Cellular Technologies Enabling the Internet of Things

November 2015

TABLE OF CONTENTS

This white paper presents the key considerations for developing an end-to-end Cellular Internet of Things (CIoT) solution. The IoT is a network of physical objects, machines, people and other devices to enable connectivity and communications to exchange data for intelligent applications and services to be developed. The devices consist of smartphones, tablets, consumer electronics, vehicles, motors and sensors capable of IoT communications. Numerous market analyses and predictions indicate that the field of IoT is expected to bring a revolution of tremendous growth opportunities with millions of new end-point and gateway (GW) devices, innovative network infrastructures and new sets of enablement protocols/technologies and exciting applications.

Wireless cellular technologies have found firm ground and enormous potential as key enablers for IoT today due to its ubiquitous connectivity. The continuous and ever increasing technology enhancements and innovations in cellular technologies are promising to be the major foundational access methodologies to enable a myriad of IoT applications.

The main challenges that affect cellular technologies are the requirements to be secure, flexible, low powered and easy to provision, manage and scale while delivering robustness and acceptable latencies in performance. LTE-Advanced technology and its evolving new enhancements is the key growth engine of 4G cellular connectivity which provides requisite features to support a range of high and low performance and cost-optimized IoT applications.

However, CIoT industry experts and analysts are essentially confronted with several questions: What are the key market drivers for IoT? What are market sizes for specific vertical applications? How can IoT be leveraged to the identified use cases? What is an effective IoT strategy for an enterprise? What is the best end-to-end architecture for an IoT solution? What technologies are to be considered for a given domain when designing an IoT system? How can an IoT solution be monetized? What are the defining standards for IoT deployment?

This paper examines the essential aspects that encompass the development of IoT uses cases specifically enabled by cellular technologies which includes IoT market drivers and the end-to-end technical framework for cellular IoT/Machine Type Communication (MTC) use cases. This paper also provides details on emerging LTE technology enhancements that enable IoT along with an overview of new MTC features with a focus on Category 0,1 and M devices. Additionally, this paper reviews innovations in low cost design and power management, and discuses the evolution of LTE MTC for 5G radio access.

An overview of various IoT vertical applications with an emphasis on cellular connectivity and a description of an IoT system with end-to-end functional architecture inclusive of the following protocol details are provided in this paper, including:

- Device Management Protocols for managing end-point devices and IoT gateways such as Open Mobile Alliance-Device Management (OMA-DM), Technical Report 069 (TR-069) and Light-Weight Machine-To-Machine (LWM2M)

- Application level data transport protocols such as http, webSockets, Constrained Application Protocol (CoAP), IP6 Low Power Wireless Personal Area Network (6LoWPAN), Message Queuing Telemetry Transport (MQTT) and Extensible Messaging and Presence Protocol (XMPP)-IoT extensions

- Link encryption protocols such as Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

This paper further details the following enablement solutions for monetization of IoT solutions:

- Discovery of data, services and applications via web search engines

- Interplay of particular IoT solution with social networks

- Policy driven IoT communication

Lastly, the paper highlights key IoT standardization development efforts by 3GPP, oneM2M, Open Mobile Alliance (OMA), GSM Association (GSMA), as well as a summary of various emerging technologies for use within context of IoT.

1 INTRODUCTION

The Internet of Things (IoT) is a network of physical objects, machines, people and other devices that enable connectivity and communications to exchange data for intelligent applications and services to be developed. These devices consist of smartphones, tablets, consumer electronics, vehicles, motors and sensors that are all capable of IoT communications. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for direct integration between the physical and digital worlds resulting in improved efficiency, accuracy and economic benefits. There is an all-round understanding and expectation that IoT communications will present tremendous opportunities for creating new devices and applications in the next decade.

IoT communications will undergo unprecedented growth in the next five years; it is predicted that over 50 billion IoT devices are expected to be connected with as much as US$8.9 trillion in annual revenue by the year 2020.[1] With increased pervasiveness of mobile broadband, cellular connectivity is becoming even more valuable as an important access methodology for IoT. A significant part of IoT communications are planned over cellular networks. According to GSMA studies and forecasts, cellular IoT communications are predicted to account for over 10 percent of the global market by 2020. Cellular technologies are already being used for IoT today in several use cases and are expected to be used even more in the future as these use cases have a need for ubiquitous mobility, resilient networks, robust security, economic scale and/or communications independent of third party access (using customer DSL, fixed lines, etc.).

The challenge for the cellular industry now is to unlock the value of this interconnected web of devices in a manner that is secured, flexible, low power and easy to provision, manage and scale while delivering robustness and acceptable latencies in performance. The goal is to identify a framework of promising solutions and cover a set of innovative approaches and technologies as building blocks to meet these challenges.

LTE-Advanced technology, the chief vehicle of 4G cellular connectivity, started to and will continue evolving to provide new features that support a range of high and low performance and cost-optimized IoT device categories. Such devices also support extended coverage for challenging locations, low energy consumption for applications requiring long battery life and optimizations to support very large numbers of devices per cell.

---

[1] *Internet of Things (IoT) 2013 to 2020 Market Analysis: Billions of Things, Trillions of Dollars*, IDC, October 2013.

There are new emerging IoT service variants in cellular technologies with new requirements such as systems requiring very high link reliability for critical control, low latency for real time operation and timely delivery of critical messages. Entirely new MTC radio access designs have begun to emerge, both as part of 5G system concepts as well as within 3GPP GSM/EDGE Radio Access Network (GERAN).

In addition, complementary middleware ecosystems such as the Open Interconnect Consortium (OIC), AllSeen Alliance and oneM2M are emerging and designed to drive discovery, provisioning and routing techniques for IoT devices.

This paper presents the various aspects of cellular technology and provides an overview of the new solutions to address the future requirements for the IoT use cases. Following are the key points in this paper:

- Cellular connectivity is an important access methodology to support and enable communications over large scale IoT devices.

- Cellular technology, in combination with local connectivity technologies such as WiFi or Bluetooth, is expected to address a variety of IoT use cases providing ubiquitous mobility, resilient connectivity and economic scale.

- Cellular technology solutions can best address some requirements of emerging IoT use cases.

- A framework of solutions, approaches and technologies are building blocks to help meet the challenge of unlocking the value of an interconnected web of devices in a secured manner with minimum power consumption, making it easy to provision and manage capabilities while delivering robustness and acceptable latencies in performance.

- Current and planned MTC features are defined in LTE-Advanced through 3GPP Releases 11, 12 and 13. These new features include extended coverage for challenging locations, low energy consumption for applications requiring long battery life and optimizations to support very large numbers of devices per cell.

- The latest LTE-Advanced features support a range of high and low performance and cost-optimized MTC device categories in the context of MTC use cases spanning emerging vertical markets that include:

  - Automotive
  - Fleet management
  - Wearables
  - Healthcare
  - Smart cities

Never has there been a scientific endeavor that approaches the scale and challenge of a future where physical objects, machines, people and devices can connect and share data. The connected future presents a tremendous challenge to the engineers and research scientists who are developing the technology standards to enable an advanced and seamlessly connected society.

2 IOT MARKET DRIVERS

A majority of industry participants recognize that M2M, and now IoT, represents one of the key growth opportunities for telecommunication service providers and enterprises of various sizes in the next decade. The main questions asked by industry participants in the early stages of considering to enter the field of M2M and IoT are the following: What are the key market drivers for IoT? What are market sizes for specific verticals applications?

2.1 EVOLUTION FROM M2M TO IOT

The Internet of Things (IoT), as a natural evolution of Machine-to-Machine (M2M) technology, is the interconnection of intelligent devices and management platforms that collectively enable the "smart world" around us. From wellness and health monitoring to smart utility meters, integrated logistics, and self-driving drones, our world is fast becoming a hyper-automated one. A multi-dimensional view on the evolution from M2M to IoT is provided in Figure 2.1.

Internet of Things

Uses any connected device
- M2M is phase 1 of IoT
- Billions of connections
- Adding B2C, B2B2C
- Horizontal/consumer devices
- Open/standardized
- Big Data critical to uncover new insights across use cases
- New business models; VAS and bundling based; regulation/EU driven

Smart environment

Is maturing
- Millions of cellular connections today
- Driven by regulation
- B2B and emerging B2C
- Vertical use cases
- Standards definition

M2M

Has reached a level of maturity
- Growth ~20% CAGR in connections
- Focus on B2B
- Vertical use cases
- Complex/proprietary
- Limited Big Data applications
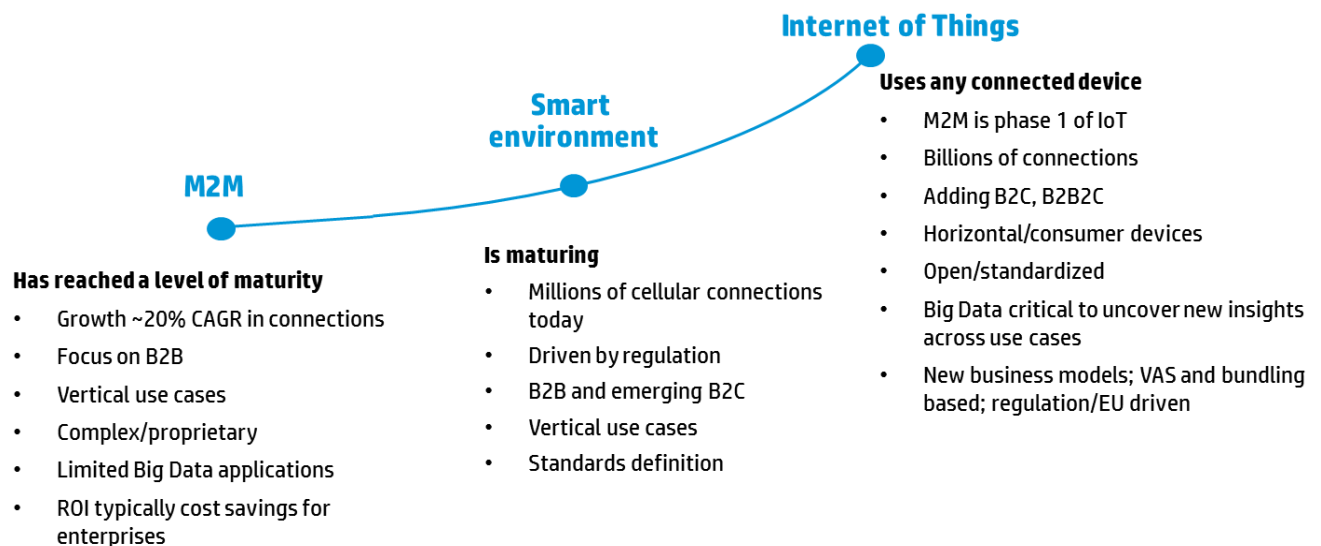- ROI typically cost savings for enterprises

Figure 2.1. M2M to IoT evolution.[2]

---

[2] *M2M insights for mobile operators*, Analysis Mason, March 2013.

The evolution from M2M to IoT was a staged process and had been driven by the shift from a device-centric to process-centric approach as shown in Figure 2.2.
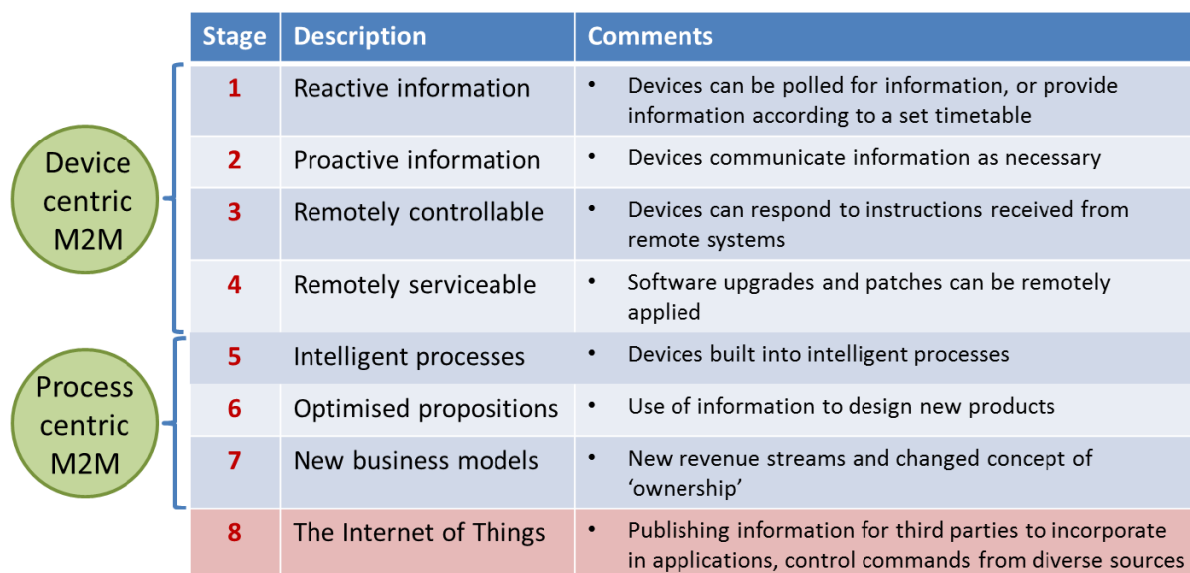
Stage	Description	Comments
1	Reactive information	• Devices can be polled for information, or provide information according to a set timetable
2	Proactive information	• Devices communicate information as necessary
3	Remotely controllable	• Devices can respond to instructions received from remote systems
4	Remotely serviceable	• Software upgrades and patches can be remotely applied
5	Intelligent processes	• Devices built into intelligent processes
6	Optimised propositions	• Use of information to design new products
7	New business models	• New revenue streams and changed concept of 'ownership'
8	The Internet of Things	• Publishing information for third parties to incorporate in applications, control commands from diverse sources

Device centric M2M — Stages 1–4

Process centric M2M — Stages 5–7

Figure 2.2. Hierarchy of evolution from M2M to IoT.[3]

Note: Going forward for the purpose of this white paper, the term IoT will primarily be used to cover both M2M and IoT, if not specifically noted otherwise.

2.2   KEY IOT MARKET DRIVERS

Some of the key IoT marker drivers for communication service providers and larger enterprises are related to a generation of new revenue stream, tremendous volumes of devices to be deployed, indication of an increase of Average Revenue Per User (ARPU) for some IoT vertical applications and a drastic increase of operational efficiencies required for operation of IoT solutions. From a business perspective, the adoption of IoT is driven by factors such as:

- Optimization of utilization of physical and financial assets

- Differentiation of products and services

- Transformation of customer engagement

---

[3] *Big Data in M2M: Tipping Points and Subnet of Things*, Machina Research. 2013.

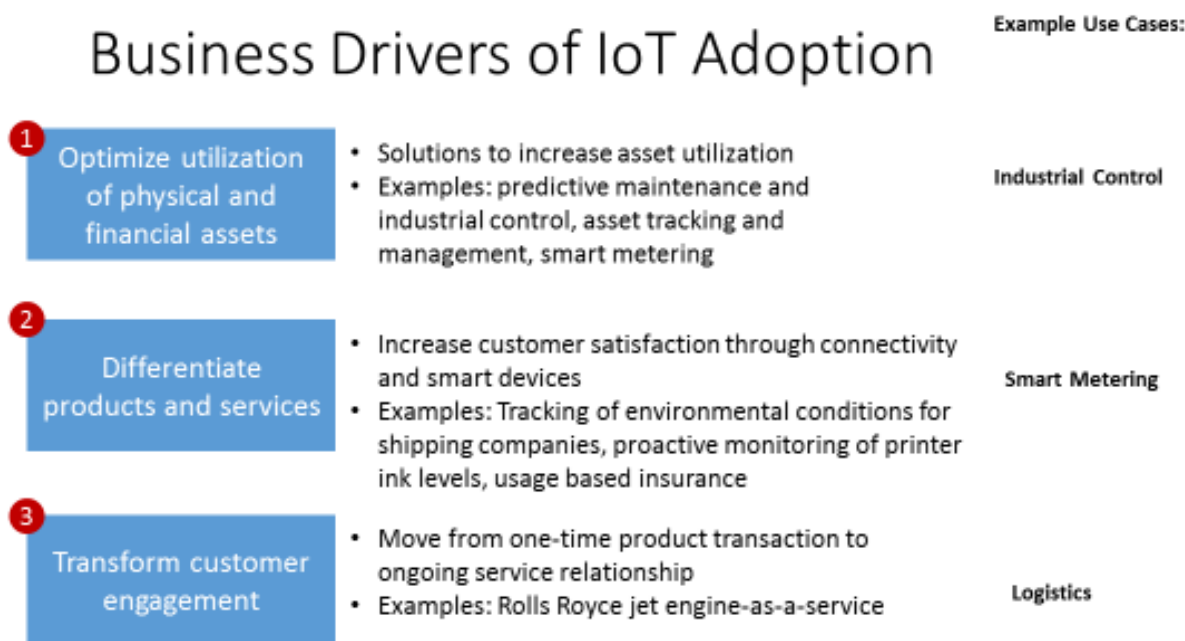Figure 2.3 summarizes the business drivers for IoT adoption as previously described.

Figure 2.3. Business Drivers of IoT Adoption. [4]

Aside from the set of business drivers for adoption of IoT, most technology enablers are now prepared to help accelerate the deployment of IoT solutions. Lower hardware costs and wireless data networks are enabling more intelligence and seamless connectivity. The market today is in a position to handle or process tremendous amounts of information that connected devices generate. [5] The availability of big data analytics tools, combined with a growing understanding of how collective data can be used, provides an opportunity to add greater efficiency to M2M and IoT applications. End users also present the IoT driver themselves. Namely, as consumers and businesses have access to, and are used to living and working with smartphones and tablets, they are eager to adopt new applications that enrich the way they live, work, commute or shop.

Various IoT industry initiatives to standardize architecture, ensure security and enable operability will accelerate the adoption of IoT and will help the IoT market evolve at an accelerated pace.

2.3   IOT MARKET SIZING AND FORECAST

As stated in the introduction of this paper, IoT communications are set for aggressive growth for the foreseeable future. With increased pervasiveness of mobile broadband, cellular connectivity is becoming even more valuable as an important access methodology for IoT. Although fixed and short range will be a significant part of IoT communications, cellular technology is forecasted to grow as the technology of choice for IoT applications as well. Figure 2.4 illustrates the forecast breakdown for various wireless technologies for use within IoT over the next decade.

---

[4] HP.
[5] "The Interoperability Enabler for the Entire M2M and IoT Ecosystem", oneM2M, January 2015.
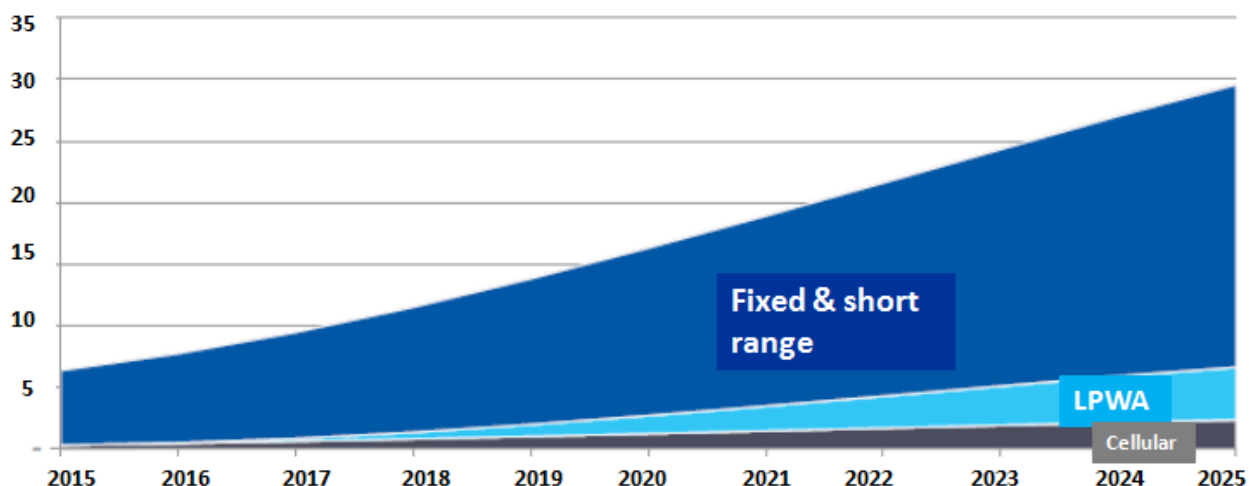
Figure 2.4. Billion global connections, 2015-2025. [6]

GSMA's recently published Global Mobile Economy report provides a view of the growth of cellular IoT connections until 2020; see Figure 2.5.

