



RADCOM

Assuring the Internet of Things (IoT)

Narrowband IoT (NB-IoT) and LTE-M (LTE Machine-type Communications) - previously known as LTE-MTC or LTE-eMTC - are cellular technology standards specified by 3GPP Release 13 (finalized in June 2016) to address the market for low power wide area connectivity and the Internet of Things.

3GPP built upon the standards already ratified in LTE Cat 1, Release 8, and LTE Cat 0, Release 12. The updated standards focus on low cost, long battery life, high connection

density, and improved support for use cases where standard mobile coverage is weak – such as for sensors deployed indoors or in remote locations.

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.










NB-IoT				LTE-M				
<ul style="list-style-type: none">• Focused on very low data rates• Ideal for simpler static applications				<ul style="list-style-type: none">• Highest bandwidth of any LPWA technology• Ideal for fixed and mobile applications				
Batch Communication - - - - -				LATENCY - - - - - Real-Time Communication				
LPWA Application								
								
Smart Meter	Pipeline Management	Home Automation	Building Automation	Smart Grid	Transportation	Retail & POS	Home Security	Patient Monitoring
20kbps - - - - -				SPEED - - - - - 350kbps				

Figure 1 - Differences between NB-IoT and LTE-M technologies and their use cases

There are additional cellular technology standards for low-power, wide-area networks (LP-WAN). For example, 3GPP-based EC-GSM - formerly EC-EGPRS- that stands for Extended Coverage. EC-GSM is an IoT-optimized GSM network. This standard has specific use cases in non-Western regions such as Malaysia, African, and Middle Eastern countries, where 2G remains popular.

Introduction

There are additional standards and vendors in the IoT space that don't use the mobile network and use unlicensed-spectrum technologies, such as Sigfox (in 60 countries) and LoRaWAN (in over 100 countries), created before the launch of 3GPP alternatives.

Most of today's cellular IoT connections generate relatively small amounts of data traffic. The typical data size for a sensor-based service is about 100–150 bytes, with a payload comprised of a device ID, timestamp, and reported data values. Currently, IoT technologies are

capable of supporting 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 volume is expected to increase as a broader range of use cases evolve along with the continued rollout of 5G and edge networks.

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. In the future, use cases will expand to include autonomous cars and traffic safety

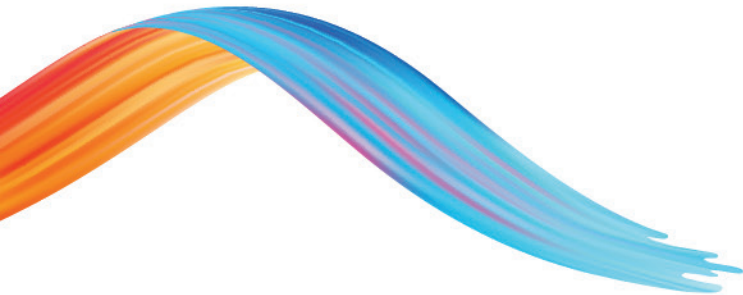
that require ultra-low latency, ultra-reliability, and high availability as well as smart electrical grid automation and industrial automation that are time sensitive and require precise positioning. These differing requirements mean that for operators, no one technology will fit all use cases, which is why most operators are deploying multiple IoT networks.


Today, 141 operators in 69 countries are known to be actively investing in NB-IoT. Whereas 60 operators in 35 countries are actively investing in LTE-M. With 20 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 2018, there were approximately 1 billion mobile IoT connections. By 2024 the number of connections is expected to reach 4.1 billion; an annual growth rate of 27%.²

