3GPP standards to deliver LTE connectivity for IoT

Almudena Díaz-Zayas, Cesar A. García-Pérez, Álvaro M. Recio-Pérez, Pedro Merino
University of Málaga, Andalucía Tech
Málaga, Spain
Email: almudiaz@lcc.uma.es, garciacesaraugusto@lcc.uma.es, amrecio@lcc.uma.es, pedro@lcc.uma.es
http://www.morse.uma.es/

***Abstract*—Nowadays, the maturity of IoT applications, networking technologies and manufacturers of "things" have caused an explosion in the number of connected devices. There are several reports which calculate that the number of connected things will reach 50 billion in the near future. This paper focuses on the provision of wide area and efficient connectivity to the Internet of Things (IoT), a key factor in such an explosion, through the usage of LTE. LTE MTC (Machine Type Communication), LTE M2M or just LTE-M are the coined terms that refer to this issue. This paper provides a detailed analysis of the standardization efforts carried out by the 3GPP to convert LTE into an IoT capable technology.**

I. Introduction

According to [1], by 2020 the number of connected devices, other than cell phones, PCs and tablets, will be 15 billion, of which 13.0 billion will use short range technologies, such as Bluetooth Smart, Wi-Fi or Zigbee, and 2.0 billion will use a cellular connection. However this report estimates that 5.5 of the 13.0 billion would be replaced by a cellular connection if that cellular technology could meet the requirements of the IoT. Moreover, in that case, the incursion in the IoT world of a cellular IoT capable technology would add 5.7 billion of connections, reaching 20 billion of things by 2020. With these numbers, mobile operators and manufacturers have found in IoT a promising market, bringing with it a myriad of promising business opportunities. In fact, IoT devices are able to use PAN, LAN, WAN or cellular networks. Furthermore, the most restrictive IoT device requirements (battery powered, low cost and high autonomy), have influenced the use of wireless technologies such as RFID, NFC, Bluetooth o Zigbee.

However, as reported by the Machina Research report, the adoption of cellular connections in the world of IoT could be a turning point, providing a significant increase in the number of connected things, which will turn cellular technology into the dominant networking option in the IoT. Nevertheless, in order to reach these numbers, mobile broadband networks have to evolve to become compatible with IoT.

Any existing cellular network could be chosen, such as GSM, UMTS or LTE. Until now, GPRS or CDMA2000 have been the technologies chosen to provide wide-area connectivity because they provide higher coverage and lower cost solutions. LTE has the greater potential to shake up the Internet of Things. The flat and flexible architecture of LTE fits perfectly in IoT ecosystems. Moreover, the efficient use of the spectrum of LTE directly translates into lower operating costs, which is key to providing global and cost-effective data connectivity. The original design of LTE didn't address all the needs of IoT. However, according to the roadmap provided in [2], 4G solutions based on LTE Release 12 will improve LTE capabilities so as to support IoT connectivity requirements.

In this paper, we provide a detailed analysis of the improvements promoted by the 3GPP in order to convert LTE into a IoT capable technology and the structural changes that these modifications imply in the current LTE architecture. Table I provides a summary of specific LTE proposals for the improvements in the communication requirements of IoT, introduced in Section II of the paper and the 3GPP standards developed in order to fulfill them. These standards are explained in Sections III and IV.

II. Communication requirements in the Internet of Things

The patterns and requirements of machine to machine (M2M) communication in the IoT are different to those of human to human (H2H) communication in traditional LTE networks. The 3GPP have identified in [4] the following requirements which are specific to M2M communications.

- Addressing. The most usual pattern of communication in the IoT is expected to be many-to-one, in which many devices, sensors for example, periodically transmit data to a central server. In general, the number of devices associated with a particular server can be huge. 3GPP envisions two scenarios: the server may have an IPv6 address, in which case the devices will be assigned IPv6 addresses by the network, or the server may be reachable through an IPv4 address. In the latter case, this address may be public or private but the devices will be assigned a private IPv4 either way, due to the scarcity of public IPv4 addresses.
- The number of required identifiers for the devices in the network is expected to be at least two orders of magnitude higher than for H2H communications. It is therefore necessary to develop a scheme that allows the network to uniquely identify each device and the subscriber to which it belongs.
- Charging. Due to the potentially large number of devices in the network and their intermittent pattern of communication, creating detailed charging records for each device may be wasteful. The 3GPP requires the network to collect charging data with just enough granularity that