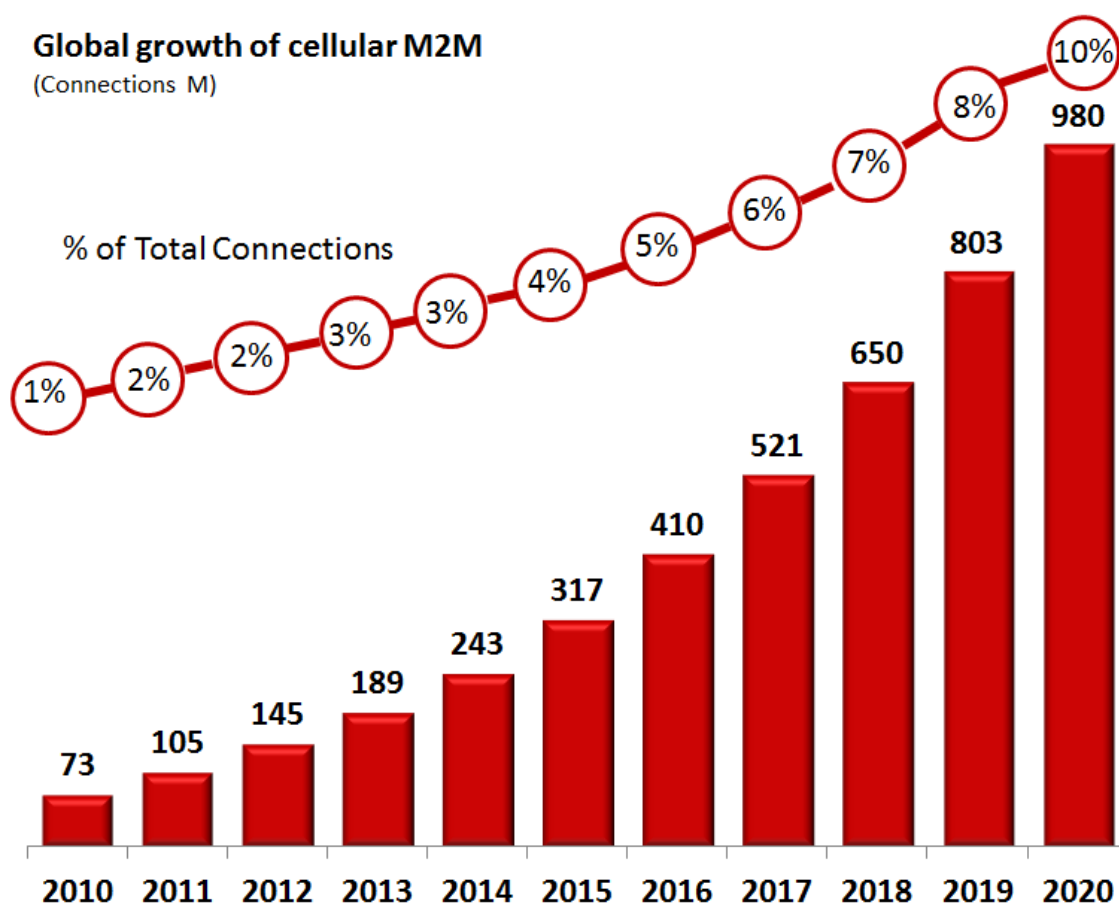**Global growth of cellular M2M**
(Connections M)

% of Total Connections

Figure 2.5. Conservatively projected growth on cellular (3GPP and 3GPP2 based) IoT connections until 2020.

---

[6] *Billion Global Connections*, Machina Research, May 2015.

These forecasts are based on known and tangible deployments, opportunities and barriers for each operator and the IoT/M2M sector. They may well prove conservative if both industry players and governments successfully enable a number of growth factors. This could lead to growth rates similar in the future to those witnessed over the past few years, resulting in uplift over the current trajectory forecasts of up to 50 percent. Such growth factors include low power network roll-out, increased standardization, improved regulation and greater assurance of end-to-end security. A further requirement is the development of new operator business models in the IoT/M2M space, particularly those that move beyond simply providing the mobile connectivity. The speed and sophistication achieved in each industry may vary due to specific needs of different segments, the availability of connectivity and other supporting technologies, and economic and regulatory environments in the local market.

Capitalizing on the opportunities, many innovators are swiftly adopting IoT technology in their respective industries as the new generation of devices is becoming more useful, affordable and easy to integrate. Additionally, national regulators in many industries are mandating IoT adoption as a technology enabler in achieving national socio-economic objectives.

Rapidly growing IoT adoption in different industries presents significant market opportunities for communications service providers. IoT connectivity revenue is expected to increase from US$6 billion in 2011 to more than US$50 billion by 2021, and at the same time, connectivity ARPU is expected to witness massive decline during the same period due to the emergence of low cost access alternatives such as Low-Power Wide-Area Network (LPWA) for some new IoT use cases (see Figure 2.6 for more details). These changing market dynamics will put more pressure on margins.
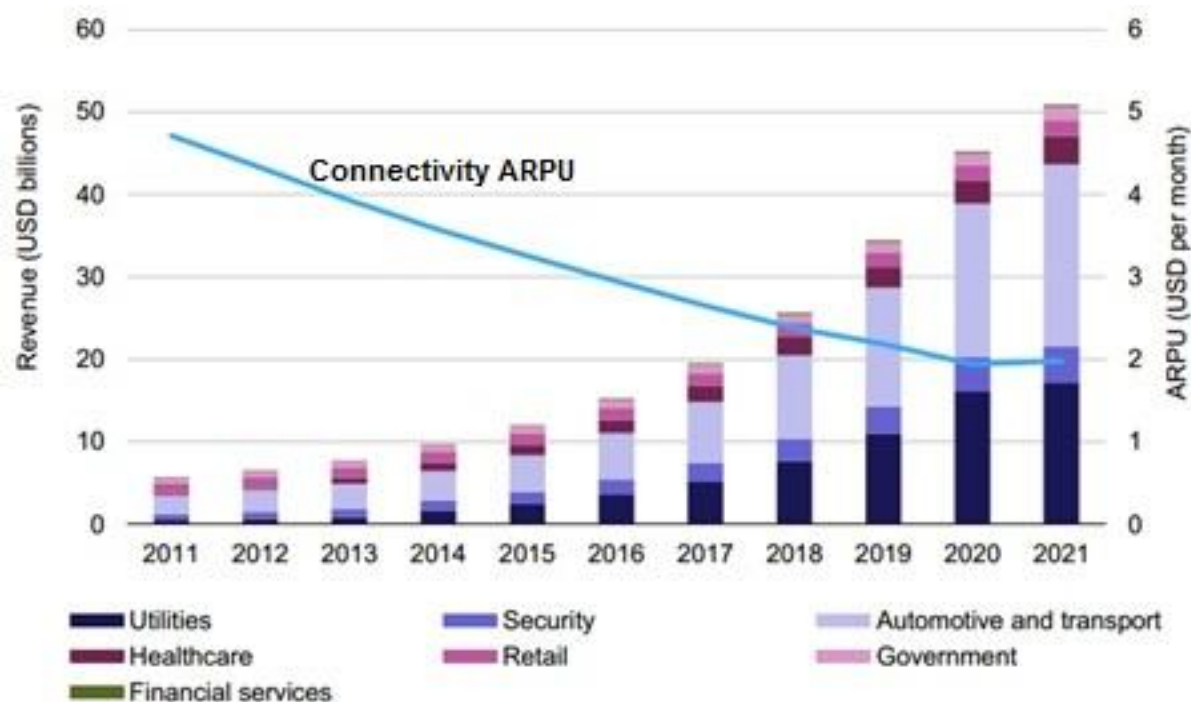
Figure 2.6. IoT connectivity revenue by industry sector and total connectivity ARPU, worldwide, 2011–2021. [7]

The evolutionary trajectory from limited-capability IoT services to the super-capable IoT ecosystem has opened up new dimensions and opportunities for traditional communications infrastructure providers and industry-specific innovators. Those that exploit the potential of this technology to introduce new services

---

[7] Analysis Mason, 2013.

and business models can deliver unprecedented levels of experience for existing services and, in many cases, transform their internal operations to match the needs of a hyper-connected world.

With the need to establish a model of "everything connected" no longer in doubt, the only question that needs to be addressed concerns the different patterns of distribution, timing, geography and areas of adoption. Utilities, security and transport are expected to witness maximum growth in IoT applications in the coming years.

For a detailed guideline on forming an effective IoT strategy applicable to communication services providers and enterprises using cellular connectives, see Appendix A.

2.4   EXAMPLE OF IOT MARKET FOR THE U.S.

The fact that IoT connections represented only 2.8 percent of all global mobile connections, or 189 million[8], indicates that the sector is still at a relatively early stage in its development. In the longer term, IoT will have a fundamental impact on the way we live and work, reducing waste and inefficiencies and delivering major social and environmental benefits in security, healthcare, transportation and logistics, education and energy, among many other sectors of the economy.

The U.S. is one of the largest and most advanced IoT markets in the world and it accounts for 10 percent of all mobile connections in the U.S. There were approximately 35 million IoT connections in the U.S. at the end of 2013, second only to China (50 million).[9] Growth for the second part of the decade is expected to be driven by the automotive and connected home sectors. IoT solutions and services are widely used in many different sectors of the U.S. economy. Utilities, automotive makers, logistics companies and the energy sector are all major users of IoT.

Although the U.S. has an advanced IoT market, it is still premature in terms of standardization and interoperability. In some sectors, there is considerable technology fragmentation which limits economies of scale and the rate of growth for cellular IoT connections. Moreover, IoT solutions and services face significant barriers for parts of the U.S. economy. For example, the use of IoT in healthcare has been held back by technology fragmentation and a lack of regulatory clarity. Potential service providers face concerns about the privacy and security of patient data, reimbursement and liability and the reliability of connectivity.

To fulfill its potential, the IoT market in the U.S. will need to overcome a number of significant challenges. Here is an overview of the key obstacles identified by the analysts and industry participants interviewed for this report:

- **Market fragmentation and complexity:** In some sectors, such as healthcare, automotive and smart homes, there is a wide range of proprietary solutions in use, which can make interoperability difficult to achieve. A lack of standards encourages the creation of applications that are highly customer-specific to a vertical sector, often involving labor-intensive development by highly specialized integrators and developers with deep vertical knowledge. A scarcity of these developers and the high cost of using them impedes the market.

- **A lack of regulatory clarity:** In some sectors, such as healthcare, there is a need for greater clarity around liability. Regulators need to find the right balance between safeguarding patient

---

[8] GSMA Intelligence.
[9] *Ibid.*

safety and encouraging innovation that could improve the effectiveness of healthcare.

- **Net neutrality and managed connectivity regulations:** There is an ongoing debate in the U.S. about the extent to which communication service providers should be allowed to manage traffic on their networks. Mobile operators will need the flexibility to efficiently manage the rising number of devices on their networks, while also being able to manage traffic in accordance with specific IoT service requirements. For example, connected medical devices will have very different traffic management requirements to a supply chain solution. Stringent net neutrality rules may limit the use of IoT solutions for "mission- critical" applications, such as the monitoring of heart conditions.

- **More partnerships between the public and private sectors:** There is relatively little co-operation between the private and public sectors in many parts of the economy.

- **Specialist M2M modules:** There may be a need for more specialist IoT modules designed for specific vertical sectors.

- **Cost of LTE modules:** There are various ways to make LTE less expensive and price comparable to 2G (GSM) and 3G (HSPA) modules, including LTE-only modules and MTC. In addition, the cost of certifying modules on operators' networks also needs to fall to allow the market to develop.

- **Network migration:** Many of the IoT solutions already deployed in the U.S. will need to migrate to use 3G or 4G networks as 2G networks become obsolete. However, some operators plan to maintain their 2G networks for the foreseeable future.

- **Need for new business models:** In some sectors, such as automotive and healthcare, analysts say the existing business models for IoT solutions are immature and need strengthening.

Despite the challenges identified above, the U.S. IoT market will continue to see strong growth. Here are some of the key growth drivers they identified:

- **Consumer demand:** As they become accustomed to digital commerce, consumers expect companies to offer personalized, real-time services. Increasingly, communication service providers are taking professional service roles to help enterprise customers use IoT to provide new services to consumers in a Business-to-Business-to-Consumer (B2B2C) model. The communication service provider's role is to enable the enterprise to change its business model so it can become a service provider in its own right.

- **Semi-autonomous vehicles:** The U.S. automotive and software industries are in the vanguard of efforts to develop vehicles that are less reliant on a human driver. In February 2014, the U.S. Department of Transportation's National Highway Traffic Safety Administration announced that it will begin taking steps to enable vehicle-to-vehicle communication technology for light vehicles.

- **Health and wellness:** There is growing interest in the use of wearable devices such as wristbands to monitor activity levels and other health-related attributes.

- **International expansion:** U.S. based companies expanding abroad are likely to call on U.S. based operators to expand their IoT solutions to other markets. In some cases, the U.S. communication service providers may set up new operations to address this demand.

- **New operating models:** As the benefits of IoT solutions become clearer, companies across the economy will increasingly adapt their operating models to be able to incorporate IoT technology quickly and efficiently.

3 INDUSTRY VERTICALS AND IOT USE CASES

Given the requirements for connectivity, many naturally see IoT in the domain of the Communication Service Providers (CSPs), such as the Mobile Network Operators (MNOs), although connectivity is a readily available commodity and therefore, low value. In addition, some IoT use cases are introducing different requirements on connectivity, both economically (lower ARPU) and technically (low power consumption, limited traffic, mobility or bandwidth), which means that a new type of connectivity option is possible to maximize efficiency and Return of Investment (ROI) of such use cases; for example, Sigfox or LoRA. However, the value creation is less on connecting devices and having them available, but rather on collecting their data, validating it, possibly enriching it with analytics, mixing it with other sources, and finally, exposing it to the applications that enable enterprises to derive business value from these services.

Many use cases/vertical applications will be successful and benefit from cellular 3GPP technology connectivity. This section of the paper explores a variety of IoT use cases/application requirements and the selection of the appropriate technology to impact business metrics such as Quality of Service (QoS)/cost efficiency and other metrics.

One classification of an IoT use case comes from oneM2M. In Table 3.1, marked in red are use cases within a particular IoT domain/vertical for which cellular connectivity is the most appropriate and applicable underlying technology of choice for success.

Table 3.1. oneM2M use cases.[10]

Note: Marked in red are subsets of use cases that are suitable for deployment via cellular networks.

Industry Segment	oneM2M Use Cases				
Agriculture	Smart Irrigation System				
Energy	Wide area Energy related measurement /control system for advanced transmission and distribution automation	Analytics for oneM2M	Smart Meter Reading	Environmental Monitoring for Hydro-Power Generation using Satellite M2M	Oil and Gas Pipeline Cellular /Satellite Gateway
Enterprise	Smart Building				

---

[10] http://www.onem2m.org/component/rsfiles/download-file/files?path=Draft_TR%255CTR-0001-Use_Cases_Collection-V1_6_0.ZIP&Itemid=238.

Industry Segment	oneM2M Use Cases				
Finance					
Healthcare	M2M Healthcare Gateway	Wellness services		Secure remote patient care and monitoring	
Industrial	On-demand data collection for factories				
Public Services	Street Light Automation	Devices, Virtual devices and Things	Car/Bicycle Sharing Services	Smart parking	Information Delivery service in the devastated area	Holistic Service Provider
Residential	Home Energy Management	Home Energy Management System	Plug-In Electrical Charging Vehicles and power feed in home scenario		Real-time Audio/Video Communication	
Residential	Event Triggered Task Execution	Semantic Home Control	Semantic Device Plug and Play		Triggering in the field domain	
Retail	Vending Machines				
Transportation	Vehicle Diagnostic & Maintenance Report	Remote Maintenance services	Traffic Accident Information collection		Fleet management service using Digital Tachograph	
Transportation	Electronic Toll Collection Services	Taxi adverts	Vehicle Data Services	Smart Automatic Driving		
Other	Extending the M2M Access Network using Satellites	M2M data traffic management by underlying network operator	Optimizing connectivity management parameters with mobile networks	Optimizing mobility management parameters with mobile networks	Leveraging Broadcasting / Multicasting Capability of Underlying Networks	
	Sleepy nodes	Collection of M2M system data	Service Provisioning for Equipment with Built-in Device			
Other	Semantics query for device discovery on inter-M2M SP	Underlying network service activation and deactivation		Personal data management system based on user's privacy preference		
	Group Registration Management	Multicast using group	Access control using group			

3.1   COMMON LIST OF 3GPP MACHINE TYPE COMMUNICATION (MTC) REQUIREMENTS

Keeping in line with the overall vision of a highly interconnected world, the number of communicating machines sending or receiving information via the cellular LTE network is expected to increase dramatically. The concept of Machine Type Communication (MTC), a terminology vastly adopted by the 3GPP standardization body, is to connect thousands of devices into one large network. The idea behind this concept is nothing new. It is the evolution of the smart devices and sensor network concepts to create a new class of wireless applications, where the user-side device is an automatically-controlled unattended machine. MTC is a term that is used to imply wide ranging requirements depending on the application, many of which are supported by cellular LTE technology. In this section, we will discuss some of the common requirements of MTC for different types of IoT applications.

As the trends depicted in Section 2 indicate, a myriad of IoT applications are foreseen to be served by the cellular networks. The requirements as to be anticipated vary widely from application to application. However, there is an effort to categorize applications in a broader framework to provide the best possible support with an appropriate technical variant of the cellular technologies. A common list of requirements for IoT use cases for IoT communications can be broadly summarized as follows:

- General requirements of data speeds for both uplink and downlink

- Relative speed of the IoT device where the application is used

- Tolerance limits on the latency response required for the application

- Number of reports or readings that are required from the IoT device for the corresponding application

- Battery requirements for IoT devices that are necessary for a given application

- Type and extent of security required to preserve the content and communications to the IoT device

For example, for applications in the domain of Fleet Management and Logistics, the typical data rates required are in the range of a few 100s of Kbps, mainly for the uplink. The IoT application that serves this category needs to ensure that the IoT devices will be moving at speeds ranging from 10 to 150 Kmph. For these applications, securing real time and accurate information is of key concern and therefore the tolerance on latency is very low. The number of reports generated by the IoT devices in this category range from 1 per hour to 1 per day. Table 3.2 provides a generic requirement framework for typical IoT use cases.

Table 3.2. Generic requirement framework for typical IoT use cases.

Application	Data Rate	Relative speed	Latency	Duty Cycle	Range	Battery	Security
Fleet Management & Logistics	Up to 100s of kbps UL	High-speed 10-150km/h	Low (Seconds)	1 report/hour~ 1 report/day	few km	Smartphone-like KPIs (car power distribution) 3 months (tracking ship containers)	High
Automotive Telematics	Up to 10s of Mbps UL	Pedestrian: <5km/h	Low (Seconds)	Ad-hoc emergency communication	few km	Smartphone-like KPIs (car power distribution)	High (Emergency)
Automation & Monitoring	50-500kbps UL	No: Fixed Position	High (Hours)	1 report/hour~ 1 report/day	few km	10 years	High
Point of Sales (PoS)		No: Fixed Position	Zero (Milliseconds)	~1 report/day	few km	Low Power	High
Security & Surveillance	05.-8Mbps UL	No: Fixed Position	Zero (Milliseconds)	Real-time UL stream	few km	Smartphone-like KPIs (connected to electrical grid)	High
Health Monitoring	50-500kbps UL	Pedestrian: <5km/h	Low (Seconds)	1 report/hour~ 1 report/day +ad-hoc emergency	< 10s of meters	2 Years	High
Wearable: e.g. sports app data sharing	Up to 10s of Mbps	Pedestrian: <5km/h	Low (Seconds)	Ad-hoc data exchange and signaling	< 10s of meters	1 week (intelligent wristband, smart watch, smart glasses)	Standard
Wearables: e.g. video streaming, file sharing, gaming	20 Mbps and above	Pedestrian: <5km/h	Low (Seconds)	Ad-hoc data exchange and signaling	<100s of meters	Smartphone-like KPIs	Standard

3.2   OVERVIEW OF MTC/IOT USE CASES

3.2.1 AUTOMOTIVE

The concept of a connected vehicle can be traced back to the mid 90's when GM launched their OnStar service for the world's first in-vehicle, hands-free voice communication system, using global positioning and satellite telecommunications to provide a link to the vehicle driver with twenty-four hour OnStar advisers ready to provide a host of services ranging from driving directions to emergency assistance.

Vehicle technology, including sensors and telematics, has continued to improve and connectivity has become more ubiquitous. The concept of a connected vehicle has evolved into a vehicle that is equipped with Internet access, and usually also with a wireless local area network; this allows the vehicle to share internet access with other devices both inside as well as outside the vehicle.

This evolution has also seen an increase in Vehicle-to-Infrastructure (V2I) use cases such as telematics/fleet management solutions, Vehicle-to-Vehicle (V2V), Vehicle-to-Cloud (V2C) and Vehicle-to-Pedestrian (V2P) communication such as vehicle safety communication and real time vehicle control.

A study by the Centre for Automotive Research (CAR) highlighted that "the average car now contains 60 microprocessors and more than 10 million lines of software code -- more than half the lines of code found in a Boeing Co. Dreamliner airplane". Cars are increasingly becoming more intelligent and by 2018, one in five cars on the road will be "self- aware" and able to discern and share information on their mechanical health, global position and status of their surroundings. This self-awareness, together with the need to be always "always on", will require reliable connectivity which is critical to the development of autonomous, "self-driving" vehicles on our roads. As the world looks toward initiative ideas to reduce traffic congestion, Amazon's proposed drone service is one example of this forward-thinking.

