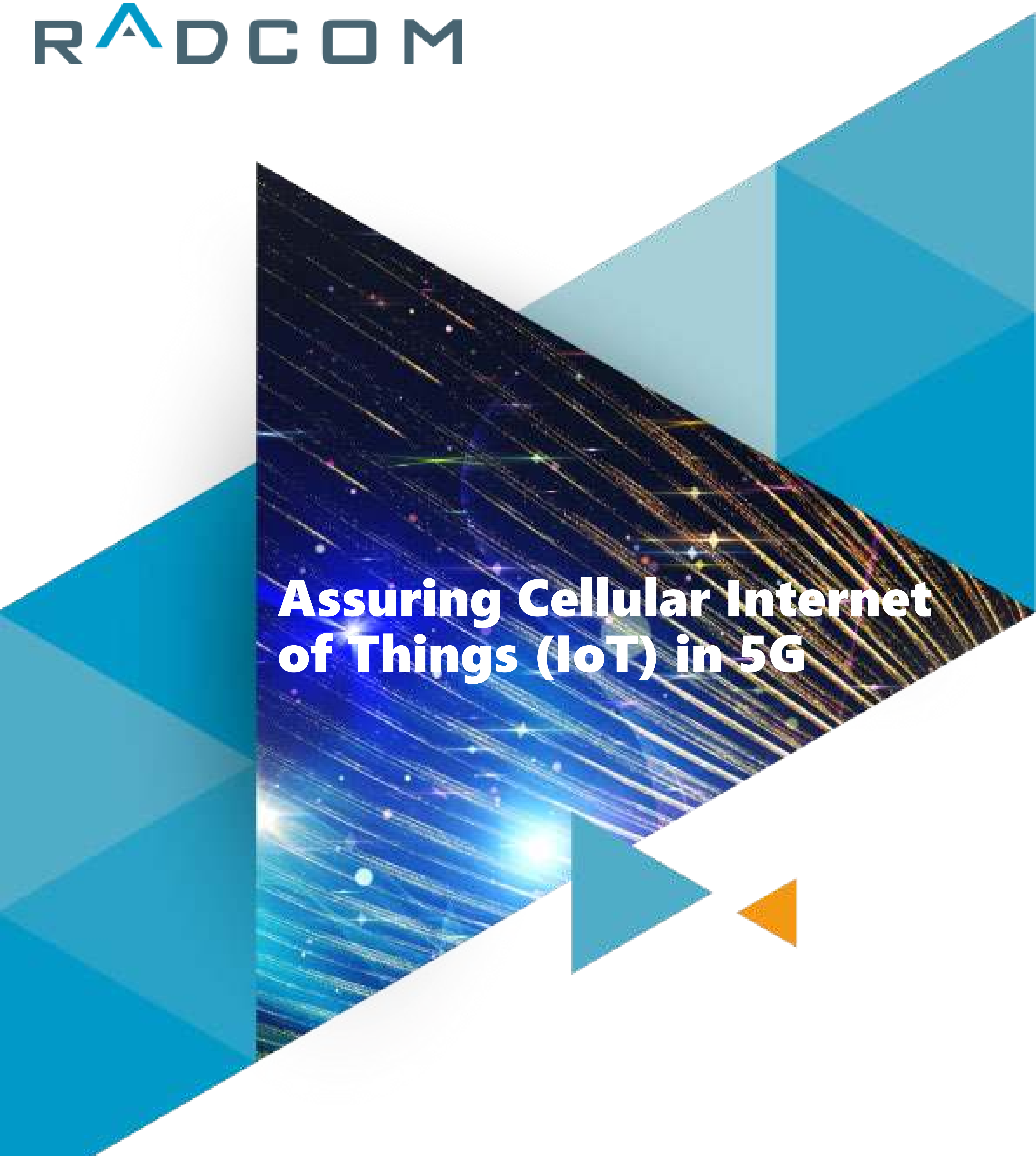
RADCOM

Assuring Cellular Internet of Things (IoT) in 5G



The information, content or material herein is provided "AS IS", is designated confidential and is subject to all restrictions in any law regarding such matters, and the relevant confidentiality and non-disclosure clauses or agreements issued prior to and/or after the disclosure. All the information in this document is to be safeguarded and all steps must be taken to prevent it from being disclosed to any person or entity other than the direct entity that received it directly from RADCOM.

The text and drawings herein are for the purpose of illustration and reference only.

RADCOM reserves the right to periodically change information that is contained in this document; however, RADCOM makes no commitment to provide any such changes, updates, enhancements or other additions to this document to you in a timely manner or at all.

