Internet of Things in the 5G Era: Enablers, Architecture and Business Models

Article *in* IEEE Journal on Selected Areas in Communications · March 2016

DOI: 10.1109/JSAC.2016.2525418

7 authors, including:

Maria Rita Palattella
University of Luxembourg
54 PUBLICATIONS **4,265** CITATIONS
SEE PROFILE

Mischa Dohler
King's College London
403 PUBLICATIONS **21,998** CITATIONS
SEE PROFILE

Luigi Alfredo Grieco
Polytechnic University of Bari
217 PUBLICATIONS **11,675** CITATIONS
SEE PROFILE

Gianluca Rizzo
HES-SO Valais-Wallis
94 PUBLICATIONS **2,391** CITATIONS
SEE PROFILE

Internet of Things in the 5G Era: Enablers, Architecture and Business Models

Maria Rita Palattella, *Member, IEEE,* Mischa Dohler, *Fellow Member, IEEE,* Alfredo Grieco *Senior Member, IEEE,* Gianluca Rizzo, *Member, IEEE,* Johan Torsner, Thomas Engel, *Member, IEEE*, and Latif Ladid

(Invited Paper)

Abstract—**The IoT paradigm holds the promise to revolutionize the way we live and work by means of a wealth of new services, based on seamless interactions between a large amount of heterogeneous devices. After decades of conceptual inception of the IoT, in recent years a large variety of communication technologies has gradually emerged, reflecting a large diversity of application domains and of communication requirements. Such heterogeneity and fragmentation of the connectivity landscape is currently hampering the full realization of the IoT vision, by posing several complex integration challenges. In this context, the advent of 5G cellular systems, with the availability of a connectivity technology which is at once truly ubiquitous, reliable, scalable, and cost-efficient, is considered as a potentially key driver for the yet-to emerge global IoT.**

In the present paper, we analyze in detail the potential of 5G technologies for the IoT, by considering both the technological and standardization aspects. We review the present-day IoT connectivity landscape, as well as the main 5G enablers for the IoT. Last but not least, we illustrate the massive business shifts that a tight link between IoT and 5G may cause in the operator and vendors ecosystem.

Index Terms—**Internet of Things, IoT, 5G, cellular, Low-Power Wifi, Zigbee, Bluetooth Low Energy, Low Power Wide Area, 3GPP, Machine-Type Communications, MTC, Standardization**

I. Introduction

The idea of an Internet of Things as a network of smart devices dates far back in the past [1], with the first applications for automated inventory systems coming as early as 1983. However, only from 1999 it took momentum, becoming part of a shared vision for the future of Internet [2]. Today, the growing pervasiveness and ubiquity, in almost any context, of small and cheap computing devices, endowed with sensing and communication capabilities, is paving the way to the realization of the IoT vision.

A large variety of communication technologies has gradually emerged, reflecting a large diversity of application domains and of communication requirements. Some of these technologies are prevalent in a specific application domain, such as Bluetooth Low Energy in Personal Area Networks [3], and Zigbee in Home Automation systems [4]. Others, such as WiFi, Low Power Wide Area Networks (LPWA) [5], and cellular communications (such as 3GPP - 4G machine-type communications, or MTC), have a much broader scope. In addition, such landscape is constantly and rapidly evolving, with new technologies being regularly proposed, and with existing ones moving into new application domains.

A rough distinction is emerging between *consumer IoT* (cIoT) and *industrial IoT* (iIoT) [6], with clear implications on underlying technologies and business models. Consumer IoT aims at improving the quality of people's life by saving time and money. It involves the interconnection of consumer electronic devices, as well as of (virtually) *anything* belonging to user environments such as homes, offices, and cities.

Conversely, industrial IoT focuses on the integration between Operational Technology (OT) and Information Technology (IT) [7] and on how smart machines, networked sensors, and data analytics can improve business-to-business services across a wide variety of market sectors and activities, from manufacturing to public services. It generally implies machine-to-machine interactions, either for application monitoring (e.g., process monitoring in chemical production plants, vehicle fleet tracking, among others), or as part of a self organized system, with a distributed control which does not require human intervention (i.e., autonomic industrial plants) [8].

Despite their evident differences, these two service domains share some *general* communication requirements, such as scalability, need for lean protocol stack implementations in constrained devices, and friendliness to the IP ecosystem.

Nonetheless, the *specific* communication requirements of iIoT and cIoT can be very different, in terms of reliability, QoS (latency, throughput, etc), and privacy. cIoT communications are typically machine-to-user, and usually in the form of client-server interactions. In cIoT, desirable features of networked things are low power consumption, ease of installation, integration and maintenance. Indeed, the *quantified self* paradigm [9] which is currently unfolding with the advent of fitness and health tracking systems, smart watches and sensor rich smartphones requires a high power efficiency, in order to enable long term monitoring by small, portable devices, as part of a ”smart” environment or integrated in our daily wearings.

At the same time, such applications need to minimize the risk of exposing such sensitive data as someone's health status or life habits. Increasing the number of nodes and of exchanged information clearly multiplies the potential vulner-

M.R. Palattella, T. Engel, and L. Ladid are with the University of Luxembourg, SnT, Luxembourg e-mail: {maria-rita.palattella, thomas.engel, latif.ladid}@uni.lu.

M. Dohler is with King's College London, UK email: mischa.dohler@kcl.ac.uk.

L.A. Grieco is with Politecnico di Bari, Italy email: alfredo.grieco@poliba.it.

G. Rizzo is with the University of Applied Sciences Western Switzerland, HES-SO Valais-Wallis, Switzerland email: gianluca.rizzo@hevs.ch.

J. Torsner is with Ericsson Research, Helsinki, Finland email:johan.torsner@ericsson.com.

Manuscript received August, 2015; revised XXX, 2015.

abilities to the system to attacks and to privacy leaks [10]. Differently from cIoT, iIoT evolves from a large base of systems employing machine to machine communications for control process automation and/or monitoring. In such domains, iIoT is the result of the integration, through the Internet, of hardwired and often disconnected islands, usually based on semi-proprietary protocols and architectures. Such integration magnifies the potential of isolated industrial plants by augmenting their flexibility and manageability, and disclosing the opportunity to deploy new services [8].

Many of iIoT communications, together with some of cIoT communications, have often to satisfy stringent requirements in terms of timeliness and reliability. Typically, the information exchanged is critical for ensuring a correct and safe behavior of the processes under control. Hence, the communication network must be engineered in order to: (i) meet stringent delay deadlines; (ii) be robust to packet losses; (iii) be safe and resilient to damages, and more generally, strike the desired balance between capital expenditure / operational expenditure (CAPEX/OPEX) costs and system / service availability. 3G and 4G cellular technologies, and especially 3GPP LTE [11], are among the most appealing technologies in the modern IoT connectivity landscape. They offer wide coverage, relatively low deployment costs, high level of security, access to dedicated spectrum, and simplicity of management. However, being designed for optimized broadband communications, they do not support efficiently MTC communications.

The advent of 5G communications[1] represents a potentially disruptive element in such a context. The *increased data rate, reduced end-to-end latency, and improved coverage* with respect to 4G hold the potential to cater for even the most demanding of IoT applications in terms of communication requirements. Its support for large amounts of devices enables the vision of a truly global Internet of Things. In addition, for its focus on the integration of heterogeneous access technologies, 5G may play the role of a *unified interconnection framework*, facilitating a seamless connectivity of ”things” with the Internet. The goal of this paper is to analyze in detail the potential of 5G for the Internet of Things, considering both the technological aspects and their implications on business models and strategies.

The paper is structured as follows. Sec. II reviews the main available IoT communication technologies, and their key performance indicators. As MTC play a special role in such context, in Sec. III we review MTC requirements and we present the main standardization initiatives. Sec. IV describes the main technical enablers of IoT in 5G. Sec. V describes two MTC architectures, SmartM2M, and OneM2M. Sec. VI presents the main business implications of 5G in the IoT domain. Finally, Sec. VII concludes the paper.

II. Modern IoT Connectivity Landscape

Nowadays, the IoT landscape includes an extreme diversity of available connectivity solutions which need first to be harmonized across multiple industries, and then properly combined together in order to meet the IoT technical Key Performance Indicators (KPIs).

First forms of IoT connectivity can be dated back to the 80s, with the legacy Radio Frequency Identification (RFID) technologies, and to the 90s, with the Wireless Sensor Networks (WSNs). Due to their attractive application scenarios, both in business and consumer market, they gained a lot of momentum. Therefore, for the first decade of the 21st century, industrial alliances and Standards Developing Organizations (SDOs)s put a lot of effort in developing standardized low power IoT solutions. The first ones, available on the market, were mainly proprietary solutions, such as WirelessHART, and Z-Wave. They actually delayed the initial take off of the IoT, due to interoperability issues, among different vendors. Then, more generic connectivity technologies have been developed by SDOs, i.e., IEEE, ETSI, 3GPP, and IETF, easing the interconnection and Internet-connection of constrained devices. Bluetooth, and the IEEE802.15.4 standard [12] are among the low power short range solutions available today, which have played an important role in the IoT evolution. Recently the IEEE802.15.4 physical (PHY) and medium access control (MAC) layer have been complemented by an IP-enabled IETF protocol stack. The IETF 6LoWPAN (today 6lo) [13] and IETF ROLL [14] WGs have played a key role in facilitating the integration of low-power wireless networks into the Internet, by proposing mainly distributed solutions for address assignment and routing. At the same time, the 3rd Generation Partnership Project (3GPP) has been working toward supporting M2M applications on 4G broadband mobile networks, such as UMTS, and LTE, with the final aim of embedding M2M communications in the 5G systems.

No one of these aforementioned technologies has emerged as a market leader, mainly because of technology shortcoming, and business model uncertainties. Now, the IoT connectivity field is at a turning point with many promising radio technologies emerging as true M2M connectivity contenders: Low-Power WiFi, Low-Power Wide Area (LPWA) networks and several improvements for cellular M2M systems. These solutions are very attractive for IoT deployments, being able to fulfill availability and reliability requirements. With the final aim of helping the understanding of this rich and variegated context the reminder of this section overviews the modern IoT connectivity landscape and characterizes in more details the technologies which would potentially have a decisive impact in enabling a global IoT in the upcoming future [15].

A. Zigbee

ZigBee is a low-cost, low-power, wireless mesh network standard which has been widely applied in Wireless Sensors Networks (WSNs)s, the first pioneering Industrial IoT appplications (e.g., for control and monitoring). ZigBee was initially conceived in 1998, standardized in 2003, and finally revised in 2006. It builds on the IEEE802.15.4-2006 Physical (PHY) and Medium Access Control (MAC) standard specifications [12]. From real deployments, realized so far, it emerged that the current IEEE 802.15.4 PHY layer(s) suffice in terms of energy

[1] In this work, with the term 5G we refer to the solutions considered for and specified by 3GPP from Release 15 onwards, including both LTE evolution beyond Release 14 and a new 5G air interface. Eventually 5G is expected to be defined by the technical solution(s) that fulfill the IMT 2020 requirements.

efficiency. In fact, it is the actual hardware implementation which dictates the exact current draws and thus the energy needed to transmit a given information bit. However, many IoT applications are expected to exchange only a few bits. Thus, it will be advisable to look into a standardized PHY layer which allows ultra low rate transmissions over very narrow frequency bands, with the consequent advantage of having enormous link budgets and thus significantly enhanced ranges [16].