978-1-4673-9948-7/16 $31.00 © 2016 IEEE
DOI 10.1109/IoTDI.2015.26

IEEE computer society

TABLE I
SUMMARY OF THE IOT REQUIREMENTS AND ITS IMPLEMENTATION IN LTE

IoT Requirements	LTE Implementation	Related Specifications
Low cost devices	Category 0 devices	3GPP TS 36.306
	Clean radio state design	3GPP TR 45.820
Long battery life	Power saving mode	3GPP TS 23.682
	Device Trigerring	3GPP TS 23.682
Remote provisioning	OMA-DM	OMA Device Management
Flexible device identification	External Identifiers	3GPP TS 23.682
Enhanced Coverage	PSD boosting	3GPP 36.888
	Relaxed requirement	
	Design new channels/signals	
	Repetition	
	Low rate coding	
	Spreading	
	RS power boosting /increased RS density	
	New decoding techniques	
	Device to device communications	3GPP TR 36.843
	ProSe Relay	3GPP TR 36.814
	Heterogeneous access	3GPP TS 23.261
Managing Congestion Control	LAPI flag	3GPP TS 23.483
	EAB	3GPP TS 36.331
	PGW back-off timer	3GPP TS 23.401
	PGW back-off timer	3GPP TS 29.274
Managing Large Number of Subscribers	Broadcast Communications	3GPP TS 23.246
	eUICC	GSMA eUICC
Device Triggering	MTC-IWF	3GPP TS 23.682

it can identify the use of resources outside the limits of the subscription.

- Security. For many applications, the devices in the IoT network face security challenges which are not present in traditional H2H communications. For example, it is not uncommon for many devices to be left unattended after installation, making them potential targets for tampering, theft or destruction. In addition, depending on the scenario, the devices may be an attractive target for malicious entities which could be interested in performing, for example, a denial of service attack on them. The 3GPP requires that optimizations for M2M communications do not degrade security with respect to H2H communications. The network should also provide secure connections between the devices and the servers.
- Triggering. For many use cases, devices in the IoT transmit data only sporadically. Sometimes, data is only transmitted when requested by a server. To optimize these use cases and avoid wasting resources, the network is required to support a device triggering mechanism. This means that the network can request a particular device to establish a connection with its server even when the device is not attached to the network or has not established a data connection.
- Low mobility. In many cases, IoT devices remain stationary for most of their lifetime. For example, power meters, pumps or vending machines remain in the same location once installed. For these devices, location updates and mobility management procedures are irrelevant and waste precious network resources. It is required that the network operator is able to change the frequency of these procedures performed by the devices.
- Time controlled communications. For some applications, it is necessary only to send or receive data at specific time intervals. As in the case of low mobility, regular procedures can become wasteful when performed outside the specified time intervals. Thus, it should be possible for the network operator to either reject or charge differently, any communication taking place outside the predefined time interval and also to alter the time interval according to local criteria such as traffic load.
- Small data transmissions. Many IoT devices need only to transmit only a small amount of data at a time, typically around 1 KB. The network must support the transmission of small amounts of data, providing an optimized procedure with little overhead for this particular use case.
- Infrequent mobile terminated communications. When the device is usually the one initiating the transmissions, the network operator should be able to reduce the frequency of mobility management procedures.
- Monitoring. The network should detect events related to the status of the device, such as change of location, loss of communication and usage of the device with a different Universal Subscriber Identity Module.
- Groups. IoT devices are frequently deployed in groups. The network should provide mechanisms to handle policies for groups of devices and also to broadcast messages among the members of a group.

TABLE II
POSSIBLE LINK-LEVEL SOLUTIONS FOR COVERAGE ENHANCEMENT OF PHYSICAL CHANNELS AND SIGNALS [3GPP TR 36.888]

Channel/Signals Solutions	PSS/SSS	PBCH	PRACH	(E)PDCCH	PDSCH/PUSCH	PUCCH
PSD boosting	x	x	x	x	x	
Relaxed requirement	x		x			
Design new channels/signals	x	x	x	x	x	
Repetition		x	x	x	x	x
Low rate coding		x		x	x	x
TTI bundling/Retransmission					x	
Spreading		x			x	
RS power boosting /increased RS density		x		x	x	
New decoding techniques		x				

