IoT connectivity – understanding the options and choices

White Paper

The broad scope of IoT requirements and business opportunities will lead to a variety of networks being built on different technologies and by different parties. IoT applications have highly diverse needs for network connectivity, reliability, security, latency, data rate, mobility and battery life; no single access technology can meet all these connectivity needs. With an IoT business strategy in place, operators will be better placed to assess its assets and processes to identify the technology choices that need to be made.

Contents

Executive summary: Navigating the complexity of IoT technology

Day by day, more and more Internet of Things (IoT) applications and use cases are being deployed. Sensors are used widely in production lines, electrical grids, logistics networks, vehicles and in the devices we wear and use. IoT applications, supported by licensed and unlicensed technologies, are boosting productivity, increasing efficiency and improving the customer experience in many vertical industries such as automotive, smart cities, public safety, utilities and more.

The broad scope of IoT requirements and business opportunities will lead to a variety of networks being built on different technologies and by different parties. Deciding on the most appropriate technologies in which an operator needs to invest begins with the setting out of a business strategy for IoT. This can then guide a thorough assessment of the operator’s existing assets and processes to identify the technology choices that need to be made.

The overall connectivity for IoT applications involves the full scope of a network including the radio access network, transport network, core network and network management, among others. However, in this white paper we look only at the radio access technologies that could be used.

Choosing the most appropriate radio access technology requires service providers to make important choices. While established operators can take advantage of their investments in licensed spectrum, other organizations may enter the market by deploying networks using the unlicensed frequencies.

Yet there is no single access technology that can meet all the connectivity needs of all IoT applications in all markets – the diversity of requirements is far too great. Each technology represents a trade-off between transmit range, data rate, power consumption, bands and business model.

High throughput, low latency and high reliability networks will be needed for applications such as video analytics in public safety and to support self-driving cars. At the other extreme, lower performance technologies with low throughput, relatively high latency and low reliability may be more cost-effective for less stringent applications such as smart metering.

For operators, success in IoT will be as much about business solutions as it will be about the technologies adopted. Expertise in network assessment, planning and maintenance is needed to navigate the fiercely complex commercial and technology choices involved.

Meanwhile, enterprises can meet their IoT needs by using operator connectivity solutions or deploy their own networks on unlicensed bands.

A wide range IoT connectivity demands

The total number of IoT connected devices (not including wearables) is expected to grow from 1.6 billion in 2014 to anywhere between 20 billion and 46 billion by 2020. Over the same period, the number of IoT-related network connections will grow by as much as 135-fold.

While the overall amount of network data traffic generated by IoT devices will be small, the signaling traffic they generate will grow hugely. A typical IoT device may need thousands of infrequent transactions over a long period to consume 1 MB of data, while the same amount of data can be consumed in a single mobile video connection (Bell Labs 2016).

The sporadic transmissions generated by billons of IoT devices will place new demands on network control plane capacity.

IoT applications also have highly diverse needs for network connectivity, reliability, security, latency, data rate, mobility and battery life. Often these requirements must also be met at extremely lost cost per bit, due to the lower value per bit of an IoT connection compared to a typical human cellular connection.

For the sake of simplicity, IoT applications can be divided into three broad categories according to the connectivity of the application and the relative importance of the cost of the device:

- Massive IoT: Billions of small scale, low cost devices, such as sensors and meters, will need to be connected. Yet these do not have stringent connectivity requirements as their application can tolerate delay and they are not generally mobile.
- Enterprise IoT: Industrial applications like maintenance monitoring and insurance telematics require more sophisticated, higher cost devices and reliable connectivity with reasonable throughput to handle higher volumes of detailed data.
- Critical IoT: At the top end of the scale are applications like connected cars, remote control and video surveillance, which demand various combinations of high throughput, complete coverage and extremely low latency.

Operators face the challenge of which connectivity technologies to adopt in order to meet the diverse demands of this huge variety of IoT applications. There is a large choice of connectivity technologies available, but which offer the most cost-effective and most appropriate set of parameters?