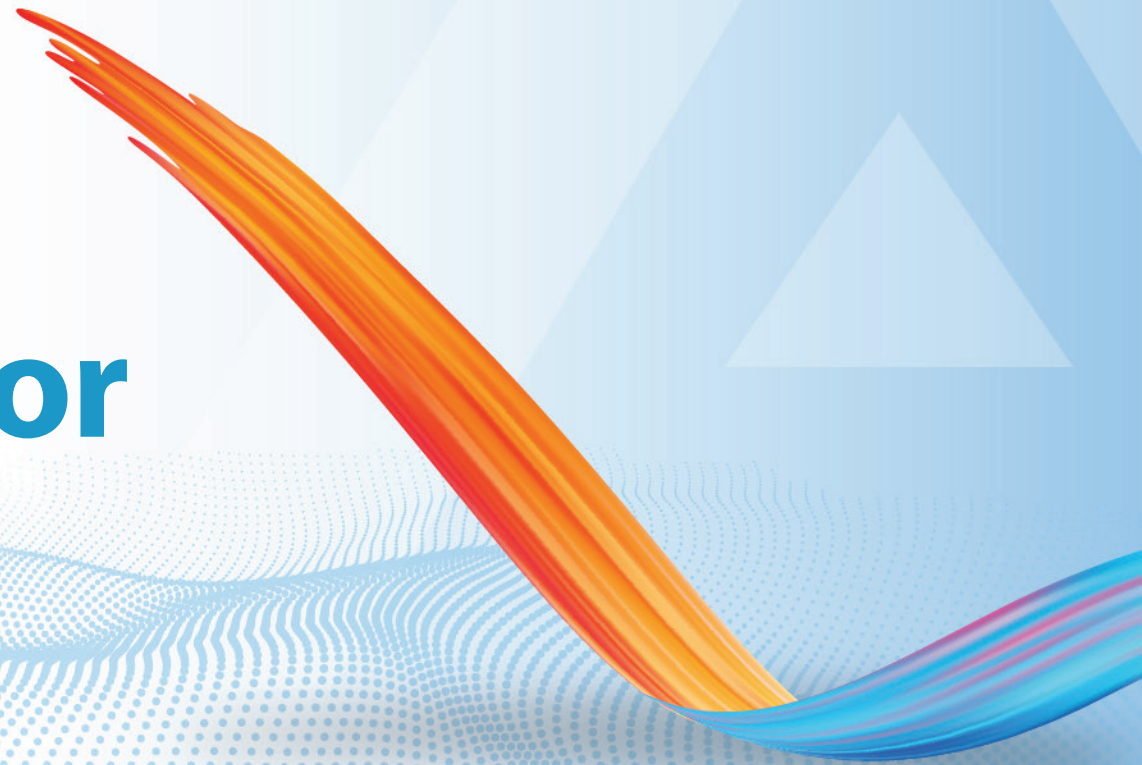
¹ GSA: NB-IoT and LTE-M: Global Ecosystem and Market Status Report, April 2019

² Ericsson Mobility Report, November 2018





Network Architecture for IoT



IoT data transportation options; advantages and disadvantages

1. Control plane transports user data or SMS messages via MME by encapsulating them in NAS (Non-Access-Stratum) which reduces the total number of control plane messages when handling a short data transaction. IoT services that occasionally transmit small amounts of data should utilize the control plane which will optimize the power consumption because the amount of signaling required and the “airtime” is reduced.
2. Services that need to send more information can benefit from utilizing the user plane connection, which can be used to send multiple packages. This approach consumes less power than sending multiple messages over the control plane. On the other hand, using non-IP over the user plane might be unrealistic simply because the benefits of using efficient protocols are nullified by using a user plane connection.
3. Non-IP allows for the use of protocols that are optimized for a specific purpose. UDP is asynchronous, but reduces the time of the connection, while TCP will keep the link open until an acknowledgment is received.

