation networks are designed to support and drive fixed-mobile convergence, massive scale, and growth of the Internet of Things and ultra-reliable machine-to-machine communications. The Allot SGVE and management systems enable operators to efficiently deliver heterogenous, resource-competing services with a customer-centric approach, based on application specific QoE.

The benefits of the Service Gateway, realized in previous generation networks, apply to 5G in many areas, including service assurance and service differentiation and even more so in network protection.

This page is left intentionally blank

www.allot.com   sales@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826

Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165

Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015

Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669

Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626

allot
See. Control. Secure.