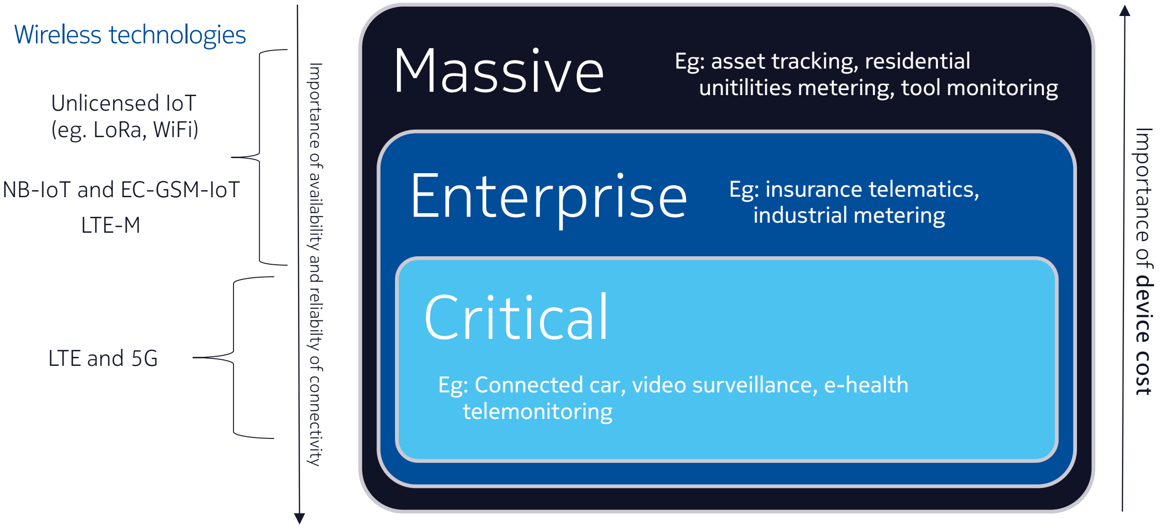

Wireless technologies
Unlicensed IoT (eg. LoRa, WiFi)
NB-IoT and EC-GSM-IoT
LTE-M
LTE and 5G
Importance of availability and reliabilty of connectivity
Massive
Eg: asset tracking, residential unitilities metering, tool monitoring
Enterprise
Eg: insurance telematics, industrial metering
Critical
Eg: Connected car, video surveillance, e-health telemonitoring
Importance of device cost

Figure 1: IoT applications can be broadly categorized into three segments related to device cost and connectivity needs

Examining some use cases - What do they need?

The Internet of Things will be characterized by a colossal range of use cases, most of which we probably cannot even imagine today. Yet it is the use cases and their specific needs that will govern the technology that operators will need to deploy.

We need to examine the use cases that we can reasonably foresee today and explore their business potential and connectivity requirements. This will provide the first step for operators deciding their IoT business strategies, which connectivity technologies will be needed and how they will need to invest in their networks.

In this paper we cannot cover all possible use cases, so we will focus on some major ones that are expected to provide substantial business opportunities for the industry. These fall into five broad categories:

- Fully automated driving
- Fleet management
- Smart cities
- Public safety
- Utilities

Use case: Connected cars towards fully automated driving

Connected cars, or Vehicle-to-Everything (V2X) communication, involves communication between vehicles and between vehicles and roadside infrastructure. Real-time communication enables vehicles to deal with situations that neither the driver nor the vehicle's sensors could otherwise identify, enabling more predictive driving. In-vehicle information-based services increase road safety, improve driver comfort and enable fully automated driving in the future.

To date, cellular communication has been the main technology for sending data from the car to the car manufacturer's cloud and to send information into the car. These applications do not need low latency communications. To support different automated driving applications, ETSI has standardized Intelligent Transportation System (ITS) messages for V2X communications, which have also been adopted for use with LTE networks.

While traffic information and diagnostics data do not generally require low latency connectivity, other applications will depend on reliable vehicle-to-vehicle communication with low latency.

When augmented with Multi-access Edge Computing (MEC), LTE advanced, NB IoT and LTE V2X, LTE can provide a viable and cost-effective solution that can accelerate the adoption of V2X communications by transport authorities and the automotive industry.

The hybrid use of the LTE portfolio will meet automotive industry needs on the way to 5G. It provides support for automated driving, increased comfort and improved infotainment and increases road safety and traffic efficiency.

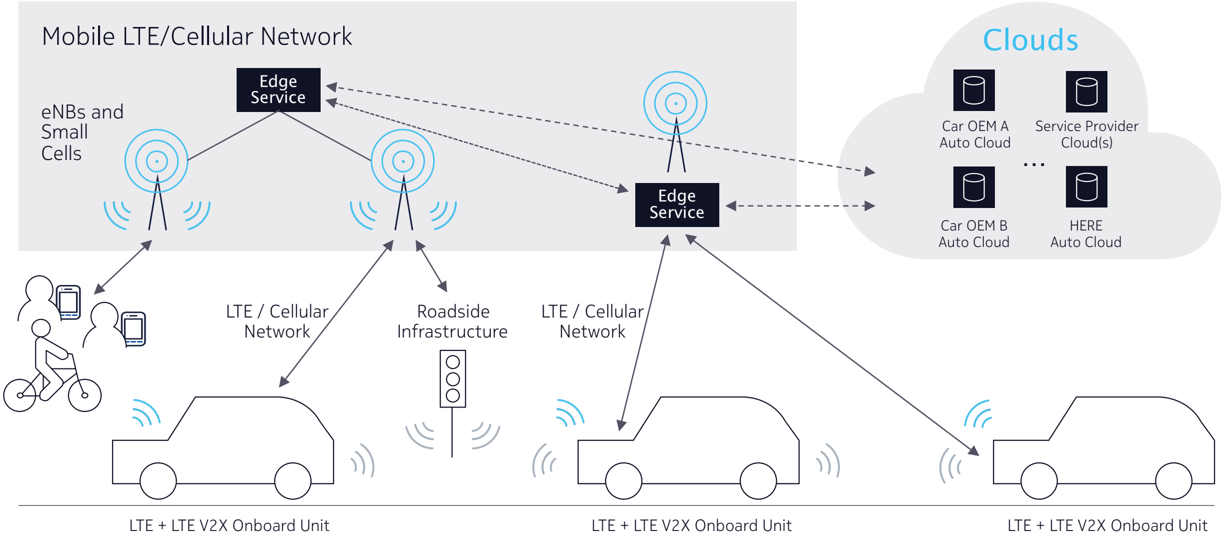


Figure 2: High level architecture of the connected cars ecosystem

Use case: Fleet management

Connected car management platforms will enable multiple over-the-air services for cars that could reduce industry and consumer costs substantially. For example, over-the-air software and firmware management could save vehicle and in-car system manufacturers about 30 percent of their warranty costs caused by software errors, including those in embedded systems.

In 2015, more than 51 million vehicles were recalled in the US[1]. However, some 30 percent of these recalled cars are not repaired because the owners are not aware of a recall or do not react to it[2]. These issues can be resolved by over-the-air software management that can remotely update in-car electronic control units (ECU).