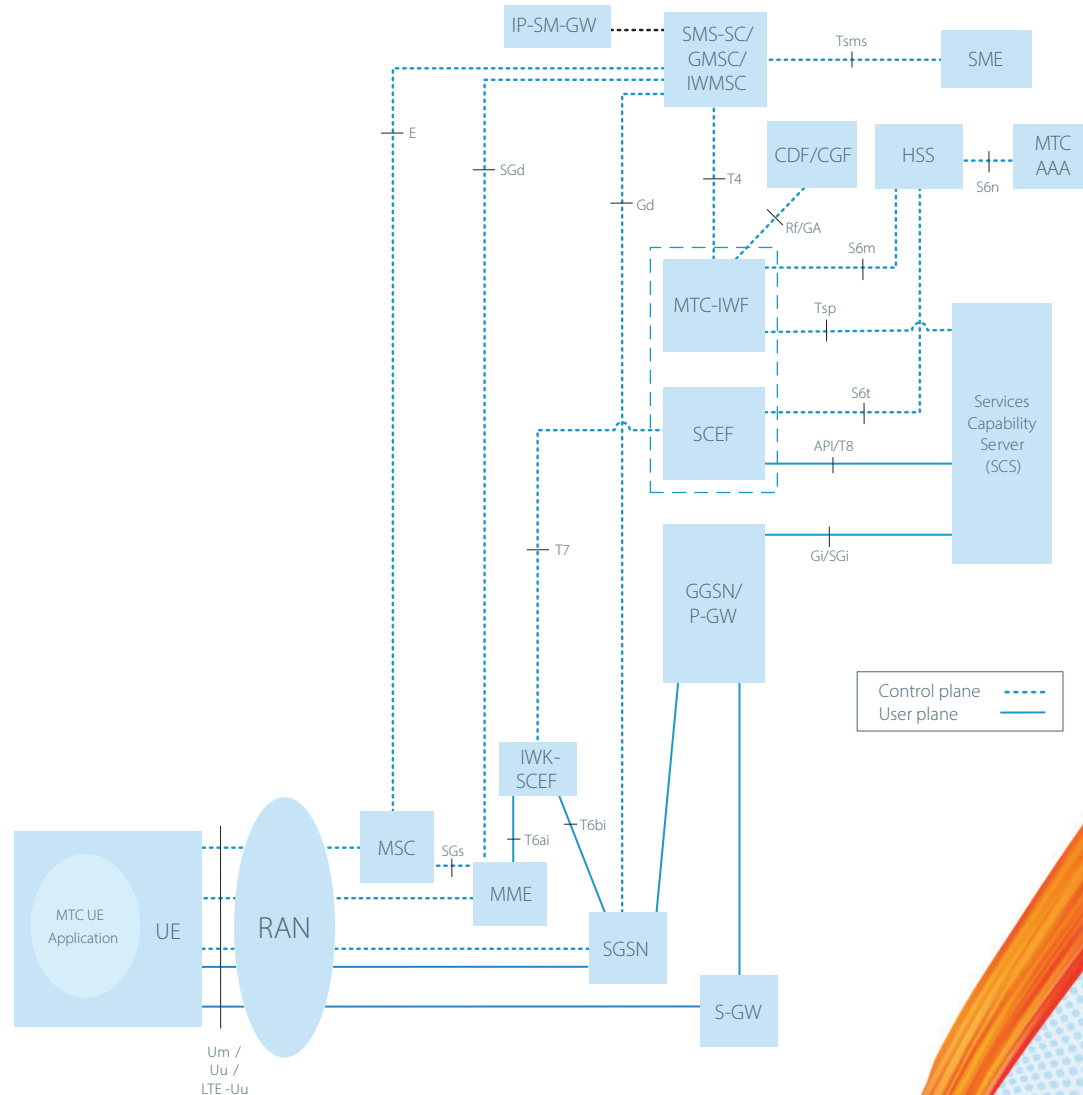


Figure 2 - 3GPP Architecture for NB-IoT and LTE-M



Deployment & Management Challenges

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

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, while others can send data continuously, 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 are essential not least because the operators' customer 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) are connecting to the network. So, security and privacy are a high priority issue for operators deploying IoT. IoT can be used to attack an operator's network from both within and outside the operators' network.



Ensuring privacy ... (cont.)

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 that 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 the 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 being 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**



Figure 3 - Monitoring IoT Service Performance

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

From assuring the service connectivity, optimizing network performance, monitoring security, to delivering automatic anomaly detection for both connectivity assurance and security. RADCOM Network Insights 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.

So, as well as 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.

The new IoT standards introduce several new paths for data to transverse through the network in which the user plane data is sent encapsulated inside the NAS protocol on the S1 MME, and then the MME can send it over to the application server (AS) in several different ways:

1. The MME can send the user plane over the S11-U (a new interface) to the SGW, then to the PGW and out to the AS. The S11-U interface is used for small data transmissions between the MME and S-GW. Based on the existing GTP-U architecture.
2. To encapsulate the user plane traffic inside the diameter message and send it on the T6a to the SCEF and then to AS.
3. Another option (if it is an SMS message) is to send it to the Short Message Service Center (SMSC) and then out to the AS (carried over a diameter-based protocol).

RADCOM supports the correlation between the S11-U and the S11 control plane and the new protocols and interfaces that include user plane captured in the control plane, several new diameter interfaces, and the new S1-MME messages and new encapsulation options for sending data over NAS.

In working with leading operators worldwide, most are looking to monitor the traffic around the MME, which provides the majority of the required information from a single monitoring point. However, RADCOM also tracks and correlates IoT traffic that goes through different paths through the network such as via the SGW/PGW and the SMSC. RADCOM's solution provides operators with KPI dashboards for IoT and supports the new IoT messages (for KPIs like success rate, average duration, etc.).

RADCOM also provides operators with a comprehensive call tracing application - QTrace - both for session tracing and drilling down from the KPI Dashboard for troubleshooting purposes. In QTrace, data sessions are correlated between S11 and S11-U to provide an end-to-end session based on the device IMSI.