Cellular mobile services are ideally suited to provide connectivity to the connected vehicle market as the need for ubiquitous coverage and bi-directional real-time communication plays to the strengths of existing cellular networks. The rollout of 4G LTE and subsequently 5G networks will further increase the capabilities of the connected vehicle and facilitate faster transmission and higher volumes of data created by V2V and Vehicle-to-Everything (V2X) use cases.

The number of connected vehicle use cases has also increased dramatically since the inception of services such as GM OnStar and BMW Connected Drive.   Such use cases can be categorized in five main categories:

- **Infotainment:** Voice communications, personalized music, etc.

- **Navigation:** Traffic info, online route planning, etc

- **Safety:** Smart SOS (eCall), roadside assistance, etc.

- **Cost Efficiency:** Insurance telematics, remote diagnostics, etc.

- **Payment:** Electronic toll collection, parking reservation and payment, etc.

The evolution of the connected vehicle from pure V2I to V2V, and increasingly V2X, presents the vehicle manufacturers with the opportunity to differentiate from their competitors based on the digital services

available to their customers. Figure 3.3 indicates the number of potential use cases found in today's connected vehicles.
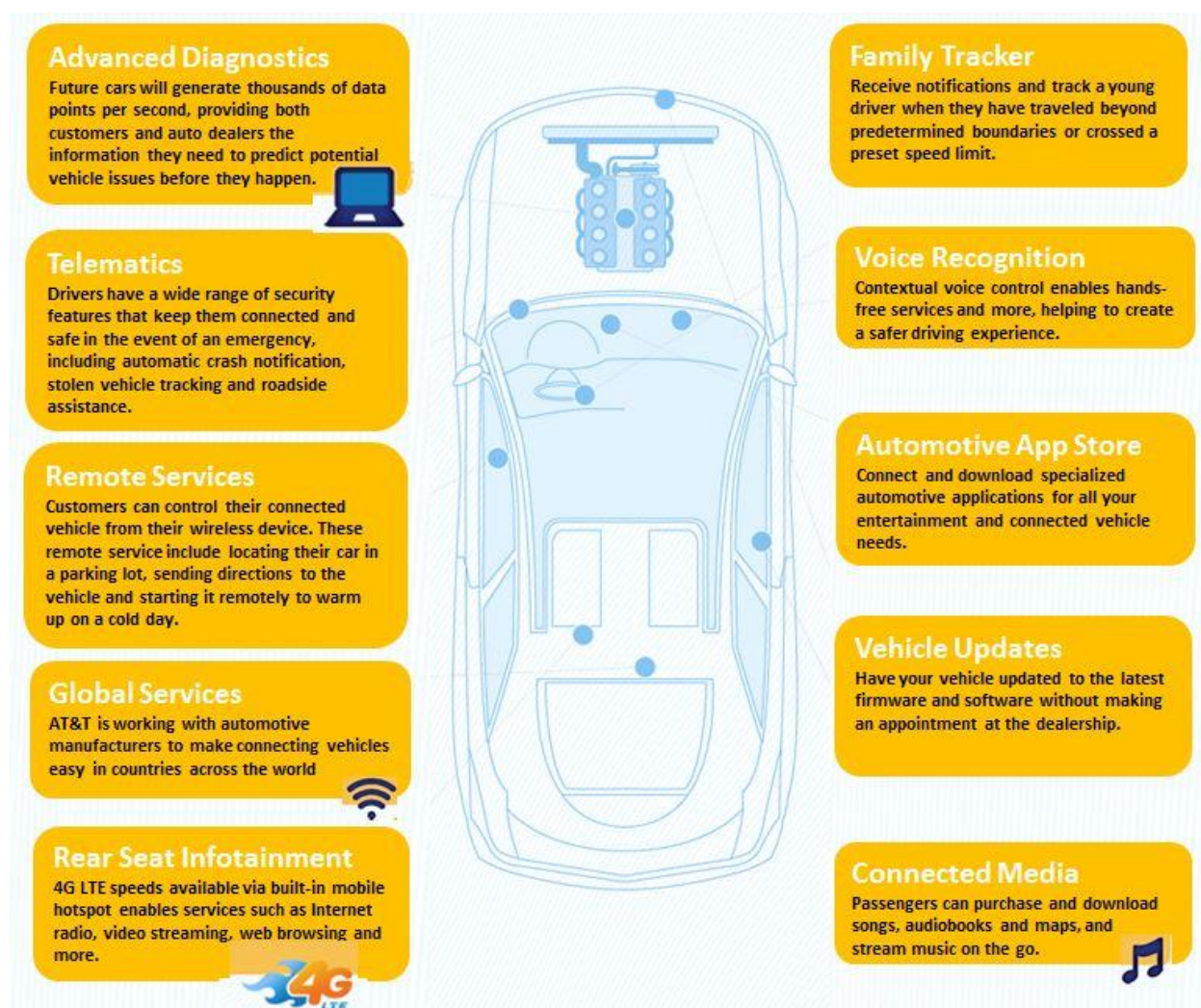

Advanced Diagnostics
Future cars will generate thousands of data points per second, providing both customers and auto dealers the information they need to predict potential vehicle issues before they happen.

Telematics
Drivers have a wide range of security features that keep them connected and safe in the event of an emergency, including automatic crash notification, stolen vehicle tracking and roadside assistance.

Remote Services
Customers can control their connected vehicle from their wireless device. These remote service include locating their car in a parking lot, sending directions to the vehicle and starting it remotely to warm up on a cold day.

Global Services
AT&T is working with automotive manufacturers to make connecting vehicles easy in countries across the world

Rear Seat Infotainment
4G LTE speeds available via built-in mobile hotspot enables services such as Internet radio, video streaming, web browsing and more.

Family Tracker
Receive notifications and track a young driver when they have traveled beyond predetermined boundaries or crossed a preset speed limit.

Voice Recognition
Contextual voice control enables hands-free services and more, helping to create a safer driving experience.

Automotive App Store
Connect and download specialized automotive applications for all your entertainment and connected vehicle needs.

Vehicle Updates
Have your vehicle updated to the latest firmware and software without making an appointment at the dealership.

Connected Media
Passengers can purchase and download songs, audiobooks and maps, and stream music on the go.

Figure 3.3. Connected cars view.[11]

This list is not exhaustive and new use cases are emerging on a regular basis across the industry from vehicle manufacturers and communication service providers and also aftermarket vendors which exploit the OBD (On Board Diagnostic) connectivity port and Over-The-Top (OTT) players such as the mobile app providers.

Connected vehicles, specifically cars, currently represent a relatively small proportion of total shipments of cars per annum; however, as availability and adoption increases, the percentage of cars shipped with connectivity will increase globally from 7.5 percent in 2015 to 75 percent of all new cars by 2020. For more details see Figure 3.4.

---

[11] http://www.att.com/Common/about_us/pdf/att_connected_car.pdf.
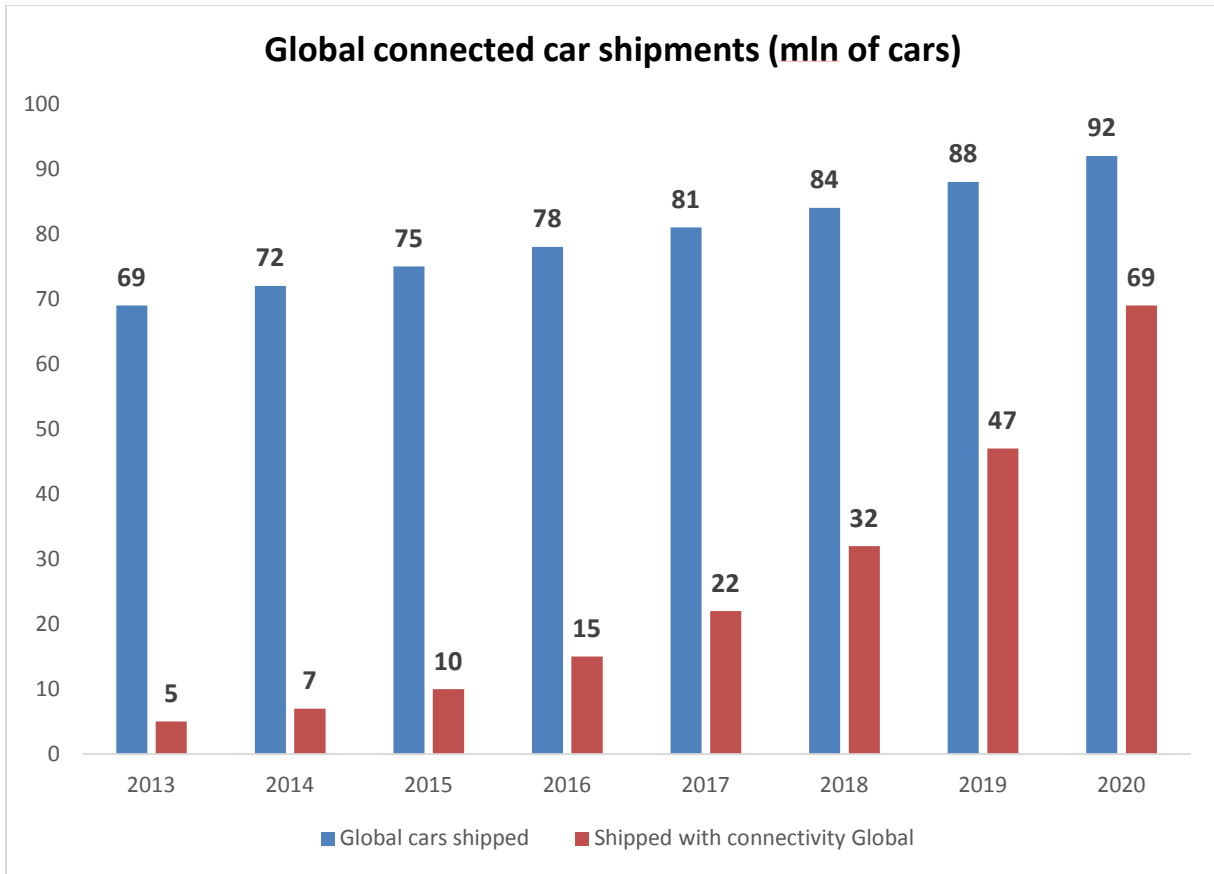
Figure 3.4. Global connected car shipments.[12]

Parks Associates report that 78 percent of drivers with a connected car will require connectivity as standard on their next purchase,[13] and a McKinsey survey of 2,000 new car buyers from Brazil, China, Germany and the United States showed that 13 percent of buyers were not prepared to consider a new vehicle without Internet access and more than a quarter prioritize connectivity over features such as engine power and fuel efficiency.[14]

However, while drivers are keen to exploit the benefits of connected cars, there is still a concern about security and data privacy among a sizeable percentage of the population which is a barrier to wide scale adoption. In the same McKinsey survey, an average of 37 percent of respondents stated that they would not even consider a connected car, although there were major regional differences. For example, in the U.S., 45 percent of respondents said that they were reluctant to use car-related connected services because of concerns about privacy, and 43 percent were afraid that their cars could be hacked into and manipulated if the car was connected to the internet.

---

[12] BI Intelligence, Scotiabank.
[13] http://www.parksassociates.com/blog/article/pr-july2014-connected-cars.
[14] http://www.mckinsey.com/insights/manufacturing/whats_driving_the_connected_car.

These concerns represent an opportunity to communication service providers, IT service providers and car manufacturers if they can demonstrate that their solution is secure from end-to-end. In doing so, they may be able to alleviate consumers' fears and differentiate their products and services. Deployments in LTE transmission encryption and security such a Secure Real-Time Transport Protocol (SRTP) can be utilized to address this.

The increase in use cases and availability of connected vehicles is driving a change in the revenue streams of vehicle manufacturers. Gartner forecasts that by 2020, 70 percent of all auto-related customer interactions will be digital. These interactions will lead to new digital business models for existing and new services. For example, connected vehicle technologies will soon enable drivers to request real-time service, product and pricing information from automakers, dealers and other companies.[15]

Similarly, Infonetics expects revenue derived by service providers for connectivity and other basic value-added services they provide to the automotive, transport and logistics (a.k.a. connected car) segment to more than triple from 2013 to 2018, to US$16.9 billion worldwide. In addition, the connected car services market is growing at a 2013 to 2018 Compound Annual Growth Rate (CAGR) of 25 percent, nearly 21 times the growth rate expected for traditional mobile voice and data services during the same time period.[16]

3.2.2 FLEET MANAGEMENT

The fleet management industry is going through a significant transformation due to the Internet of Things empowered by cellular communications technologies. Fleet management has several challenging problems especially dealing with expense control of fuel costs, maintenance expenses, driver and passenger safety and delivering good customer service. The emerging Internet of Things with the prospects of more reliable connections, seamless coverage across wide geographical areas and remote locations with evolved cellular technologies provides new opportunities to improve fleet performance and customer satisfaction.

The market for fleet management is growing at a tremendous pace and this trend appears to continue in the near future. In North America, the fleet management market is growing at a CAGR of 15.3 percent and is expected to grow from four million units in 2013 to 8.1 million units by 2018.[17] In Europe, the fleet management market is expanding at a CAGR of 14.2 percent from 3.65 million units in 2013 to 7.10 million by 2018.[18]

The fleet management application category encompasses several scenarios and some of the use cases are described below:

- **Route Optimization:** Wirelessly access driver location, dynamically communicate task assignments based on truck location and inventory levels which minimizes the use of number of trucks and delivery time windows

- **Workforce Management:** Wirelessly track worker location on a real-time basis, providing drivers with the ability to remotely clock in and out which allows companies to track the time to complete tasks

---

[15] http://www.autonews.com/article/20140110/OEM06/301109910/the-race-to-market-the-connected-car.
[16] http://www.infonetics.com/pr/2014/m2m-connected-car-connections-svcs-market-Highlights.asp.
[17] *Fleet Management in the Americas, M2M research series, Strategic Research Report*, Berg Insight, 2015.
[18] *Fleet Management in Europe, M2M research series, Strategic Research Report*, Berg Insight, 2015.

- **Driver Behavior Management:** Gives instant feedback to drivers using systems which integrate information about weather, traffic and other factors for safe driving practices to minimize driver errors and achieve better gas mileage. Also includes the creation of detailed plans to advise drivers on eliminating unsafe driving behaviors like speeding, fast cornering, hard breaking or acceleration.

- **Geo-fencing:** Ensures a vehicle is within a virtual geographic area, otherwise sending an alert if boundaries are crossed

- **Telematics:** This information provides valuable insights for fleet companies. The real-time telematics data is collected from sensors located inside the vehicle and sends it over an internet connection to the cloud where it can be distributed to nodes or further processed by data analytics software. The telematics data which includes fuel consumption rates, tire pressure, mileage, speed and braking style among others, are used by the IoT data management platforms to enable trucking managers to fine tune their operations.

- **Diagnostics:** These applications enabled by sophisticated IoT systems help identify maintenance requirements and updates drivers on a variety of performance metrics to avoid roadside breakdowns, minimize costly repairs, enhance safety and improve efficiency of the vehicles.

- **Smart Surveillance:** In this use case, the IoT systems enable drivers and managers of the control systems in real-time to monitor the state of the inventory and condition of the passengers to ensure safety by utilizing wireless communications of video streams

- **Operation Management:** Enhanced IoT systems help address various other aspects of dynamic fleet management operations such as sophisticated supply chain systems for ordering and tracking that maximizes the efficiencies of deliveries and better integrates truck loads with customers.

The cellular IoT fleet management application requirements at a system level include the following:

- Ubiquitous and enhanced coverage
- Reliable connectivity
- Moderate to high data rates
- Precise positioning

The 2G and 3G systems have been the backbone of this important application category which enables IoT features. Evolved 4G and 5G cellular technologies with new capabilities promise to create and build out new generations of infrastructure that will provide even higher data throughput and premium capabilities such as wireless IP-based video, location and presence which ultimately improves efficiencies in operations.

3.2.3 WEARABLES

Wearables are defined as the computing devices that are always-on, always accessible and easily worn on the body. Wearables are now one of the most promising new categories going through a rapid innovation phase to potentially become as ubiquitous as the internet today. The rapidly growing market of wearables is expected to lead a surge in mobile traffic volume in the coming years.

Cisco forecasts that wearables will grow from 109 million in 2014 to 578 million devices in use worldwide by 2019. There are already exciting new products in the market with many new devices to be launched in the future. Wearables are already seen in many areas of our lives such as health, fitness, fashion, gaming, mobile money, education, senior care and child safety, among others.

There are several use cases emerging, but the following are the prominent categories of product and applications defining the wearable landscape:

- Fitness and wellness
- Healthcare and medical
- Industrial
- Infotainment
- Augmented reality: Glasses and cameras
- Smart clothing
- Authentication
- Gaming headsets

The key requirements of the applications associated with wearable devices are form factor, power consumption, high performance, high performance microcontroller and processor functionalities, and user experience. Importantly, the wearable device requirements for cellular connectivity range from as few as 100 kpbs to tens of Mbps.

3.2.3.1 FITNESS AND WELLNESS

The IoT applications in fitness and wellness are emerging today as the largest markets for wearables. The important requirements for this application are the need for devices to acquire data from our bodies and the environment to communicate to a destined receiver over the cellular network in a way that is contextually relevant and meaningful.

ABI Research predicts that the market for wearables in the sports and health sector will grow to nearly 170 million devices by 2017 which represents an annual growth rate of 41 percent.

3.2.3.2 AUGMENTED REALITY

This class of items which belongs to the consumer focused electronics category allows specialized features to interact with devices using audio commands to take pictures, record video, display directions, send messages and perform search functions using cellular IoT communications. This category of applications encompasses specially designed glasses with an augmented reality feature designed with computer generated audio, video and graphics projected in a real world environment.

3.2.3.3 SAFETY

The market for wearables in the area of children safety is growing at a rapid pace. The applications range from watches to backpacks that enable tracking. There are other features that enable an exact location of a child based on GPS and cellular connectivity.

3.2.3.4 HEALTHCARE

There are innovative new product classes that are being developed in the area of healthcare. Some of the product categories that are expanding their reach and providing major value in this area are the following:

- Blood pressure monitors
- Glucose monitoring
- Hearing aids
- Defibrillators
- Electrocardiogram (ECG) monitors
- Insulin pumps
- Pulse oximetry

3.2.3.5 INFOTAINMENT

This sphere of applications encompasses product classes such as smart glasses, smart watches, im-paging products, headsets and head-up displays. One of the key features of this product category is the smartphone acting as the hub of information that enables the user to connect the wearable device to exchange data.

3.2.4 OTHER CELLULAR IOT VERTICAL APPLICATIONS

Additional domain/vertical applications that would benefit from the use of cellular 3GPP connectivity as part of its IoT solution though deployable wireless/wireline technologies are listed below along with details of potential use cases in those domains:

- **Healthcare/non-wearable:** Remote monitoring of patients, hygiene monitoring and access to medical care via the internet/mobile devices

- **Industrial automation:** Smart factory (energy management such as monitoring energy consumption and conditions and resource management, stock control, factory automation such as production line control, security and safety, and video surveillance), oil and gas (preventive/conditional based maintenance for pipelines and heavy plants, use of sensors and big data analytics to determine what needs to be repaired and when, pipeline management, sensors along long remote pipelines measuring pressure and flow rates for management and maintenance)

- **Connected consumers:** Smart transportation including traffic congestion which is becoming a major issue in many urban areas leading to productivity loss, environmental pollution, and degradation of quality of life. Cellular technologies like 4G LTE will enable real-time collection of massive data from vehicles, drivers, pedestrians, road sensors and cameras to help streamline traffic flow.[19] For example, it can help optimize traffic lights and road usage, direct public transportation to where it is needed most, navigate vehicles to avoid congestion, raise tolls to limit traffic entering a congestion zone, etc.

---

[19] *5G Spectrum Recommendations*, 4G Americas, August 2015.