Providing advanced remote monitoring and diagnostics via over-the-air fleet management is becoming an urgent priority for the automotive industry.

While Low Power Wide Area (LPWA) connectivity can support some basic fleet management monitoring apps, the need to deliver software updates will call for higher bandwidth that is best provided by technologies such as Wi-Fi and/or mobile broadband in the shape of LTE and future cellular technologies.

Use case: Smart Cities

Centralized data is the key enabler of most smart city services. There are many sources for this data including:

- City agency operations such as demographic and household data, school rolls or highway repairs
- Data contributed by citizens via smartphone applications, web pages and messages
- Data from automated smartphone apps that use the devices' embedded sensors
- IoT generated data from vehicles, buildings, infrastructure, controllers and embedded sensors

[1] Reuter 2016, http://www.reuters.com/article/us-autos-recalls-nhtsa-idUSKCN0UZ2UB
[2] JD Power and Associates, http://www.jdpower.com/cars/articles/safety-and-mpg/many-recalled-vehicles-go-without-remedy

A broad range of applications are emerging under the smart city umbrella, far too many to describe in this paper. Instead, we can explore applications that are the focus of significant development - smart parking and connected street furniture.

Smart Parking: A smart parking scheme involves equipping parking locations with cameras that feed information back to a central reporting system on their availability. Drivers can see availability and can reserve a space. Cameras at the parking location recognize the vehicle and could allow the driver to see their parked car at any time on their smart devices. Multiple types of connectivity are needed to make this efficient and reliable, from LPWAN for parking bay sensors, to broadband to support video streaming.

Connected street furniture: Billboards, bus shelters, lamp posts – most street furniture involves a significant capital cost, yet provides a relatively limited benefit. IoT applications can add to their value by helping to improve the quality of life for citizens and stimulate economic development. A good example is a recent project in Auckland, New Zealand[3] in which fiber and Wi-Fi connectivity was used to turn bus stops into valuable assets that enterprises can rent for services such as digital advertisements and Wi-Fi hot spots.

Smart cities will need a broad range of connectivity. Robust broadband access, sensor networks, cloud technologies, security and IoT platforms must deliver connectivity that is secure, reliable, highly available and with prioritization capabilities.

Future 5G networks will build on LTE to provide more capacity and ultra-low latency that will enable new use cases with even higher bandwidth requirements. Some of the IoT use cases in a Smart City can also be built with LPWA technologies, such as NB-IoT and LoRa, such as environmental monitoring, parking place occupancy and connected trash bins, where messages are relatively small and infrequent.

Use case: Public safety

Public Safety networks provide mission-critical voice communication and data services to government and civic authorities such as police and fire departments, civil defence and paramedic services. Public safety agencies and communications around the world are looking at how they can benefit from advanced applications such as video orchestration, video and sound analytics, road safety systems, traffic management (including UAVs) and wearable technology for the safety of emergency service personnel.

The development of IoT and smart cities will introduce billions of connected objects. Reliable networks will enable these developments to provide new applications, data services and products for public safety, enhancing the safety of citizens and emergency service workers. True collaboration, shared infrastructure and seamless services between different governmental agencies will also become more common.

Until recently, two standards have had a major stake in the public safety market. In North America and other large markets such as Brazil, India and Russia, the leading standard has been APCO P25, whereas in Europe and more than 60 other countries, the leading standard has been TETRA. Additionally, there are several proprietary systems in use.

Although these narrowband technologies support mission-critical voice communications, their main disadvantage is their limited data connectivity. LTE technology can fill this gap.

The main requirements for today's public safety networks are high availability, resilience, guaranteed security and Quality of Service differentiation. Public safety also requires coverage in areas where commercial network coverage is not viable or has been compromised. To fully utilize the benefits of UAVs in public safety work, mobile networks need to be optimized for connected flying vehicles. LTE vehicle to everything communications also plays an important role in enabling unmanned aerial vehicle (UAV) traffic management. All this will require a combination of LTE and 5G development, with MEC playing a key role.

[3] http://ngconnect.org/wp-content/uploads/2016/03/PR1512017052EN_Innovation-2020-Connected_Bus_Shelter_Report.pdf

Use case: Utilities

New energy sources, new regulations, and new market forces are profoundly changing the way electricity is generated, water is distributed and natural gas is managed and consumed. Smart meters for gas, water and electricity are already being rolled out widely in many countries, while more advanced smart grid applications, like advanced metering infrastructure, distribution automation, and/or substation automation will open up new ways to address issues such as emissions regulations, and take advantage of more diverse power generation and new energy storage technology.

Utility companies face tremendous challenges to adapt an often aging infrastructure and workforce to the new environment, while guaranteeing and maintaining the highest level of safety and security for their operations.

To deal with these issues, utilities worldwide are investing more in smart networks that will help them to improve their operational economics, energy efficiency and grid reliability. Global utility spend for smart grid and smart city networking and communications is projected to grow from $5.3 billion in 2016 to $8.4 billion in 2025[4].

Electricity generation and distribution, for example, is no longer purely an engineering problem, but a question of infrastructure built around the incorporation of information and communications technology. The ultimate success of a smart grid depends on the ability of individual devices and systems to interconnect and share information with each other, securely and reliably.

A guide to IoT connectivity technologies

There is a wide range of available connectivity technologies running over licensed and unlicensed spectrum. Each offers its own performance characteristics to serve IoT applications. No single technology will be able to serve all the diverse performance needs of all IoT use cases.