From a MAC perspective, the IEEE802.15.4-2006 MAC layer(s) did not suffice the needs of IoT applications. Its single-channel nature makes it unreliable, especially in multi-hop scenarios, where it incurs in an high level of interference and fading. Moreover, it produces high energy consumption, requiring router/forwarding nodes to be always on, regardless of their actual traffic [16]. To overcome such limitations, the IEEE802.15 Task Group 4e (TG4e) was created in 2008 to re-design the existing IEEE802.15.4-2006 MAC standard and obtain a low-power multi-hop MAC better suitable for emerging embedded industrial applications. The IEEE802.15.4e standard [17], published in 2012 as an amendment of the IEEE802.15.4-2011 MAC protocol, defined three new MACs. Among these, the Timeslotted Channel Hopping (TSCH) mode is the most promising one, facilitating energy efficient multi-hop communications, while reducing fading and interference. The basic concept on which TSCH builds on (i.e. the combination of time synchronization and channel hopping) was introduced for the first time by Dust Networks in 2006 in its proprietary Time Synchronized Mesh Protocol (TSMP) [18]. The core ideas of TSMP then made it into standards such as WirelessHART (2007) [19] and ISA100.11a (2009) [20]. These standards have targeted the industrial market, which requires ultra-high reliability and ultra-low power. IEEE802.15.4e TSCH inherits directly from these industrial standards, which are already deployed as commercial products in ten of thousands of networks in operation today. TSCH is thus a proven technology. One important difference with existing industrial standards is that IEEE802.15.4e TSCH focuses exclusively on the MAC layer. This clean layering allows for TSCH to fit under an IPv6-enabled upper protocol stack. The IETF 6TiSCH Working Groups (WGs) [21], charted in 2012, has defined an open standards-based Industrial IoT protocol stack which combines IEEE lower layers (IEEE 802.15.4 PHY and IEEE 802.15.4e TSCH), with IETF higher layers (6LoWPAN). Such protocol stack designed for Industrial IoT networks, is able to fulfill their stringent requirements, in terms of low latency, ultra low jitter, and high reliability [7].

B. Bluetooth Low Energy (BLE)

In 2010 the Bluetooth Special Interest Group (SIG) proposed BLE in the Bluetooth 4.0 specification [22], nowadays updated to version 4.1. BLE is a *smart* low energy version of Bluetooth, still designed for short-range communication (up to 50 m), but, mainly suitable for low-power, control and monitoring applications (e.g., automotive, entertainment, home automation, etc.). BLE operates in the 2.4 GHz Industrial Scientific Medical (ISM) band, and defines 40 channels, with 2 MHz channel spacing. To the final aim of achieving low power usage, BLE uses (and thus, scans) only 3 advertising channels, which are used for device discovery, connection set up, and broadcast transmission. Their center frequencies have been assigned to minimize interference with the IEEE802.11 channels 1, 6, and 11, widely used in several countries. The other 37 data channels are dedicated to bidirectional exchange of short bursts of data between connected devices. BLE also sets up connections very quickly, which further minimizes the radios on time. An adaptive frequency hopping algorithm is used on top of the data channels, to reduce sensitivity to interference, and multi-path fading [3]. BLE has emerged in parallel with other low-power solutions, such as ZigBee, 6LoWPAN, and Z-Wave, which were targeting applications with multi-hop scenario. However, BLE currently only supports a single-hop topology, namely *piconet*, with one master device communicating with several slaves node, and a broadcast group topology, with an advertiser node broadcasting to several scanners. In 2015, the Bluetooth SIG announced the formation of the Bluetooth Smart Mesh working group to define the architecture for standardized mesh networking for BLE. This will enable extended communication range and simplify deployments of BLE networks for IoT. BLE is destined to be a key enabling technology for some short-range Internet of Things applications, such as in healthcare, smart energy, and smart home domains [4]. Its potential was recognized since its early birth, as shown by the interest it gained quickly at IETF, where the 6LoWPAN Working Group (today 6lo), developed a specification for allowing the transmission of IPv6 packets over BLE [23]. BLE is expected to become a *de facto* standard for short-range IoT services. In fact, more than one billion smartphones are shipped every year, all equipped with BLE interfaces. As a consequence, this technology will become very soon the most commonplace communication medium for consumer applications: from one hand, a so broad market will let decrease the costs of BLE hardware; on the other hand, motes equipped with the BLE stack will have much chance to be used in all those scenarios where user-to-machine interactions are needed (i.e., smart living, health care, smart building, and so forth) [24].

C. Wifi and Low-Power Wifi (LP-Wifi)

The IEEE802.11 standard, better known as Wifi, was released in its first version in 1997, and designed without IoT in mind. In fact, its final aim was to provide high throughput to a limited number of devices (called stations), located indoor, at a short distance between each other. Even though nowadays widespread, Wifi has not been applied into M2M-IoT use cases, due to its large energy consumption, fairly high compared to other standards. For instance, Bluetooth, with its shorter propagation range, (between 1 and 100 m), offer a lower power consumption; while ZigBee have fairly long range, but much lower data rate.

To overcome such energy-related limitation (which impacts on the battery life of devices), duty cycling and hardware optimization have been adopted by the IEEE802.11 community, achieving in this way, extremely energy efficient solutions. Despite the reduced energy consumption, Wifi still suffers of poor mobility and roaming support. In fact, it does not offer any guaranteed QoS, and it is affected by high interference, due to sharing the unlicensed 2.4 GHz band, together with ZigBee, Bluetooth, and many others ISM band devices.

To reduce interference issues, the IEEE 802 LAN/MAN Standards Committee (LMSC) has proposed the use of the sub 1GHz (S1G) license-exempt bands, which have better propagation properties, especially in outdoor scenario, compared to traditional WiFi 2.4 ad 5 GHz bands. It is possible to increases the transmission range up to 1 km, while still using the default transmission power of 200 mW. However, due to the extremely scarce available spectrum, S1G does not allow the use of wide bands (like those adopted by .11n, and .11ac, $>$ 20 MHz). Therefore, accurate design considerations, such as new modulation and coding schemes were introduced in the .11ac amendment.

In 2010, LMSC formed the IEEE802.11ah Task Group (TGah), also called Low-Power Wifi, responsible of extending the application area of Wifi networks, to meet the IoT requirements (large number of devices, large coverage range, and energy constrains). In many IoT applications (e.g., smart grids, industrial automation, environmental monitoring, healthcare, fitness systems), an access point (AP) has to cover hundreds, or even thousands of devices (sensors and actuators), which periodically transmit short packets. One of the main challenges for the adoption of legacy IEEE802.11 has been the limited number of stations that can be simultaneously associated with the same AP. The IEEE802.11ah standard overcomes such shortcoming, by introducing a novel *hierarchical method* which defines groups of stations, and allows support for large number of devices [25].

IEEE802.11ah uses sub-1GHz frequency bands and the PHY layer design is based on the IEEE 802.11ac standard. To accommodate narrower channel bandwidths, the IEEE 802.11ah physical layer is obtained by down-clocking ten times the IEEE 802.11ac physical layer. The TGah has put a lot of effort into improving the IEEE802.11 MAC layer to obtain power efficiency, and reduce the overhead due to (a) short packet transmission, and (b) long time features of Wifi PHY. Both issues implies a large amount of channel resources, occupied by frame headers, interframe spaces, control and management frames, and wasted for repeated channel access procedure (following collisions). New short frame formats, advanced channel access mechanisms, novel power managements mechanisms are among the solutions designed by TGah, which allows low-cost connectivity with Wifi in unlicensed bands. First performance studies [26] show that IEEE802.11ah will support a large set of M2M scenarios, such as agriculture monitoring, smart metering, industrial automation. It will be able to provide a QoS level higher than currently provisioned in mobile networks, and enable scalable and cost-effective solutions.

D. Low Power Wide Area (LPWA)

The LPWA technology has recently emerged specifically focusing on low-end IoT applications which require low cost device, long battery life time, small amounts of data exchanged, an area for which traditional cellular M2M systems have not been optimized . The term LPWA which was introduced by Machina Research to the market, stands for *high reach, low cost, low power* Wide Area Networks [5]. Primarily designed for M2M networking, it operates in unlicensed spectrum, and it is currently available in many different proprietary solutions (Amber Wireless, Coronis, Huawei's CIoT, LoRa, M2M Spectrum Networks, NWave, On-Ramp Wireless, Senaptic, Sigfox, Weightless, among many others). While most of these technologies have been present in the market for some time, it is Sigfox with its Network Operator strategy that has recently kick-started the LPWA market. Aware of its potential, the LoRa Alliance, Sigfox, amd Weigthless are engaged in LPWA standardization activities, aiming towards licensed spectrum, and overcome interoperability issues which may delay its roll-out. According to Machina Research, which has first forecast the market opportunity for such technology in early 2013, LPWA will allow to interconnect a large number of low-cost devices (up to 60% by 2022, with 3 billions LPWA M2M connections, by 2023), making the M2M solution business profitable, and providing a platform to build a large IoT business [5].

The key features of LPWA can be summarized as follow: (i) wide area coverage (up to some tenths of Km), (ii) low cost communication, (ii) long battery life (up to 10 years from a single AA battery), and (iv) low bandwidth communication. The latter limits the LPWA range of applications to a set of M2M use cases, characterized by low data rate, and infrequent transmissions (few hundred bytes of data) [27].

LPWA is not intended to replace cellular connections, but rather it will be complementary to existing cellular technologies. As discussed later in the paper 3GPP has also initiated work to make cellular systems, such as GSM and LTE, more suitable for low end MTC applications.

Despite its appealing and promising features, LPWA presents some downsides, mainly due to the use of unlicensed spectrum for long-range communication. Notably, the effective radiated power (ERP) in that part of the license-exempt band is heavily regulated in terms of allowed transmission powers (after antenna gain), duty cycles and access mechanisms. Since antennas at the basestation and at the IoT device have entirely different gain capabilities, the link capabilities in up and downlink are skewed with the uplink having a link budget advantage of up to 19dB. While European regulation allows for a boosted downlink power of 13dB, a difference of at least 6dB remains which means that truly symmetrical connectivity cannot be guaranteed. This means that simple operations, like sending an acknowledgement, cannot be executed seamlessly as in 3GPP technologies. Consequently, only a limited set of IoT applications can be supported through this technology.

Moreover, LPWA cannot fulfill the scalability requirements of large-scale IoT deployments, due to an impeding spectrum congestion [28]. According to Cisco IBSG prediction there will be 50 billion devices connected to the Internet by 2020. With such explosion of devices connected through IoT, millions of devices may appear within the coverage area of a single LPWA base station. Many of those will be using other radio technologies that share the spectrum with LPWA, such as LP-Wifi, Z-Wave, Zigbee, IEEE 802.15.4g, etc. All these transmission will be perceived as interference by the LPWA device, having low receiver sensitivity for long-range communication.

