IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 23, 2017, accepted November 23, 2017, date of publication December 4, 2017, date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2779844

A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges

GODFREY ANUGA AKPAKWU[1,2], (Student Member, IEEE), BRUNO J. SILVA[1], (Student Member, IEEE), GERHARD P. HANCKE[1,3], (Senior Member, IEEE), AND ADNAN M. ABU-MAHFOUZ[1,4], (Senior Member, IEEE)

[1]Department of Electrical, Electronic, and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa
[2]Department of Electrical and Electronic Engineering, University of Agriculture at Makurdi, Makurdi 2373, Nigeria
[3]Department of Computer Science, City University of Hong Kong, Hong Kong
[4]Meraka Institute, Council for Scientific and Industrial Research, Pretoria 0184, South Africa

Corresponding author: Godfrey Anuga Akpakwu (godfreyspa@ieee.org)

This work was supported in part by the Department of Research and International Support, University of Pretoria, South Africa, and in part by the Meraka Institute, Council for Scientific and Industrial Research, South Africa.

ABSTRACT The Internet of Things (IoT) is a promising technology which tends to revolutionize and connect the global world via heterogeneous smart devices through seamless connectivity. The current demand for machine-type communications (MTC) has resulted in a variety of communication technologies with diverse service requirements to achieve the modern IoT vision. More recent cellular standards like long-term evolution (LTE) have been introduced for mobile devices but are not well suited for low-power and low data rate devices such as the IoT devices. To address this, there is a number of emerging IoT standards. Fifth generation (5G) mobile network, in particular, aims to address the limitations of previous cellular standards and be a potential key enabler for future IoT. In this paper, the state-of-the-art of the IoT application requirements along with their associated communication technologies are surveyed. In addition, the third generation partnership project cellular-based low-power wide area solutions to support and enable the new service requirements for Massive to Critical IoT use cases are discussed in detail, including extended coverage global system for mobile communications for the Internet of Things, enhanced machine-type communications, and narrowband-Internet of Things. Furthermore, 5G new radio enhancements for new service requirements and enabling technologies for the IoT are introduced. This paper presents a comprehensive review related to emerging and enabling technologies with main focus on 5G mobile networks that is envisaged to support the exponential traffic growth for enabling the IoT. The challenges and open research directions pertinent to the deployment of massive to critical IoT applications are also presented in coming up with an efficient context-aware congestion control mechanism.

INDEX TERMS Internet of Things, long-term evolution, machine-type communications, 5G new radio.

I. INTRODUCTION

The Internet of Things (IoT) is an emerging and promising technology which tends to revolutionize the global world through connected physical objects. IoT deals with low-power devices which interact with each other through the Internet. The concept of the IoT [1]–[6] has drawn the attention of the research community with the end goal of ensuring that wearables, sensors, smart appliances, washing machines, tablets, smart-phones, smart transportation system, etc., and other entities are connected to a common interface with the ability to communicate with each other. IoT interconnect "Things" and enables machine-to-machine (M2M) communication, a means of data communication between heterogeneous devices without human intervention [7]. According to [8], this can be achieved through a seamless communication medium. IoT is expected to enable a conducive environment that will impact and influence several aspects of everyday-life and business applications and contribute towards growing the world's economy, through Massive and Critical IoT, depending on the nature of applications to be deployed. Massive IoT applications require that enormous number of smart devices are connected which could be deployed in shipping environments, smart-homes (buildings) and smart-cities, smart power systems, and agricultural monitoring environments, etc., which requires frequent updates to the cloud with low end-to-end cost. For instance, imagine a scenario in smart-homes, where residents will be able to utilize such application to automatically open their garage on arrival to their homes, switch on lights in their homes or specific area, and have the coffee-maker prepare the early morning coffee for breakfast, control the climate system and other smart appliances. Applications in this domain require low-cost user equipment (UE) with low energy consumption, extended coverage area, and high scalability for effective deployment of Massive IoT. On the other hand, Critical IoT applications including remote healthcare system (for clinical remote monitoring and assisted living), traffic control and industrial control (Drone/Robot/Vehicle) and tactile Internet etc., require higher availability, higher reliability, safety and lower latency to guarantee the end user experience as failure to such applications would result to severe consequences. In general, the various applications opportunities enabled by the IoT are countless and its full potential will only be realized by ensuring that more smart devices are connected through the Internet.