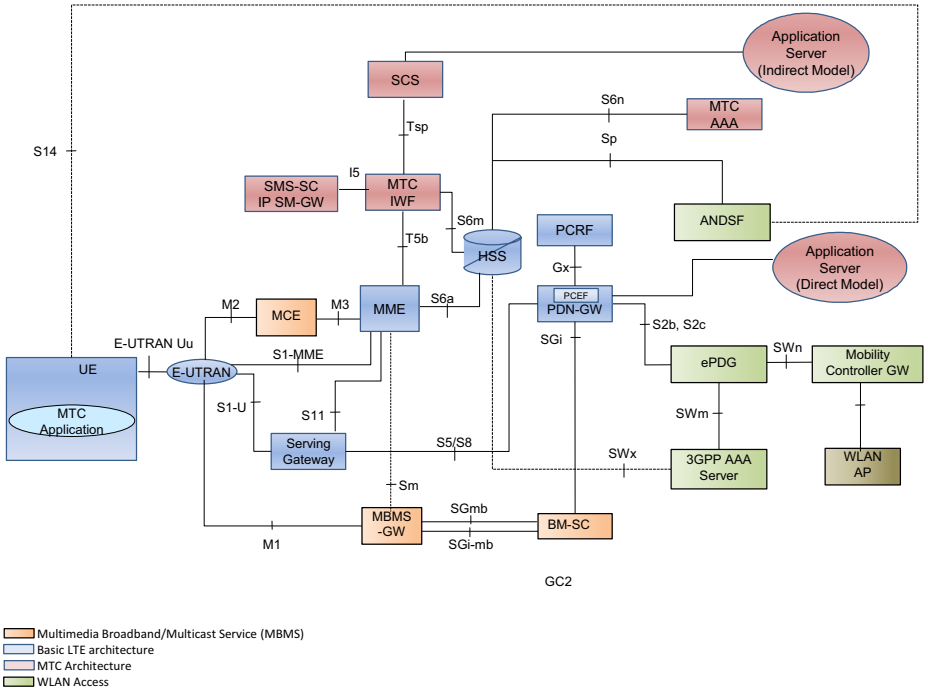

Fig. 1. LTE Architecture for MTC

III. LTE FOR IOT, WHAT IS COMMING?

A. Low cost LTE devices

In order to provide initial support for lower cost devices in LTE, 3GPP has added an additional category 0 in Release 12. The capabilities of a category 0 UE (User Equipment) are specified in 3GPP TS 36.306 [5]. The main factors enabling cost reduction in category 0 devices are those related to the reduction of the data rate by limiting the maximum transport block size (TBS) per subframe. Specially, reductions of up to 50% are envisaged.

As a reference, the maximum DL-SCH (Downlink Shared Channel) TBS has been reduced to 1000 bits from the former limit of 10296 bits in category 1 devices. Note also, the huge contrast with the highest performance capabilities such as DL Category 16 that have been also introduced in the standard in preparation for the forthcoming Gbps data rates. In addition, the number of receiving chains is also limited to a single layer.

As an optional feature, category 0 devices can also support a half-duplex type B operation. This new half-duplex scheme allows them to increase the guard period by skipping a full DL subframe before and after uplink subframes, as defined in TS 36.211 [6].

Additional specification enhancements are expected in 3GPP release 13 in the context of the proposals from TS 36.888 [7]. Multiple aspects are being analyzed to further reduce the cost of devices while enhancing coverage where required.

Specifically, up to 75% cost reductions [8] compared to category 1 are expected, mainly linked to the limitation of the reception bandwidth used and data rates.

B. Long battery life

Many use cases for IoT demand that devices can be deployed once and remain unattended for their lifetime. In many

cases, these devices are powered by batteries that can never be recharged. A Nokia white paper [10] estimates that these devices should be able to operate for at least 10 years, drawing power from a pair of long life AA batteries.

Release 12 introduces a power saving mode (PSM) that can dramatically extend battery life for devices that send data from time to time. When a device supports PSM, the network sets the duration of an active timer during the Tracking Area Update (TAU) procedure. Once the device switches to idle mode, the timer starts. While the timer is running, the device remains in idle mode, checking for paging during Discontinuous Reception (DRX) as usual. When the timer expires, the devices enter PSM, stopping any checking for paging and becoming unreachable until the device initiates transaction. Additional improvements may be studied for Release 13. [10] notes that there is a trade-off between reachability of the device and battery life extension when using longer sleep cycles. For example, when establishing the DRX cycle to 2 minutes, the lifespan of a device powered with two AA batteries which transmits 100 bytes daily reaches 111 months with no additional modifications.