Nevertheless, LPWA is expected to be a key enabler for IoT deployments in early market rollouts and for limited IoT applications.

E. 3GPP Cellular: MTC

Within the cellular context, the IoT connectivity solution is referred to as machine-to-machine (M2M) and within the 3GPP standardization body it is referred to as machine-type communications (MTC). The industry vision is to enable connectivity between machines in an autonomous manner where such a connectivity was traditionally facilitated by means of wires. Even though the wired M2M market will remain , scalability can only be achieved through an untethered approach. Wireless MTC solutions have thus emerged which offer viable business benefits but also exhibit shortcomings.

MTC is attractive when compared to wired solutions for a variety of reasons, such as robustness against single point of failures or ease of deployment. The main challenge for wireless solutions however is related to the cost of the radio, the power consumption but also the variety of M2M services. Compared to the other technologies which were reviewed in previous sections, cellular MTC is able to offer quality of service (QoS) support, mobility and roaming support, as well as billing, security and global coverage. Another area where cellular MTC excels today is the ability to connect the sensors/devices through a standardized API to the core enterprise systems, all in real-time, scalable and secure.

Despite the convincing advantages, some serious challenges remain to make MTC an underlying connectivity backbone for the Internet of Things. These challenges affect the device and networking levels, as well as viability of business models.

In the following Sec. III-IV, we describe all the current initiatives in 3GPP, and the effort still needed for making MTC a key enabler of the IoT ecosystem.

III. 3GPP MTC Requirements & Standards

One of the major differences between the 4G and 5G design efforts is the support of a truly large number of devices so as to enable the vision of a truly global Internet of Things. Given the vast array of connectivity technologies developed over past decades (presented in previous Section II), the emergence of a cellular technology as a true contender may seem rather surprising since power consumption is significant and both capital expenditure (CAPEX) and operational expenditures (OPEX) perceived to be very high. On the other hand, the undisputed global coverage, the massive inter-operable ecosystem and the ability to service critical data traffic give a lot of credibility to this technology family.

To this end, in this section we review in more details the 4G Generation, the MTC requirements and we explain respective standardization initiatives.

A. MTC Generation Tradeoff

Considering the stringent requirements of M2M, the 2G technology family, i.e. GSM and GPRS/EGPRS, is ideal as power consumption and cost are low, coverage global and the eco-system is developed; however, from an economic point of view it is perceived to be much more viable to revise the bands for next generation systems.

The 3G family, i.e. UMTS and HSPA, has a lower power efficiency and higher modem cost than 2G. The capabilities exceed the requirements of many low end IoT applications and may therefore be a less preferable choice for such applications. 3G has however proven popular for e.g. automotive M2M applications and other more demanding M2M applications due to the wide range of data rates required.

4G technologies, i.e LTE and LTE-A, are interesting again since the capabilities meet the requirements for very demanding MTC applications; the air interface, OFDM(A), allows the scaling of the bandwidth according to needs. Modem cost in early LTE releases is however an issue and the coverage is in some markets still patchy even if coverage increases quickly on a global level. A further argument for use of 4G LTE for MTC applications is to benefit from improved spectral efficiency and the bandwidth flexibility offered by 4G systems and longevity of the technology as a future cellular system. Uptake, due to a rather patchy 4G coverage, is only catching up now and the challenge of adapting a 4G LTE system (that was specifically designed for efficient broadband communication) to also deliver and support MTC applications remains.

5G may thus be a timely technology offering lower cost, lower energy consumption and support for very large number of devices. Indeed, these requirements are at the forefront of the 5G MTC design and – if successful – will undoubtedly be an integral part of the Internet of Things in years to come. The requirements and standardization initiatives which lead into these design developments are reviewed in the following Section III.

B. MTC Technical Requirements

3GPP cellular systems were primarily designed for human voice and data use, and less so for machine needs. A important point to consider for all the requirements is backwards compatibility. This is because IoT devices, whether cIoT or iIoT, will likely stay for a longer time in the field which impacts technology migration, among others.

1) Need for ”Zero-Complexity”: One of the most stringent requirements are those on lowering device complexity to virtually zero. This will positively impact the cost of the devices, since silicon costs are virtually absent. To this end, 3GPP study items identified several features that are not required for MTC devices and could reduce device complexity significantly. Notably, it was proposed for LTE to limit device capability to a single receive RF chain, restricting supported peak data rates to the maximum required by IoT applications, reducing supported data bandwidth and support of half duplex operation as key to reduce device complexity, among a few others. Standardization work is needed to ensure that maintaining system performance with normal 3GPP devices with additional scheduler restrictions to serve these low complexity devices is achievable. Considering the timeline, 3GPP has closed some of the complexity reduction specifications for LTE in Release 12; the remaining and new complexity items are dealt with in Release 13 and subsequent releases.

2) Need for Long battery life time: A large fraction of the IoT devices will be battery operated and may be located in remote areas where changing or charging batteries may not be possible or economically feasible. Miniaturization of devices also imply that the physical size of batteries will be smaller which means that the total available energy in a battery may not increase even if battery technology evolves. The communication module in IoT devices therefore needs to be very energy efficient in order to enable battery life times of decades. A battery life time of 10 years is already feasible for infrequent data transmissions with both LPWA technologies and in LTE Rel-12 ; the challenge for 5G may therefore be to allow battery life time of more than one decade also for more frequent data transmissions.

3) Need for Coverage Improvement: Many of the industrial and even consumer IoT applications will require high levels of coverage. Examples of such applications are smart metering, factory automation with basement coverage, etc. Many of the connectivity business models only work if and only if almost all devices in the network can be reached. Due to the nature of the wireless channel providing 100% coverage including indoor locations for example in basements is very costly. There is a need to reach also the last few percent of devices in challenging locations without adding significantly to the total cost of the complete solution. Increasing the number of base stations is in theory a solution but comes at the additional cost of site acquisition/rental, backhaul provisioning, among others. A viable approach could be to improve coverage levels in some critical application contexts without adding significantly to the overall cost of the solution. To this end, 3GPP is stipulating low complexity and improved coverage MTC devices to facilitate a scalable IoT uptake. Notably, coverage improvement is achieved by repetition of information with more details provided in 3GPP Release 12, Stage 3.

4) Need for MTC User Identification & Control: A large part of the low-cost MTC devices will have a SIM integrated; however, it is envisaged that – for scalability, configuration and complexity reasons – some MTC devices will not contain a SIM. In that case it is essential to be able to individually regulate access using prior defined SIM profiles. In general, the SIM card contains the IMSI of the subscriber with direct link to the HLR; the latter includes details about subscribed MTC services and feature profile. Operators are already able to support customized MTC services based on the subscription profile, such as optimal data packet size, optimal routing with dedicated Access Point Name (APN) for MTC services, etc. Through the IMSI, specific charging policy for MTC subscription is provisioned by the operator and the operator has complete control over the subscriber that is allowed in the network. 3GPP is likely to define one or more new LTE UE categories for MTC. This will be one of the means to identify and isolate MTC devices if they are impacting performance of the network and be able to restrict access for MTC devices. One of the concerns operators share is restricting access to roaming devices. Notably, the operator should be able to identify such roaming MTC devices from MTC specific user equipment (UE) category and be able to restrict access to the devices if the operator does not wish to service those devices.

5) Service Exposure and Enablement Support: 3rd party support to the 3GPP system is rather important from a scalability point of view. Therefore, service exposure and enablement support are instrumental for MTC to succeed as a connectivity solution for the emerging IoT. Standardization work related to M2M service enablement is on-going in standardization organisations outside 3GPP (e.g. ETSI TC M2M and the oneM2M Global Initiative, described in Section V). 3GPP's support for service exposure and enablement however allows 3GPP capabilities to be natively offered outside the 3GPP core. For this to work, additional information (e.g. transmission scheduling information or indications for small data, device triggering, etc.), and new interfaces between the 3GPP Core Network and application platforms will need to be provided. Importantly in this context, to ensure privacy for consumer IoT, exposed network information needs to be delinked from private user/subscriber information.

C. 3GPP MTC Standardization

3GPP technologies and their continuous enhancements are staged in different releases in 3GPP (see Figure 1. An important aspect contributing to the success of 3GPP technologies for cellular use is maintaining backward compatibility with legacy releases and tight interworking between technologies and efficient roaming support which is also key for M2M/MTC applications that require support for mobility.

3GPP specification work is roughly grouped into RAN, SA, GERAN and CT. Each of these groups is responsible for defining functions, requirements and interfaces of 3GPP systems. More specifically, RAN is responsible for the radio access part of 3G, 4G and now 5G. GERAN is responsible for radio access part of 2G and its evolution. SA has the responsibility for the overall architecture and service capability. And CT is responsible for specification of terminal interfaces and capabilities and the core network part of 3GPP systems.

3GPP features are phased into releases and the work may be preceded by a study to ensure a rough industry consensus and a better understanding of the problem at hand; lately, all new features are preceded by a study phase. 3GPP has adopted the notion of releases to ensure a stable platform for implementation while facilitating introduction of new features.

While the idea of cellular underpinning the connectivity of the emerging IoT is rather new, actual standardisation work started as early as 2005! Notably, 3GPP TSG SA1 (group defining services) started with a feasibility study to conclude with a report during 2007 as captured in 3GPP Technical Report (TR) 22.868. 3GPP Release 10 Technical Specification (TS) 22.368 specifies the Machine-to-Machine communications requirements. Then, refinement of requirements, logical analysis was captured in 3GPP TR 23.888

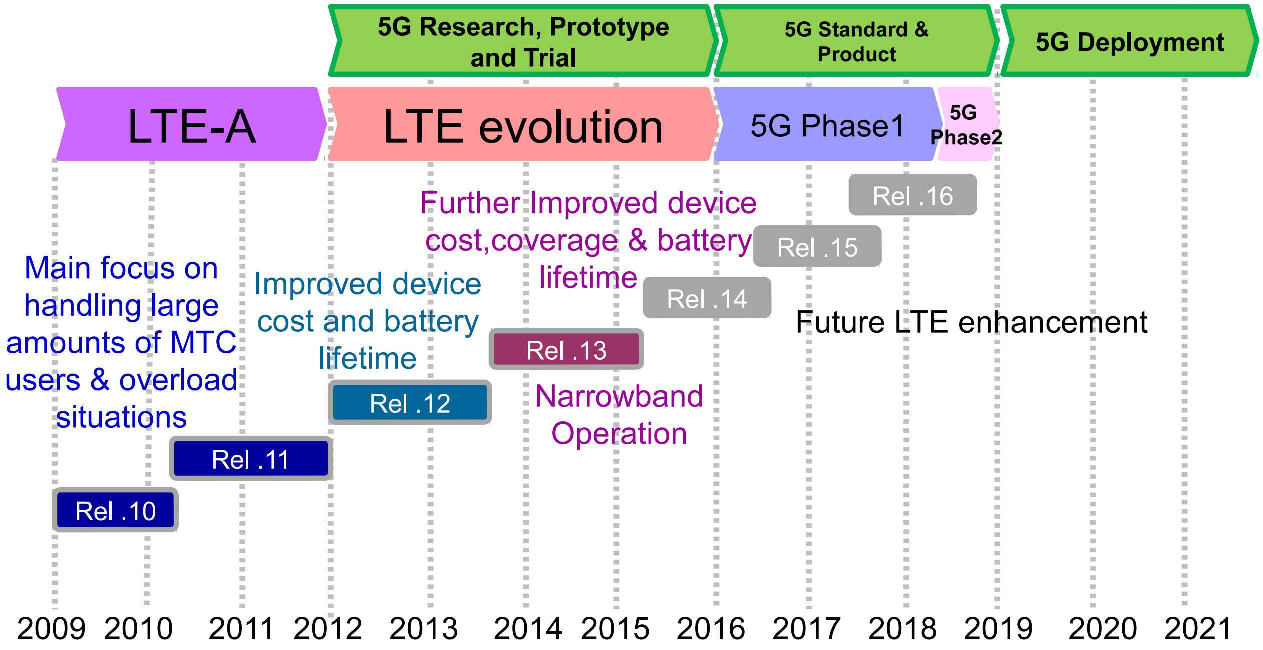

Fig. 1. 3GPP releases and timeline.