While there is no agreed categorization of the technologies, they fall roughly into two groups according to the signal range directly between the gateway and the endpoint. Low Power Wide Area (LPWA) and 3GPP technologies generally reach further than 500m. Short Range Low Power (SRLP) technologies are those with less than 500m range.

Low power consumption is essential to enable devices to run for ten or more years on a single AA-sized battery. An additional feature is reduced device chip/module cost.

Of course, IoT connectivity depends on more than just the radio access, with the core network and other systems playing vital roles in the overall performance of the application. However, in this paper, we address only the radio access technologies that may be used.

[4] (Source: Navigant Research. https://www.giiresearch.com/report/pike371924-networking-communications-smart-grids-smart-cities.html)

Current proprietary Low Power, Wide Area (LPWA) technologies, such as LoRa, typically operate on unlicensed spectrum, while 3GPP-standardized cellular IoT technologies, such as NB-IoT and LTE-M, operate on licensed spectrum.

	LoRa	GSM (Rel.8)	EC-GSM-IoT (Rel. 13)	LTE (Rel. 8)	eMTC (Rel. 13)	NB-IoT (Rel.13)
LTE user equipment category	N/A	N/A	N/A	Cat.1	Cat.M1	Cat.NB1
Max.Coupling Loss	160 dB	144 dB	164 dB	144 dB	156 dB	164 dB
Spectrum	Unlicensed <1GHz	Licensed GSM bands	Licensed GSM bands	Licensed LTE bands In-band	Licensed LTE bands in-band standalone	Licensed LTE in-band guard-band standalone
Bandwidth	<500KHz	200KHz	200KHz	LTE band carrier bandwidth (1.4-20MHz)	1.08MHz (1.4MHz carrier bandwidth)	180kHz (1.4kHz carrier bandwidth)
Max. data rate*	<50kbps (DL/UL)	<500 kbps (DL/UL)	<140kbps (DL/UL)	<10Mbps(DL) <5Mbps(UL)	<1Mbps (DL/UL)	<170 kbps (DL) <250 kbps (UL)

LPWA IoT and legacy LTE connectivity overview

*Max data rates provided are instantaneous peak

Wide area technologies for licensed bands

Today, GSM modules are the dominant solution for IoT, but the fastest growth will be in new LPWA modules that offer low power, wide area and low cost modules.

GSM and EC-GSM-IoT evolution

EC-GSM-IoT has the best possible coverage among the LPWA networks but also one of the lowest bitrates, therefore it is particularly suitable for those devices transmitting very small packets, such as smart metering where coverage is particularly challenging, such as remote rural areas

GSM is the most widely deployed cellular technology today, covering more than 90 percent of global population. GSM could be a key IoT enabler under the guise of Extended Coverage GSM IoT (EC-GSM-IoT). EC-GSM-IoT is a 3GPP Rel. 13 technology that can pave the way for operators to use their GSM networks for IoT, via a purely software upgrade for easy deployment.

The Nokia EC-GSM- IoT solution relies on repeated transmission of user and control plane data and a new coding scheme which allows an increased coverage by 20dB or roughly seven times, to provide reliable connectivity. The solution also extends the device battery life to up to 10 years through the use of 3GPP features such as Power Saving Mode (PSM) that allows the device to connect to the network, transact and then inactive, and eDRX that allows longer inactivity periods, from milliseconds to tens of minutes.

As well as offering the lowest device cost among 3GPP technologies, IoT over GSM will re-use the existing infrastructure and spectrum (via refarming), thus no additional CAPEX is needed. A GSM IoT network with EC-GSM IoT could use as little as 600 kHz of spectrum.

LTE and its evolution for IoT

The evolution of LTE for IoT meets the needs of applications where low (NB-IoT) to medium (LTE-M) bandwidth is needed. NB-IoT is likely to have lower cost chips, making it particularly suitable for use cases where devices should be as cheap as possible.

LTE has so far supported IoT with so-called Cat.1 devices, while LTE-Advanced extends device battery life to ten years. LTE-Advanced Pro further optimizes coverage, device battery life and costs, as well as capacity for a massive number of connected devices with the introduction of two new technologies:

- LTE-M (LTE-Machine, known also as eMTC enhanced Machine Type Communication) is an evolution of LTE for IoT. Released in Rel.12 in Q4 2014, further optimization was included in Rel.13 with specifications completed in Q1 2016 and commercial availability in 1H 2017.
- NB-IoT (NarrowBand-Internet of Things) is the narrowband evolution of LTE for IoT in 3GPP RAN, included in Rel.13 with specifications completed in Q2 2016 and commercial availability in 1H 2017.

NB-IoT has three deployment options (in band, guard band, stand-alone) and can be deployed on refarmed GSM as well as LTE (TDD and FDD) spectrum. LTE-M can only be deployed in LTE TDD spectrum

LTE-M and NB-IoT are better able to satisfy the connectivity needs of IoT than regular LTE networks. By upgrading existing networks, the technologies provide optimized device battery life, coverage and cost, along with the benefits of licensed spectrum, such as coexistence with other cellular networks. LTE-M and NB-IoT address different use cases, with higher capacity on LTE-M and slightly lower cost and better coverage on NB-IoT.

LTE-M and NB-IoT can operate in spectrum shared with existing LTE or GSM networks. Their deployment depends on an operator's installed base. To benefit from good propagation and penetration characteristics, all solutions should be deployed in sub-1 GHz bands. Some operators may have GSM deployed in the 900MHz band without enough LTE spectrum to deploy LTE-M or NB-IoT within the LTE band. In such cases, EC-GSM-IoT could enable sharing of the carrier capacity in the GSM band. Alternatively, a refarmed GSM carrier would enable deployment of NB-IoT operating in 180 kHz bandwidth.