1) Device identification: IoT devices might be small, sealed and therefore difficult to reach once they have started operating, so the current solution of using different USIM (Universal Subscriber Identity Module) for each operator is unworkable. To overcome this situation, the GSMA has standardized [11] a remote provisioning architecture that enables the change of the data stored in the UICC (Universal Integrated Circuit Card) over the air. Using the architecture defined by the GSMA the following parameters can be provisioned:

- Network Access Credentials and Algorithms, including the security key, the Milenage parameters or any other required algorithms.
- Network Information, such as the PLMN (Public Land Mobile Network), the MSISDN (Mobile Station Integrated Services Digital Network), etc.
- Mobile Network Operator Applications, roaming management, backup services, etc.

This functionality requires a new component in the network, the Subscription Manager, which is an entity that stores the eUICC access keys, which is trusted by one or more Mobile Network Operators. Apart from this information, IoT devices may have external identifiers, which are unique identifiers that can be used by external applications, servers to communicate with the UE from outside the network without knowing its IP (see section Device Triggering). These identifiers should have a domain identifier component, used by the mobile network operator to identify the services that can be accessed for this UE and the local identifier, which must permit the derivation of the IMSI (International Mobile Subscriber Identity).

C. Enhanced coverage

TS 36.888 [7] introduces several techniques to obtain 20 dB of improvement in the coverage. A first set of techniques is composed by TTI (Transmission Time Interval) bundling, HARQ (Hybrid Automatic Repeat Request) retransmission, repetition, code spreading, RLC (Radio Link Control) segmentation, low rate coding, low modulation order and new decoding techniques, which can be used to accumulated energy in order to improve coverage by prolonging the transmission time. Power boosting can be also used to transmit more power from the base station or Evolved Node B (eNB) to the MTC UE, while PSD (Power Spectral Density) boosting enables power to be concentrated in a reduced bandwidth at the eNB or the UE. Due to relaxed requirements of MTC communications, performance of some LTE channels can be relaxed. In the case the coverage improvement requirement cannot be fulfilled, new channels or signals can be designed. Also, small cell deployments can be used to improve coverage. Which techniques depends on the channel, as shown in Table II.

Existing coverage improvement solutions deployed for normal LTE UE such as directional antennas, external antennas can be applied. Single Frequency Network (SFN) multicast may also be used. This technology consists in sending redundant broadcast signals from all cells, helping to increase coverage especially at the cell edges. Finally, LTE Direct device-to-device (D2D) communications [12] can help extend coverage. D2D was introduced in Release 12 for traditional subscribers and public safety use cases enabling reliable one-to-many communications between devices in and out of coverage. In Release 13, D2D has been extended with new discovery and communication mechanisms such as out-of-coverage and multi-carrier. Also device-to-network relays [14] have been introduced for Public Safety uses cases. For Release 14 and beyond, additional D2D communications capabilities are being considered such as multi-hop communication, which has been proposed for vehicle-to-vehicle (V2V) communications.

D. Device triggering

The device triggering function was introduced in Release 11 (3GPP TS 23.682 [13]) in order to enable the reachability of dormant devices by MTC servers applications using a unique external identifier. Using these external identifiers, the provider can access the terminals using SMS without having to allocate an IP. Once the UE receives the SMS it must be able to identify the application and trigger the appropriate actions, analyzing the payload.

E. Managing congestion control

One of the most important characteristics of IoT is the expected number of connected devices connecting to the network, which can lead to congestion which can affect all users (both things and humans) in the network. This congestion could be for many reasons, simultaneous synchronization of the things, faulty transmissions or signalling storms after a period of outage in the network. LTE already provides some generic functions to avoid congestion [24].

The eNB can detect insufficient resources and reject RRC (Radio Resource Control) connection attempts or bearer creation or reconfiguration; it also can use an RRC back-off function. The MME (Mobility Management Entity) can also reject

connections, if it has received a back-off indication from the PGW (Packet Data Network Gateway). In the case it hasn't, it tries to create a session with the SGW (Serving Gateway), which is forwarded to the PGW, which, in turn, can detect congestion for a specific APN (Access Point Name). This then rejects the creation, setting the flag to APN congestion (3GPP TS 29.274 [18]) or it can reject a PDN (Packet Data Network) creation. This enables a back-off time for the MME which rejects all requests for a specified time (3GPP TS 23.401 [19]). Furthermore, the 3GPP has studied on solutions for managing core network overload (3GPP TR 23.843 [20]) which provide information on the use or modification of diameter, GTP-C (GPRS Tunneling Protocol user plane Control) and SS7 interfaces to manage overload.