and protocol implementation were staged for release 11 and captured in respective TS document of responsible working groups. Furthermore, charging requirements were addressed by SA5 to reuse existing 3GPP functions (e.g. session initiation and control) to the extent possible. 3GPP architecture work on MTC started. In Rel-10 and in Rel-12 SA2 worked on efficient transmission of Small Data Transmissions and Low Power Consumption UEs. Ever since, the amount of study items and technical specifications for MTC have increased steadily and are now a core ingredient of standardization work.

The standardization of a new 5G air interface is foreseen by 3GPP to be divided in phases where the first phase, with a finalization targeted during 2018, is focusing on early commercial deployments and a subset of the 5G requirements. The second phase of the standardization, targeted to be finalized at the end of 2019, targets fulfillment of the full set of 5G requirements.

D. 3GPP Security

The security framework used in 3GPP systems was originally developed for GSM to provide a basic connectivity service for human to human communication. The security features of GSM were encryption of the air interface to avoid eavesdropping and strong authentication mechanism of the users. The main security solution was kept for 3G and 4G, but enhancements were done to enhance the security level such as introducing state of the art encryption algorithms, more elaborate key management systems, integrity protection of signaling and mutual authentication. The 3GPP security framework is based on the tamper resistant SIM card, which holds the credentials of the subscriber. By using the credentials of the SIM card and corresponding credentials stored in the network, the device and the network mutually authenticate each other. The authentication mechanism also produces keys, which are then used for encryption and integrity protection of the communication on the radio interface. Subscriber privacy in 3GPP systems is considered by using randomly assigned temporary identifiers to make tracking of devices and users more difficult.

Recently 3GPP have worked on enhancements specifically aimed at MTC applications. The new requirements emerged due to characteristics of MTC such as reduced signaling and even 10 years battery lifetime are being taken into account in the security work. 3GPP is working on to enhance the security level of GPRS in order to support the so called GPRS-based cellular IoT system [29]. Another work is to develop security solutions for 3GPP systems to support very low complexity and low cost devices targeting 10 years battery lifetime [30]. The challenges of the removable SIM card to meet the requirements of MTC, like remotely changing the subscription and fitting a SIM card into a tiny device, were studied in 3GPP some years ago, but the standardization work was started in GSMA and ETSI, and it still continuing under the name of embedded SIM.

IV. 5G IoT Enablers

In order to enable the ubiquitous connectivity required for many of the IoT applications, many more features and functionalities will need to be added to the currently predominantly broadband approach. This inherently leads to a strong heterogeneous networking (HetNet) paradigm with multiple types of wireless access nodes (with different MAC/PHY, coverage, backhaul connectivity, QoS design parameters, among others). HetNets will offer the required seamless connectivity for the emerging IoT through a complex set of mechanisms for coordination and management [31]–[35]. Evolved 4G and emerging 5G networks will thus be characterized by interoperability and integration between multiple radio access networks, including unlicensed frequencies. The aim of this section is to review recently finished 4G, currently ongoing 4G-Evolution as well as emerging 5G design efforts towards accommodating IoT in such a heterogeneous networking setting.

A. 4G-Evolution Feature Enhancements

Some of the requirements outlined in Section III have already been addressed by the 3GPP community, which constitutes an important step towards IoT connectivity. Some of the most important solutions are briefly summarized below.

1) Narrowband operation: Work is ongoing in 3GPP to specify a narrowband version of LTE named narrowband IoT (NB-IoT) especially targeting MTC applications with low data rate and need for low module cost and long battery life time. With a bandwidth of 180 kHz NB-IoT can be deployed in a re-farmed GSM carrier offering an alternative use of GSM spectrum. Alternatively it can be deployed in the guard bands of LTE spectrum allocations or using part of an operators LTE spectrum. The details of the air interface design are still to be settled and the higher layer protocols starting from Layer 2 and upwards will be common between NB-IoT and LTE. By making the solution similar to LTE the large eco-system for LTE modules can be mobilized to secure availability of device chipsets and a fast rollout. The performance requirements for NB-IoT are similar as for the wideband LTE MTC solution, the main benefit lies in that the narrowband operation leads to flexibility in the deployment.

2) Low Cost & Enhanced Coverage: 3GPP developed techniques enabling reduced UE complexity and improved coverage compared to normal LTE user equipment. Details are captured in 3GPP TR 36.888 [11]. Release 12 introduces a new UE category with reduced peak rate (1Mbit/s), a restriction in MIMO modes to a single receive antenna and half duplex operation.

Release 13 aims at further reducing the complexity by specifying a reduced bandwidth (1.4 MHz) and a lower UE power class to facilitate single chip implementations with integrated power amplifier instead of having it as an external component.

The Bill of Materials of a Rel-12 and Rel-13 MTC optimized device has been estimated to be by 3GPP [11], respectively, 50 percent and 75-80 percent lower than for the early Rel-8 Category 1 UE.

Finally, coverage improvement through data repetition is enabled; but this feature is only recommended for delay-tolerant MTC devices.

3) Device Power Saving: The main source of the energy consumption for MTC devices in pre-Release 12 devices is the periodical listening for possible paging messages which needs to be done at least once every 2.56s (the maximum cycle of the discontinuous reception (DRX)), and performing various link quality measurements. For typical MTC traffic patterns, the energy required for transmitting messages is only a small fraction of the total energy consumed. A mechanism to reduce the power consumption for MTC devices was introduced in 3GPP Release 12, the Power Saving Mode (PSM). In PSM the device can turn off all functionality requiring the device to listen while in idle mode. Consequently the device does not receive paging messages or perform link quality measurements in PSM. Since the device remains attached to the network, less signaling is required compared to the approach where the device would be completely shut off when not transmitting. The device can transmit up-link data at any time but is only reachable in down-link when the device has been active in up-link, which happens at configurable time instances or when the device has transmitted up-link data.

4) Overload & Congestion Control at RAN/CN: MTC devices cause signalling overload as they simultaneously recover triggering registration and other procedures causing increased signalling and core network overload when trying to respond simultaneously. Specifically on network failure, there could be a sudden surge in signalling as MTC UE associated with the network reselect to alternate network (possibly roaming) simultaneously to the not yet failed network. A Rel-10 study item on Network Improvements for Machine-type Communications (NIMTC) studied core network aspects of overload and congestion control. A Rel-11 study item on RAN improvements for MTC was started Q4, 2009. A Rel-11 umbrella work item on system improvements to MTC started in May 2010; this work item also addresses RAN overload control for UTRAN and E-UTRAN. In essence, a mechanism to prevent and control such scenarios is performed by configuring MTC UEs ”low priority access” indicator identifying the devices as delay tolerant devices; this can be used by the network to control various procedures. In UTRAN or E-UTRAN the RAN (RNC for UTRAN and eNB for E-UTRAN) would reject the connection request from the UE with an extended wait time of up to 30 minutes when overload is indicated by the Core Network to the RAN.

5) Other Enhancements: 3GPP Release 12 dealt with further MTC enhancements which were not addressed in previous releases. For example, the issues for optimisations of clusters of MTC devices, MTC group addressing, and other group features have been considered through fine-tuned broadcast message protocols. Furthermore, enhancements to the roaming of MTC devices have been specified and optimized by using the low access priority indication provided by the UE; a eNB steers UEs configured for low access priority to specific MMEs. Currently, 3GPP Release 13 and future releases are expected to enable further support for efficient delivery of MTC services and mass deployments of MTC devices.

B. 4G-Evolution & 5G RAT Enablers

We now consider some pertinent radio access technologies (RATs) in evolved 4G as well as 5G systems. We discuss their relevance to Internet of Things (IoT) and Machine-to-Machine (M2M) services. Given that coverage extension was such an important design item, we start discussing the role of relaying. We then discuss the relevance of the much-discussed mm-wave and device-to-device (D2D) technologies.

1) Relaying for Increased Coverage: Relaying is a key technology for 5G systems [36]. In its classic formulation, it is meant for extending the communication range of a Base

Station (BS) and improve throughput by means of Relay Stations (RSs). In 4G/5G systems, relaying techniques can also include chains of relaying nodes and mobile relaying nodes in order to improve coverage, support bandwidth hungry services, and provide connectivity to M2M systems. RSs can help reaching users that are either outside or inside the coverage of the BS [37]. In the first case, the RS simply extends the perimeter of a cell so that it is possible to reach also users that are far from the BS. In the second case, the RS enables multipath diversity techniques to magnify the connectivity strength to users that are weakly served by the BS.

Four different transmission schemas can be used by RSs: *Amplify and Forward*, *Demodulate and Forward*, *Selective Decode and Forward*, and *Buffer Aided*, which are ordered by increased latencies and reliability [38]. With *Amplify and Forward*, the RS simply repeats an amplified copy of received signals. With *Demodulation and Forward*, received signals are demodulated (without decoding) by the RS, which also makes a hard decision before modulating and forwarding the new signals to the next hop. With *Selective Decode and Forward*, received signals are fully decoded and checked. In case of successful decoding, the signals are encoded and forwarded to the next hop. With *Buffer Aided* approaches data are temporarily stored by the RS in order to encode and forward them as soon as the channel quality is sufficiently high. This kind of scheme can only be used for services not sensitive to delay. Another relevant aspect for RSs is the spectrum used for access and backhaul links, which can be overlapped (inband relaying) or disjoined (outband relaying) [39]. With outband schemes, RS can enable full duplex communications; In contrast, with inband mechanisms, interference between access and backhaul links can arise, so that time division multiplexing is required.