4 TYPICAL FUNCTIONAL ARCHITECTURE AND COMMONLY USED PROTOCOLS IN IOT

4.1 FUNCTIONAL ARCHITECTURE

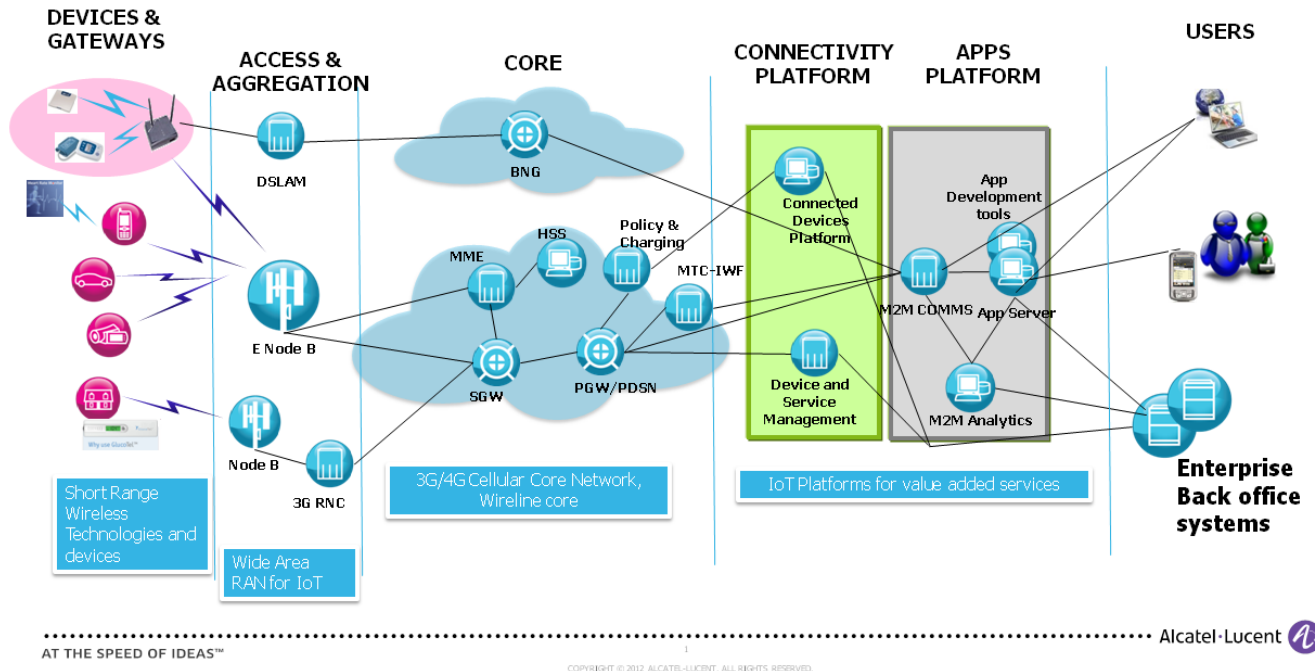The typical end-to-end architecture of IoT solutions is shown Figure 4.1.

Figure 4.1. Typical end-to-end architecture of IoT solutions.

Each of the major components is discussed below.

4.1.1 DEVICE/GATEWAY

In an IoT solution, a machine such as a washing machine or automobile is embedded with a communication device that connects to a network, thereby enabling the machine to interact with a cloud based application (the other 'machine' in IoT), applications on other devices such as smart phones and tablets, or other various machines. The communication device may be connected to a local gateway through a short range network such as WiFi, Zigbee or Bluetooth or directly to a wide area network such as the mobile cellular network. The gateway device may be connected through a wireline access network instead of wireless; for example, a home automation solution. The gateway enables the local communication between the connected devices and bridges the local network to the wide area network.

4.1.2 ACCESS NETWORK

In IoT, the wide area access network is often wireless. The choice of the network depends on the application requirements such as whether or not mobility is required or commercial or private networks are desirable. Increasingly, the ubiquity and convenience of the mobile cellular network is driving wide area IoT applications towards mobile operator networks. In mobile networks, the radio access network (RAN) is shared across consumer and IoT traffic. Mobile networks have traditionally been designed for

low latency, high throughput consumer traffic and not optimized for IoT. However, since 2011, 3GPP has been defining several IoT/MTC optimizations to 2G/3G/4G for extending coverage for low throughput devices deployed deep within buildings such as in basements which consequentially reduce signaling traffic and device cost and improve battery life. At the same time, IoT optimized wide area wireless networks are being developed and deployed.

4.1.3 MOBILE CORE NETWORK

Although mobile core network functions are not defined separately for IoT, a large amount of effort has been made and will continue to be made to optimize the 3GPP core network for IoT services and devices. Two major forces are at play; one is the current ongoing MTC work in 3GPP and the other is the application of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) technologies in the mobile core network that will provide new capabilities that can support a variety of use cases including IoT more efficiently. 3GPP MTC work is focused on cellular system optimization for IoT services and support for low complexity and low power consumption devices, as well as efficient small data transmission (see Section 7.1 for more information).

NFV and SDN technologies allow a modular and software based core network architecture where the core network can be dynamically 'sliced' and 'scaled' based on use cases, types of devices and other parameters. It is conceivable that a network operator can create mobile core instances suitable for IoT rather than one core network that has to fit all of the current scenarios. The combination of these new technologies will result in an access agnostic and software-based next generation mobile core network that will support the diverse use cases of telecommunications in the near future.

4.1.4 CONNECTIVITY PLATFORM

Low average ARPU associated with IoT and some unique requirements such as the need for bulk provisioning have driven mobile operators to reduce their operations cost by deploying a platform for handling SIM pre-provisioning, provisioning, activation, deactivation and self-diagnosis of device communication issues. The rating requirements for IoT have required substantial flexibility depending on the specific enterprise and the number and usage of devices. The connectivity platform typically includes a configurable rating system (separate from the rating system deployed for consumers) that connects to the operator's traditional charging systems. The connectivity platform sometimes also includes a communications server that performs, stores and forwards message routing and protocol translation, essentially gathering data from devices and making them available to applications. In many cases the data communications server is included in the application platform as discussed in the following section 4.1.5. The management platform includes device management functions for firmware upgrades, configuration and diagnostics, and application life cycle management.

4.1.5 APPLICATION PLATFORM

An application platform (also called the Application Development and Execution Platform (ADEP) or Application Enablement Platform (AEP)) is used to build and run the application in IoT solutions. The application platform includes the basic functions needed for any application: gather, store and process data and present useful information to users of the application. The platform includes the communications server, a rule engine for processing data and a data base for storing device data. Asset management involving onboarding and decommissioning of assets, associating them with communication devices or SIMs is provided. More sophisticated IoT analytics can also be treated as part of this layer. Application Program Interfaces (APIs) in the form of a software development kit are provided to easily use

the services of the platform. Standalone applications or applications running on the platform are sometimes integrated into enterprise back-office systems such as SAP.

4.1.6 ADDITIONAL NETWORK RELATED CONSIDERATIONS

In addition to the above mentioned IoT network infrastructure domains, several items need to also be taken into consideration:

- Remote and automated operation, administration, management and provisioning

- Virtualization on majority of network domains like virtual Radio Access Networks (vRAN)/vAccess, vCore and virtual Operations Support Systems/Business Support Systems (OSS/BSS) for dynamic scalability and other purposes

- Discoverability of data, services and applications via search engines

Various IoT applications/use cases have different requirements regarding key parameters like data rate, relative speed, latency, range, battery life and security. Figure 4.2 illustrates the cellular (primarily LTE) technologies used for the subset of IoT applications/use cases.
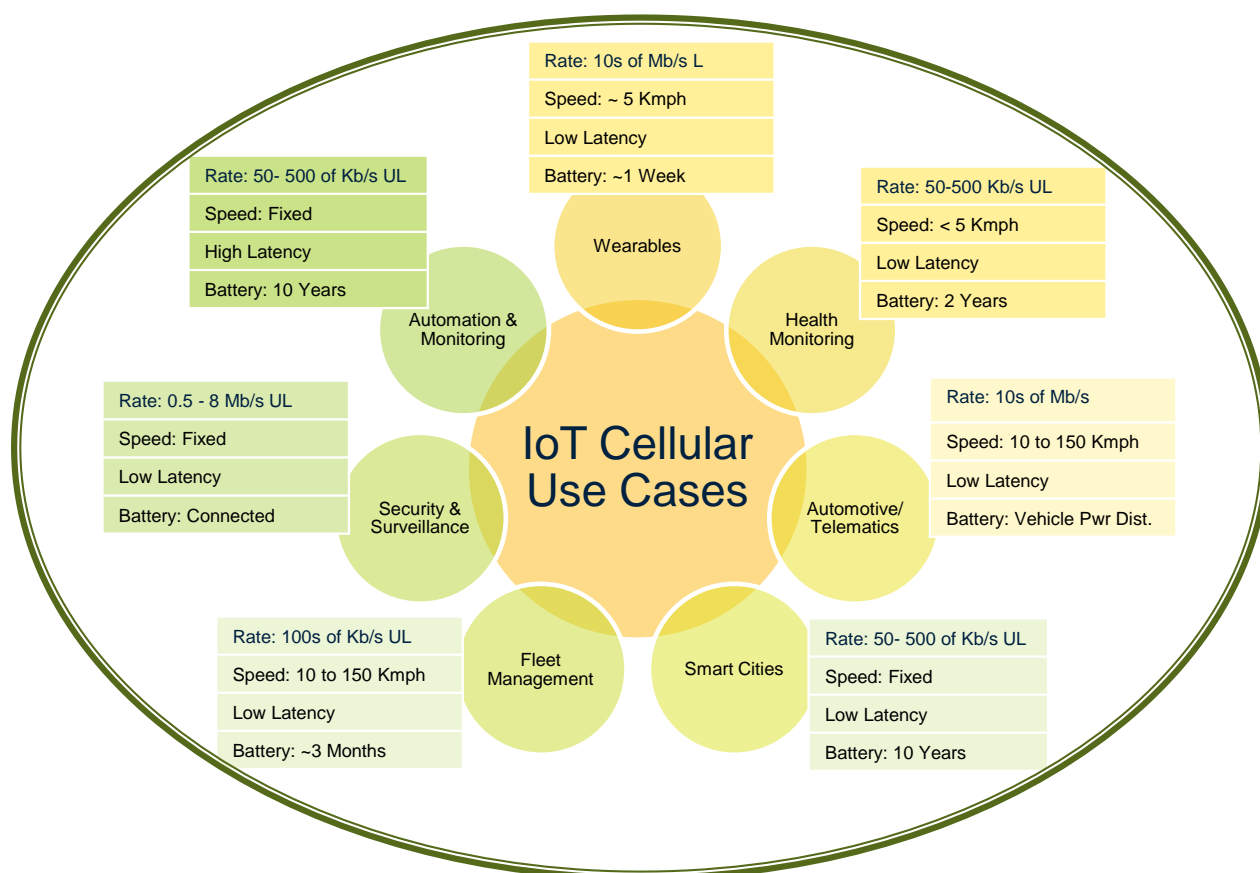

Figure 4.2. Typical requirements for typical cellular IoT use cases.

4.2   COMMONLY USED PROTOCOLS IN IOT

4.2.1 IOT PROTOCOLS CATEGORIZATION

There are a variety of protocols used in IoT for various purposes. These protocols are in use in both fixed and cellular deployments and the majority of them are IP-based. In general, all of them can be categorized in the following manner:

- Device management protocols for managing end-point devices and IoT gateways (examples are OMA-DM, TR-069 and LWM2M)

- Application level data transport (examples are http, webSockets, CoAP, 6LoWPAN, MQTT, XMPP-IoT extensions)

- Link encryption (TLS and DTLS)

4.2.2 IOT PROTOCOLS: CURRENT AND FUTURE USES IN CONTEXT OF IOT

Current uses of OMA-DM in the context of IoT are mainly for IoT gateways with built-in cellular connectivity. In the future, use of this protocol in IoT is expected to be much smaller due to its robustness and complexity for IoT domain.

As wireless embedded modules are certified for use by a mobile network operator and integrated into various host devices, the International Mobile Station Equipment Identity (IMEI) Type Allocation Code (TAC) range of the module is often leveraged by the integrator on the host device. As part of the device certification, the Personal Communication Service Type Certification Review Board (PTCRB) requirement is not more than 10,000 units of what the host device can use in the IMEI TAC range of the module; however, it has frequently been seen that those rules are not always followed. In this situation, an MNO has no traceability to the type of host device that the module is installed in and the number of those devices which are present on the network. This lack of traceability is problematic for several reasons including when field issues are discovered with a particular device making it impossible to exactly pinpoint those devices on the network.

To overcome this issue, a requirement has been developed for wireless embedded modules to support the ability to report information to an MNO database allowing the MNO to discretely identify each device in the network which leverages the IMEI TAC range of the module (it is assumed that devices not utilizing an embedded module should have a dedicated TAC range assigned). This service utilizes a subset of the OMA-DM standard and is known as Device Host Identity Reporting (DHIR). New custom OMA-DM nodes have been created to collect the information from the host device into which the module is integrated.

To complete the service, the MNO must also make it mandatory for integrated device manufacturers which leverage the module IMEI TAC to support this module-based service within their devices. The MNO must define a server for the OMA-DM client to use to report this information to the network. Upon incorporation into devices, the proper service functionality will need to be verified as part of certification testing and will be expected to be capable of reporting to an active server with all required information.

Current uses of TR-069 in context of IoT are for broadband based Customer Premise Equipment (CPE), while in the future it is expected that TR-069 can find its use for smart home and connected appliances/connected consumer electronics type of IoT applications.

Current uses of LWIOT in context of IoT are for device management and services enablement for resource constrained devices, while in the future the uses are expected to expand to sensors in smart city and premise, oil and gas field operation and healthcare (with location tracking need) type of applications.

Current uses of webSockets in context of IoT are for the IoT environment where bundles of data are transmitted continuously within multiple devices. At this stage it is still too early to state which additional use cases webSocket may be used for in the future in context of IoT.

Current uses of CoAP in context of IoT are for web transfer for use with constrained nodes and constrained (e.g., low-power, lossy) networks, while in future this protocol will potentially find its use also for applications such as smart energy/smart grid, building automation, intelligent lighting control, industrial control systems, asset tracking and environment monitoring. Combined with the Datagram Transport Layer Security (DTLS) protocol, CoAP can provide highly secured applications in above mentioned domains in the future.

Current uses of 6LoWAPAN in context of IoT are for the IPV6 solution for wireless sensor networks, while in the future it may potentially also be used for applications such as building/home automation with sensors and actuators, street light monitoring and control, residential lighting, smart metering, smart factory type of applications, monitoring perishable product with multi-domain sensors in transportation applications, monitoring premature babies sensitive to temperature changes and generic IoT applications with internet connected devices.

Current uses of MQTT in context of IoT are for publish/subscribe messaging protocols for constrained Internet of Things devices and low-bandwidth, high-latency or unreliable networks, and it is expected that this protocol will not find its use cases in the future outside of its current set.

The XMPP Standards Foundation community has initiated a new interoperable XMPP based extension series to enable sensors and actuators to communicate in the IoT world. All those extensions are envisioned to run on top of XMPP that was originally designed to enable Peer-to-Peer (P2P) communication via text messages.

One of the core values of the technology is that XMPP already has a large federated server-to-server infrastructure for messaging. Using this will create an open interoperable middleware for IoT where any device in a domain can freely choose to interact with any other device through the federation and friendship mechanisms, just as the chat network is used today.

In the IoT context, XMPP offers an easy way to address a device. This is especially handy if that data is going between distant, mostly unrelated points, just like the P2P case. It is not designed to be fast; in fact, most implementations use polling or checking for updates only on demand.

XMPP is best in addressing, security and scalability making it ideal for consumer-oriented IoT applications.

4.2.3 IOT PROTOCOL CHALLENGES

Ultimately, applications decide individually when to use communication resources. However, sometimes this is not efficient due to latency and reliability requirements. This area needs improvement and there is an ongoing effort to address it in various standards organizations.

Applications are distributed (devices/gateway/network domain) and need several functions in a service layer to make communication more efficient, development more simple, and deployment and operation more cost-effective.

The real challenges with IoT protocols that need to be taken into consideration in practical implementations are the following:

- Efficiency
- Interworking/interoperability
- Sharing mechanisms

In most cases, the end application is in charge of efficiency. Applications (on devise/gateway/cloud) are in charge of when to burn communication resources. Use of communication resources with such modes of operation can become very inefficient and not all decision power on resources usage should be given to end applications. Instead, efficiency can be addressed in two domains:

- RAN/Core Network and/or
- Middleware on top of IP

The dilemma of achieving interworking and interoperability among various IoT protocols is typically resolved by usage of different protocols or same protocols with different data models which results in isolated solutions. There is a need for common language to resolve interworking and interoperability issues in a more holistic manner.

A single source of data could be used in many different IoT solutions. As an example, window sensors are an isolated silo for only an alarm system while they could also be utilized for additional purposes such as for heating sensors. There is a need to have functions in the IoT system that support better sharing and distribution of data and events.

The recommendation is to also consider capabilities of device management protocols to address fault tolerance, diagnostics, repair and replacement of faulty devices as well as device presence detection.

And finally, end-to-end reliable bi-directional signaling and data transport across a heterogeneous set of protocols is also of interest while considering IoT protocols.

4.2.4 MISCELLANEOUS EMERGING IOT PROTOCOLS

In addition to above mentioned protocols that can be clearly categorized, there are sets of protocols not originally designed for IoT, that are lately finding a place in the IoT, for example, XMPP-IoT extensions, DHIR and Device Management (DM).

4.3   SECURITY IN IOT

IoT will fundamentally change how the world sees data security and privacy. Every end point device or gateway device and connection that gathers, transmits, stores or processes sensitive data is a potential risk. A study by HP found that 70 percent of the most commonly used IoT devices contain security vulnerabilities. Details on HP's finding of top ten security problems with IoT devices is listed below:

- Insecure web interface
- Insufficient authentication

- Insecure network services
- Lack of transport encryption
- Privacy concerns
- Insecure cloud interface
- Insecure mobile interface
- Insufficient security configurability
- Insecure software
- Poor physical security

The diversity of IoT assets makes achieving effective governance and cyber security challenging.[20]

In a mature IoT world, there will be millions of intelligent endpoints, each equipped with multiple active sensors and a large number of lines of code. Many of these endpoints will be accessible, often physically, to hackers. The network connections that these endpoints use to communicate may also be vulnerable, giving access to central applications and databases.

Because IoT is all about physical "things", hackers that gain access cannot only perform the usual digital attacks like stealing data, moving money or shutting down websites — they can also cause havoc by tampering with infrastructure like electrical grids and traffic signals, or put lives at risk by meddling with healthcare devices, airplanes or elevators.

Privacy is also a major concern. IoT applications gather large volumes of data about people's behavior. Consumers and employees are increasingly concerned about how the data might be used and the risk of criminals stealing it during a breach. Companies need to address these privacy concerns and be prepared for changes in data protection regulation.

Demands for an extremely high level of security in context of IoT is achievable in most use cases via mobile/cellular networks over short-range wireless technologies compared to some other technologies considered for use for IoT.

4.3.1 WAYS TO SECURE A COMPANY'S IOT INFRASTRUCTURE

Even the most security-conscious sectors may be unprepared for the security impact that IoT connected devices can have. Below is a set of recommendations on the protection of a company's IoT solutions:

- Build security from the start of the initiative

- Evaluate the specific threats facing one's application

- Authenticate and authorize connections; verify both identity and access rights

- Provide appropriate security for data transfers

- Consider the user experience. If security measures (such as passwords) become cumbersome, users will either circumvent or avoid using the IoT service entirely

---

[20] *Verizon State of the Market The Internet of Things*, 2015.

- Reduce data risk, particularly with regard to personal data

- Plan for what to do if something goes wrong, understand that compromise will happen and plan a workflow for getting compromised credentials out of the system

- Communicate about security and privacy; educate employees, partners and customers about what you are doing to protect them, particularly if sensitive data is at risk

The Internet of Things continues to impress with both its promise and offerings as we enter 2015. Products, services and ecosystems around IoT will increasingly offer a wide range of benefits that can entice both consumers and businesses.

This research does not aim to dampen that enthusiasm, but to inform users that these capabilities come with risks, and that it is in everyone's best interest to understand those risks before activating these systems.

4.3.2 RECOMMENDATIONS

Some key recommendations for those looking to implement IoT devices in a more secure manner are:

- **Consumer:** Include security in the feature considerations when evaluating potential IoT product purchases, avoid using system defaults for usernames and passwords whenever possible and choose good passwords when the option is available

- **Enterprise:** Implement segmentation between IoT devices and the rest of the network using a firewall or other filtering technology, configure supplemental security features (that may not be enabled by default), examples might include password strength policies, account lockouts, event logging and two-factor authentication.

5 ADVANCEMENTS IN LTE FOR MACHINE TYPE COMMUNICATION

5.1 OVERVIEW OF LTE-ADVANCED MTC FEATURES

Technical studies and normative work for the support of Machine Type Communication (MTC) as part of 3GPP LTE-Advanced (LTE-A) specifications for Radio Access Network (RAN) began in LTE Release 12 (Rel-12) and are continuing with the goals of developing features optimized for devices with MTC traffic. These features are typically characterized by small and infrequent data transmission/reception and a higher level of delay-tolerance compared to devices supporting Human-Type Communication (HTC). These devices are expected to have a complexity level that is significantly lower than a Category 1 User Equipment (UE), ultra-long battery life and are expected to support enhanced coverage operation within LTE-A networks. Additionally, these MTC/IoT services are expected to coexist seamlessly with today's mobile broadband services, so mobile operators can efficiently integrate them with existing and planned LTE-A spectrum and networks.

As of 2015, low data rate requirements and the latency-tolerant nature of MTC traffic have enabled operation of MTC applications mostly on Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS) networks. However, it was identified that significant revenue potential can be harvested by network operators with a successful migration of MTC traffic from 2G to LTE networks

and, with the extensive proliferation of LTE deployments worldwide, benefit from the economies of scale. In addition, superior longevity of 4G LTE networks compared to 2G networks needs to be emphasized as it is important to many IoT applications that are deployed for a long period of time. Thus, the MTC features already supported or currently being developed include defining UEs that are cost competitive with GSM/GPRS devices and can target coverage improvements of up to 15-20 decibels (dB) to address use cases where such MTC UEs are deployed deep inside buildings.