Publication Date: August 2022

Website: http://www.radcom.com

Introduction

For the next generation Cellular Internet of Things (IoT), 5G will build on the foundations offered in 4G and significantly enhance these capabilities to provide services across a wide range of use cases from Consumer IoT to Industrial IoT as well as Massive IoT.

4G introduced Machine Type Communications (MTC), which refers to two non-smartphone objects communicating. MTC was initially considered only for low-data-rate devices and applications. 5G opens the door for communicating more sophisticated and higher data rate objects that must meet stricter latency and reliability requirements.

5G brings significant improvements in latency and data rate compared to 4G. These improvements are vital in meeting the strict requirements in vertical markets such as factory automation (industry 4.0), transport, energy, or entertainment, including augmented and virtual reality.

Cellular connectivity, especially in harsh industrial environments, has an inherent advantage over Wi-Fi and even wired technologies. Wi-Fi is less secure and more susceptible to interference than cellular by design. Wired technologies are less flexible and more difficult to update or change in a factory layout. Thus, 5G will be a key technology for industrial applications, especially when deployed as a private network where the network owner has full network control.

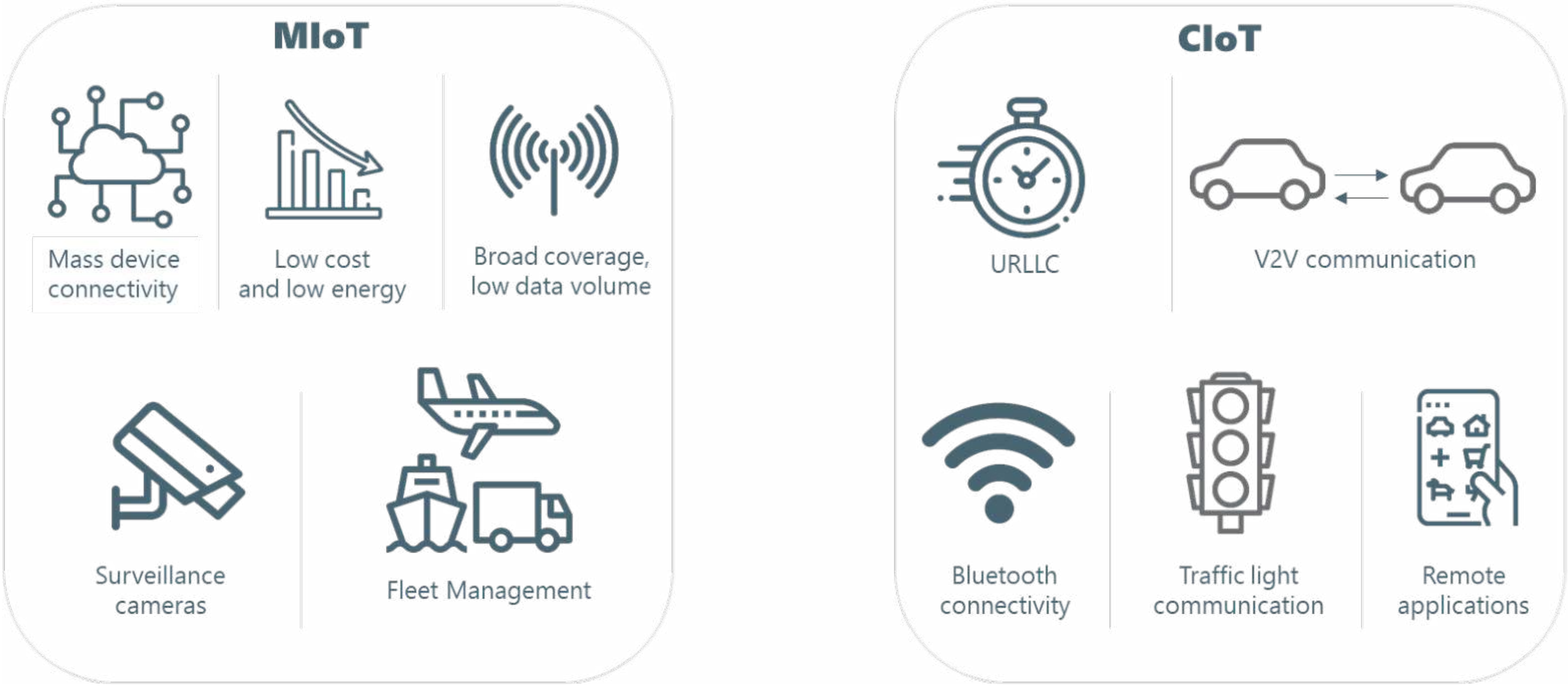


Figure 1 - Differing requirements for Massive and Critical IoT applications

5G IoT includes both Narrowband- IoT (NB-IoT) and LTE Category M1 (LTE-M) and adds additional security, automation, and management functions to the 5G radio and core networks to enable the ultra-reliability requirements for Critical IoT and the connection density for Massive IoT across many vertical domains.