According to forecasts from Ericsson [9], it is estimated that about 28 billion of smart devices will be connected across the global world by 2021, with more than 15 billion of these devices to be connected through M2M and consumer-electronics devices. Research has also shown that roughly 7 billion of these devices will be connected by cellular technologies such as 2G, 3G and 4G which are currently being used for IoT but not fully optimized for IoT applications and Low-Power Wide-Area (LPWA) technology [10] and with a revenue of about 4.3 trillion dollars [11] to be generated across the entire IoT sector globally. The current demand for Machine-Type Communications (MTC) applications such as smart community [12], smart building and surveillance [13], smart cities [14], smart grid [15]–[19], remote maintenance and monitoring systems [20]–[22], and smart water system [23] etc., has brought about massive connected devices which pose a major research issue in terms of capacity for currently deployed and future communication networks [24]. In developing applications to implement MTC technologies, there are considerations that need to be taken into account to ensure that each aspect is carefully examined, such as application development protocols, suitability of network connection and available middleware frameworks. In addition to this, IoT devices are resource-constrained and characterized by low capabilities in terms of both computation and energy capacity. Considering the heterogeneous nature of IoT resource-constrained devices and use cases for MTC, there are a number of requirements that need to be addressed. One of the basic and most fundamental issues for IoT applications is the support for low power operations, because most IoT devices are battery powered sensor nodes which could either be installed on bridges or in basements (for indoor applications for instance) at inaccessible regions [25], and replacing or recharging the batteries of such devices is not feasible. Consequently, such IoT devices are expected to be functional and reliable for a specific number of years. Besides the issue of energy efficiency as a requirement, interoperability is a major issue for MTC applications because these devices are manufactured by different vendors which lack standardization and make interaction between heterogeneous devices a challenge. IoT devices may communicate and disseminate data in various formats, use different application protocols and interfaces for implementation, posing a challenge in achieving flexible communication between heterogeneous devices, mainly caused by the absence of a unique middleware framework for MTC applications. Security and privacy are also very important requirements to be considered for the IoT because of the inherent heterogeneity of Internet connected smart objects and the ability to ensure that sensitive information which are transmitted and physical objects connected through the communication medium are properly monitored and controlled.

Realizing the IoT vision can only be achieved through the integration of various enabling telecommunication technologies to provide connectivity solutions for MTC. The majority of IoT devices were not built or designed to interface with high-bandwidth networks, since these devices were mainly designed with low-power operation in mind. The Long-Term Evolution (LTE) standard for instance, was conceived mainly for mobile broadband. In this context, the Institute of Electrical and Electronics Engineer (IEEE) working group 802.11ah enhanced communication development to support M2M applications. Among these are Bluetooth Low Energy 4.0 [26], ZigBee [27], and Wi-Fi/IEEE802.11 to support short-range communication for MTC. LPWA technologies including Ingenu Random Phase Multiple Access (RPMA) [28], SigFox [29] and LoRa [30] etc., are promising technologies operating in the unlicensed Industrial, Scientific, and Medical (ISM) spectrum band for providing low-power and long-range communications as proprietary solutions. At the same time, in order to ensure that M2M applications are efficiently supported in 2G, 3G, and LTE Cat-1 and higher networks, the 3rd Generation Partnership Project (3GPP) proposed enhancements in its future release for MTC including Enhanced Machine-Type Communications (eMTC), Extended Coverage-Global System for Mobile Communications for the Internet of Things (EC-GSM-IoT) and Narrowband-Internet of Things (NB-IoT) as cellular-based LPWA technologies for the IoT. It is worth mentioning that enabling modern IoT connectivity in the licensed approved spectrum bands will be a key enabler for massive to critical IoT use cases since it offers diverse applications with different service opportunities within a single network. The challenge however, is how the fifth generation (5G) mobile network will meet the diverse requirements of the IoT.