Another important functionality, introduced in Release 11, is the use of the Low Access Priority Indicator, a flag that can be enabled in the UEs in production or via the OMA-DM (OMA Device Managment) or OTA (Over-the-air) interfaces. This flag is provided in the attach request to the eNB and is shared with the other elements of the network. This allows it to be used in the event of congestion to differentiate priority from non-priority traffic and also to increase the timer to trigger location update procedures, reducing the overload for this type of equipment. The terminals using this flag can also send messages with normal priority (for instance for terminals that might require higher priority in certain situations like alarms or emergencies). To reduce signalling procedures, the Extended Access Barring (3GPP TS 36.331 [21]) was introduced in Release 10. Using this feature the cell can indicate, via SIB14 (System Information Block), that the access is barred for certain access classes so no connection attach is attempted.

F. Security considerations

Devices in the IoT can be a potential target for malicious attacks due to, among other factors, their potentially limited processing and memory resources, the monetary or strategic value of the device to which they are attached, or the potential to launch denial of service attacks due to the large number of devices present in the network. Legacy 2G systems are considered insecure and there are already a number of vulnerabilities that have been discovered in IoT systems. Cellular IoT systems should be designed under the assumption that communications can be eavesdropped and thus, additional layers of encryption should be used [22].

As mentioned, the large number of devices that the IoT can serve makes the possibility of signalling storms more likely. Specifically, NAS (Non-Access Stratum) signalling procedures have been identified as a potential target for this. Another possible attack of this type can be performed by sending small data packets to a large number of devices, creating a huge number of RRC state transitions and potentially overloading the network core. Even if not created by a malicious entity, signalling storms can occur spontaneously due to the nature of the pattern of communication that many IoT devices exhibit, consisting in small but frequent transmissions. As in the previous case, these bursts translate into a large number of RRC state transitions, leading to congestion or denial of service. This is especially likely when many devices try to transmit data at the same time which can happen, for example, when these devices come back online after a power outage. The 3GPP is actively working on techniques to avoid the likelihood of such signalling storms.

IV. Improvements in the core network, an LTE architecture for IoT

3GPP 23682 [13] specifies architecture enhancements to improve MTC communications according to the use cases and service requirements defined in TS 22.368 [4], TS 22.101 [23], and related 3GPP requirements specifications.

Additionally the authors have identified a further two 3GPP subsystems which can also enhance IoT communications:

- Broadcast architecture, based on the MBMS (Multimedia Broadcast Multicast Services) standard, to support downlink multicast communication.
- Trusted and untrusted non 3GPP access, the use of Wi-Fi is proposed as a cheap alternative in extremely difficult locations.

The complete identified architecture is depicted in Figure 1, each subsystem is denoted by a different color.

The MTC architecture enables the communication between a UE running an MTC application and MTC services, as well as optionally providing some network functionality via the SCS (Service Capability Server). The components of the architecture are:

- MTC AAA (MTC Authentication, Authorization and Accounting), is in charge of returning external identifiers associated with an IMSI, and it might query the HSS to retrieve the values. The component can act as a proxy, in that case it will translate from IMSI to external identifier and vice versa.
- MTC IWF (MTC Inter Working Function), in charge of displaying device trigger functionalities for the SCS (reception of request, use of identifiers to activate the UE, selection of the mechanism, etc.), authenticate connection request from the SCS.
- SCS, an entity that connects to the 3GPP network exposing functionality that can be used by one or more MTC applications. The model of deployment can be direct, when the application server directly accesses the operator network, or indirect, when the application server accesses to the functionality via the SCS (which can be owned by the operator or by the MTC service provider), or hybrid, a mixture of both. This element is directly related to the device triggering function, introduced in the previous section. The SCS will send an SMS that contains the Trigger Payload, which is the information destined for the application running in the UE and the information to route it. The SCS will also provide functions to replace a previously sent SMS with a new one.

The MBMS architecture is described in detail in 3GPP TS 23.246 [15]. The broadcast architecture provides elements that

support the provision of multicast services, the architecture also requires modifications on the UE side to support the newly defined channels, the components are:

- MBMS-GW (Multimedia Broadcast/Multicast Service Gateway), that provides both control and data interfaces for the MBMS bearers coming from the BM-SC and is in charge of the multicast distribution via the M1 interface.
- BM-SC (Broadcast-Multicast Service Centre), which is the entry point for service provisioning and delivery, as well as service authorization and allocation of MBMS bearers.
- MCE (Multicast Coordination Entity), is a logical entity in many implementations and is provided as part of the eNB. It is in charge of the admission control and allocation of resources used by the eNBs.