5G

A 5G solution for cellular IoT is expected to be part of the new standards set by 3GPP in the next few years. Supporting diverse throughput, latency and reliability requirements, 5G will be highly adaptable to efficiently and flexibly address the needs of all use cases across multiple verticals, something not possible with 4G alone.

5G provides more than simple connectivity, it will allow the intelligent control of all machines and enable the automation of everything.

There is nearly complete industry consensus about the technology foundation of 5G resulting in an ambitious and accelerated standardization roadmap. By the end of 2017 the standardization of 5G radio Phase 1 is expected to be complete, ahead of the original timeline.

5G will be a collection of technologies that achieve very high performance targets in terms of capacity, throughput, latency, spectral efficiency and energy efficiency. The biggest difference between 5G and previous generations is the diversity of applications that 5G networks will support.

5G technology will enable operators to provide all stakeholders with solutions tailored to their specific needs. Devices, data and services critical to vertical customers can be allocated the appropriate resources throughout a 5G network to ensure reliability and availability. Network slicing will enable a single physical network to support a vast variety of 5G applications by creating sub-networks from existing resources in radio, core, transport, application servers, edge clouds and central clouds.

5G networks will be able to address the most challenging use cases such as remote surgery, autonomous vehicles, industrial robots, broadcast streaming of multi-view 4K and 8K media, and collaborative virtual reality.

Wide area technologies for unlicensed bands

Technologies operating in unlicensed bands must conform to maximum transmit power requirements defined by the regulator in the region where they are deployed. Additionally, unlicensed spectrum is open for anybody to use. With the help of expert professional services, operators and enterprises can mitigate the risks of interference in the channel.

MulteFire for IoT

MulteFire combines the high performance (enhanced capacity, range, coverage, security, mobility and quality-of-experience) of LTE with the simple deployment of Wi-Fi. Using unlicensed spectrum, it can be deployed by operators, cable companies, Internet Service Providers (ISPs), building owners and enterprises.

MulteFire enables LTE to fairly share unlicensed spectrum with other technologies, such as Wi-Fi. MulteFire is suitable for services where “any deployment” can serve “any device” out-of-box, using unlicensed spectrum like 5 GHz.

Major benefits for mobile operators include access to markets where they don’t have licensed spectrum, co-existence with LTE licensed, simple and rapid deployment using small cells without needing costly licensed spectrum and carrier grade security.

MulteFire provides a cost-effective, predictable network for a large number of IoT sensors, whereas Wi-Fi is not designed to support many IoT connections.

For internet service providers (ISPs) and enterprises, MulteFire offers the chance to own and control their own LTE network to provide wide coverage and improved performance. Enterprises will gain the scalability to serve an ever increasing number of users and IoT devices.

MulteFire offers superior mobility combined with a smooth handover to 3GPP technologies. It also provides end-to-end quality of service and experience and a seamless connection.

LoRaWAN

LoRaWAN™ is an open global specification for secure, carrier-grade IoT LPWA connectivity. Backed by the LoRa Alliance, an open, non-profit association, the standard is supported by a certification program that ensures interoperability.

According to the LoRa Alliance, LoRaWAN™ (long range) is a Low Power Wide Area Network (LPWAN) specification intended for wireless battery operated Things in regional, national or global network[5]. It supports a variety of bandwidths suited to the data requirements of the application as well as the link conditions. The selection of the data rate is a trade-off between communication range and message duration.

LoRaWAN data rates range from 0.3 kbps to 50 kbps[6]. An adaptive data rate (ADR) scheme is used to change the transmit power levels in order to maximize device battery life and overall network capacity.

LoRaWAN is optimized for low power consumption to support large networks with millions of devices. LoRaWAN includes support for redundant operation, geolocation, low cost and low power devices that can run on energy harvesting technologies for mobility and ease of use of IoT.

[5] (source: https://www.lora-alliance.org/What-Is-LoRa/Technology)
[6] (https://www.lora-alliance.org/What-Is-LoRa/Technology)

Short range connectivity

Wi-Fi and Wi-Fi HaLow

Wi-Fi is well positioned to serve IoT connectivity needs whenever a device needs to connect to a cloud service. Wi-Fi is a strong candidate to provide wireless connectivity for IoT devices from domestic appliances and surveillance cameras to small control devices like thermostats.

Beyond this, standardization organizations are developing Wi-Fi features aimed specifically at IoT to simplify connectivity, extend range, operate at low power and provide location information.

Since the first Wi-Fi technical specification was released by the Institute of Electrical and Electronics Engineers (IEEE) in 1997, further features have been developed for ever higher bit rates and throughput. Wi-Fi is commonly perceived as the way to connect wirelessly to the internet in closed locations such as homes and in public hotspots such as hotels.

All Wi-Fi devices use IP for connectivity and that applies also in the IoT domain. An IoT device may use IP and Wi-Fi to connect to a cloud service similarly to smartphones, laptops and internet tablets.