3GPP specified a new class of UE that is identified as Category 0 UEs with a reduction of modem complexity by approximately 50 percent compared to a Category 1 UE (the lowest complexity UE defined until then) and with a Bill of Material (BoM) cost approaching that of an Enhanced General Packet Radio Service (EGPRS) modem. These low complexity UEs are targeted for low-end (e.g., low average revenue per user, low data rate and delay tolerant) applications and possess reduced transmission and reception capabilities compared to other LTE UE categories.

Currently, work is ongoing in 3GPP towards defining an even lower complexity LTE-based device, informally referred to as Category M or Category "-1" devices using additional complexity reduction techniques. At the same time, support of coverage enhancement features is being pursued for MTC UEs with delay-tolerant traffic. Such coverage enhancement techniques are applicable to the to-be-introduced Category M devices as well as other more capable UEs (e.g., Category 0, 1 UEs). Additionally, enhancements to support reduced device power consumption are also being developed as part of Rel-13 enhancements for LTE-based MTC. Figure 5.1 depicts the projected timeline of 3GPP standards for cellular MTC/IoT evolution.
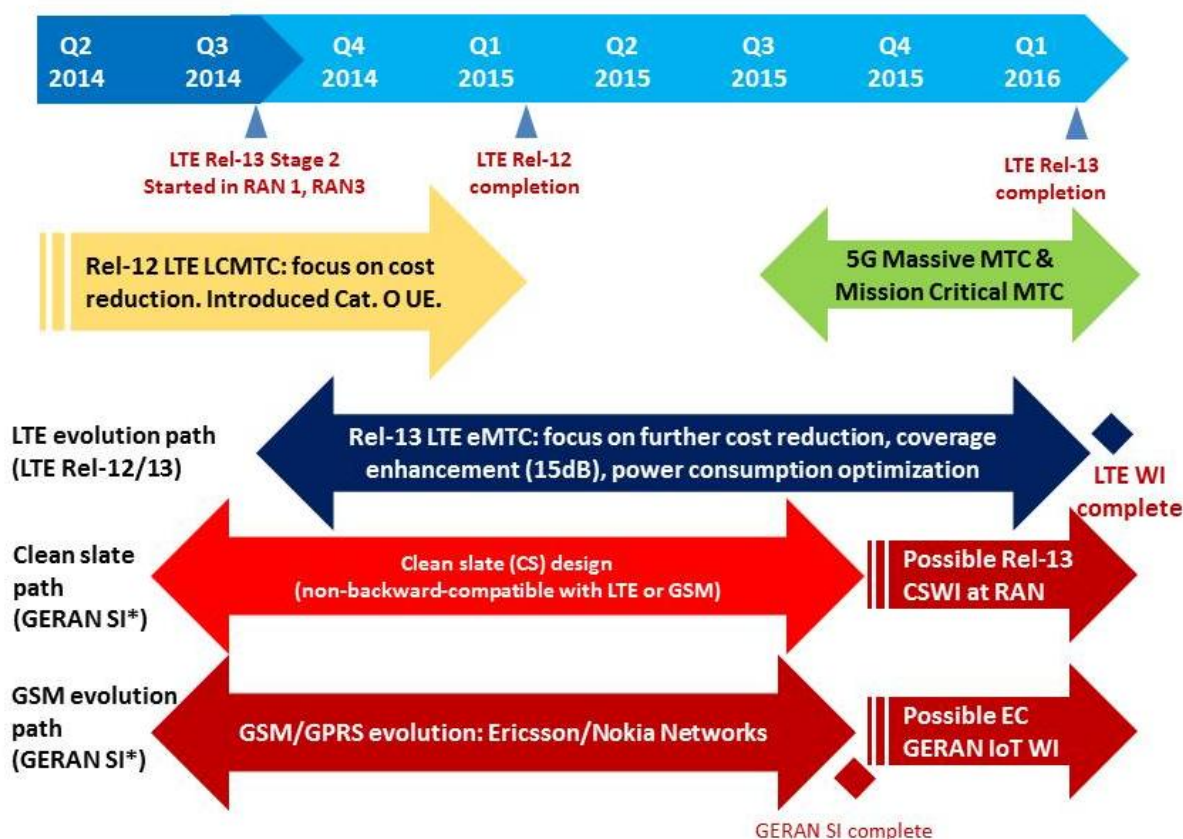

Figure 5.1. Projected timeline of 3GPP standards for cellular MTC/IoT evolution.

In addition to the above features for support for LTE-based MTC devices, solutions aiming to reduce device power consumption like Power Saving Mode (PSM) and extended Discontinuous Reception (eDRX) are either already available or are being developed currently. Such features, optimized to enable prolonged battery life, play a key role in the success of LTE-based MTC solutions as attractive options for cellular IoT applications.

As discussed further in sub-section 6.6, further evolution of LTE-based and new Radio Access Technology (RAT)-based solutions (e.g., as part of developments towards 5G cellular technology) for MTC devices are currently foreseen. Such efforts would aim to further optimize system-level support for traffic and requirements specific to MTC applications including handling a really massive number of MTC devices in the network or support of mission critical MTC applications that demand extremely low latency and/or very high reliability.

5.2   APPLICATION OF LTE MTC FEATURES FOR MAJOR USE CASES

LTE-based MTC solutions find application in various realizations of MTC ranging from home and industrial automation to consumer electronic devices like connected wearables. LTE-based MTC solutions provide a significantly expanded set of opportunities as a cellular IoT service by virtue of its ubiquitous presence, reduced power consumption and higher range of supported data rates of up to 1 Mbps compared to other local IoT connectivity solutions. Table 5.1 lists some examples of the major use cases identified for application of cellular IoT solutions and their technical requirements.

Table 5.1. Examples of major use cases for MTC or cellular IoT.

Application	Data rate	Mobility	Latency tolerance	Duty cycle	Range	Battery-life
Fleet Management & Logistics: *Real-time and accurate information across supply chain*	Up to 100s of Kbps UL	High speed: 10-150km/h	Low (seconds)	1 report/hour ~ 1 report/day	Few km	Smartphone-like (car power distribution) 3 months (tracking ship containers)
Automotive Telematics: *Post crash systems, emergency support calls and remote diagnostics*	Up to 10s of Mbps UL	Pedestrian: <5km/h	Low (seconds)	Ad-hoc emergency communication	Few km	Smartphone-like (car power distribution)
Automation & Monitoring: *Asset management, Remote monitoring of utility-based equipment for gas/water metering applications*	50-500 of Kbps UL	No: Fixed position	High (hours)	1 report/hour ~ 1 report/day	Few km	10 years
Point of Sale (PoS): *Connection to the network*		No: Fixed position	Zero (milliseconds)	~1 report/day	Few km	Low power

Application	Data rate	Mobility	Latency tolerance	Duty cycle	Range	Battery-life
Security & Surveillance: *Real-time monitoring and control, e.g. video surveillance*	0.5-8 of Mbps UL	No: Fixed position	Zero (milliseconds)	Real-time UL stream	Few km	Smartphone-like (connected to electrical grid)
Health Monitoring *Health care delivery and monitoring*	50-500kbps UL	Pedestrian: <5km/h	Low (seconds)	1 report/hour ~ 1 report/day + ad-hoc emergency	Less than 10s of meters	2 years
Wearables: *Personal Proximity Network: D2D discovery and synchronization for data exchange, e.g. sports app data sharing*	Up to 10s of Mbps	Pedestrian: <5km/h	Low (seconds)	Ad-hoc data exchange and signalling	Less than 10s of meters	1 week (intelligent wrist-band, smart watch, smart glasses)
Wearables: *Proximity Social Services: D2D communication, e.g. video streaming, file sharing, gaming*	20 Mbps and above	Pedestrian: <5km/h	Low (seconds)	Ad-hoc data exchange and signalling	<100s of meters	Smartphone-like

The summary in Table 5.1 indicates a diverse class of applications with a wide range of requirements in regard to data throughput, latency tolerance, coverage range and battery life. Regarding the coverage support, although in terms of distance-based range, most applications target short distances and the actual radio coverage requirements for many of these applications can be much more demanding than how it appears from the distance-based range listed in Table 5.1 due to the need to overcome building penetration loss for MTC devices deployed deep inside buildings.

It should be acknowledged that while many of the use cases listed in Table 5.1 are addressed by LTE-based MTC solutions, certain use cases may be better addressed with the evolution of MTC and cellular IoT solutions as part of future LTE releases or 5G radio access technology. Some such examples include applications requiring extremely low latency and very high reliability like crash-warning systems, remote surgery for mobile healthcare applications, wearables requiring extremely low device complexity and very long battery lifetimes. These use cases are expected to be addressed with further evolution of MTC and cellular IoT technology and are presented in Section 5.6.

The reachability of LTE-based MTC devices is further extended by coverage enhancement techniques that are being developed as part of LTE Rel-13 enhancements to MTC thereby enabling, for example, efficient support of different smart metering applications that may be physically located deep indoors (e.g., basements) and with radio links suffering from high Building Penetration Loss (BPL).

The objective of achieving ultra-long battery life for Category M devices aims to address IoT applications (e.g., metering applications like utility monitors). These metering devices may be equipped with batteries of about 5 Watt-hour (Wh) capacity and designed to operate without any further human intervention after their initial installation for prolonged periods of time spanning several years.

Mobility support available in LTE-based MTC solutions, albeit in a simplified form compared to more capable LTE UEs, provides the clear advantage of ubiquitous Wireless Wide Area Network (WWAN) coverage for various consumer electronic IoT devices like wearables and in-vehicle devices, and paves the path for the realization of IoT devices being always connected to the cloud in the near future.

In summary, there is a need for significant reduction in the device complexity and cost to be comparable to or even more attractive than EGPRS modems. Superior coverage for both Downlink (DL) and Uplink (UL), ultra-long battery life for various applications and the economies of scale for LTE-based solutions are the fundamental components that make LTE-based MTC solutions including Category 0 and M UEs attractive choices for various emerging as well as already-developed IoT markets and applications.

5.3   LOW COST DESIGN INNOVATIONS FOR LTE-BASED IOT DEVICES

In this subsection, the primary designs and enhancements to realize reduced cost and complexity for LTE-based IoT devices are discussed. First, the focus is on the cost reduction attributes for Category 0 UEs as specified in LTE Rel-12, and this is followed by a discussion on the main complexity reduction features that can be expected to be specified for Category M UEs as part of Rel-13 work on further physical layer enhancements to LTE-based MTC.

5.3.1 LOW COST ATTRIBUTES FOR CATEGORY 0 UEs

As mentioned in subsection 5.1, various cost reduction techniques and simplifications have been specified in LTE Rel-12 in defining low complexity UEs suitable for MTC applications.

5.3.1.1 SINGLE RECEPTION ANTENNA AND SINGLE RECEIVING RF CHAIN

One of the important cost reduction features is support for a single antenna and receiving Radio Frequency (RF) chain for MTC UEs. The cost reduction is achieved due to various factors that include reduction in the reception filtering requirements by half, need for only a single receiving RF chain and simplified baseband processing requirements for the DL, (e.g., 50 percent reduction in Fast Fourier Transformation (FFT) operations at the receiver, 50 percent reduction in the channel estimation requirements for DL reception, a single Analog to Digital Convertor (ADC) compared to multiple ADCs for other UE Categories, etc). Assuming a ratio of RF to baseband cost of 40 percent:60 percent, the overall cost saving from having a single receiving RF chain is expected to be around 15 percent to 38 percent compared to a reference LTE modem (Category 1 UE).

Although a single reception antenna and receiving RF chain implies a degradation in the DL reception capability, it may translate to a reduced DL coverage of around 4 dB on the average compared to other LTE UE categories. It should be noted that the DL coverage with a single antenna and receiving RF chain is still better than that of a GSM/EGPRS device. Further, it can be expected that effective coverage enhancement techniques would be available in Rel-13 to compensate for the loss in DL coverage resulting from the reduction in the number of reception antennas and receiving RF chains. As a direct consequence of a single reception antenna requirement, only single layer and stream reception is possible for Category 0 UEs.

5.3.1.2 HALF-DUPLEX FDD (HD-FDD) OPERATION

The RF implementation complexity and cost can be significantly reduced with half-duplex operation in FDD systems as the UE would not be required to transmit and receive on the paired UL and DL carriers

simultaneously. This enables use of only a switch instead of a full duplexer which is much more expensive and accounts for about 25 percent of the RF module cost. Further, the baseband requirements are also reduced in terms of required memory and processing power as simultaneous handling of DL and UL operations is not necessary. Depending on the implementation optimizations, a range of 4 percent to 19 percent of cost reduction relative to a Category 1 UE can be facilitated with the support of Half-Duplex Frequency Division Duplex (HD-FDD) operation.[21]

In order to support HD-FDD operation, additional switching times for the MTC UE to switch between DL and UL and vice-versa are provisioned. A common value of 1 millisecond (ms) of switching time is specified for DL to UL and UL to DL switching for HD-FDD UEs. During this switching time, a HD-FDD UE is not expected to either receive or transmit on the DL or UL carriers respectively. This switching time includes the time needed for carrier frequency retuning between DL and UL, application of Timing Advance (TA) (that can be up to ~ 670 µs long) as the UE switches from reception on the DL to transmission on the UL, any power ramping down/up needed, settling of the Phase Locked Loop (PLL), and Automatic Gain Control (AGC) and Analog to Digital Convertor (ADC) settling times.

It should be noted that support of HD-FDD operations comes at the expense of increased complexity at the network side (e.g., at the enhanced Node B (eNodeB), since the eNodeB needs to ensure that a UE may not be scheduled for UL/DL transmissions/reception when it is receiving/transmitting respectively or during DL$\leftarrow\rightarrow$ UL switching periods. Thus, such scheduler constraints need to be handled by the eNodeB scheduler in a network supporting HD-FDD MTC UEs. Further, considering 1ms switching times, a reduced number of Hybrid Automatic Repeat reQuest (HARQ) processes from 8 to 3 can be supported in practice for HD-FDD UEs. This leads to a maximum throughput of 375 kbps for both DL and UL as against a maximum supported throughput of 1 Mbps for regular FDD and TDD Category 0 MTC UEs.

5.3.1.3 REDUCED PEAK DATA RATES

Considering the reduced requirements for typical cellular IoT applications, Category 0 UEs support reduced peak data rates for the DL and UL. The peak data rate reduction is based on a reduction in the maximum Transport Block Size (TBS) used for transmitting/receiving unicast data in a single Transmission Time Interval (TTI) of 1ms. As a design principle, a minimum requirement of satisfying the data rates for EGPRS multi-slot class 2 devices of 118.4 kbps on the DL and 59.2 kbps on the UL was considered. For Category 0 UEs, it is specified that a maximum TBS of 1000 bits needs to be supported for unicast reception/transmission leading to a peak data rate of 1 Mbps for user data. This marks more than 10-fold and 5-fold reductions in the TBS values that a Category 1 UE needs to support for DL reception and UL transmission respectively.

For common control broadcast information like System Information Block (SIB), Random Access Response (RAR) and paging transmissions, the maximum TBS for Category 0 UEs is maintained at the same level as Category 1 UE at 2216 bits. The maximum TBS for multicast transmission on the Physical Multicast Channel (PMCH) was also limited to 4584 bits for Multimedia Broadcast Multicast Service (MBMS)-capable MTC UEs.

The primary benefits of reduced peak data rates come from reduced processing requirements for UL data packet transmissions, turbo decoding for DL reception and buffering for HARQ operations. Overall, about 10 to 21 percent of cost savings can be expected considering both DL and UL peak data rate reduction via reduction in the supported TBS values.

---

[21] 3GPP TR 36.888.

5.3.2 LOW COST ATTRIBUTES FOR CATEGORY M UES

Although work is currently underway in 3GPP RAN Work Groups (WGs towards defining a new MTC UE category (referred to as Category M here) and specifying enhancements for further complexity and possibly cost reduction, here, we highlight some of the already agreed complexity reduction features that can be expected to define Category M UEs with further reduced complexity compared to Category 0 UEs.

5.3.2.1 UEs WITH REDUCED BANDWIDTH CAPABILITY

All LTE UEs, including Category 0 UEs, currently need to support all specified LTE system bandwidths (BWs) that include 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz, and 20 MHz. In prior studies in 3GPP, it was recognized that one of the effective complexity reduction techniques for MTC UEs is to specify support of UEs with reduced Bandwidth (BW) capability. In this regard, two main candidates to realize reduced BW capability were considered.

The first candidate involves reduction of the supported BW to 1.4 MHz for DL and UL only for the baseband while the RF engine still supports up to 20 MHz frequency. This can realize most of the cost reduction benefits from BW reduction by requiring reduced sizes for FFT/Inverse Fast Fourier Transformation (IFFT) blocks and lower complexity baseband receiver blocks in the baseband. About 28 percent cost savings, with respect to a Category 1 UE, was estimated for this option.[22]

The second candidate involves reduction of the supported BW for DL and UL to 1.4 MHz for both baseband and RF. In addition to the benefits of the first option, this primarily helps reduce power consumption as a fewer number of subcarriers needs to be processed at the RF and converted to digital domain for baseband operations. In terms of cost savings, depending on implementation assumptions and optimizations, this option was reported to provide about 20 percent to 30 percent savings in RF transceiver design including Low Noise Amplifiers (LNAs), mixer and local oscillator (LO). Overall, an average of about 39 percent cost saving was estimated compared to a Category 1 UE.[23]

As part of Rel-13 enhancements for LTE-based MTC, it has been agreed to support the second option above (i.e., the new low complexity MTC UEs need to support only a reduced BW of 1.4 MHz for both baseband and RF with the ability to retune its carrier frequency from one narrow-band region within the larger system BW to another).

While reduced bandwidth support can enable significant reduction in device complexity and device power consumption, the system design and operation for these MTC UEs needs to address the deviation from the capabilities of LTE devices defined up until Rel-12 specifications. Specifically, it would not be possible for Category M devices to receive legacy DL control channels (legacy Physical Downlink Control Channel (PDCCH), Physical Control Format Indicator Channel (PCFICH), Physical Hybrid Automatic Retransmission Request Indicator Channel (PHICH) that are transmitted in a wideband manner) (i.e., they are transmitted across the entire span of the LTE system bandwidth for a particular deployment). To address this, certain solutions are being adopted, including defining a new DL physical control channel (called Physical Downlink Control Channel for MTC (M-PDCCH)) based on the existing Enhanced Physical Downlink Control Channel (EPDCCH) for Category M UEs. Unlike PDCCH, PCFICH and PHICH, EPDCCH is not a wideband physical channel and hence, is a suitable candidate to carry the physical DL control channel information for Category M devices with reduced bandwidth support. Additionally, a finite amount of retuning time of about one to two Orthogonal Frequency Division

---

[22] 3GPP TR 36.888.
[23] *Ibid.*

Multiplexing (OFDM) symbols (spanning approximately 143 μs) needs to be accommodated whenever the UE needs to retune from one 1.4 MHz narrow-band region to another within the system BW. For instance, a UE may be allocated resources to monitor for DL transmissions on a set of six Physical Resource Blocks (PRBs) (spanning 1.4 MHz) at the edge of the system BW but may need to retune to the central 72 subcarriers in order to perform neighbor cell synchronization and measurements or for serving cell time-frequency resynchronization or Primary Broadcast Channel (PBCH) reacquisition. This can be enabled by possible introduction of short time gaps in the reception or transmission ability during which the UE will not be expected to receive or transmit radio signals.

5.3.2.2 FURTHER REDUCTION OF PEAK DATA RATES

For Category M UEs, the peak data rate for common control message transmissions (SIB, RAR and paging messages) is reduced from 2.216 Mbps to 1 Mbps. This implies that for common control messages, the maximum TBS supported would also be 1000 bits (i.e., the same as for unicast data). While handling simultaneous reception of multiple unicast and/or broadcast Transport Blocks (TBs) in cases where the total TBS carried by all scheduled PDSCH exceeds the UE's processing capability, it is left up to UE implementation for Category 0 UEs; Category M UEs are not required to support simultaneous reception of multiple unicast and/or broadcast TBs in either normal or enhanced coverage. Explicit removal of such requirements of simultaneous reception of multiple TBs helps simplify UE buffering requirements and provisioning for increased processing complexity. The need to define necessary prioritization rules in cases of conflicts between certain unicast and/or broadcast messages is being evaluated.

5.3.2.3 SUPPORT OF REDUCED MAXIMUM TRANSMISSION POWER

Another technique for cost reduction includes support of reduced maximum transmission power for the UL from 23 decibel-milliwatts (dBm) to 20 dBm in order to enable integrated Power Amplifier (PA) implementation. It is expected that both options of maximum transmission power of 23 dBm and 20 dBm are to be supported from a specifications perspective with the final choice left up to device implementation. Use of integrated PA as opposed to dedicated PA implementation can be expected to provide cost savings. Additionally, reduction of the maximum transmission power can facilitate reduced power consumption due to a potential decrease in the DC power consumption. A consequence of reducing the transmission power is reduction in the UL coverage that is expected to be compensated using coverage enhancement techniques.