NB-IoT and LTE-M technologies will continue evolving as part of the 5G specifications, meaning that operators can leverage their current investments in IoT today and build on them as part of the 5G evolution. The main differences between the standards are the latency and speed. NB-IoT is designed more for static sensor applications and LTE-M for mission-critical applications (with a latency of 10ms vs.1.6-10 seconds) as well as enabling an increased data throughput compared to NB-IoT. Both standards will also coexist in the same networks as other 5G New Radio (NR) components, like enhanced mobile broadband and critical communications, which means that the long-term status of these technologies is established.

Most of today's cellular IoT connections generate relatively small amounts of data traffic. The typical data size for a sensor-based service per transaction is about 100–150 bytes, with a payload comprised of a device ID, timestamp, and reported data values. Currently, IoT technologies can support data rates of approximately 170 kbps (DL) and 250 Kbps (UL) for NB-IoT and 1 Mbps for LTE-M (DL/UL). However, this data rate is expected to increase as a broader range of use cases evolve along with the continued rollout of 5G and edge networks.

Using 5G Massive Machine Type Communication or mMTC will make it possible for networks to connect up to 1,000,000 devices per square kilometer. The type of devices that can be connected will also expand beyond the more limited selection we have under 4G. Making sure that all these devices and connections are safe is a key to keeping your customers' devices running smoothly. Hence, having a comprehensive assurance solution is critical for managing all this complexity.

These new use applications will include traffic safety, automated vehicles, drones, and industrial automation, which will have strict requirements on availability, latency, and reliability and will generate significantly more data traffic. IoT covers a broad spectrum of use cases and applications. From smart metering and asset management that require significant numbers of low-cost devices to send small amounts of data, to drones and VR/AR applications that have high throughput, low latency, and large data volumes. All these use cases will require dynamic, real-time assurance to monitor the different IoT performance requirements for each service and ensure SLA compliance.

Network slicing will also allow operators to deploy new, IoT services with low-energy, and cost-effective sensors at scale with the ability to adjust the network capacity on-demand, while bringing in new revenue streams. The enterprise customer will gain a single, secure private network. With isolated traffic protected within the slice and network security configured according to their specific needs. Network slicing will also allow sharing across agencies and organizations while meeting performance and security requirements. For these slices service assurance needs to offer a multi-tenant solution that monitors each slice while providing each enterprise customer access to his own data.