The Wi-Fi standardization organizations like IEEE 802.11 Working Group (WG) and Wi-Fi Alliance are developing features for IoT. The most relevant of these developments include:

- A Wi-Fi variant for sub-1 GHz license-exempt bands for extended range and lower power energy consumption Wi-Fi networks, compared to conventional Wi-Fi networks in the 2.4 GHz and 5 GHz bands. The Wi-Fi Alliance has introduced Wi-Fi HaLow for products incorporating IEEE 802.11ah technology.
- Mechanisms for easy and secure setup of devices and their connectivity are being developed in Wi-Fi Alliance in programs like Device Provisioning Protocol and Wi-Fi Aware. These will facilitate the use of Wi-Fi in IoT devices and extend Wi-Fi's capabilities with an energy-efficient discovery mechanism.
- It's essential to know the location of a device in many IoT cases. The Wi-Fi Alliance is developing a Wi-Fi-enabled location component for an interoperable indoor location solution, while the IEEE 802.11 WG is specifying a variant that enables absolute and relative position to be determined accurately.
- The IEEE 802.11 WG is defining low power wake-up radio as a companion radio for Wi-Fi. The objective is to reduce overall power consumption of a Wi-Fi device significantly while also potentially decreasing downlink delays.

Z-Wave and ZigBee

Z-Wave provides reliable, low-latency transmission of small data packets at up to 100 kbps making it suitable for control and sensor applications. A Z-Wave network can support up to 232 devices, and bridging networks can be used if more devices are required.

ZigBee is a standard for low-cost, low-power, wireless mesh networks to support long battery life devices sued for control and monitoring. ZigBee chips are typically integrated with radios and with microcontrollers that have between 60-256 KB of flash memory.

Z-Wave and ZigBee both use the unlicensed industrial, scientific and medical (ISM) band and are low rate technologies unlike Wi-Fi and other IEEE 802.11-based wireless LAN systems designed primarily for high data rates.

Z-Wave devices can communicate with each another by using intermediate nodes in the mesh network arrangement to route around and household obstacles or radio dead spots that might occur in the multipath environment of a house. Communication range is about 30m, but messages can hop up to four times between nodes providing enough coverage for most residential homes. However, several hops may introduce a delay between the control command and the desired result.

On the other hand, ZigBee devices have low latency. ZigBee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate WPANs. The specification includes four additional key components: network layer, application layer, ZigBee device objects (ZDOs) and manufacturer-defined application objects which allow for customization and favor total integration. ZDOs run various tasks, including tracking device roles, managing requests to join a network, and device discovery and security.

Bluetooth Low Energy (BTLE)

The low power version of classic and well-known Bluetooth, Bluetooth Low Energy (BTLE) is aimed at devices that need to run for long periods on small batteries or energy-harvesting devices. Bluetooth technology is supported by every major operating system to support a broad range of connected devices, from home appliances and security systems to fitness monitors and proximity sensors.

Bluetooth Low Energy (BTLE) is classed as a low data-rate technology for control and telemetry application, but offers a higher throughput, of about 200 kbps, than ZigBee and Z-Wave. Bluetooth Smart technology operates in the same spectrum range (the 2.400 GHz-2.4835 GHz ISM band) as classic Bluetooth technology, but uses a different set of channels.

BTLE is built on a new development framework using Generic Attributes, or GATT. GATT is extremely flexible from a developer's perspective and can be used for just about any scenario. Bluetooth not only connects devices together in an ultra-power efficient way, but also directly connects devices to applications on a smartphone, PC or tablet[7].

Planning and implementing a successful IoT strategy

As we have described, different IoT devices need different connectivity services. Some only need to send a few bytes at long intervals, while others require continuous high bandwidth connectivity with low latency. Operators, therefore, need to define a strategy that describes in which segments they want to compete and which will then guide them on how to tailor services for these segments and what technologies to deploy.

Frequency licenses are a key operator asset. If the operator has available FD-LTE capacity in sub-GHz frequencies, implementing NB-IoT functionality is a natural choice. If TDD-LTE capacity is available, then both NB-IoT and LTE-M are feasible. If GSM is available, EC-GSM IoT can be deployed and if 3G is available, spectrum can be refarmed to support NB-IoT.

If no sub-GHz capacity is available, then LoRa is the choice to enter the LPWA market.

Even when an operator has sub-GHz frequencies available, it may be feasible to implement LoRa (in addition to NB-IoT).

Correct pricing and price differentiation are essential. As the LPWA IoT market expands, lower prices for connecting devices to the internet will support the emergence of new applications with new types of sensor.

For operators, IoT connectivity is a clear differentiator against companies like Amazon, IBM and Microsoft which all compete in the IoT arena, but offer no IoT connectivity.

As well as connectivity, operators can offer additional services such as devices and device management, as well as applications and services related to those devices. There are a huge number of different applications, so operators need to select which applications to provide. This is important because applications could potentially generate the biggest share of all IoT-related operator revenues.

[7] (Source: https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works)

Planning of IoT use cases in LPWA

Working with other involved parties, operators can have an important influence on the building of the IoT use case. To explore how, consider the various aspects of smart metering supported by an LPWA network.

Network connectivity and range: The location of smart meters are usually known and do not require communications network mobility. Network design need only be based on the required data rate, the type of device and surrounding infrastructure. Nevertheless, network design for IoT is never a trivial task and a poor design will inevitably lead to dissatisfied customers.

Battery life and power consumption: Battery life depends on the size of the battery and the number of IoT messages sent. As battery size is limited by the physical size of the IoT device, extending battery life means reducing the number of messages and IoT device design.

All LPWA technologies allow the IoT-device to become idle, but when moving from idle to transmit, power consumption in IoT use cases can vary. In smart metering, wake up is mostly governed by a changed meter reading. Other IoT use cases might need multiple ways to wake up the device, resulting in the device's idle mode consuming more power.

Reducing the number of transmissions is also important. For example, a smart meter could be set to take readings every 15 minutes, then collect the data of multiple readings and send all the data in one transmit message. If a transmission is set to every two hours then messages are reduced eight-fold compared to when a message is sent for every reading.