5.3.2.4 ADDITIONAL COMPLEXITY REDUCTION TECHNIQUES

In addition to the above design elements to reduce device complexity, various other design considerations to help reduce both the device complexity and cost are being considered as part of Rel-13 enhancements for MTC. Some of these include simplification of the requirements on radio link quality measurements and reporting, potential reduction in the number of HARQ processes from the current value of eight for unicast data reception/transmission, reduction in the number of blind decoding attempts that an MTC UE may need to make for receiving the M-PDCCH, reduction in the number of DL Transmission Modes (TMs) that an MTC UE needs to support, among others.

Simplifications in terms of reduced number of measurement and reporting instances compared to a Category 0 UE are currently being evaluated and discussed in the 3GPP RAN WGs. These include measurements and reporting related to Channel State Information (CSI) feedback (e.g., Channel Quality

Information (CQI), Precoder Matrix Information (PMI) and Rank Indicator (RI) which may be used at the eNodeB for user scheduling for the DL). For instance, it has been agreed that reporting of RI is not needed for MTC UEs and that periodic CSI feedback need not be supported, at least when the UE is operating with a large amount of coverage enhancement. In general, considering the decreased measurement accuracy due to reduced BW capability, reduced mobility characteristics for various IoT applications and potential operations in enhanced coverage, the benefits of periodic Channel State Information (CSI) feedback may not be attainable in practice. Instead, the eNodeB performs scheduling based on aperiodic CSI feedback triggered either by the eNodeB or by the UE. Simplifications are also being considered for Radio Resource Management (RRM)-related measurements and reporting (e.g., Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ) reports which are used for mobility management and hand-over purposes).

Reduction in the number of HARQ processes and support of techniques like Limited Buffer Rate Matching (LBRM) for HARQ combining can help reduce the buffering requirements for DL reception.

For more information on the design elements for MTC in Release 13, reference the 4G Americas white paper, *Mobile Broadband Evolution Towards 5G: 3GPP Rel-12 & Rel-13 and Beyond.*[24]

5.4   POWER MANAGEMENT INNOVATIONS FOR LTE MTC DEVICE IMPLEMENTATIONS

Specifying solutions aiming to reduce device power consumption for MTC applications has been identified as an important objective for the ongoing work on further physical layer enhancements for LTE-based MTC.

One of the most basic approaches to reduce device power consumption is to reduce the active transmission or reception times for the UE. Others include complexity reduction techniques like simplification of measurements and reporting requirements, a reduced BW capability at both baseband and RF and the number of blind decoding attempts a UE needs to make to receive DL control channel, among others. Thus, purely at the physical layer, while there may not be many techniques that unilaterally aim to reduce power consumption, the design of complexity reduction and coverage enhancement techniques should be developed carefully with sufficient focus on reducing device power consumption.

As an important example, for Category M UEs and other UEs operating in enhanced coverage, the System Information Block (SIB) that carries common control information from the cell is transmitted without dynamic scheduling using DL control channel. This feature is expected to be supported in 3GPP Rel-13 as part of eMTC. Instead, the scheduling information including time/frequency resources, Modulation and Coding Scheme (MCS) and Transport Block Size (TBS) used for transmitting the different System Information (SI) messages are to be indicated potentially using a combination of information in the Master Information Block (MIB) carried by the Physical Broadcast Channel (PBCH), information in the MTC SIB Type 1 (for scheduling information regarding SI messages carrying other MTC SIBs) and using predefined rules defined in the specifications. This enables an MTC UE to avoid decoding many repetitions (especially if the cell supports enhanced coverage operations) of the DL control channel to obtain the scheduling information for the SI messages, thereby saving device power. Further, it has been agreed to branch out from the legacy SIBs to define new "MTC SIBs" with the aim of defining only the most necessary information and parameters needed for MTC UEs so as to reduce the size of MTC SIBs to the bare minimum. Such efforts are directly aimed towards minimizing device power consumption and increasing the resource utilization at the system-level.

---

[24] *Mobile Broadband Evolution Towards 5G: 3GPP Rel-12 & Rel-13 and Beyond*, 4G Americas, June 2015.

Two other Media Access Control (MAC) layer techniques are directly applicable towards enabling reduced UE power consumption. The first is Power Saving Mode (PSM) that has already been introduced as part of Rel-12 enhancements to LTE, while the second being specified is support for extended Discontinuous Reception (eDRX), a feature that is currently being developed in the 3GPP RAN WGs.

PSM is similar to a powered-off state, with the exception that the UE still remains attached to the network and there is no need to re-attach or re-establish Packet Data Network (PDN) connectivity. Accordingly, the Access Stratum (AS) at the device is turned off, implying that the baseband and RF engines can be powered off as well and the UE would not have to monitor for paging messages or perform any RRM measurements. Thus, significant power consumption reduction can be possible with the use of PSM for devices with infrequent MTC traffic (e.g., a few hundreds of bytes transmitted per day or every few hours). Figure 5.2 shows a representative power consumption profile for a device supporting PSM with estimates for battery lifetimes for PSM assuming different current drain based on currently available technology (referred to as "Short-term forecasts") and considering future enhancements to silicon and battery technology (referred to as "Long-term forecasts").
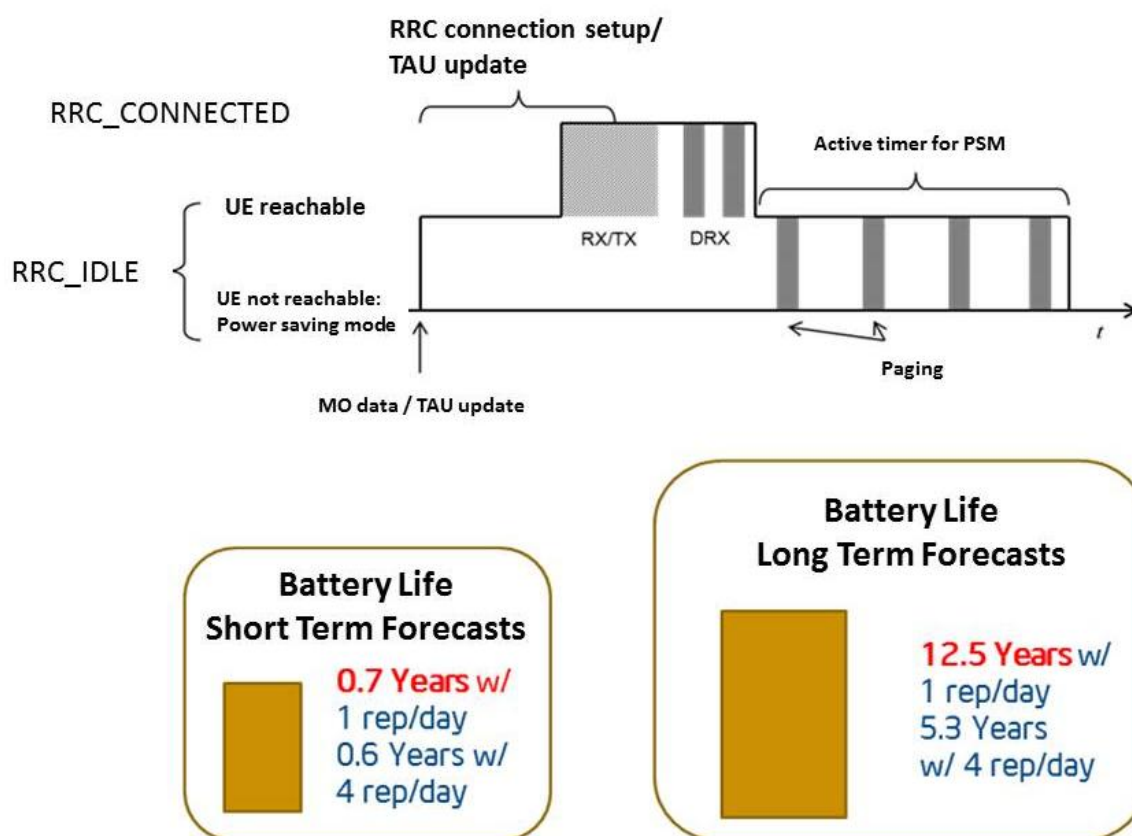

Figure 5.2. Schematic showing device power consumption states and battery lifetime estimates for PSM.

During this period of "deep sleep" state, the UE can wake up on its own based on mobile originated traffic, while it would not be possible for the network to reach a UE using PSM for mobile terminated traffic unless it is in Radio Resource Control (RRC)_IDLE mode after a period of "active time". Alternatively, the network needs to wait for the UE to wake up based on any instance of mobile originated traffic.

One challenge with PSM is that frequent UE reachability in the DL is not possible while the UE is in PSM, the duration of which is in the range of the periodic Tracking Area Update (TAU) frequency. This can significantly affect the latency performance for mobile terminated traffic. While the periodic TAU can be configured to occur more frequently to match the UE's delay requirements, such an approach introduces additional signaling overhead from unnecessary periodic TAU procedures and increased UE power consumption.

To augment the PSM feature, eDRX is being developed that enables significantly long DRX durations, (e.g., ~80 seconds) that can provide similar power consumption reduction compared to PSM. At the same time, the eDRX cycle can be flexibly adjusted to trade-off between power consumption reduction and various delay requirements for mobile terminated traffic without imposing additional signaling overhead.

5.5   OVERVIEW OF CATEGORY 0, 1 AND M LTE MTC DEVICES

As mentioned in Section 5.1, LTE and LTE-Advanced offer multiple categories of UE that can be suitable for MTC or cellular IoT applications. These include Category 1, Category 0 and Category M (to be specified in Rel-13) UEs as low complexity devices.

Category 1 UEs are the lowest complexity legacy LTE UEs that have been introduced since LTE Release 8. Subsequently, Category 0 and Category M UEs provide further device complexity reduction with respect to Category 1 UEs. The key attributes to facilitate such complexity reduction were discussed in Section 6.3. In Table 5.2, a summary of the technical characteristics of these low complexity devices is presented.

Table 5.2. Summary of LTE-Based MTC devices: Category 1, 0, and M.

	Cat1 – 2 RX	Cat1 – 1 RX	Rel-12 Cat0	Rel-13 Cat-M
DL peak rate	10 Mbps	10 Mbps	1 Mbps	1 Mbps
UL peak rate	5 Mbps	5 Mbps	1 Mbps	1 Mbps
Spatial rank	1	1	1	1
# RX	2	1	1	1
Duplex mode	Full duplex FDD/ HD-FDD (optional) / TDD	Full duplex FDD/ HD-FDD (optional) / TDD	Full duplex FDD / HD-FDD (optional)/ TDD	Full duplex FDD / HD-FDD (optional)/ TDD
UE maximum TX/RX bandwidth	20 MHz	20 MHz	20 MHz	1.4 MHz
Maximum TX power	23 dBm	23 dBm	23 dBm	Optional between: 20dBm or 23 dBm
3GPP target complexity	100%	50% < X% << 100%	50%	25%

As indicated in Table 5.2, the device complexity declines with the reduction in the number of reception antennas, and further, with other simplifications and reduced requirements including reduction in the supported data rates for DL and UL, simplified duplex operation and reduced bandwidth support among others. The complexity is estimated to be as low as 25 percent compared to a Category 1 MTC UE.

Given the reduced transmission and reception capabilities of Category 0 and M, it is necessary that these UEs can be identified by the network appropriately and at the same time, the network must have the ability to control access to the network and indicate network support for such low complexity UEs. While the detailed mechanisms for Category M UEs are currently under discussion in 3GPP working groups, various enhancements have been specified that include allowing an LTE eNodeB to broadcast information in support of Category 0 UEs and facilitate identification of Category 0 UEs at the network side.

The network broadcasts support of Category 0 UEs in the System Information Broadcast Type 1 (SIB1) message. Accordingly, a Category 0 UE may access the cell only if the SIB1 message includes the *category0Allowed* Information Element (IE), otherwise the UE considers the cell as barred. Such mechanisms allow the eNodeB to control access to the network resources for MTC UEs with minimal impact on the signaling overhead and device power consumption.

For initial device identification, a Category 0 UE indicates its device category information during the initial Radio Resource Control (RRC) connection setup as part of the Random Access (RA) procedure. This enables the serving cell to identify that such UEs should not be granted with resources for UL data transmissions with transport block sizes beyond 1000 bits. Further detailed level of identification and UE capability information is provided by the UE in response to UE capability request from the serving cell. Table 5.3 summarizes LTE MTC features by 3GPP release.

Table 5.3. Summary of LTE MTC features by 3GPP release.

	Cost/Complexity Reductions	Power Management	Deeper Coverage
Release 12	Cat-0	PSM	None
Release 13	Cat-M	eDRX Simplification of measurements and reporting requirements	+15-20 dB

5.6   EVOLUTION OF LTE MTC FOR 5G RADIO ACCESS

As part of the discussion on the application of LTE-based MTC solutions to Cellular Internet of Things (CIoT) use cases mentioned in Section 5.2, further evolution of LTE MTC beyond Category M UEs is expected.

A possible evolution of LTE-based MTC developed in Release 13 could be a Narrowband-LTE (NB-LTE) design; wherein a Narrowband (NB) system with a maximum of 200 kHz bandwidth could be considered for both DL and UL. Such NB-LTE systems may be deployed in re-farmed GSM bands or in LTE guard-bands, or even as "in-band" deployments within existing LTE system bandwidths. The last realization can

be achieved by allocating a single LTE PRB in a frequency domain spanning 180 kHz to operate the NB-LTE system. Additionally, such multiple NBs can be defined at the system level for system scalability to address a large number of CIoT devices. Thus, the NB-LTE solution can be seen as a near-future evolution of the present LTE-based solution of Category M devices. NB-LTE devices would only need to support a maximum of 200 kHz bandwidth compared to 1.4 MHz bandwidth support required for Category M devices.

Further enhancements to RAT design for support of a massive number of MTC devices or to address mission critical MTC applications can be expected as part of 5G radio access technology development. As part of massive MTC support, an extremely large number of CIoT devices, potentially on the order of a few million devices per square kilometer, would need to be supported. Ultra-low energy consumption that can enable more than ten years of battery life is another expected target. To address such technical requirements, various design considerations ranging from optimizations to basic physical layer numerology like subcarrier spacing and TTI duration to the introduction of new technology features need to be considered. Some such new features may include introduction of lightweight connection-less Layer 2 and Layer 3 protocols, non-orthogonal multiplexing to support a large number of devices, grant-less UL transmissions for small packet transmission to minimize signaling overhead, and use of capillary networks to enable traffic offloading, coverage extension and to facilitate a simplified protocol stack. For the last example, such capillary networks may include Device-to-Device (D2D)-assisted MTC that can address the needs of future wearables and health monitoring systems. Specifically, the wearables or health monitoring sensors may only support a very simple protocol stack and communicate only with an aggregator node (e.g., a smartphone or a smart watch) with the latter forming the gateway or capillary to the Internet cloud via the infrastructure network.

Another dimension of the future evolution of MTC solutions in next generation cellular systems involves the support of MTC applications that require extremely low latency performance, ultra-high reliability, and depending on the application, a diverse range of low to high packet data throughput. Such mission critical MTC applications include use cases like industrial automation wherein ultra-high reliability and ultra-low response times are essential. In the domain of mobile healthcare, telepresence-based use cases like that of a "moving ambulance" or remote surgery fall in this category.

The "moving ambulance" use case aims to provide life-critical treatment and minimize delays while in transit from incident location to the hospital. According to this use case, ambulances are connected to the hospital and start transmission of medical data and test reports that may include high-resolution images and/or video transmissions (e.g., tele-ultrasonography). Additionally, real-time feedback from the hospital regarding the medical treatment while inside the ambulance would be necessary. Thus, for such applications, technical requirements may include moderate-to-high UL data throughput, end-to-end low latency and enhanced mobility support.

Another example involving real-time control and tactile feedback includes the use case of remote surgery as a specific example of remote object manipulation. For such use cases, technical requirements may be expected to include very high reliability of the order of 10^{-9} Packet Error Rate (PER), ultra-low latency of the order of sub-milliseconds, high availability in indoor and outdoor environments and high throughput requirements similar to that of real-time video streaming. It should be noted that such applications may be less sensitive to device cost and solutions relying on usage of large bandwidth and very short symbol time may be considered.

In summary, while significant progress has already been made in the domain of Cellular IoT support based on LTE with the introduction of low complexity device categories like Category 0 and Category M UEs, a considerable amount of research and development work is still needed to define solutions based

on 5G cellular technology for MTC use cases. Such efforts would be necessary in order to truly exploit the potential of IoT and ubiquitous connectivity for different types of devices covering verticals like industrial automation, public safety, healthcare, infotainment and electronic commerce.

6 ENABLEMENT OF IOT COMMUNICATIONS

In addition to the selection of suitable end point devices, for the successful planning, design, implementation and lifecycle management of end-to-end IoT solutions, there are many important elements including:

- Access and concentrator devices
- RAN
- Core network infrastructure
- Connectivity platforms
- The layer that provides enablement of IoT applications

The enablement of the IoT application layer will represent a significant portion of the end-to-end IoT value chain as it provide tools for additional monetization of an IoT solution. With the diversity of things, people and applications involved in this domain, capabilities for searching, eventing, sharing and interacting in a very efficient and web-oriented way are keys to success.

Optimization of the utilization of available resources, depending upon the type of the traffic is another important aspect for IoT solutions. One interesting approach is through so-called "policy driven IoT communication".

In the following sub-sections, a summary of some of the elements of the layer in charge of enablement of IoT applications such as discovery via search engines, interactions of IoT solutions with social networks and policy driven communications in IoT is provided.

6.1 DISCOVERY OF DATA, SERVICES AND APPLICATIONS VIA SEARCH ENGINES

Given the diversity and scale of the models in IoT, it is important to be able to access and search different types of catalogs. It is also key to carefully handle permission and privacy, so at the end of the day each user and partner has his or her own virtual catalog view of discoverable things, data streams, services and applications (see Figure 6.1). In this approach, API access control and rules management is fundamental.
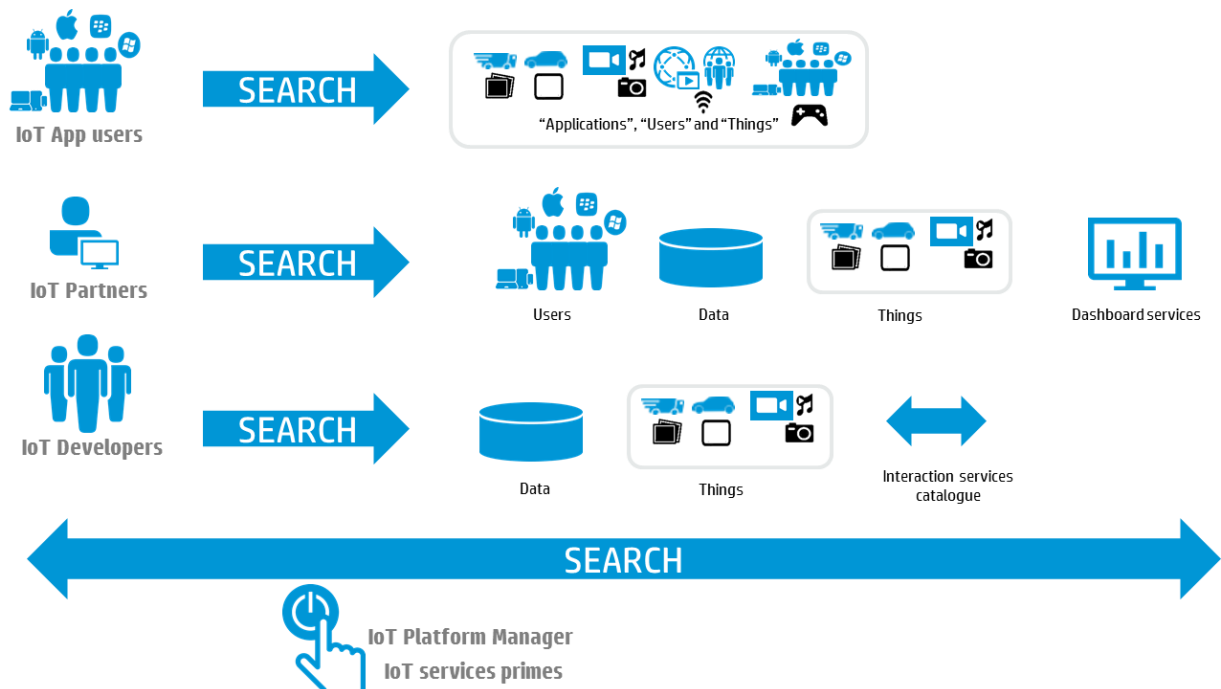
Figure 6.1. Discoverable things: Data streams, services and applications.

All of this needs to be made available through simple web Graphical User Interfaces (GUIs) as well as APIs as management functions for different stakeholders to be able to leverage the search capability from their own app and web environment.