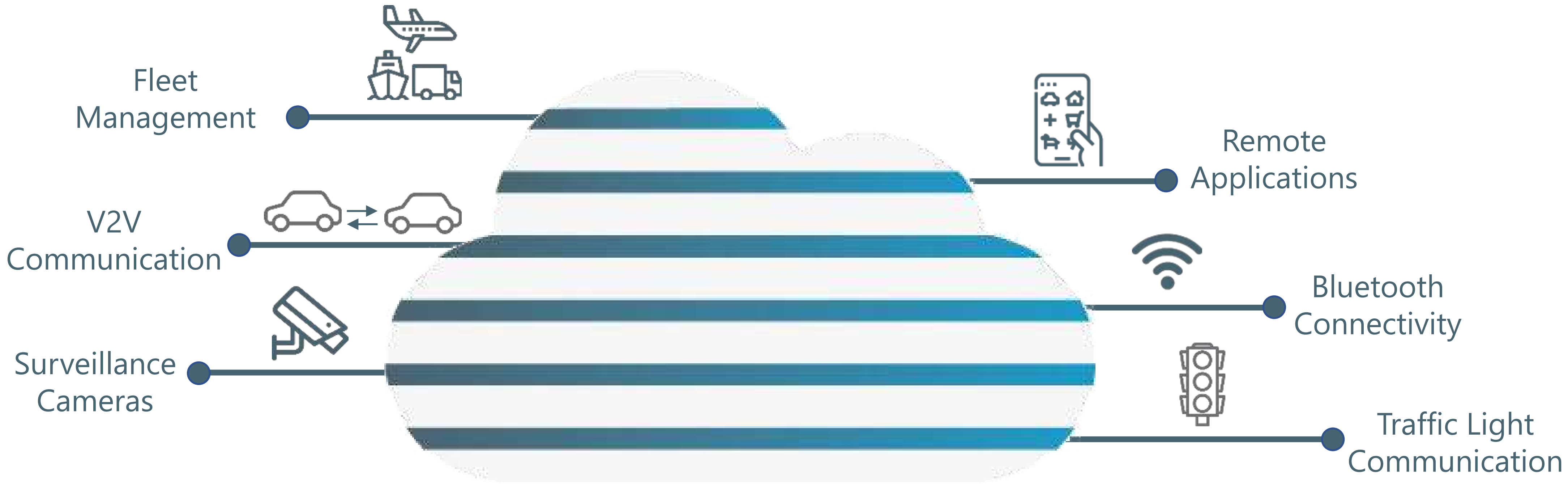


Figure 2 – Different network slices in the cloud

In the future, use cases will expand to include autonomous cars and traffic safety that require ultra-low latency, ultra-reliability, and high availability as well as smart electrical grid automation and industrial automation that are time sensitive and require precise positioning.

Today, 166 operators in 102 countries are known to be actively investing in NB-IoT. Whereas 74 operators in 53 countries are actively investing in LTE-M. With 39 operators having deployed both NB-IoT and LTE-M.[1] Operators are rolling out major IoT initiatives in areas such as smart homes, agriculture, robotics, smart cities, and intelligent energy that are all leveraging the potential of IoT.

Operators recognize significant revenue opportunities across a diverse range of new IoT applications and offer a wide range of services; from basic IoT connectivity and service management right up to complete end-to-end solutions and vertical-specific offerings. At the end of 2021, there were approximately 1.9 billion mobile IoT connections. By 2027 the number of connections is expected to reach 5.5 billion; a compound annual growth rate, (CAGR), of 19%.

As 5G continues to rollout globally, 4G IoT will continue to evolve and operate seamlessly, with the new 5G network. So, either 4G or 5G cores will support current IoT deployments allowing 5G to leverage current IoT investments fully.

[1] GSA: NB-IoT and LTE-M: Global Ecosystem Member Report, February 2022

Deployment and management challenges

As the telecom industry tends to focus on the customer experience, IoT brings a different set of challenges to the operators

Monitoring high-capacity IoT services

As the 5G rollout advances and the technology of IoT advances, the need for assurance services becomes ever more important. When dealing with industrial and critical IoT, the machine to machine~~,~~ big data learning requires high-speed and highly reliable network connectivity. Other use cases could involve video streaming for remote control capabilities. If faults occur and systems malfunction, this could have serious consequences. Being able to track data, compartmentalize network slices and catch anomalies are all functions that will gain prominence as time goes on.

Guaranteeing service connectivity

Unlike subscribers, IoT devices are not going to be calling customer support if they have problems connecting to the network. So, a critical part of delivering quality IoT services is ensuring network availability and IoT service connectivity.

Providing connectivity with some devices only communicating sporadically, others can send data continuously. In contrast, others will send huge amounts of data in real-time (for example remote control of heavy industrial machinery or mining equipment) makes it challenging for operators to anticipate, and therefore assure, the necessary coverage.

Also, as IoT gains momentum more and more critical use cases such as smart monitoring of utilities (electricity, water, gas), agriculture (for crops and livestock) and the environment (water/air quality, fire prevention) these devices need to work when expected otherwise the fallout could be significant.

Therefore, maintaining service connectivity and rigorous SLAs with customers is essential, not least because the operators' customers can be a municipality or government deploying thousands of devices.

Ensuring privacy and security

IoT brings excellent revenue opportunities for operators but also risks as thousands of devices (with sometimes sensitive information) connect to the network. So, security and privacy are a priority issue for operators deploying IoT. IoT can be used to attack an operator's network from both within and outside the operator's network. Meaning that IoT devices can be hacked and forced into becoming bots. With a network of such devices, hackers can then carry out DDoS attacks. Having so many devices spread across the network means it only takes access to one device for an attacker to tap into the network and steal sensitive data or cause havoc.

With IoT covering services such as health care, transportation, energy, and industrial sectors, operators need to ensure that security and privacy mechanisms are in place to:

- Identify and authenticate all the devices
- Provide access control to the different IoT entities that need to be connected to create the service
- Enable data protection to guarantee security (confidentiality, integrity, availability, authenticity) and privacy
- Guarantee availability of network resources and protect them against attack

Management IoT services at scale

With the vast number of devices deployed, operators need to be able to manage their IoT services at scale and utilize as much automation as possible. The level of this challenge will only increase as 5G rollouts continue with the proposed minimum standard for

5G networks are able to support one million device connections per square kilometer. Operators need to deploy a solution that is proactive and helps assure connectivity, safeguard the security, and manage IoT service complexity at scale.