Next generation 5G mobile networks are envisaged to ensure that massive devices and new services such as enhanced Mobile Broadband (eMBB), massive Machine-Type Communications (mMTC), Critical Communications and Network Operations are efficiently supported. It is hoped that basic requirements such as high throughput, low latency in terms of data delivery, high scalability to enable massive number of devices, efficient energy consumption technique and the provision of ubiquitous connectivity solution for end-users will be efficiently supported using the 5G mobile network for the IoT. Consequently, considering the security mechanism of existing cellular networks which are based on protecting basic connectivity and privacy of end-users, the 5G cellular system is expected to ensure that enhanced security mechanism is established on the entire network to address issues on authentication, authorization, and accounting (AAA) for heterogeneous interconnected IoT devices.

M2M communications have been extensively reviewed in the literature [1], [31]–[36]. Pereira and Aguiar [31] discussed on European Telecommunication Standard Institute (ETSI) standard and application protocols while considering mobile devices such as smartphones to be used as mobile gateways for other connected devices with constrained capabilities and the process of aggregating data from embedded sensors in M2M network architecture. Biral *et al.* [32] presented the problems of radio resource allocation which are related to massive Machine-Type Devices and profile solutions to address these issues while considering major challenges which are associated with currently deployed cellular networks to accommodate M2M Communications. Ghavimi and Chen [33] presented the architectural enhancements required to deploy M2M applications for 3GPP LTE/LTE-A network. The article also highlighted issues on diverse random access overload control to prevent congestion which are basically caused by random channel access of M2M devices in LTE-A networks. Condoluci *et al.* [34] discussed various communication standards. In the literature, 5G network is presented for MTC considering design options that could be used for femtocells. According to [35], currently deployed and future cellular technology are promising to deploy and enable M2M communication. Palattella *et al.* [1] in their analysis, provide a detailed investigation of emerging 5G technologies to enable global IoT, while considering both the standardization and technological scenarios and also presented the market view for globally deployed ecosystem. Ali *et al.* [36] presented a survey on M2M communications architectures, with related technologies, protocols and application development for the IoT.

Considering most of the white papers in which operators and vendors based their review connectivity approach against the IoT requirements with emphasis on the likely potential threats that may arise from new connectivity solutions and the various reviews which have been presented on infrastructure-based network for M2M communication, we hereby present a comprehensive review related to emerging LPWA IoT solutions including EC-GSM-IoT, eMTC, NB-IoT and other existing technologies with main focus on 5G mobile network that is envisaged to support the exponential traffic growth and new service requirements including mMTC, eMBB, Critical Communications and Network Operations towards enabling efficient IoT use cases. The main objective of this review is to provide a complete scope of MTC use cases development and requirements, exploring the available connectivity landscape options and promising network enabler to enable the 5G new service requirements and coming up with a context-aware congestion control (CACC) mechanism for lightweight CoAP/UDP-based IoT networks for an efficient resource utilization. To the best of our knowledge, the Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges is the first review paper to comprehensively emphasize an absolute concept on 5G mobile network for the IoT. The structure of this paper is as follows: Section II presents the various application requirements for IoT. Section III discusses existing communication technologies for IoT, including low power wide area networks, short-range wireless networks and cellular networks. Section IV presents the emerging cellular low power wide area standards to enable MTC, such as EC-GSM-IoT, eMTC, and NB-IoT. In Section V, we present new 5G enhancements for the IoT, which is followed by network enablers for the IoT in Section VI. The research challenges and future directions in IoT are discussed in Section VII. Section VIII presents the lessons learned and finally, the concluding remarks are presented in Section IX.