With reference to IoT systems, relaying technologies could improve the scalability of network access operations to ensure the required coverage extension. . In fact, in cells with a very high density of IoT devices it is possible to let them associate to different RSs so that the burden of network access is distributed among many nodes. In other words, without RSs, all IoT devices within one cell associate to the same BS, which causes network overload. In addition, the adoption of RSs can improve the fault tolerance of the communication infrastructure because the BS is no longer a single point of failure. Because relaying technologies strengthen the signal to noise ratio, the reliability and timeliness of message exchanged with IoT services are improved and the support to mission critical applications becomes easier. For group based communications, multicast services on top of multi-hop networks of RSs need to be defined. Another challenge (which is common to 4G and 5G systems) is the coordination of the communication activities between the RSs in order to optimize the channel usage with a limited signaling overhead.

2) Millimeter Wave Technologies: As the demand for capacity in mobile broadband communications increases dramatically every year, wireless carriers must be prepared to support up to a thousand-fold increase in total mobile traffic by 2020, requiring researchers to seek greater capacity and to find new wireless spectrum beyond the 4G standard. Recent studies suggest that mm-wave frequencies could be used to augment the currently saturated 700 MHz to 2.6 GHz radio spectrum bands for wireless communications. The combination of cost-effective CMOS technology that can now operate well into the mm-wave frequency bands, and high-gain, steerable antennas at the mobile and base station, strengthens the viability of mm-wave wireless communications. Further, mm-wave carrier frequencies allow for larger bandwidth allocations, which translates directly to higher data transfer rates.

Among the main issues which need to be tackled are the high propagation losses at the mm-wave frequencies, which call for high density of antennas, particularly in difficult environments like city centers; effects such as reflections and fading pose serious technical obstacles which need to be addressed. The great capacity offered by mm-wave would enable high-rate MTC applications, such as automatic video surveillance cameras. Furthermore, the short range of mm-wave could be interesting for D2D situations (see below). Albeit seemingly an overdesign for largely low-rate IoT applications, mm-wave offers the interesting possibility to construct very, very short over-the-air data packets. This, in turn, allows an even more aggressive duty cycling of MTC devices and thus possibly vital energy savings to extend the IoT devices' lifetime. In fact, low power mm-wave interfaces would be used in D2D communications, thus saving the energy required by the cellular radio interface.

3) Device-to-Device Communications: Device to Device (D2D) communications represents a turning point in cellular systems. They entail the possibility that two devices can exchange data without the involvement of the BS or with just a partial aid from the BS [40]. In contrast to WiFi and Bluetooth technologies, which provide D2D capabilities in the unlicensed band, with D2D communications the Quality of Service (QoS) is controllable because of the use of the licensed spectrum. A new generation of scenarios and services in 5G systems can hence be enabled, including device relaying, context-aware services, mobile cloud computing, off load strategies, and disaster recovery. Four different types of D2D communications can be distinguished:

- Device relaying with operator controlled link establishment: any device can broaden the coverage of the BS, by acting as a relay node.
- Direct D2D communication with operator controlled link establishment: any pair of network nodes can directly interact due to a D2D link, which is set up under the control of the operator.
- Device relaying with device controlled link establishment: the endpoints of a data session are in charge of setting up a relaying infrastructure made of one or more relaying devices.
- Direct D2D communication with device controlled link establishment: any pair of devices can exchange messages thanks to a D2D link, which is established without any operator control.

Enabling IoT communications in the licensed band is essential to strengthening the support to mission critical applications and group communications. Besides these advantages of D2D communications, security, trust, interference management, resource discovery, and pricing issues should be addressed to capitalize the potential of this technology. These issues become very challenging when the D2D link is set up without any involvement of the BS. Moreover, new business models are required to answer the ”pay for what” question. In fact, devices that act as relays will deplete their own resources (as battery, storage, communication, and processing) to assist theD2D model. Cross-operator D2D capability is an open challenge complicated by the fact that FDD spectrum bands are different for different operators.

C. 4G-Evolution & 5G RAN Enablers

T The RATs, illustrated in Sec. IV-B, will need to be supported by a suitable RAN. Some interesting propositions have been made w.r.t. RAN which are briefly discussed here.

1) Decoupled Down/Uplinks: The traditional notion of a cell is changing dramatically given the increasing degree of heterogeneity. Rather than belonging to a specific cell, a device would choose the most suitable connection from the many possible of connections available. In such a setting, given that transmission powers differ significantly between downlink (DL) and uplink (UL), a wireless device that sees multiple BSs may access the infrastructure in a way that it receives the DL traffic from one BS and sends UL traffic through another BS. This concept had recently been introduced and is referred to as Downlink and Uplink Decoupling (DUDe) [41]–[43]. DUDe was shown to yield significant throughput gains and, more importantly in the context of the IoT, orders of magnitude improvements in reliability. The high-level system architecture is shown in Figure 2 where some IoT devices in a given area are connected in DL/UL to the macrocell, some are connected in DL/UL to the smallcell; and some have a decoupled access.

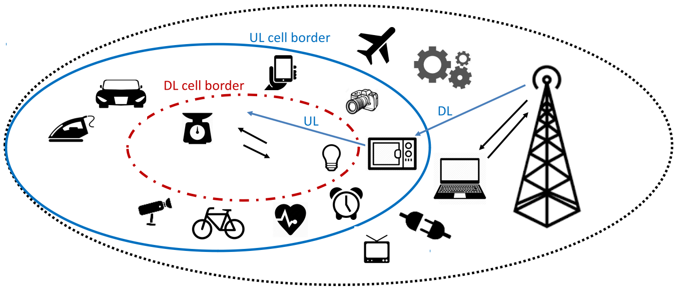

Fig. 2. DUDe system model for UL/DL decoupling.

2) License Assisted Access: Recently, the 3GPP commenced a work item on License Assisted Access (LAA), where licensed and unlicensed carriers are aggregated. LAA uses licensed spectrum for control-related transmissions while sending data over both licensed and license-exempt carriers. Whilst mainly designed for high-capacity applications, the approach could be beneficial in the context of a ever-increasing amount of IoT devices with increasing data rate demands. Notably, all non-critical IoT traffic could be transmitted via the licence-exempt band whilst being controlled from the licensed band.

3) Radio Access Network as a Service: The solution space of 5G management architectures spans from centralized to fully distributed ones. Based on the degree of centralization different scalability, stability, and optimality targets can be reached. To sustain flexible management approaches the Radio Access Network as a Service (RANaaS) concept has been developed [44]. With the RANaaS, Radio Access Network (RAN) resources are virtualized and exposed through cloud platforms. By using this approach, management functionalities can be split between BSs and the cloud based on the degree of centralization that is required in any specific networking context. Of course, when BS functionalities are migrated to the cloud some extra delay may be incurred in the , execution of management operations, so that the degree of centralization should be proportional to the capacity of the backhaul. RANaaS enables : (i) dynamic wireless capacity allocation in time and space varying 5G systems; (ii) increased flexibility of management platforms due to a technology independent state representation of hyper-dense 5G deployments; (iii) new stores of management functionalities provided by third parties (i.e., new business opportunities); (iv) easy coexistence of multiple operators, sharing the same physical infrastructure.

With reference to IoT systems, *self-** capabilities, including *self-healing, self-configuration, self-protection, and self-optimization*, can improve the flexibility and extensibility of the communication infrastructure due to modern orchestration of available radio access and IoT technologies [45]. In critical applications, self-* functionalities could allocate extra bandwidth to those IoT devices that detected some dangerous events and hence need to communicate at the maximum speed (and with the highest reliability and timeliness). Also, self-* functionalities can ease the optimization of radio resources so that a higher number of devices can be connected to the network, which is essential for a mass scale IoT deployments. The key challenge related to *self-** capabilities is tuning degree of centralization and to enable radio resource optimization also in presence of coexisting operators that share the same physical infrastructure.

D. 4G-Evolution & 5G Network Enablers

Finally, we discuss the emerging network enablers which are pertinent to supporting the above IoT RAT/RAN enablers. From several possible enablers, we shall focus on software defined networking (SDN) and Network Function Virtualization (NFV).

1) Software Defined Networking: The Software Defined Networking (SDN) paradigm initially designed for wired networks (e.g., data centers), has recently gained a lot of interest into the wireless environment [46], and it is seen as a key technology enabler for 5G networks [47], [48]. SDN separates the data plane (i.e., the traffic forwarding between network devices, such as switches, routers, end hosts) from the control plane (i.e., the decision making about the routing of traffic flow - forwarding rule) [49]. SDN centralizes network control into a logical entity, namely SDN controller, and allows programmability of the network, by external applications. With its centralized view of the network (topology, active flows, etc.), SDN provides dynamic, flexible, and automated reconfiguration of the network. SDN will be able to address flexibility and interoperability challenges of future multi-vendor, multi-tenant 5G scenarios. In fact, with SDN it will be possible to deploy a vendor-independent service delivery platform, able to proactive respond to the changing business, end-users and market needs. Therefore, SDN will simplify network design, management and maintenance in heterogeneous networked environments [50].

With the explosion of devices connected through IoT, traditional network architectures will not be able to manage both the volume of devices, and the amount of data they will be dumping into the network. There will be need to efficient manage the load of traffic and the network resources in the 5G era, to avoid possible collapse of the network, and allow the coexistence of different services with different Quality of Service (QoS) requirements [51]. SDN will be among the technologies addressing such issues in future IoT applications, as envisaged by the current emerging activities at IETF (DetNet, 6TiSCH).

2) Network Function Virtualization: Network Function Virtualization (NFV) is a complementary technology of SDN, destined to impact future 5G networks. NFV aims to virtualize a set of network functions, by deploying them into software packages, which can be assembled and chained to create the same services provided by legacy networks. The NFV concept comes from the classical service whereby many virtual machines running different operating systems, software and processors, can be installed on the same server. By moving network functions from dedicated hardware into general purpose computing/storage platforms (e.g. servers), NFV technologies will allows to manage many heterogeneous IoT devices. Moreover, by implementing the network functions in software packages that can be deployed in virtualized infrustructure, NFV offers scalability and large flexibility in operating and managing mobile devices. With NFV it will be possible to reduce both CAPEX and OPEX. Currently, the use of NFV is under discussion in the context of virtualizing the core network, and centralizing the base band processing within Radio Access Networks (RAN) [52].

V. MTC Architecture in 5G

M2M architectures allow the different actors of an IoT system to exchange data, check the availability of resources, discover how to compose complex services, handle device registration, and offer a standardized output to any vertical application [53]. Currently, the main challenge with M2M architectures is the vertical fragmentation of the IoT market; according to the Global Standards Collaboration Machine-to-Machine Task Force, more than 140 organizations are involved in M2M standardization worldwide. In this perspective, the reasons behind the proliferation of M2M architectures come from long ago; the first ancestors of the todays' M2M systems were the industrial fieldbuses, designed in the seventies to support process control applications. At that time, each production plant was adopting its own M2M technology and, as a legacy, the same approach has been applied, in the last twenty years, to define currently available M2M specifications. Nowadays, each vendor adopts its own protocols and data formats so that interoperability remains an utopian requirement, while vendor lock-in issues worsen the quality-price tradeoff and hinder the diffusion of IoT technologies. Recently, two noticeably international standardization projects (i.e., ESTI SmartM2M and oneM2M) have been formulated to resolve fragmentation issues in M2M systems, based on a RESTful design [54]. Both of them target the definition of an horizontal service layer that is able to embrace different existing communication technologies and to include future extensions to 5G systems.