The non 3GPP access architecture included to support WLAN is based on the following components:

- ANDSF (Access Network Discovery and Selection Function), allows the discovery of access networks and the provisioning of policies for the UE to select a technology.
- ePDG (evolved Packet Data Gateway), provides a secure tunnel for the UE, thereby providing a secure data path over untrusted 3GPP networks.

Other architecture enhancements introduced in Release 13 and centered on M2M communications are: Architecture Enhancements for Service Capabitlity Exposure (AESE) [25], which displays network services to 3rd parties, Monitoring Enhancements (MONTE)[26], which shows network information to 3rd parties for troubleshooting and Group based Enhancements (GROUPE)[27], which covers group based policies and group based addressing, Dedicated Core Networks (DECOR) [28], which enables core network nodes be selected based on subscription information (for example, special MME for M2M users). Finally extended DRX cycle for power consumption (eDRX) and optimizations to support high latency communications (HLCom) are working items.

V. Conclusion

As shown in this paper 3GPP Release 12 and Release 13 introduce optimizations for efficient machine-type communications. Concretely, the improvements in Release 12 have reduced by 50%, the complexity of UEs compared to Category 1, and have extended the battery life to 10 years for downlink delay-tolerant traffic. Release 13 has introduced techniques to increase coverage by 15-20 dB, the UE complexity has been reduced by a 75% and battery life has been extended beyond 10 years for new use cases. Furthermore these optimizations can be combined with other existing 3GPP technologies providing an excellent solution for IoT scenarios.

The improvements presented in this paper shown the evolution of LTE technology to tackle IoT requirements, providing multi-year battery life, reduced complexity, deeper coverage and high node density. These enhancements together with the advantage offered by standard LTE (flat and flexible architecture, built-in security, spectral efficiency, etc) make this technology the future of IoT.

Acknowledgment

This work has been funded by the Government of Andalusia (grant P11-TIC-7659), the Spanish Ministry of Economy and Competitiveness (grant TIN-2012-35669) and the European Commision under grant agreement No 688712 and FEDER.

References

[1] Machina Research. Global M2M Modules Report: Advancing LTE Migration Heralds Massive Change in Global M2M Modules Market. Machina Research, December 2013.
[2] Alcatel Lucent, Ericsson, Huawei, Neul, NSN, Sony, TU Dresden, u-blox, Verizon Wireless, Vodafone, A Choice of Future m2m Access Technologies for Mobile Network Operators, 2014
[3] 3GPP TR 45820, Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things
[4] 3GPP TS 22368, Service requirements for Machine-Type Communications (MTC); Stage 1
[5] 3GPP TS 36306, Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities
[6] 3GPP 36.211, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation
[7] 3GPP 36.888, Study on provision of low-cost Machine-Type Communications (MTC) UEs based on LTE
[8] Ericsson and Nokia Siemen Networks, LTE Evolution for Cellular IoT, 2014
[9] Open Mobile Alliance, Device Management Architecture, 2013
[10] Nokia White Paper, Optimizing LTE for the Internet of Things, 2014
[11] GSMA Association, Embedded SIM Remote Provisioning Architecture, Version 1.1, 2013
[12] 3GPP TR 36,843, Study on LTE device to device proximity services; Radio aspects
[13] 3GPP TS 23.682, Architecture enhancements to facilitate communications with packet data networks and applications
[14] 3GPP TR 36.814, Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects
[15] 3GPP TS 23.246, Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description
[16] 3GPP TS 23.261, IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2
[17] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses
[18] 3GPP TS 29.274, 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
[19] 3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
[20] 3GPP TR 23.483, Study on Core Network Overload (CNO) solutions
[21] 3GPP TS 36.331 Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification
[22] R. Piqueras Jover, Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations, 2015
[23] 3GPP TS 22.101 Service aspects; Service Principles
[24] NTT Docomo Technical Report, "Core Network Infrastructure and Congestion Control Technology for M2M Communications", 2013
[25] 3GPP TR 23.708 Architecture Enhancements for Service Capability Exposure (AESE)
[26] 3GPP TR 23.789 Monitoring Enhancements (MONTE)
[27] 3GPP TR 23.769 Technical Specification Group Services and System Aspects; Group based Enhancements (GROUPE)
[28] 3GPP TR 23.707 Architecture enhancements for dedicated core networks; Stage 2