6.2 INTERPLAY BETWEEN IOT AND SOCIAL NETWORKS

The digital economy is largely based on sharing. The notion of sharing and interacting through social networks can be seen from different angles in the IoT context:

- Sharing IoT information on a social network based on specific triggers, rules and permissions (e.g., automatically share your home presence sensor status change with family members)

- Handling a personal network of things and people like a social network on its own (e.g., different sensors registered in your home as well as in your car and on your smartphone, and you have specified which family members and friends can see which object or send instructions to which object). This is illustrated in Figure 6.2 below.
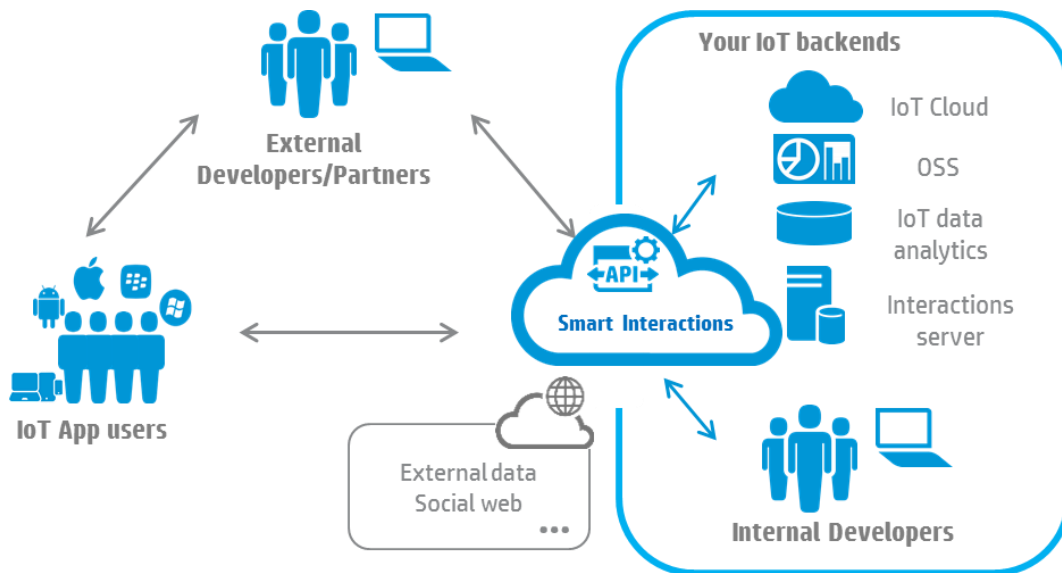
Figure 6.2. Smart interactions.

The top value of IoT is where the user experience for connected things is seamless with services spanning across various IoT ecosystems, verticals and social networks (existing and purpose built). An example of the deployment for interaction of social networks and IoT is detailed in Figure 6.3.
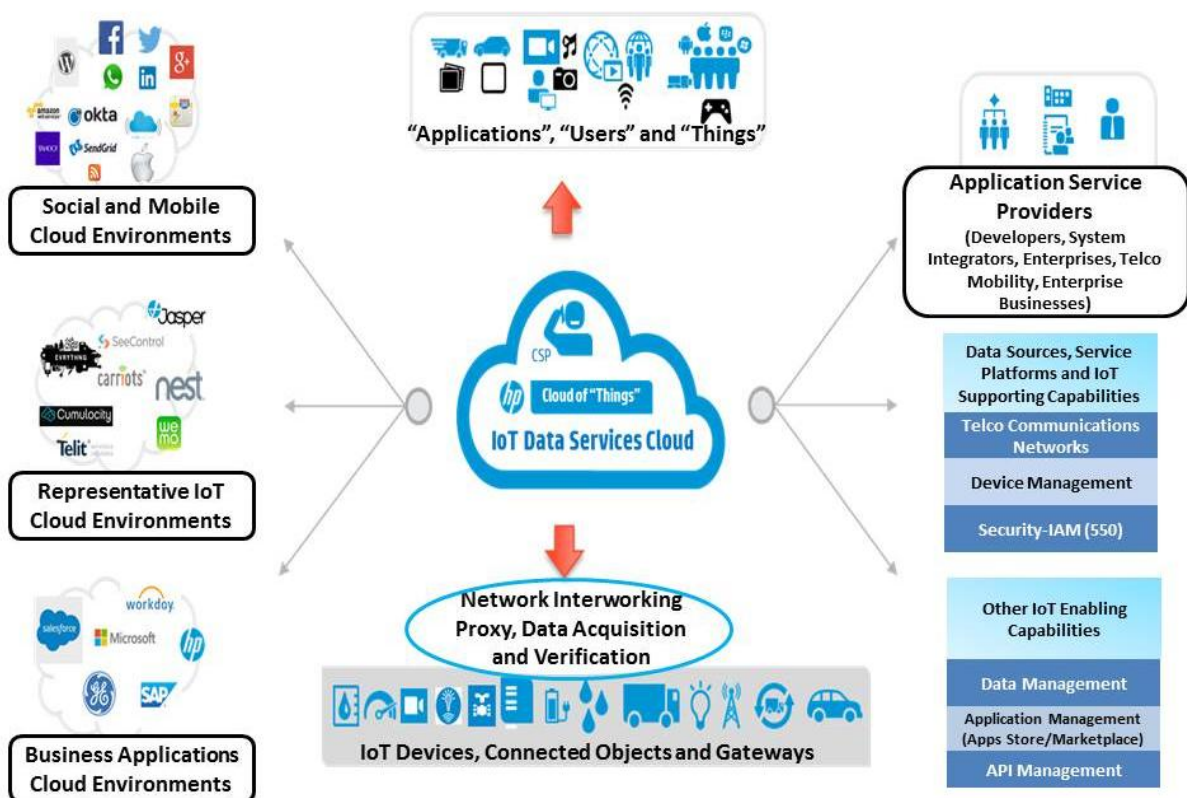

Figure 6.3. IoT data service cloud as enabler for interaction between social networks and IoT[25]

---

[25] DSC Solution, HP.

6.3   POLICY DRIVEN COMMUNICATIONS IN IOT

The industry needs the means to protect network resources and control of when and which type of IoT communication is heavily consuming network resources. The key word is "policy-driven communications". In the future, the industry needs to be able to define with greater granularity which traffic gets transported over which resources. Otherwise, connecting billions of devices will not become a reality or networks may either get congested and/or the IoT might create too much cost.

To prevent network overload, IoT service providers and underlying network service providers should have the appropriate means to control network usage by developing communication policies, which also provides the consumer with IoT services that have the flexibility to balance cost and communication efficiency needs.

To enable policy-driven communications, IoT applications should assign each individual IoT message a set of characteristics in terms of, e.g., delay tolerance, lifespan, priority level or Event Category and criticality of data loss. These characteristics then can be exploited by the policy enforcement scheme of the IoT system.

IoT devices capable of access fixed and/or mobile systems, and possibly capable of choosing between different network access technologies, should be provisioned with a set of policies which generally define constraints on network usage. Such policies may be differentiated depending on Event Category/priority associated with the message. Delay-critical high priority messages will still be transferred as fast as possible, while low-priority messages can be delivered at a suitable time at the lowest cost for the entity (organization or individual user) charged for the network services.

Policy-driven communications typically rely on efficient Store-And-Forward mechanisms which make use of the following concepts:

- Schedules which define when access to which available network is permitted and at what cost

- Aggregation of messages addressing the same destination, taking into account possible constraints on the maximum or minimum size of the data unit to be transferred for each network usage

- Incorporation of dynamically changing network status information (e.g., radio conditions and network load) available to the IoT device.

Policy-driven communications also requires efficient means to provision billions of IoT devices with those policies. This could be done either "out of band" using efficient standard device management technologies or with in-band mechanisms enabled by the employed IoT technology itself. Policies may also be pre-provisioned at the manufacturing stage.

Policies provisioned to the IoT devices may be subdivided into rules for different purposes such as:

- **Defaults:** Defining default characteristics applicable to IoT messages which do not indicate any special characteristics (in order to keep the message size as small as possible)

- **Limits:** Defining constraints on the message characteristics permitted to be used by an application

- **Network Usage:** Defining the conditions when usage of a specific underlying network is allowed for messages with a given Event Category and e.g., defining back-off parameters in the case the network access fails

- **Buffering:** Defining limits of supported buffer size to be used for storing pending messages with a given event category and their priorities when deletion cannot be avoided

7 IOT STANDARDS DEVELOPMENT

7.1   3ᴿᴰ GENERATION PARTNERSHIP PROJECT (3GPP)

Cellular Internet of Things (CIoT) is a hot industry topic which is creating huge opportunities for mobile network operators to make full use of the emerging IoT market, and there are different dedicated network approaches to solve narrowband IoT connectivity currently bidding for market attention. In support of IoT, 3GPP has been working on all several related solutions and generating an abundance of LTE-based and GSM-based proposals. As a consequence, 3GPP has been developing three different cellular IoT standard- solutions in Release-13:

- LTE-M, based on LTE evolution
- EC-GSM, a narrowband solution based on GSM evolution, and
- NB-LTE, a narrowband cellular IoT solution, also known as Clean Slate technologies

However, in October 2015, the 3GPP RAN body mutually agreed to study the combination of the two different narrowband IoT technical solutions, EC-GSM and NB-LTE, for standardization as a single NB-IoT technology until the December 2015 timeframe. This is in consideration of the need to support different operation modes and avoid divided industry support for two different technical solutions. It has been agreed that NB-IoT would support three modes of operation as follows:[26]

- 'Stand-alone operation' utilizing, for example, the spectrum currently being used by GERAN systems as a replacement of one or more GSM carriers,
- 'Guard band operation' utilizing the unused resource blocks within a LTE carrier's guard-band, and
- 'In-band operation' utilizing resource blocks within a normal LTE carrier.

Following is a brief description of the various standard solutions being developed at 3GPP by October 2015:

LTE-M: 3GPP RAN is developing LTE-Machine-to-Machine (LTE-M) specifications for supporting LTE-based low cost CIoT in Rel-12 (Low-Cost MTC) with further enhancements planned for Rel-13 (LTE eMTC). LTE-M supports data rates of up to 1 Mbps with lower device cost and power consumption and enhanced coverage and capacity on the existing LTE carrier.

EC-GSM: In the 3GPP GERAN #62 study item "Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things", narrowband (200 kHz) CIoT solutions for migration of existing GSM carriers sought to enhance coverage by 20 dB compared to legacy GPRS, and achieve a ten year battery life for devices that were also cost efficient. Performance objectives included improved indoor coverage, support for massive numbers of low-throughput devices, reduced device

---

[26] 3GPP RP-151621, "New Work Item: Narrowband-IoT (NB-IoT)"

complexity, improved power efficiency and latency. Extended Coverage GSM (EC-GSM) was fully compliant with all five performance objectives according to the August 2015 TSG GERAN #67 meeting report. GERAN will continue with EC-GSM as a work item within GERAN with the expectation that standards will be frozen by March 2016. This solution necessarily requires a GSM network.

NB-LTE: In August 2015, work began in 3GPP RAN Rel-13 on a new narrowband radio access solution also termed as Clean Slate CIoT. The Clean Slate approach covers the Narrowband Cellular IoT (NB-CIoT), which was the only one of six proposed Clean Slate technologies compliant against a set of performance objectives (as noted previously) in the TSG GERAN #67 meeting report and will be part of Rel-13 to be frozen in March 2016. Also contending in the standards is Narrowband LTE Evolution (NB-LTE) which has the advantage of easy deployment across existing LTE networks.

Rel-12 introduces important improvements for M2M like lower device cost and longer battery life. Further improvements for M2M are envisioned in Rel-13 such as enhanced coverage, lower device cost and longer battery life. The narrowband CIoT solutions also aim to provide lower cost and device power consumption and better coverage; however, they will also have reduced data rates. NB CleanSlate CIoT is expected to support data rates of 160bps with extended coverage.

Table 7.1 provides some comparison of the three options to be standardized, as well as the 5G option, and shows when each release is expected to be finalized.

Table 7.1. Comparison of 3GPP IoT proposals.

	LTE-Evolution	Narrowband Solutions		Next Generation
	LTE-M Rel-13	**NB-LTE Rel-13**	**EC-GSM Rel-13**	**5G**
Range (Outdoor)	< 11 km	< 15 km	< 15 km	< 15 km
MCL	156 dB	164 dB	164 dB	164 dB
Spectrum	Licensed (7-900 MHz)	Licensed (7-900 MHz)	Licensed (8-900 MHz)	Licensed (7-900 MHz)
Bandwidth	1.4 MHz or shared	200 kHz or shared	2.4 MHz or shared	shared
Data Rate	<1 Mbps	<150 kbps	10 kbps	<1 Mbps
Battery Life	>10 years	>10 years	>10 years	>10 years
Availability	2016	2016	2016	2025

7.2 OPEN MOBILE ALLIANCE (OMA)

The Open Mobile Alliance (OMA) has focused on enabling IoT devices by providing protocols to connect and manage IoT devices and its applications. Light-Weight Machine-to-Machine (LWM2M) and device management protocols are relevant for the IoT area.

7.2.1 OMA LIGHT-WEIGHT MACHINE-TO-MACHINE

The OMA LWM2M (Light-Weight Machine-To-Machine) protocol provides the capability for applications to communicate and manage IoT devices. LWM2M is based on the Internet Engineering Task Force (IETF) Constrained Application Protocol (CoAP) providing communication between a LWM2M Server and a LWM2M client (where the client is located in a constrained IoT device). The core interfaces between the server and the client are categorized into:

- Bootstrap
- Client registration
- Device management and service enablement
- Information reporting

OMA LWM2M is unique in the aspect that it converges both management and application control functionality within one communication session allowing for efficient handling of IoT devices. Since OMA LWM2M protocol is based on IETF CoAP, the OMA LWM2M protocol allows different transport bindings (e.g., User Datagram Protocol (UDP), Short Message Service (SMS)) and is secured using IETF DTLS protocol.

The device management features defined by OMA for release 1.0 of LWM2M are:

- Software management for applications inside the client
- Lock and wipe of the device from misuse
- Connection management for choosing various radio methods by the client
- Device capability management to identify the capabilities existing in the device
- Gateway introduction between the server and device

The object registry provides a unique way of identifying the necessary and relevant objects. The object registry is maintained by Open Mobile Naming Authority (OMNA). It includes categories for interleaving 3rd party management objects and application objects into the OMNA system from vendors and other standards organizations (e.g., Internet Protocol for Smart Object (IPSO) Alliance and oneM2M).

7.2.2 OMA M2M INTERFACE

The OMA M2Mi (M2M interface) defines requirements between LWM2M server and the M2M Service layer. These requirements establish practices and guides interactions for management of IoT devices.

The requirements for the M2M interface are defined for the following areas:

- Security
- Session establishment
- Session operations
- Events

- Resource discovery

7.2.3 OMA DEVICE MANAGEMENT

The OMA Device Management (OMA-DM) protocol is well established in the market and is used in over two billion mobile devices. The OMA-DM protocol is suitable for non-constrained IoT devices.

The following OMA-DM enablers are relevant for the management of IoT devices:

- **Software Management** (OMA-DM SCOMO) allowing not only the installation and the removal of applications on the mobile, but also the retrieval of the inventory of software components already installed on the device

- **Diagnostics and Monitoring** (OMA-DM DiagMon MO) which enables remote diagnostics, e.g., to query the device for memory and battery status or to collect radio measures and QoS parameters, and remote monitoring by defining trap and reports

- **Connectivity** (OMA-DM ConnMO) which allows the configuration of bearers and proxies

- **Device Capabilities** (OMA-DM DCMO) which allows a management authority to remotely enable and disable device peripherals like cameras, Bluetooth, USB, etc.

- **Lock and Wipe** (OMA-DM LAWMO) which allows for remotely locking and/or wiping the device, for instance, when the device is stolen or sold, or when personal or enterprise data are compromised

- **Browser** (OMA-DM BMO) which allows remote management of browser favorites and settings

- **Virtualization** (OMA-DM VirMO) which enables remote management of virtual machines running on the device

- **Management Policy** (OMA-DM Management Policy MO) which allows the deployment of policies to the device which the DM client can execute and enforce independently; if some events happen, then some operations may be performed

- **Gateway Functionality** (OMA-DM GwMO) which allows an OMA-DM server to manage devices that:
    - are not directly accessible, for example, because they are deployed behind a firewall
    - can be clustered in a group, for instance, when they are deployed in a very large number (like sensors) using fan out mechanisms
    - support other management protocols than OMA-DM (like Zigbee, Bluetooth etc.)

7.3 GSM ASSOCIATION (GSMA)

The GSMA spearheads a key initiative known as the Connected Living program. This is aimed at helping operators to add value and accelerate the delivery of new connected devices and services in the IoT market. This is achieved by industry collaboration, appropriate regulation, optimizing networks as well as developing key enablers to support the growth of IoT in the immediate future and IoT in the longer term.

The GSMA's basic vision is to enable IoT where consumers and businesses enjoy rich new services, connected by an intelligent and secure mobile network.

The Internet of Things is dependent on the efficient and intelligent use of the mobile network. The GSMA develops connection efficiency guidelines ensuring that IoT device and application developers can follow a common approach to create efficient, trusted and reliable IoT services that can scale as the market grows.

The connectivity of billions of IoT devices in a scalable network depends on all stakeholders following a common approach, ensuring everyone can enjoy the benefits of efficient connectivity. The GSMA works with the IoT ecosystem to establish guidelines on how machines communicate via the mobile network in the most intelligent and efficient way.

One of the major contributions of the GSMA is its Embedded SIM Specification for remote M2M provisioning. The GSMA Embedded SIM Specification is geared towards accelerating growth and operational efficiency in the M2M/IoT world. The GSMA's Embedded SIM technical specification enables the remote provisioning and management of embedded SIMs to allow the "over the air" provisioning of an initial operator subscription and the subsequent change of subscription from one operator to another.

The GSMA is also engaged in another effort to establish common capabilities among mobile operators to enable a network that supports value creation for all stakeholders. These capabilities include security, billing and charging and device management which can enhance the Internet of Things by enabling the development of new services.

7.4   oneM2M

oneM2M is a global standards organization for M2M and IoT established by the European Telecommunications Standards Institute (ETSI) to develop an IoT architecture and standard for M2M communication across different sectors and industries such as telematics and intelligent transportation, healthcare, utilities, industrial automation and smart homes among others. oneM2M develops technical specifications that "address the need for a common M2M service layer that can be readily embedded within various hardware and software to connect the myriad of devices with all intended M2M application servers worldwide". The oneM2M specifications enable users to build platforms, regardless of existing sectors or industry solutions. It provides a common service framework that can address the common needs of diverse IoT sectors and domains with a common architecture, protocols, security, management, data collection and sharing, abstraction and semantics, and interworking across vertical industry domains.

One of the important elements at the core of oneM2M is to provide an interworking framework. oneM2M facilitates in creating a distributed software layer akin to an operating system which in turn provides a framework to interact between different technologies. The objective of oneM2M is to standardize interfaces to enable interoperability among devices, applications, data collection and storage across geographies and the entire ecosystem.

Essentially, oneM2M develops technical specifications and technical reports for:

- Use cases and requirements for a common set of service layer capabilities

- Service layer aspects with high level and detailed service architecture, in light of an access independent view of end-to-end services

- Protocols/APIs/standard objects based on this architecture (open interfaces and protocols)

- Security and privacy aspects (authentication, encryption and integrity verification)

- Reachability and discovery of applications

- Interoperability, including test and conformance specifications

- Collection of data for charging records (to be used for billing and statistical purposes)

- Identification and naming of devices and applications

- Information models and data management (including store and subscribe/notify functionality)

- Management aspects (including remote management of entities)

- Common use cases and terminal/module aspects including service layer interfaces/APIs between:

  o application and service layers
  o service layer and communication functions

oneM2M issued its Release-1 set of specifications in January 2015. These have been published by various regional standards organizations; including the Alliance for Telecommunications Industry Solutions (ATIS), ETSI, Telecommunications Technology Association (TTA) and Telecommunication Technology Committee (TTC).[27]

In December 2014, oneM2M members, LG U+ and SK Telecom of Korea, both announced that they will make the first commercial deployments of Internet of Things (IoT) platforms based on oneM2M specifications. Solutions using oneM2M technology were demonstrated at various showcase events throughout Europe, the U.S. and Asia in mid-2015.

oneM2M is working on its Release 2 specifications with a focus on advanced security features, generic interworking framework, semantic interoperability, application developer APIs and guidelines, and home domain and industrial domain enablement. One of the new work items in Release 2 is to specify the 'interworking with 3GPP Rel-13 MTC feature'. It provides an interworking standard between oneM2M architecture and 3GPP Rel-13 service capability exposure architecture so 3GPP network capabilities can be utilized by oneM2M architecture with standard interfaces. This is an important work item that binds the IoT service framework to the 3GPP network.

Release 2 of oneM2M is planned for delivery in autumn 2016. In parallel with the development of Release 2, a revised set of Release 1 specifications is in preparation to take account of early implementation experience. These will be released in autumn 2015.

---

[27] http://onem2m.org/technical/published-documents.