II. IoT APPLICATION REQUIREMENTS

A. EMERGING IoT APPLICATIONS

Given recent advances in ubiquitous computing, there are currently a myriad of diverse IoT applications for many different environments which are expected to enhance and improve the quality of everyday-life for the end-user community. The variety of these applications dictate that there is no *one-fits-for-all* solution, as each of these applications have different characteristics, and they can be broadly categorized into a number of different fields, since they also have different latency and data rate requirements. A number of these applications are discussed below, with focus on the differences in requirements between application domains.

1) SMART HOME

The idea of a smart home [37] is where devices are connected to the Internet and can make decisions autonomously based on information originating from sensors, thereby contributing and improving on the personal lifestyle of end-users which makes it easier to monitor and control home appliances and systems. Smart homes are expected to communicate regularly with their environments (internal and external) [17]. The internal environment can be considered as all Internet-connected smart devices and home appliances. On the other hand, external environment refers to entities which are not in control of the smart home such as smart grid entities. An example is an automatic lighting system which senses the presence of a human being and switches on the lights in a specific area of a house accordingly. This also includes smart appliances which can optimize their energy consumption based on clever scheduling mechanisms and can be remotely switched ON or OFF over the Internet. From an IoT perspective, smart home is one of the main application domains and there are various applications which have been proposed [38]. ZigBee, based on IEEE 802.15.4, is perhaps the most popular standard used in the smart home domain. Proprietary solutions such as Z-Wave [39] are also used, but are not as popular.

2) INTELLIGENT TRANSPORTATION SYSTEM

Intelligent transportation systems (ITS) are used to ensure that the transportation network is efficiently monitored and controlled [40], [41]. ITS is designed to make use of the following network components including vehicle subsystem (which are global position system (GPS), radio frequency identification (RFID) reader, on board unit (OBU), and communication), ITS monitoring unit, station subsystems (such as road-side equipment) and security subsystems to ensure that system reliability, availability, efficiency and safety of the transportation network are guaranteed. Recent research has shown the on-going potential development in autonomous cars (i.e. self-driving cars). Google is a major pioneer in this project [42]. Google in its recent announcements, introduced their prototype vehicles which drove some miles [43] and other autonomous car projects are in development from Audi (Piloted Driving), Ford (Automated Fusion Hybrid), and Mercedes-Benz (Mercedes-Benz Intelligent Drive) etc. Regulatory bodies are currently working on developments that will enable vehicle-to-vehicle communications in new automobiles for future IoT use cases.

3) SMART CITY

There is an extensive number of applications (ubiquitous services) which are envisaged to improve and enhance the quality and lifestyle for city residents through gathering relevant information which are relevant to their needs [44], [45]. This will enable smart technologies to be interconnected in order to ensure that basic services required by residents are provided including (transportation, health, homes and buildings etc.,) which fall under this category, with the most popular being environmental monitoring, smart grid, traffic congestion (which includes vehicle to vehicle communication) and waste management system, amongst others [46]. Similarly to smart homes, the communication devices in these applications are meant for low power operation but can also be spread out over very large areas and require much longer communication ranges than devices in smart homes. Typically, the communications requirements can be considered similar to the smart home case. Meter reading for electricity or water usage [47], for instance, requires much less frequent updates than other applications. LoRa is prominent in smart city applications due to the long ranges it can readily provide.

4) INDUSTRIAL

Unlike the smart city and smart home counterparts, data reliability in the Industrial Internet of Things (IIoT) (especially in process monitoring and control) has to be high [48]. For wireless communication in industrial environments, data is usually deterministic as it has strict time constraints, and is characterized by low latency and jitter for applications like motion control for instance [49]. For monitoring and supervision such as vibration or temperature sensing, delays in the second scale are acceptable, but for close loop control, latency in the millisecond scale (10 – 500 ms) is required [49]. Therefore, the medium access control (MAC) layer in industrial wireless networks usually make use of Time Division Multiple Access (TDMA) such that medium access by sensor nodes is deterministic. Two of the major issues that have inhibited the vision of the IIoT from being realized include the inability of low-power wireless networks to fulfill the requirements of high reliability and small energy consumption, and the IP protocol stack for end-to-end communications was not adapted to the requirements of constrained leaf devices [50]. Additionally, unlike the other application domains previously mentioned, the industrial domain is notorious for proprietary solutions which limit interoperability, whereas the other applications domains are usually more open and use standardized protocols more extensively. Nevertheless, ISA100.11a and WirelessHART are standards based on IEEE802.15.4 which have been specifically designed for industrial applications and can be connected to an Internet Protocol (IP) network.