A. ETSI SmartM2M

One of the most relevant attempts to resolve fragmentation issues has been put in place by European Telecommunications Standards Institute (ETSI), which defined a horizontal service platform for M2M interoperability. The resulting SmartM2M standard platform is based on a RESTful Service Capability Layer (SCL) [55] and it is accessible through open interfaces. Using this horizontal service layer it becomes possible to set up IoT services in a technology independent way.

The different instances of the SCL can run on top of devices, gateways, and network instances (see also Fig. 3) to enable generic communication, reachability, addressing , remote entity management, security, history and data retention, transaction management, , and interworking proxy.

The smartM2M architecture is made of two domains: the Device/Gateway Domain and the Network Domain. The former includes devices and gateways. The latter represents an abstract system that enables all the services entailed by the smartM2M architectures by leveraging the resources available at the lower domain.

An M2M Device can run M2M Applications using a local instance of the SCL. In this case, it is connected directly to the Network Domain via the Access network and it may provide services to other devices. It can also be connected to the Network Domain via an M2M Gateway. The M2M Network provides connectivity between M2M Devices and M2M Gateways. An M2M Gateway also runs M2M Applications using a local instance of the SCL and acts as a proxy between M2M Devices and the Network Domain and may provide service to other devices [53].

ETSI M2M adopted a RESTful architecture style, thus an SCL contains a resource tree where the information is kept. The resource tree structure that resides on an SCL as well as the procedure for handling the resources have been also standardized. A Resource is a uniquely addressable entity in the RESTful vocabulary. Each resource has a representation that may be transferred and manipulated with the Create, Retrieve, Update, and Delete verbs. A resource shall be addressed using a Universal Resource Identifier (URI). Operation on resource among Applications and SCLs, and between SCL instances are supported by means of Methods that constitute the communication on the several interfaces of the SmartM2M architecture. Each method conveys a set of information defined as Method Attributes.

An SCL resources tree (see also Fig. 4) includes different kinds of resources as follows: sclBase, scls, scl, applications, application, and henceforth. The *sclBase* resource describes the hosting SCL, and is the root for all other resources within the hosting SCL. The *scl* resource stores information related to distant SCLs, residing on other machines, after successful mutual authentication. The *application* resource stores information about the application after a successful registration on the hosting SCL. The *container* resource acts as a mediator for data buffering to enable data exchange between applications and SCLs. The *contentInstance* resource represents a data instance in the container. The *accessRight* resource manages permissions and permissions holders to limit and protect the access to the resource tree structure. The *group* resource enhances resources tree operations by adding the grouping feature. For instance, a group resource could be used to write the same content to a group of M2M resources. The *registration* resource allows subscribers to receive asynchronous notification when an event happens such as the reception of new sensor event or the creation, update, or delete of a resource. The *announced* resource contains a partial representation of a resource in a remote SCL to simplify discovery request on distributed SCLs. The *discovery* resource acts as a search engine for resources. The *collection* resource, groups common resources together.

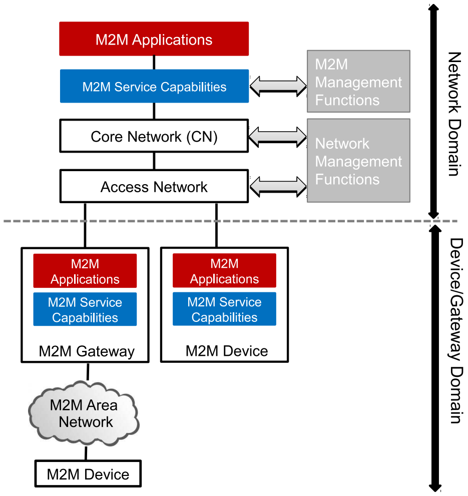

Fig. 3. SmartM2M high level architecture.

With reference to security issues, the standard also defines an M2M security framework, encompassing authentication, key agreement and establishment, M2M service bootstrap, and M2M service connection procedures, grounded on a clearly defined key hierarchy of the M2M node [56].

The SmartM2M architecture is very flexible and extensible, but, as pointed out in [57], it may suffer scalability issues because all transactions are mediated by the M2M Network, which can easily become a single point of failure or a bottleneck.

B. From SmartM2M to oneM2M

With similar objectives but with a broader partnership, the oneM2M Global Initiative has been recently chartered as an international project. oneM2M also targets the definition a horizontal service layer that interconnects heterogeneous M2M hardware and software components on a global scale. oneM2M has been kicked off by seven telecom standards organizations: Association of Radio Industries and Businesses (ARIB) and Telecommunication Technology Committee (TTC), Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and Telecommunications Industry Association (TIA), United States; the China Communications Standards Association (CCSA), China; the European Telecommunications Standards Institute (ETSI), Europe; and the Telecommunications Technology Association (TTA), Korea. These organizations involve around 270 companies that are actively contributing to oneM2M [58].

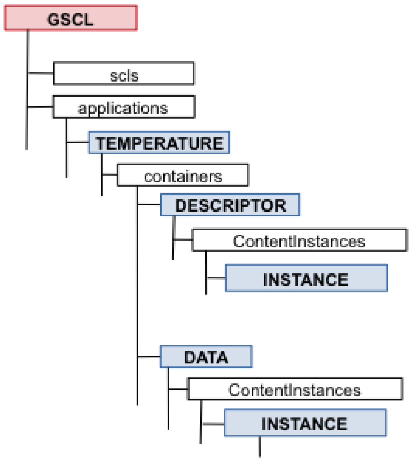

Fig. 4. ETSI URI resource tree structure (example).

From an architectural point of view, both oneM2M and ETSI SmartM2M adopt a RESTful design, name resources through a hierarchical name space, and are grounded on the concept of horizontal service layer. In contrast to SmartM2M, oneM2M relaxes scalability restraints by adopting an hierarchical organization of the different actors in the system, so that a logical tree of nodes is obtained, which include application dedicated node (ADN), application service node (ASN), middle node (MN), and infrastructure node (IN). Nodes consist of at least one common services entity (CSE) or one application entity (AE). A CSE is a logical entity that is instantiated in an M2M node and comprises a set of service functions called common services functions (CSFs). CSFs can be used by applications and other CSEs. An AE is a logical entity that provides application logic, such as remote monitoring functionalities, for end-to-end M2M solutions.

The standard also defines a security architecture articulated over three layers: security functions, security environment abstraction, and secure environment. Security functions include: identification, authentication, authorization, security association, sensitive data handling and security administration. Security environment abstraction offers many security primitives, such as key derivation, data encryption/decryption, signature generation/verification, and security credential read/write from/to the secure environments. This layer is not specified in the initial release but is expected to be considered in future ones. The security environment layer contains one or multiple secure environments that provide different security services related to sensitive data storage and sensitive function execution [59].

VI. Flip of Business Models

The Internet has undergone a massive transformation from being infrastructure-driven (Ethernet cables, routers, computers, etc.) to business-driven (Facebook, eBay, Google). The Internet of Things is undergoing a similar transformation. Today, we expend significant efforts to design sensors, connectivity radios, gateways and basestations. In a few years' time, efforts will hopefully be on business opportunities, e.g. a "Google of Things"; business opportunities here, however, are strongly dependent on regulation around privacy and trust in the technology. In this section, we therefore discuss this transformation and the role the telecommunications ecosystem will likely play.

A. Demand-Side Problem in IoT

The number of connected "things" in the Internet of Things is not meeting the predictions made a few years back. In general, the IoT rollout lags behind in terms of what market research has predicted. This is really surprising to many since there is no doubt that instrumenting the planet with IoT capabilities would yield significant operational savings and/or financial gains. To understand the underlying market dynamics, one has to understand that for new technologies to succeed, three things need to come together: i) supply of the technology itself; ii) proven business models which link supply to demand; and iii) a strong market demand.

From previous sections of this paper, we can see that there is a large supply of connectivity technologies and standards available today. These have been tested and many of them are used successfully in various deployment around the world. Claims that there is a lack of technologies or standards to unlock the IoT market are largely unfounded.

From a business modeling point of view, numerous models are available today and some of them have been successfully tested in real commercial deployments. For example, in the smart city market, the city hall could use smart parking sensors, smart garbage bin sensors and/or smart street- lighting sensors. The smart parking sensors are not only able to guide drivers to vacant parking spots (and thereby reducing driving time, pollution, etc) but also correlate the occupancy data with the payment data; the latter allows infringements to be spotted more efficiently and thus improve the city's financial income from parking. The smart bin sensors are able to detect when exactly the bin needs to be emptied, thereby improving pick-up schedules and saving money to the city hall. The smart street-lighting sensors are able to regulate the usage of the lamps according to ambient light conditions, as well as movement in the street (i.e. if nobody passes at 3am in the night, they switch off); this yields an estimated saving of 30% in the electricity bill in cities.

Why, given the supply of technology and strong business models, is the IoT not taking off as quickly as we had hoped? The reason is because market demand remains consistently low. This is entirely normal with new technologies and markets. For instance, the Internet took more than a decade to gain widespread use: people were doing accounting and shopping for years without the Internet, to change that habit took time. In the IoT smart city context: the city was manually measuring air pollution for many years − why would they start using autonomous sensors now? That is arguably the biggest challenge for the IoT today, i.e. create a genuine demand among industries and consumers. Once that demand is created and procurement as well as supply chains adapted, the IoT will take off exponentially, just as the Internet has around 2000.

B. IoT Return-of-Investment

To support the strength of today's IoT business models, let us examine the typical return of investment (ROI) metrics used. The ROI is a major driver in the adoption of any technology, as it indicates the ability to return the initial financial investment. There are three major ROI arguments to use IoT technologies:

1) Real-Time Instrumentation ROI: A study by General Electric has identified the enormous efficiency benefits stemming from real-time instrumentation by means of industrial IoT technologies [60]. The study has looked at verticals like transportation, health, manufacturing, etc. While the study has not considered the cost of the instrumentation, the strong ROI drive has become evident.
2) Big Data Value ROI: Not so well quantified as of 2015, there is understood to be an enormous value in cross-correlating data from different verticals to give unique insights which would not be evident on their own. An example can be found in smart city transportation where IoT data from traffic is cross-correlated with weather and sports data, thus allowing to define viable traffic management strategies on days where congestion is likely. That is probably the most important ROI and signals the true shift from an infrastructure to a data-driven ecosystem.
3) Wireless ROI: A fairly straightforward but nonetheless important drive in rolling out wireless IoT is the fact that getting rid of cables allows achieving substantial CAPEX and OPEX gains. While electronics and sensors become cheaper over time, human labor and cable costs (due to copper) increase. Going wireless saves cable costs (CAPEX), installation efforts (CAPEX) and system maintenance (OPEX).

Above ROI argumentations highlight that there is not only utility in using IoT technologies but there are clear financial returns. Once demand has picked up, the market up-take will almost certainly be guaranteed.