Network design is also influenced by how readings are collected. When smart meters are located close to base stations or gateways, they benefit from faster data rates which reduce the time taken to transmit data. This means the payload of each message can be increased, leading to lower power consumption.

Data rate and traffic: The data rate achieved depends on network design and smart meter design. Extending the battery life by collecting data readings and sending them less frequently will reduce uplink traffic but may increase the downlink traffic. When a collection of readings is sent the network may need to send confirmation back to the device by sending a downlink message. This confirmation message allows the smart meter to free up space for future readings. Yet if no confirmation is received, the smart meter would need to resend the data.

This situation could be avoided if, with the customer's approval, missing readings are interpolated from previous and subsequent readings.

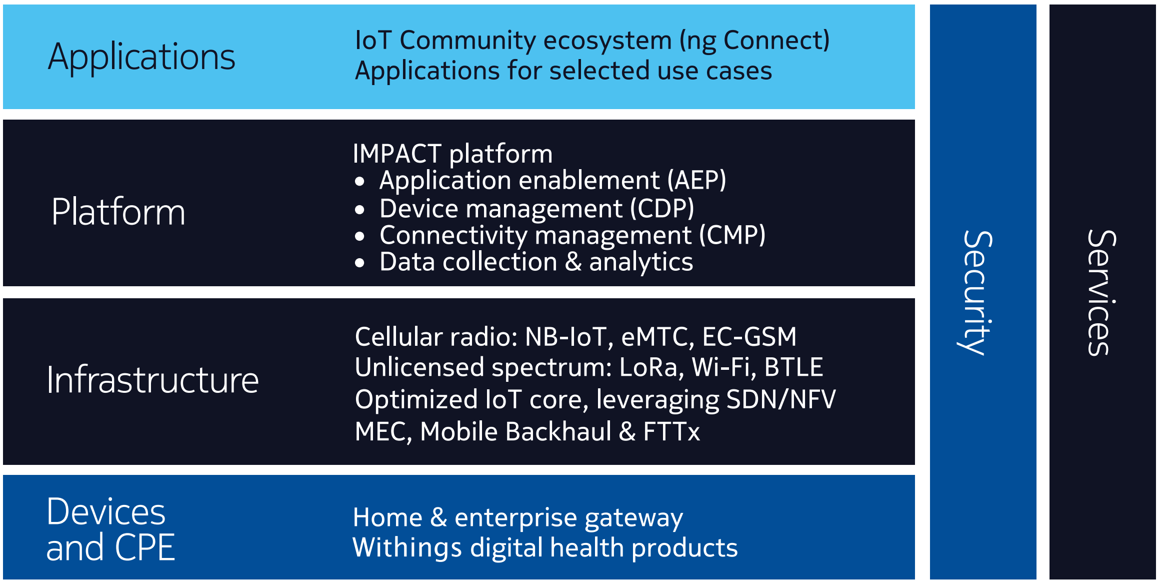
Reliability: Smart metering use cases will vary, affecting reliability requirements. For example, a water meter measuring consumption by a household may tolerate longer intervals between submitted meter readings than a water meter monitoring a mains supply. A household's water bill will not be affected significantly by using interpolation of missing readings. However, a utility company would require fast detection of leaks, requiring greater reliability in the network. An IoT network can be designed to cost-effectively fulfil both customer needs.

Latency: Smart metering messages mainly use the uplink, where latency is not an issue with any technology. A wider scope for smart metering would be to include the control of water or gas valves, or electricity switches, in which case latency would play a more important role.

Mobility: Typically, mobility has no role in most smart metering use cases. However, technology evolves and it is not inconceivable that the future could bring new demands. For example, a robot moving inside a water pipe and measuring water quality using multiple sensors or measuring pressure to monitor water flow would need mobility to be considered during IoT network design.

The Nokia approach to IoT operator business

As an end-to-end IoT solution provider, Nokia takes a horizontal management approach to the various vertical markets as shown in figure 3.



Applications

IoT Community ecosystem (ng Connect)
Applications for selected use cases

Platform

IMPACT platform

- Application enablement (AEP)
- Device management (CDP)
- Connectivity management (CMP)
- Data collection & analytics

Infrastructure

Cellular radio: NB-IoT, eMTC, EC-GSM
Unlicensed spectrum: LoRa, Wi-Fi, BTLE
Optimized IoT core, leveraging SDN/NFV
MEC, Mobile Backhaul & FTTx

Devices and CPE

Home & enterprise gateway
Withings digital health products

Security

Services

Figure 3: Nokia's approach to the IoT market

The bottom layer contains customer premises equipment and devices.

Above this sits the infrastructure level, which includes a wide range of radio access technologies, the optimized core network to deal with the specific requirements of IoT traffic, and the Multi-Access Edge Computing capability to meet the low latency requirements of some use cases.

The platform layer comprises the Nokia IMPACT (Intelligent Management Platform for All Connected Things) platform which provides operators, enterprises and governments with a standards-based platform for securely managing any device, protocol or application.

In the applications layer, Nokia offers a two-sided approach. On one hand is the IoT Community ecosystem, which has more than 70 partners and is growing, while at the same time is the development of use cases for selected vertical markets.

Security and services are applied to all these horizontal layers. With the growing volume of IoT devices and applications, security is essential for operators, enterprises and users. The Nokia NetGuard portfolio monitors IoT devices, detects malware, draws correlations between events in different parts of the network, and sets security parameters to minimize the chance of successful attacks.