5) SMART HEALTHCARE

The IoT is expected to strongly impact and influence the medical and healthcare system. Recent developments in wearables arena have opened up opportunities for connected healthcare, where advanced sensor devices are attached to patients to collect medical data and vital signs (including blood pressure, body temperature, cholesterol level, heart rate etc.,) from a patient and be able to diagnose conditions [51], track progress and indicate anomalies directly to the healthcare provider, without significant human involvement. This simplifies the process of collecting patient data and providing an insurmountable quantity of data that can be used to advance scientific studies in disease cures, diagnosis, etc. [52], where low power wearables equipped with sensors serve as data sourcing platforms for doctors and service providers. For instance, Masimo Radical-7, is a special device that can be used remotely to monitor the patient's current health status and report anomalies directly to the clinical staff [53]. In recent research, IBM introduced RFID technology at the OhioHealth's hospital to be used for tracking hand washing after patients have been diagnosed [54], [55]. This will definitely reduce the high rate of infections that causes high rate of death in most patients.

It is evident from the descriptions above that the characteristics for these applications are different, therefore a standard

TABLE 1. Overview of typical characteristics/requirements of IoT application.

Application	Application Domain	Tolerable Delay	Update Frequency	Data Rate
Structural Health [56]	Smart City	30 min	10 min	Low
Waste Management [56]	Smart City	30 min	1 hour	Low
Video Surveillance [57]	Smart City	Seconds	Real Time	High
Air Quality Monitoring [56]	Smart Home	5 min	30 min	Low
Monitoring and Supervision [49]	Industrial	Seconds or ms	Seconds	Low
Closed loop control [49]	Industrial	Milliseconds	Milliseconds	Low
Interlocking and Control [49]	Industrial	Milliseconds	Milliseconds	Low
Patient's Healthcare delivery & Monitoring [57]	Healthcare	Low (seconds)	1 report per hour/day	High
Real-time emergency response & remote diagnostics [57]	Healthcare	Low (seconds)	Requires Ad-hoc emergency communication	High
Real-time management and accuracy of information across supply chain [57]	ITS	Low (seconds)	1 report per hour/day	High

that supports them has to cater for this diversity. Table 1 highlights and summarizes the differences in requirements for these applications. Although, as highlighted above, IoT comprises a diverse set of applications with varying requirements. On one hand, there are delay tolerant applications but there are also applications like closed loop control which require low latency and high reliability, with latencies in the region of 1 to 10 ms, this results in an ecosystem with heterogeneous devices and technologies. Also, independent of what the data rate or latency is, different applications require different reporting intervals. For industrial applications, or alarms in homes, the update interval might be much higher (i.e. every couple of seconds) than applications like in application domains such as smart cities, where only daily updates might be needed.

B. IoT DESIGN REQUIREMENTS

In order to ensure that the cellular LPWA technologies are able to provide an efficient connectivity solution for the different use cases across both Massive IoT to Critical IoT, this section presents some of the key requirements that are needed when considering massive deployment of these services including low deployment cost, long battery life, low device cost, extended coverage area, support for massive number of connected devices (scalability) and security and privacy. The key requirements for the various use cases are shown in Fig. 1.