C. Zero-Capex IoT Business Models

In the context of smart cities, many municipalities as well as governments are striving to deliver a higher quality of public services; however, they are usually challenged by the lack of funding and poor financial capabilities [61]. So far the most common means for a city to become smart is to receive governmental funds; for instance, Glasgow (UK) recently won a governmental grant of 24 $M£$ to become the countrys first smart city. Even though these awards could be perceived as a good start for smart city initiatives, such awards are not self-sustaining of deploying IoT technologies.

Given IoT business models are generally solid (and accepted), the demand up-take can be accelerated by covering the often large CAPEX costs by the operational gains. An ideal scenario is where all up-front CAPEX costs are covered by a bank through a loan which is being paid back over time through the financial returns or savings. This approach is is just beginning in the context of the IoT and smart cities, but early results are available from [62].

Notably, [62] observes that most IoT business models have a given CAPEX cost c and an operational income which scales roughly linearly over time with gradient a. The operational income is composed of the revenues/savings from using the IoT technology, diminished by the OPEX costs (typically in the order of 10% of the CAPEX cost per annum). Three different models are investigated, i.e. i) the quickest rollout by deploying all IoT technologies at once; ii) the lowest CAPEX rollout by deploying the technology with the lowest c first and then deploy the second-lowest c the moment it can be paid by the first technology due to making financial gains; and iii) deploy in such an order that risk to investors is minimized by understanding the different growth estimation errors.

D. 3GPP's Universal Control Capabilities?

Let us assume there is a massive demand for IoT by 2020 and the rollouts are increasing exponentially. Three operational models are possible:

1) The ”Bluetooth Model”, i.e. where the consumer and industry purchase the IoT equipment and handle connectivity themselves. As explained in Section II, the disadvantage is that many critical IoT applications will probably not work well.
2) The ”Wifi Model”, i.e. local connectivity is provided and largely managed through an IoT operator which bills the customer on a monthly basis. While the operational pain is taken out for the customer, the IoT operator is not able to guarantee delivery of critical IoT data since license-exempt spectrum is used.
3) The ”Cellular Operator Model”, i.e. truly global connectivity is provided using a cellular IoT provider (which does not need to be the traditional operator). While a few technical challenges still need to be solved, the advantage is obvious in that reliable and accountable connectivity can be provided globally which is an important value add to both consumers and business relying on IoT technologies.

The third ”Cellular Operator Model” opens up other interesting operational, in addition to those already discussed above in this paper. Notably, if/once 3GPP opens up to other IoT connectivity technologies (see below), then it could act as a truly global IoT control engine. Using 3GPP's authentication, security, billing and SLA capabilities (to mention a few), it could provide all these services as an umbrella while the underlying technologies can be 3GPP-based or non-3GPP-based. Technology enablers, such as license-assisted access (LAA), local IP access (LIPA), capillary networking architectures (as developed in ETSI M2M), among many others, are available already today. In addition, the recent proposition by Vodafone to fast-track Neul[2]-like technologies in 3GPP will likely accelerate such a development.

From a business point of view, this means that 3GPP would slowly shift from providing data pipes to rather controlling an ensemble of data pipes. That would signal an important shift for operators from business-to-consumer (B2C) driven business to rather business-to-business (B2B) driven one. In principle, this is an important opportunity to scale sales as cellular servicing is extended to any available wireless system.

E. Shake-Up in Cellular Value Chain?

From above, it is obvious that the IoT could enable a true transformation in the cellular ecosystem. While the per-bit value of IoT is rather low, the value due to a holistic orchestration and big data exploitation is enormous. Let's briefly examine the possible shifts in the ecosystem for both operators and vendors.

Operators will add an important value due to global orchestration, relying on roaming and other agreements already struck in the ecosystem. This saves a lot of operational hassle and it difficult to reproduce by e.g. the Wifi community. Furthermore, a lot of the IoT deployments will be critical which requires e.g. application/content-hosting cloud technologies to be placed right at the edge, i.e. into the operators networks. In addition, net-neutrality regulations may apply less stringently to machines and – through SDN – operators have all the technical means to reserve special data pipes for IoT traffic and thus giving an operator-run IoT deployment a cutting-edge over other deployment approaches. For all this, operators will be able to charge premium rates to an extent which other communities are not able to do which is a fundamental shift on how this market will run.

Vendors, on the other hand, will likely capitalize on the unique characteristics of industrial IoT deployments. Notably, that market will be heavily B2B-driven and less B2C-driven. The latter is well-understood by operators while the former is much better understood by vendors. We will thus likely see many B2B alliances struck between a vendor and an industrial IoT B2B company. Understanding that IoT equipment is typically deployed for many years, the vendors lock themselves into the IoT market which brings them into a strong market position. Indeed, they will be able to procure the best operator offer and thus have operators compete for their IoT equipment

[2] http://www.neul.com/neul/

deployments. This is a fundamental shift in how the cellular market operates.

F. IoT Data Privacy and Trust

Above business opportunities will not emerge if some fundamental issues around IoT data privacy and trust are provided. Notably, new trust models are expected to emerge, raising new extended requirements for authentication between different actors, accountability and non-repudiation. In 5G scenarios, several different devices will be interconnected together, each of them with its own security requirements. Thus, for a device to not represent a potential attack for the whole network, it will not be enough to be compliant to the standard it implements. On top of this, very-low cost devices will need to be protected using lighter-solutions which do not impact too much on their lifetime. Obviously the current trust model does not fulfill the needs of the evolved business and technological 5G scenario. Therefore, it should be re-designed, identifying the crucial shortcoming, and proposing new suitable solutions [63].

Together with faster and more efficient techniques for handling security procedures (especially needed for low-latency scenarios), the 5G security architecture will have to pay particular attention to *protection of personal data* [64]. The increased privacy concern has already emerged in society and been discussed by the European Commission, standardization bodies, including 3GPP and IETF, and many other forums. Actually, since 2G, user privacy has been carefully considered. But, till now the advantages offered by the International Mobile Subscriber Identity (IMSI) protection have not appeared to outweigh the complexity of its implementation. Thus, solutions for *location and identity privacy* should be improved, with respect to those currently used for 4G, trying to minimize the overhead they introduce.

Recently, some important vulnerabilities have been disclosed in current 4G LTE systems [65]. They are based on the inevitable tradeoff between performance and security which any system must made. 5G puts together and integrates a heterogeneous set of wireless access technologies, enabling seamless connectivity. This might result into an increase of the potential set of vulnerabilities. For data traversing several different connectivity technologies, vulnerabilities on one of them could be exploited to gain access and attack the whole system.

VII. Conclusions

5G technologies and the Internet of Things are among the main elements which will shape the future of the Internet in the coming years. In this paper, we have analyzed in detail the potential of 3GPP-defined 5G technologies for the IoT, by placing them in the context of the current connectivity landscape for IoT. Differently from previous cellular technologies which were designed essentially for broadband, the requirements which the future 5G networks will have to satisfy, and particularly those for MTC make 5G communications a particularly good fit for IoT applications. By offering lower cost, lower energy consumption and support for very large number of devices, 5G is ready to enable the vision of a truly global Internet of Things.

Table I summarizes the main 5G KPIs [66], and highlights which of the available/emerging technologies are able to meet them. Cellular technologies, and especially 3GPP LTE, are among the most appealing technologies in the modern IoT connectivity landscape. They offer wide coverage, relatively low deployment costs, high level of security, access to dedicated spectrum, and simplicity of management. With the MTC optimized Rel-12/13 and the introduction of NB-IoT, LTE is also both low cost (communication module cost sub 10 USD) and low power (10 year life time).

The global coverage, along with solid Radio Resource Management (RRM) algorithms, yields a robustness and reliability not offered by any competing technologies. The already deployed infrastructure, which is in essence subsidized through data/voice traffic, does not require the deployment of an additional IoT infrastructure, such as observed for Zigbee or LPWA. This, in turn, lowers the deployment barrier of entry and the running costs to the point that total cost of ownership (TCO) is one of the lowest when compared to competing solutions (despite the higher modem costs and data plans).

One of the most interesting features of MTC is the ability to offer SLAs even for the most critical and demanding industry applications. Such agreements can be honored since the spectrum is exclusively owned by the operators, in contrast to the ISM band used by Zigbee/LP-Wifi/LPWAs. The result is that Industrial IoT companies, such as Worldsensing [3], can focus on attracting new customers rather than spending resources on solving (and being liable for) connectivity . This is a very important business proposition which may prove decisive in the battle for market share.

Despite the convincing advantages, some serious challenges remain to make MTC an underlying connectivity backbone for the Internet of Things. These challenges are pertinent at device and networking levels, and when it comes to a viable business proposition.

From a device point of view, the two largest issues to date (2015) are energy consumption and modem cost. Regarding the energy consumption, given that transmission powers cannot be reduced significantly if communication ranges are to be maintained, the only solution is to facilitate MTC data transmission and reception in the shortest time possible. At device level, this requires a novel approach to device duty cycling (i.e. the ability to put the MTC device in an ultra-low power state). Regarding modem cost, the performance requirements of current MTC devices are unnecessarily high for many low end IoT applications. Current 3GPP efforts thus concentrate on reducing the performance requirements and complexity which will enable simplified device implementations and lowered cost.

From a network point of view, the biggest challenge pertains in facilitating the data transfer from and to the devices as quickly as possible. Currently, delays occur in radio bearer establishment and due to congestion in the wireless channel. Therefore, entirely novel approaches in radio-bearer establish-

[3] http://www.worldsensing.com/

TABLE I
IoT Key Performance Indicators (KPIs) covered by modern connectivity technologies.

	ZigBee	BLE	LP-Wifi	LPWA	3GPP Rel8	LTE Rel13 & NB-IoT
Scalability	✗	✗	✓	✗	✓	✓
Reliability	✗	✓	✓	✗	✓	✓
Low Power	✓	✓	✓	✓	✗	✓
Low Latency	✗	✓	✓	✗	✓	✓
Large Coverage	✗	✗	✓	✓	✓	✓
Low module cost	✓	✓	✓	✓	✗	✓
Mobility support	✗	✗	✗	✗	✓	✓
Roaming support	✗	✗	✗	✗	✓	✓
SLA support	✗	✗	✗	✗	✓	✓

ment for very short and infrequent IoT data is required in 5G. Furthermore, if scalability is to be ensured, novel random access protocols need to be designed which are able to cope with both IoT as well as voice/data traffic.

Our analysis puts in evidence that such a synergy and mutual shaping between 5G and IoT might also have interesting implications from the point of view of business models. Specifically, we have identified the role which 5G communications might play in the shift of IoT from infrastructure-driven to business-driven, and we have given some indications on how the cellular value chain might get transformed by massive IoT deployments. Our analysis concludes that, once market demand for IoT services will be created, 5G will constitute an essential enabler of a full IoT roll-out.

Acknowledgment

This work was partially funded by the European Commission H2020 5GPPP projects NORMA, VirtuWind, and by the FANTASTIC-5G project, which receives funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement ICT-671660. It was also partially supported by the CoSDN project, INTER/POLLUX/12/4434480, funded by the Fonds National de la Recherche Luxembourg. The authors would also like to thank Prakash Bhat, Vodafone, UK, and Sama Thareefeh for their valuable input.