7.5   EMERGING TECHNOLOGIES

Within the past five plus years, several new wireless network Radio Access Technologies (RAT) have emerged, primarily to support the demand from IoT devices. One major concern for devices, such as body-worn sensors, embedded devices in buildings and roadways among others is that they will be primarily battery-powered and potentially inaccessible for the duration of their life.

Table 7.1. Current RATs used for IoT.

Technology	Topology	Outdoor	Application	Long Range
802.15.4g/6LowPAN	Mesh	Yes	Smartgrid, Metering, Oil&Gas	No
WirelessHart	Mesh	No	Industrial	No
Zigbee/ZigbeePro	Mesh	No	Smart Home/Building	No
ISA100	Mesh	No	Industrial	No
Proprietary 802.15.4	Point-to-Multipoint	Yes	Smart Parking, Traffic	No
Enocean	Mesh	No	Building Automation	No
StarSense RF	Mesh	Yes	Smart Lighting	No
Z-Wave	Mesh	No	Smart Home	No

This means that devices need to be designed with a multi-year (10+) battery life while retaining the requirements of security and data-processing for their application.

Wide-area coverage is also a requirement. Many existing low-power wireless solutions can only provide very localized coverage, meaning that overlay networks with access-points close to the devices must be built in parallel to the existing MNOs. Many times, this is not a practical solution.

While the cellular 2G/3G/4G solutions can provide wide-area coverage, this tends to be at the cost of short battery-life on the devices; typically the mechanisms used to support the rapid mobility required in cellular networks causes issues with current consumption.   IoT devices are mobile in that they will move to a particular location or require re-homing to a different serving node on cell-division, but they do not require the rapid cross-cell mobility that a car or other fast-moving UE does.

IoT devices are therefore characterized as having low mobility, long battery life, low amounts of data, low throughput requirements and very low devices costs; quite a different set of requirements (see typical set for end point device requirements for IoT use cases in Table 7.2) from the requirements on typical smart-phone.

Table 7.2. Typical set for end point device requirement for IoT use cases.

Characteristic	Order of magnitude	Typical value
Spectrum	Unlicensed/Light Licensed	<1GHz, 2.4/5 GHz
Range	Long	10's km (w/out relay)
Objects	Many	Many thousands
Data volume	Small	Up 10's kB per day
Data rate	Low	Up to100kb/s
Latency	Low to high	Up to minutes
Battery life	Long	5 to 20 years
Module cost	Low	<$5
Service cost	Low	<$10 per year

Consequently, a number of new LPWA RATs have emerged in the past few years, targeting such IoT devices.

RATs such as Weightless, LoRa and OnRamp Wireless all offer multi-year battery life and long-distance (~10km) operation, usually in Industrial, Scientific and Medical (ISM) bands (868 MHz, 915 MHz, 2.4 GHz) using a mixture of modulation schemes.   "Whole Offer" service providers have also appeared providing wide-area connectivity and data processing. Recently, ETSI has taken action to standardize the LPWA solution under the Low Throughput Networking group.

However, with a proliferation of RATs comes the potential of sub-optimal treatment of data; for example, an application may require the guaranteed service level provided by GPRS or LTE for one set of data, but is comfortable operating in an unlicensed band for day-to-day status reporting.

This gives cellular operators a unique opportunity to own and manage network access over both cellular air interface and the LPWA technologies. The work towards a definition of 5G sees this potential. The University of Surrey's 5G Innovation Centre describes its work towards "…development of a 5G infrastructure capable of providing connectivity for future technologies, including the Internet of Things (IoT), Machine Type Communications (MTC)…"

Whether a reliance on unlicensed spectrum alone, especially given the very small global allocations at 868 and 915 MHz, is enough to provide reliable access to the projected number of IoT devices is an open question; movement towards utilization of TV and other white space plus licensed spectrum access is generally considered to be required, with several standards such as Weightless-W being in trials in conjunction with national Television White Space (TVWS) databases.

Again, this is area where, uniquely, existing cellular operators have the resources and skills to own and manage spectrum.

8 CONCLUSION

The Internet of Things, as a natural evolution of M2M technology and an interconnection of intelligent devices and management platforms, is heading for a major revolution in enabling the "smart world" around us. It is becoming increasingly apparent that the world is evolving extensively using wireless means where millions, if not billions, of devices operate in one large network.

The world is rapidly moving beyond the traditional human-centric applications to an increasing number of machines communicating; examples include surveillance cameras, smart electrical grids, connected homes and intelligent transportation systems. Smart devices and sensor networks are creating a new class of wireless applications where devices are becoming automatically controlled by an unattended machine.

A highly interconnected world involves billions of connected devices that are typically associated with very little traffic; however, the sheer number of connected devices poses a challenge in terms of the need for efficient signaling protocols.

The cellular networks based on LTE technologies with the latest enhancements are gearing up to be capable of handling massive traffic increases while providing the well-known benefits of a ubiquitous presence. Also, numerous advancements in LTE technologies are in order to meet subsidiary challenges of supporting the requirements of IoT communications to a much larger number of devices compared to today.

This white paper addressed the key challenges facing the wireless industry for unlocking the value of securing an interconnected web of devices while meeting the diverse requirements of applications in terms of low power consumption and latencies, wide range of data throughputs and the delivery of robust and high levels of performance. This white paper significantly provides a framework using key building blocks and state of the art technological enhancements in developing innovative IoT solutions. The key framework aspects related to the design of a cellular IoT system which is highlighted in this white paper is summarized as follows:

- Detailed understanding of specific IoT uses cases and/or applications' technical and business requirements

- Applicable functional architecture of an end-to-end IoT solution:

  - Device/gateway models and corresponding management protocol technologies
  - Access and eventual aggregation domain technologies and features leveraged within those like MTC Rel-11 and later
  - Core domain technologies and its features leveraged and considered inclusion of new deployment models like NFV/SDN-based
  - IoT platforms for Value-Added Services (VAS) like device connectivity, service management, AEP/ Application Development Platform (ADP) and others
  - IoT applications interfaces with end-users and enterprise(s) back-office systems
  - Exchange-to-Exchange (E2E) security

- Applicable IoT communication enablement solutions for monetization of IoT via:

  - Discovery of data, services and applications via web search engines

        o   Interplay of particular IoT solutions with social networks like Facebook, Twitter, etc.

LTE continues to evolve as a very flexible platform that is continuously evolving to address new requirements and additional scenarios. 3GPP is currently working on Release 13; this release will improve and enhance LTE in several aspects and strengthen its capacity to serve as a platform for the emerging highly interconnected world by providing data access and sharing anytime and anywhere.

An evolution of LTE technologies and enhancements is presented in this white paper to show how the latest enhancements provide low device cost and energy consumption, the possibility to run on a single AA-type battery for ten years. These are important aspect expectations of the new LTE technology enhancements and MTC features with a focus on Category 0,1 and M devices.

In addition, this white paper provides an overview of IoT standardization efforts and specific focus areas for:

- 3GPP for MTC Rel-11, 12 and 13 radio access and core features
- OMA for LWM2M device management
- GSMA for various IoT/M2M items
- oneM2M for service management
- Various emerging technologies like LoRA, 6LoWPAN. etc.

The emerging 5th generation technologies are expected to address the upcoming future of an even further interconnected world with more sophisticated use cases. The era of massive IoT communications is dawning, where emerging use cases include remote control of door locks and street lights, road sensors for smarter traffic management, tactile and sensory feedback applications.

APPENDIX A: GUIDELINE FOR FORMING AN EFFECTIVE IOT STRATEGY FOR COMMUNICATION SOLUTION PROVIDERS AND ENTERPRISES

While communication service providers are still trying to understand how small, data-only devices are impacting their business, the enterprise, consumer and public sectors are swiftly adopting all kinds of new connected gear, machinery and devices. Here are the key considerations when forming an effective IoT strategy.

FINDING THE RIGHT BUSINESS MODEL

IoT presents a unique opportunity for any organization to expand in the vertical industry it serves. At the same time, non-Telco players are presented with equal opportunities to provide unique applications totally independent of a communication service provider's or by tapping a communication service provider's mainly as a pipe to deliver services to customers.

Due to a wide variety of components and players involved in delivering an IoT service, defining the right business model is one of the biggest challenges in designing and delivering an end-to-end IoT solution. Some of the major designs currently adopted are:

- **Communication service providers-led solution:** These are mostly ad-hoc solutions for specific customer needs using specific sensors and types of connectivity. In this model, communication service providers own the customer experience and take full accountability of designing, installing and managing the solution.

- **Non-Telco led solution:** In this scenario, non-Telco players build a highly productized solution to serve its customers. It manages the entire service on its own and uses communication service providers only as a connectivity service provider. Usually, it is possible to employ multiple types of connectivity from multiple communication service providers to deliver an end-to-end solution.

- **Partnership between communication service providers and non-Telco players:** In this approach, both players jointly design, build and maintain the end-to-end service to meet customers' specific needs, leveraging their independent customer relationship for the common benefit.

Due to the nature of the relationship between communication service providers and their customers as well as an industry's specific needs, some business models are more commonly implemented than others in each domain.
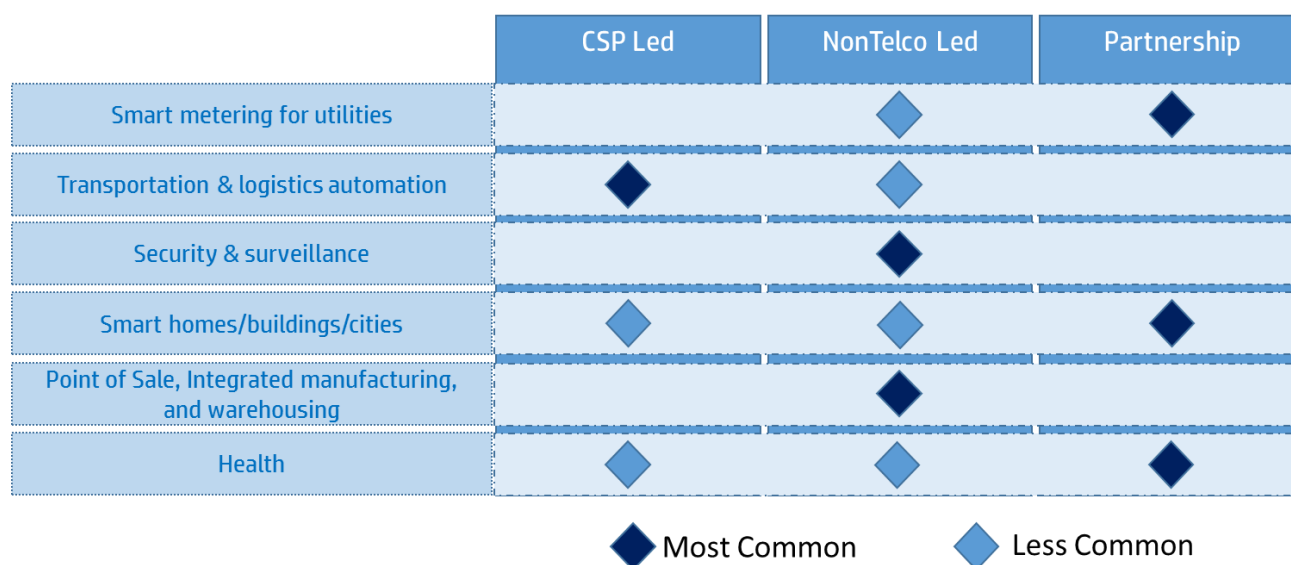
	CSP Led	NonTelco Led	Partnership
Smart metering for utilities		Less Common	Most Common
Transportation & logistics automation	Most Common	Less Common	
Security & surveillance		Most Common	
Smart homes/buildings/cities	Less Common	Less Common	Most Common
Point of Sale, Integrated manufacturing, and warehousing		Most Common	
Health	Less Common	Less Common	Most Common

◆ Most Common   ◆ Less Common

Figure A.1. Common business models per industry verticals.

In many companies' view, the best approach is collaborative. This means working with industry verticals to identify and implement use cases, and with the right business model, it is mutually beneficial to all parties involved.

Working together with industry partners will provide opportunities for everyone—and in particular to communication service providers—to play greater value-add roles. By leveraging the technical know-how and ownership of the underlying infrastructure, communication service providers can become a systems integrator or managed administration provider of IoT applications and services.

The greater the value service providers can add, the greater the share of the revenue they can control. Hence, it is necessary to keep inventing new business models as well as revising existing ones to create new partnerships.

TECHNOLOGY IMPLICATIONS

Traditionally, a communication service provider's key role in the delivery of IoT applications is to be the provider of the connectivity backbone in the form of a SIM card. This helps communication service providers monetize their investments in the underlying cellular access infrastructures such as 2G, 3G and LTE.

However, there are many IoT applications/use cases that require alternative access methods not typically provided by traditional communication service providers. This fact in context of revenue generation has to be taken into consideration as part of the strategy development for IoT by ecosystem players.

Therefore, when it comes to designing their networks, communication service providers must start thinking about alternative access method enablement and the provision of seamless connectivity via multiple access technology. Convergence technologies such as IMS (IP Multimedia Subsystem) and unified access, authentication and charging architecture will become key components in delivering a diverse set of IoT services across multiple industries with varying access requirements.

SECURING IOT SERVICES AND INFORMATION ASSETS

While different components of the IoT ecosystem need to deliver specific applications that may be owned and managed by independent entities, it is extremely important that these entities are integrated in a cohesive manner. This ensures the delivery of a seamless end-to-end service without any impact on the user. It also underscores the importance of security and end-to-end service delivery and assurance for complex IoT services.

Some key security aspects are:

- Using identity management and authentication of the device or sensor

- Securing connectivity

- Managing fraud, such as stolen and switching devices, and blocking illegal use such as voice calls and roaming, among others

MANAGEMENT PLATFORMS

In terms of volumes, margins and the way IoT services are sold, activated, charged for, and supported, it is clear that the traditional BSS and OSS systems may not be the best fit for a communication service provider's IoT strategy. Some important considerations include:

- **OSS/BSS software licensing:** BSS/OSS solutions are mostly licensed per subscription by system vendors. Service providers need to implement dynamic network resource provisioning, such as SIM, to conserve the license capacity

- **SIM lifecycle management:** Traditional mobile, consumer-oriented SIM card lifecycle is not applicable to IoT solutions; therefore, management platforms should require the adoption of IoT-specific lifecycle management with many controls provided to the customer via self-service

- **Device management:** Device/sensor configuration and management solutions require integration with the rest of the OSS

- **Provisioning and activation of IoT services:** Network resource optimization should be considered while activating IoT services in order to avoid unnecessary overloading of communication service provider network and systems

- **Charging and billing:** Real-time charging, policy control and sharing of bandwidth across a customer's IoT solution are necessary requirements for such services and, hence, charging and billing systems must be enhanced and scaled accordingly

- **Fraud management:** IoT requires strengthening of fraud detection to ensure devices/sensors and the underlying infrastructure is not misused intentionally or unintentionally.

- **Resource inventory:** Typically, inventory systems maintain very minimal information about SIM cards; IoT applications require comprehensive modeling of IoT services, underlying infrastructure and resources such as SIMs and devices

- **Self-administration:** IoT services, by nature, demand a much greater degree of self-administration. This can be done in a fully automated fashion or by limited involvement of the customer's IT function, without the involvement of traditional brick-and-mortar support functions. This would require significant reshaping of the architecture and relevant business processes would have to adapt accordingly.

A dedicated and purpose-built IoT platform should be considered to support any IoT deployment. This should cater to the traffic volumes generated by such services without requiring corresponding exponential growth in Total Cost of Ownership (TCO). It should include licenses and infrastructure, enable greater self-administration and provide seamless integration with the customer's own management systems.

3GPP	3rd Generation Partnership Project
6LoWPAN	IP6 Low Power Wireless Personal Area Network
ACG	Automatic Gain Control
ADC	Analog to Digital Convertor
ADEP	Application Development and Execution Platform
ADP	Application Development Platform
AEP	Application Enablement Platform
API	Application Programming Interface
ARPU	Average Revenue Per User
AS	Access Stratum
ATIS	Alliance for Telecommunications Industry Solutions
B2B2C	Business to Business to Consumer
BoM	Bill of Material
BPL	Building Penetration Loss
BSS	Business Support System
BW	Bandwidth
CAGR	Compound Annual Growth Rate
CAR	Centre for Automotive Research
CIoT	Cellular Internet of Things
CoAP	Constrained Application Protocol
CPE	Customer Premise Equipment
CQI	Channel Quality Information
CSI	Channel State Information
CSP	Communication Service Provider
D2D	Device-to-Device
dB	Decibel
dBm	decibel-milliwatts
DHIR	Device Host Identity Reporting
DL	Downlink
DM	Device Management
DTLS	Datagram Transport Layer Security
E2E	Exchange-to-Exchange
eCall	Smart SOS
ECG	Electrocardiogram
EC-GSM	Extended Coverage GSM
eDRX	Extended Discontinuous Reception
eDRX	extended Discontinuous Reception
EGPRS	Enhanced General Packet Radio Service
eNodeB	enhanced NodeB
EPDCCH	Enhanced Physical Downlink Control Channel

ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transformation
GERAN	GSM/EDGE Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSMA	GSM Association
GUI	Graphical User Interface
GW	Gateway
HARQ	Hybrid Automatic Repeat Request
HD-FDD	Half-Duplex Frequency Division Duplex
HTC	Human-Type Communication
IETF	Internet Engineering Task Force
IFFT	Inverse Fast Fourier Transformation
IMEI	International Mobile Station Equipment Identity
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IPSO Alliance	Internet Protocol for Smart Object Alliance
ISM	Industrial, Scientific and Medical
LBRM	Limited Buffer Rate Matching
LPWA	Low-Power Wide-Area Network
LTE-A	LTE-Advanced
LTE-M	LTE-Machine-to-Machine
LWM2M	Light-Weight Machine-To-Machine
M2M	Machine-to-Machine
M2Mi	M2M interface
MAC	Media Access Control
MBMS	Multimedia Broadcast Multicast Service
MCS	Modulation and Coding Scheme
MIB	Master Information Block
MNO	Mobile Service Operator
M-PDCCH	Physical Downlink Control Channel for MTC
MQTT	Message Queuing Telemetry Transport
ms	millisecond
MTC	Machine Type Communications
NB	Narrowband
NB-CIoT	Narrowband Cellular IoT
NB-IoT	Narrowband-IoT
NB-LTE	Narrowband-LTE
NFV	Network Functions Virtualization
OBD	On Board Diagnostic
OFDM	Orthogonal Frequency Division Multiplexing

OIC	Open Interconnect Consortium		RAR	Random Access Response
OMA	Open Mobile Alliance		RAT	Radio Access Technology
OMA-DM	Open Mobile Alliance-Device Management		RF	Radio Frequency
OMA-DM BMO	OMA-DM Browser		RI	Rank Indicator
			ROI	Return of Investment
OMA-DM ConnMO	OMA-DM Connectivity		RRM	Radio Resource Management
OMA-DM DCMO	OMA-DM Device Capabilities		RSRP	Reference Signal Received Power
			RSRQ	Reference Signal Received Quality
OMA-DM DiagMon MO	OMA-DM Diagnostics and Monitoring		SDN	Software-Defined Networking
OMA-DM GwMO	OMA-DM Gateway Functionality		SIB	System Information Block
			SMS	Short Message Service
OMA-DM LAWMO	OMA-DM Lock and Wipe		SRTP	Secure Real-Time Transport Protocol
OMA-DM Management Policy MO	OMA-DM Management Policy		TA	Timing Advance
			TB	Transport Block
OMA-DM SCOMO	OMA-DM Software Management		TBS	Transport Block Size
			TCO	Total Cost of Ownership
OMA-DM VirMO	OMA-DM Virtualization		TLS	Transport Layer Security
OMNA	Open Mobile Naming Authority		TM	Transmission Mode
OSS	Operations Support System		TR-069	Technical Report 069
P2P	Peer-to-Peer		TTA	Telecommunications Technology Association
PA	Power Amplifier		TTC	Telecommunication Technology Committee
PBCH	Primary Broadcast Channel		TTI	Transmission Time Interval
PBCH	Physical Broadcast Channel		TVWS	Television White Space
PCFICH	Physical Control Format Indicator Channel		UDP	User Datagram Protocol
PDCCH	Physical Downlink Control Channel		UE	User Equipment
PDN	Packet Data Network		UL	Uplink
PER	Packet Error Rate		v	Virtual
PHICH	Physical Hybrid Automatic Retransmission Request Indicator Channel		V2C	Vehicle to the Cloud
			V2I	Vehicle to Infrastructure
PLL	Phase Locked Loop		V2P	Vehicle to Pedestrian
PMCH	Physical Multicast Channel		V2V	Vehicle to Vehicle
PMI	Precoder Matrix Information		V2X	Vehicle to Everything
PRB	Physical Resource Block		VAS	Value-Added Service
PSM	Power Saving Mode		WG	Work Group
PSM	Power Saving Mode		Wh	Watt-hour
PTCRB	Personal Communication Service Type Certification Review Board		WWAN	Wireless Wide Area Network
QoS	Quality of Service		XMPP	Extensible Messaging and Presence Protocol
RAN	Radio Access Network			

ACKNOWLEDGEMENTS