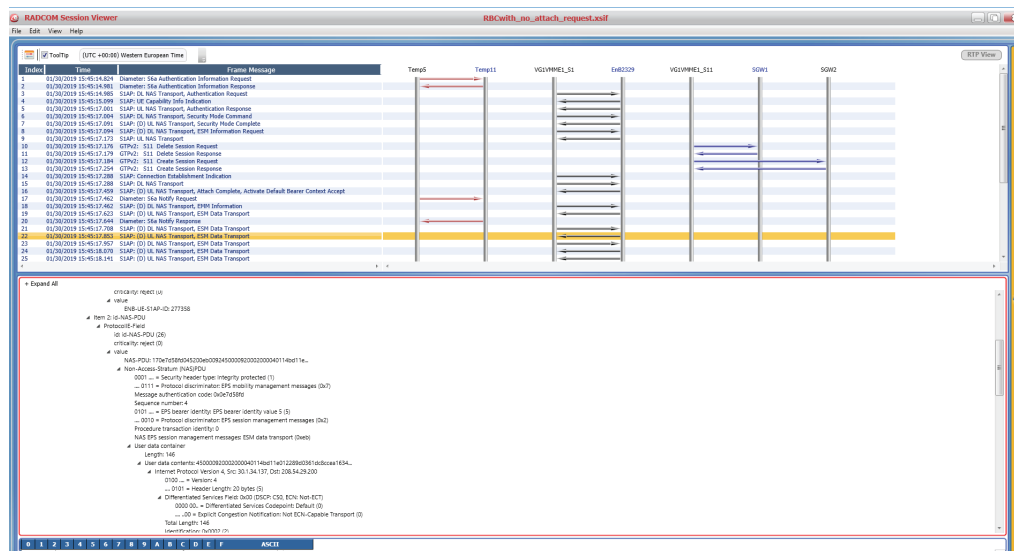



Figure 4 - Troubleshooting IoT services with RADCOM's call trace application - QTrace



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 real-time alerts and lower time to detection and resolution.

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

Automated anomaly detection can also be used to detect and resolve security issues as well as for connectivity and service performance.

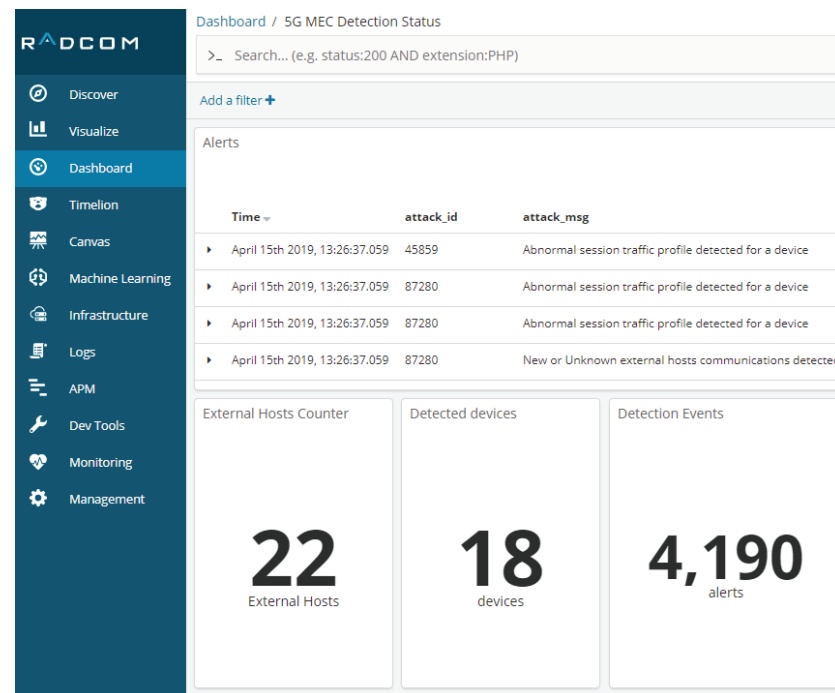


Figure 5 - Utilizing RADCOM's automatic anomaly detection for IoT services

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 Automatic Anomaly Detection

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 are receiving 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 SLA's 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.

Conclusion



www.radcom.com

© 2019 RADCOM Ltd. ALL RIGHTS RESERVED.

This document and any and all content or material contained herein, including text, graphics, images and logos, are either exclusively owned by RADCOM Ltd., its subsidiaries and/or affiliates ("RADCOM") or are subject to rights of use granted to RADCOM, are protected by national and/or international copyright laws and may be used by the recipient solely for its own internal review. Any other use, including the reproduction, incorporation, modification, distribution, transmission, republication, creation of a derivative work or display of this document and/or the content or material contained herein, is strictly prohibited without the express prior written authorization of RADCOM. 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: June 2019



RADCOM

RADCOMize
your
NETWORK