RADCOM IoT Service Assurance

RADCOM provides operators with a comprehensive IoT Service Assurance solution, including a range of capabilities that help alleviate the challenges and ensure that customers receive IoT services that meet stringent SLAs.

From ensuring service connectivity, optimizing network performance, and monitoring security, to delivering automatic anomaly detection for connectivity assurance and security. RADCOM ACE displays real-time intelligence on the behavior of the network, highlighting any issues in connectivity as well as device and network performance.

The operator can then drill down to a specific device or location, pinpointing the root cause of any network issue, ensuring smooth connectivity, and maintaining SLA's. While the "things" in IoT are essential, how devices relay information and perform are equally important.

In addition to individual devices or device types, the operator can also examine the overall service performance. As well as network/device performance and connectivity, RADCOM's solution provides the geolocation of devices. For some IoT devices, this is important as specific devices are expected to be static, and so if they move, this means there could be an issue.

Having IoT assurance can help keep you informed of what is happening inside of your networks, making sure there is no break in the connectivity, and can even help you identify what is going on with key performance indicators, (KPIs), in different slices of your network.

RADCOM Automatic Anomaly Detection

With more and more IoT devices connecting to an already complex network using Machine Learning, will be crucial for mass deployments of IoT devices, identifying baselines and then automatically detecting anomalies.

When a device fails to connect to the network, it is unable to notify the operator as a regular human subscriber would. So, to ensure IoT service connectivity and performance, IoT devices need to be continually analyzed to provide operators with real-time alerts and lower time to detection and resolution.

RADCOM gives operators built-in anomaly detection and near real-time feeds to 3rd party tools. RADCOM detects IoT anomalies by utilizing Machine Learning to define a baseline per device and automatically generates alarms if the baseline threshold is crossed.

Anomaly Detection System

Figure 3 – Machine learning automated anomaly detection loop

Automated anomaly detection can also be used to detect and resolve security issues as well as for connectivity and service performance. RADCOM's solution sets the baseline and monitors anomalies according to the following categories:

Data volume

Typically, a machine will send the same amount of data (~100 -150 bytes) in the same frequency. If the device suddenly starts sending significantly more data, this would be considered abnormal and could mean that someone has hacked the device or there is a malfunction.

Traffic destination

An IoT device sends the data to a specific application server using a particular IP address, and RADCOM's solution will learn this address automatically. If the device starts sending to a new server, then RADCOM will sound an alarm.

Data transmission frequency

RADCOM determines how often and when data is sent per device and so if the schedule or rate changes, an alert will be generated by RADCOM's system.

RADCOM NWDAF

A comprehensive IoT Service Assurance solution for 5G must have both automated and manual options. Operators can move to a closed-loop approach to managing their IoT services by deploying automated assurance based on a Network Data Analytics Function (NWDAF).

While most issues can be automatically resolved using the closed-loop approach and NWDAF, some of the most complex issues will still require more traditional assurance tools such as KPI/KQI dashboards with the ability to drill-down to session and packet views for manual deep-dive troubleshooting. RADCOM can provide both automated and manual options for IoT assurance.

RADCOM NWDAF offers the following automated capabilities:

- Detecting misbehaving devices by observing abnormal traffic patterns
- Determining the correct policy for background data transfer by analysis of traffic volume, transfer frequency and load status information
- Dynamic traffic routing to the edge by analyzing network status (for example load information based on time and space), which service is available at the edge, and the device’s location
- Collecting and analyzing the status of network slices to automate IoT service slices
- Synchronizing with the network orchestrator to scale up or scale down the resources for IoT network slices

Conclusion

Operators need to deploy an efficient assurance solution for managing millions of IoT devices that generate data in different patterns and varying regularity to analyze and understand what’s happening in the network in real-time. Only then can they optimize their IoT service performance and ensure their most demanding customers, such as government agencies, municipalities, and large enterprises, receive the expected service.

RADCOM IoT Service Assurance provides a comprehensive end-to-end view of the overall IoT service with troubleshooting capabilities that enable operators to meet stringent SLAs with their customers across a wide range of IoT implementations and use cases. With automated anomaly detection, RADCOM ensures service performance, device functionality, security, and connectivity in a more efficient and viable way for operators to deliver quality IoT services to customers while providing a secure and fully optimized network.

RADCOM

Visit RADCOM at:
www.radcom.com