References

[1] M. Weiser, "The computer for the 21st century," *Scientific american*, vol. 265, no. 3, pp. 94–104, 1991.

[2] J. Pontin, "Bill joy's six webs," in *MIT Technology Review*, September 2005.

[3] C. Gomez, J. Oller, and J. Paradells, "Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[4] M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? comparative measurements with zigbee/802.15.4," in *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*. IEEE, 2012, pp. 232–237.

[5] M. Research, "The need for low cost, high reach, wide area connectivity for the internet of things. a mobile network operator's perspective." *white paper*, 2014.

[6] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011. [Online]. Available: http://dx.doi.org/10.1007/s11277-011-0288-5

[7] M. R. Palattella, P. Thubert, X. Vilajosana, T. Watteyne, Q. Wang, and T. Engel, "6tisch wireless industrial networks: Determinism meets ipv6," in *Internet of Things*. Springer, 2014, pp. 111–141.

[8] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 4, pp. 2233–2243, 2014.

[9] M. Swan, "The quantified self: Fundamental disruption in big data science and biological discovery," *Big Data*, vol. 1, no. 2, pp. 85–99, 2013.

[10] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146 – 164, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[11] 3GPP, "Study on Provision of Low-Cost Machine-Type Communications (MTC) User Equipments (UEs) Based on LTE," June 2013.

[12] IEEE std. 802.15.4, *Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE standard for Information Technology, Sep. 2009.

[13] IETF WG, "IPv6 over Low power Wireless Personal Area Networks (6LoWPAN)." Available online: http://tools.ietf.org/wg/6lowpan/.

[14] ——, "Routing Over Low Power and Lossy Networks (ROLL)." Available online: http://tools.ietf.org/wg/roll/.

[15] S. Andreevy, O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy, "Understanding the IoT connectivity landscape: A contemporary m2m radio technology roadmap," *Communications Magazine, IEEE*, to appear.

[16] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 3, pp. 1389–1406, 2013.

[17] IEEE std. 802.15.4e, *Part. 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendament 1: MAC sublayer*, IEEE standard for Information Technology, April 2012.

[18] K. Pister and L. Doherty, "Tsmp: Time synchronized mesh protocol," in *IASTED International Symposium on Distributed Sensor Networks (DSN08)*. Orlando, Florida, USA: IEEE, Nov. 2008.

[19] Industrial Communication Networks - Wireless Communication Network and Communication Profiles, "WirelessHART - IEC 62591." Available online: http://www.hartcomm.org, 2010.

[20] ISA/IEC, "ISA100.11a, Wireless System for Automation, IEC 62734." Available online: http://www.isa100wci.org/enUS/Documents/PDF/3405-ISA100-WirelessSystems-Future-brochWEB-ETSI.aspx, 2011.

[21] IETF WG, "IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH)." Available online: http://tools.ietf.org/wg/6tisch/.

[22] The Bluetooth Special Interest Group, "Specification of the Bluetooth System, Covered Core Package," 2010.

[23] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez, "Ipv6 over bluetooth(r) low energy," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-6lo-btle-17, August 2015, http://www.ietf.org/internet-drafts/draft-ietf-6lo-btle-17.txt. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-6lo-btle-17.txt

[24] R. Want, "The physical web," in *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*, ser. IoT-Sys '15. New York, NY, USA: ACM, 2015, pp. 1–1. [Online]. Available: http://doi.acm.org/10.1145/2753476.2753496

[25] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on ieee 802.11 ah: An enabling networking technology for smart cities," *Computer Communications*, vol. 58, pp. 53–69, 2015.

[26] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "Ieee 802.11 ah:

the wifi approach for m2m communications," *Wireless Communications, IEEE*, vol. 21, no. 6, pp. 144–152, 2014.

[27] T. Rebbeck, M. Mackenzie, and N. Afonso, "Low-powered wireless solutions have the potential to increase the m2m market by over 3 billion connections," *report*, September 2014.

[28] ETSI GS LTN 001, "Low Throughput Networks (LTN): Use Cases, Functional Architecture, an Protocols," September 2014.

[29] 3GPP TR 33.860, "Study on Security aspect of cellular systems with support for ultra low complexity and low throughput Internet of Things," Sept 2015.

[30] 3GPP TR 33.863, "Study on battery efficient security for very low throughput Machine Type Communication Devices," Sept 2015.

[31] J. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *Communications Magazine, IEEE*, vol. 51, no. 3, pp. 136–144, March 2013.

[32] H. Ali-Ahmad, C. Cicconetti, A. de la Oliva, M. Drxler, R. Gupta, V. Mancuso, L. Roullet, and V. Sciancalepore, "Crowd: An sdn approach for densenets," in *Proceedings of the 2013 Second European Workshop on Software Defined Networks*, ser. EWSDN '13. Washington, DC, USA: IEEE Computer Society, 2013, pp. 25–31. [Online]. Available: http://dx.doi.org/10.1109/EWSDN.2013.11

[33] B. Soret, K. Pedersen, N. Jorgensen, and V. Fernandez-Lopez, "Interference coordination for dense wireless networks," *Communications Magazine, IEEE*, vol. 53, no. 1, pp. 102–109, January 2015.

[34] F. Boccardi, R. Heath, A. Lozano, T. Marzetta, and P. Popovski, "Five disruptive technology directions for 5g," *Communications Magazine, IEEE*, vol. 52, no. 2, pp. 74–80, February 2014.

[35] M. Condoluci, M. Dohler, G. Araniti, A. Molinaro, and K. Zheng, "Toward 5g densenets: architectural advances for effective machine-type communications over femtocells," *Communications Magazine, IEEE*, vol. 53, no. 1, pp. 134–141, January 2015.

[36] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5g of terrestrial mobile telecommunication," *IEEE Communications Magazine*, May 2014.

[37] X. Zhang, X. Shen, and L.-L. Xie, "Joint subcarrier and power allocation for cooperative communications in lte-advanced networks," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 2, pp. 658–668, February 2014.

[38] N. Zlatanov, A. Ikhlef, T. Islam, and R. Schober, "Buffer-aided cooperative communications: opportunities and challenges," *Communications Magazine, IEEE*, vol. 52, no. 4, pp. 146–153, April 2014.

[39] X. Tao, X. Xu, and Q. Cui, "An overview of cooperative communications," *Communications Magazine, IEEE*, vol. 50, no. 6, pp. 65–71, June 2012.

[40] M. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions," *Communications Magazine, IEEE*, vol. 52, no. 5, pp. 86–92, May 2014.

[41] H. Elshaer, F. Boccardi, M. Dohler, and R. Irmer, "Downlink and uplink decoupling: a disruptive architectural design for 5g networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*. IEEE, 2014, pp. 1798–1803.

[42] ——, "Load & backhaul aware decoupled downlink/uplink access in 5g systems," *arXiv preprint arXiv:1410.6680*, 2014.

[43] F. Boccardi, J. Andrews, H. Elshaer, M. Dohler, S. Parkvall, P. Popovski, and S. Singh, "Why to decouple the uplink and downlink in cellular networks and how to do it," *arXiv preprint arXiv:1503.06746*, 2015.

[44] P. Rost, C. Bernardos, A. Domenico, M. Girolamo, M. Lalam, A. Maeder, D. Sabella, and D. Wbben, "Cloud technologies for flexible 5g radio access networks," *Communications Magazine, IEEE*, vol. 52, no. 5, pp. 68–76, May 2014.

[45] H. Lateef, A. Imran, M. Imran, L. Giupponi, and M. Dohler, "Lte-advanced self-organising network conflicts and coordination algorithms," *IEEE Wireless Communication Magazine*, in press.

[46] F. Granelli, A. Gebremariam, M. Usman, F. Cugini, V. Stamati, M. Alitska, and P. Chatzimisios, "Software defined and virtualized wireless access in future wireless networks: scenarios and standards," *Communications Magazine, IEEE*, vol. 53, no. 6, pp. 26–34, June 2015.

[47] H.-H. Cho, C.-F. Lai, T. K. Shih, and H.-C. Chao, "Integration of sdr and sdn for 5g," *Access, IEEE*, vol. 2, pp. 1196–1204, 2014.

[48] A. Hakiri and P. Berthou, "Leveraging SDN for the 5g networks: Trends, prospects and challenges," *CoRR*, vol. abs/1506.02876, 2015. [Online]. Available: http://arxiv.org/abs/1506.02876

[49] D. Kreutz, F. M. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[50] M. Mendonca, K. Obraczka, and T. Turletti, "The case for software-defined networking in heterogeneous networked environments," in *Proceedings of the 2012 ACM Conference on CoNEXT Student Workshop*, ser. CoNEXT Student '12. New York, NY, USA: ACM, 2012, pp. 59–60. [Online]. Available: http://doi.acm.org/10.1145/2413247.2413283

[51] M. Amani, T. Mahmoodi, M. Tatipamula, and H. Aghvami, "Sdn-based data offloading for 5g mobile networks," *ZTE communications Magazine*, vol. 2, July 2014.

[52] "Cloud ran," *Ericsson White Paper*, Sept 2015.

[53] D. Boswarthick et al, *M2M Communications: A Systems Approach*. Wiley Publishing, 2012.

[54] L. Richardson and S. Ruby, *RESTful web services*. " O'Reilly Media, Inc.", 2008.

[55] M. B. Alaya, Y. Banouar, T. Monteil, C. Chassot, and K. Drira, "Om2m: Extensible etsi-compliant {M2M} service platform with self-configuration capability," *Procedia Computer Science*, vol. 32, pp. 1079 – 1086, 2014.

[56] ETSI TS 102 690, "Machine-to-Machine communications (M2M); Functional architecture," October 2013.

[57] L. Grieco, M. Ben Alaya, T. Monteil, and K. Drira, "Architecting information centric etsi-m2m systems," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, March 2014, pp. 211–214.

[58] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song, "Toward a standardized common m2m service layer platform: Introduction to onem2m," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 20–26, June 2014.

[59] TS-0003.V1.0.1, "Security Solutions," January 2015.

[60] (2015) GE M2M study. [Online]. Available: http://www.forbes.com/sites/greatspeculations/2014/11/12/ge-is-beginning-to-see-strong-returns-on-its-industrial-internet-investments/

[61] A. Frost, "Smart city as a service," *white paper*, 2015.

[62] S. Thareefeh, "Zero-capex smart city," MSc Thesis, King's College London, Tech. Rep., September 2015, supervised by Prof. M. Dohler.

[63] Ericsson, "5g security, scenarios and solutions," *white paper*, June 2015.

[64] G. M. Koien and V. A. Oleshchuk, *Aspects of Personal Privacy in Communications-Problems, Technology and Solutions*. River Publishers, 2013.

[65] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," *arXiv preprint arXiv:1510.07563*, 2015.

[66] NGMN Alliance, "5G White Paper - Executive Version," *NGMN White Paper*, Dec 2014.