Nokia Services experts design, plan, integrate and manage the device, connectivity, platform and application layers to meet the needs of different vertical markets. Nokia IoT Readiness Services help operators to assess the network's ability to support IoT models, identify gaps and provide a transformation roadmap to a high-performance IoT-optimized network.

Nokia Services experts help evaluate and choose the right access technology across 3GPP and unlicensed bands for specific use cases, taking into account techno-commercial constraints while making the most efficient use of network resources. Multivendor systems integration expertise ensures interoperability between different layers for applications, platforms, connectivity and sensors.

The Nokia worldwide IoT network grid ('WING') as a managed service simplifies global IoT connectivity by spanning technologies and borders. This gives enterprises in the health, safety, transport and utilities markets access to a global IoT connectivity grid with subscription and device management, security and analytics all included. Our services approach opens up new business opportunities, accelerates time to market, optimizes cost of ownership and enables new global revenue streams from IoT for operators.

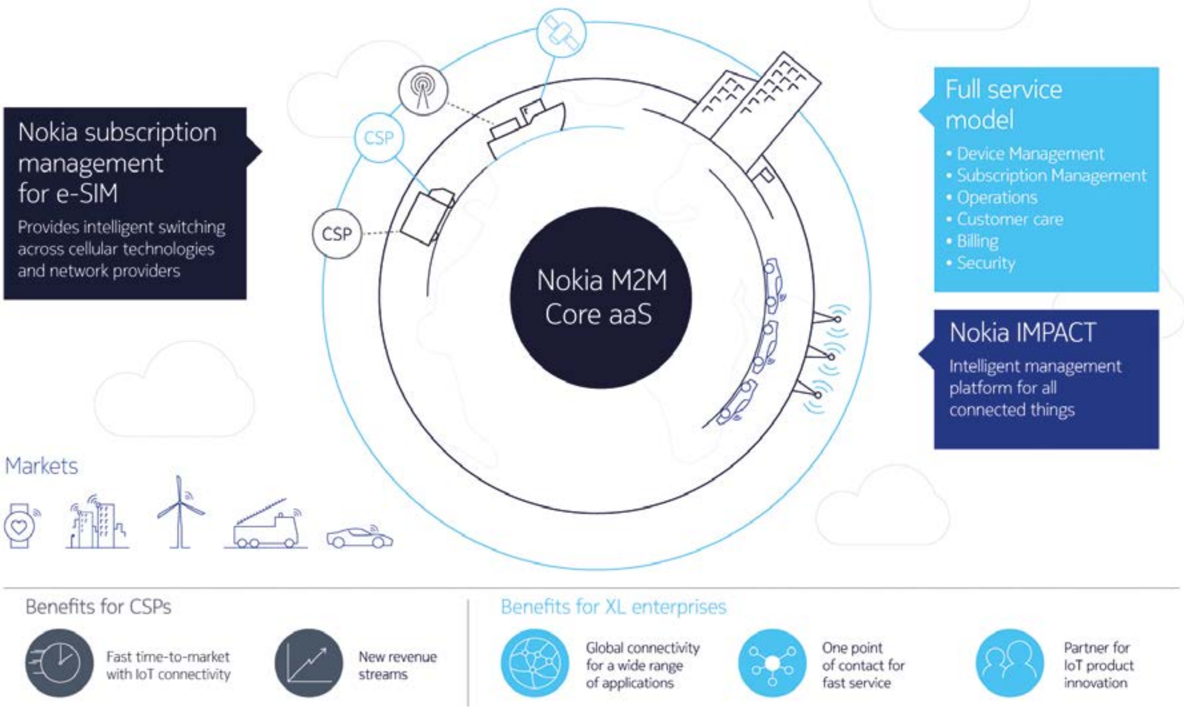

Nokia subscription management for e-SIM
Provides intelligent switching across cellular technologies and network providers
CSP
CSP
Nokia M2M Core aaS
Full service model
• Device Management
• Subscription Management
• Operations
• Customer care
• Billing
• Security
Nokia IMPACT
Intelligent management platform for all connected things
Markets
Benefits for CSPs
Fast time-to-market with IoT connectivity
New revenue streams
Benefits for XL enterprises
Global connectivity for a wide range of applications
One point of contact for fast service
Partner for IoT product innovation

Figure 4: Nokia WING is a global IoT connectivity managed service that meets the needs of operators and enterprises

Conclusion: Many use cases, many requirements

Without doubt, IoT presents a wide and complex panorama of opportunities for operators. At the same time, there is a wide choice of approaches and technologies that operators could adopt to address the market.

While there are many radio technologies to choose from, it’s important to consider that this is only a piece the whole IoT network design process where other factors, beyond the application requirements, are the network topology, the business model and the total cost of ownership.

With this in mind, Nokia advises its customers to first establish a process for setting the strategy to achieve their vision for IoT business. This needs to include a structured assessment of current processes and legacy assets and how these may affect network design, capacity management, change management, network and service operations.

This structured approach needs to be technology independent, but it will drive requirements for new technology and services. For example, should an IoT solution be run completely in the operator’s cloud environment, or could some parts of the network be outsourced as-a-service to a supplier’s cloud?

The process of creating IoT business success has many different phases and few operators will have all the expertise and experience in-house that will be needed. Nokia has an end-to-end service capability in IoT, which includes connectivity, platforms, applications and devices over a wide span of market segments. We believe we are well-positioned to provide expert support to help operators build their business case and plan, implement and run a successful, tailored IoT strategy.

Find out more about the Nokia IoT portfolio at: https://networks.nokia.com/innovation/iot

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code SR1701006127EN