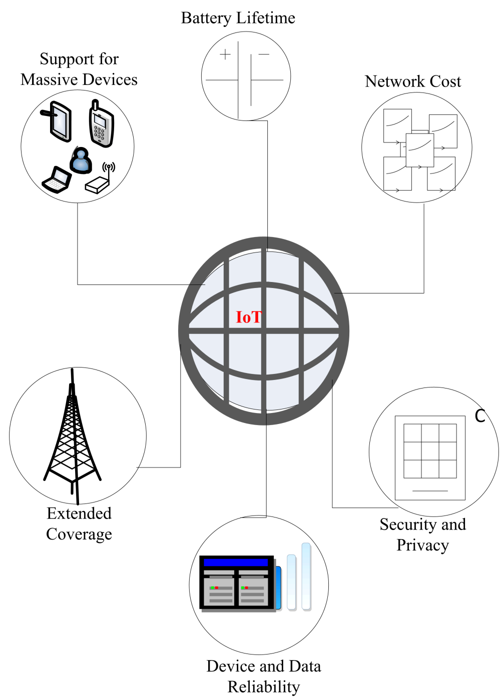

FIGURE 1. IoT key design requirements.

1) LOW DEVICE COST

IoT connectivity is expected to serve very low average revenue per user (ARPU) which is a reduction in revenue generation when compared to mobile broadband subscriptions. This implies that reduction in the device complexity will at the same time be a key enabler for massive-volume, mass-market applications, which will therefore enable most of the IoT use cases. Considering cellular LPWA solutions for business perspective, it is expected that the total cost of production of devices including that of ownership should be extremely very low to aid the massive deployment of IoT use cases.

The summary shown in Table 1 gives a diverse class of use cases with a wide range of requirements in regard to tolerable delay, data throughput and update frequency.

2) LOW DEPLOYMENT COST

To achieve Massive IoT applications, the entire network of IoT connectivity, including both the Capital expenditure (CAPEX) and the annual Operational expenditure (OPEX) should be kept at a minimum cost. This can be achieved by using software upgrades on existing cellular networks to deploy LPWA IoT connectivity solution which will reduce the entire cost of new hardware and site planning, thereby maintaining both CAPEX and OPEX to the best minimum in order to deploy massive IoT use cases.

3) LONG BATTERY LIFE

Energy efficiency is perhaps the most important aspect of IoT, in particular because most IoT devices are battery powered and are expected to be operational for a very long period without human intervention. For instance, let us imagine a scenario where a fire alarm system sends data directly to the fire management department. The time interval it takes between changing batteries for such a smart connected device is a major cost factor to be considered. Previous research has shown that most energy expended in IoT devices is due to communication [58]. Energy efficiency has to be considered in the design of both hardware and software. There are several medium access control (MAC) protocols which support duty cycling, allowing the radio to be put to sleep (i.e. low power mode) for periods when it is not expecting to receive data, therefore extending battery life. Energy management techniques also play an important role in low power operation through the use of lightweight protocols and scheduling optimization, for instance [59] as well as energy harvesting, where IoT devices have the capability of harvesting ambient energy from various sources. Moreover, this would also allow the connectivity of new smart device applications which are not currently deployed and also a minimum of 10 years battery life span of operation will be achieved for daily connectivity of these devices.

4) EXTENDED COVERAGE

Extended coverage is a major design requirement for Massive IoT connectivity when considering applications such as smart metering which are installed in basements with very low coverage and other indoor applications such as elevators. The end goal is to ensure that deeper indoor coverage is provided as an equivalent of signal penetrating a wall or floor, which would at the same time increase the indoor coverage to support massive deployment of IoT use cases. A promising technique for IoT connectivity link budget for coverage enhancement is being targeted to increase the existing Maximum Coupling Loss (MCL) between the device (UE) and the base station to a maximum of 164 dB.

5) SECURITY AND PRIVACY

Several aspects regarding security and privacy are major design requirements to be considered in IoT applications. The mobile IoT user's real identity should be well protected from the public but should be traceable by authorities if the need arises and location privacy is of utmost importance as this can reveal the physical location of the IoT device. Additionally, forward and backward security should be supported for effective deployment of IoT use cases [60].

6) SUPPORT FOR MASSIVE NUMBER OF DEVICES

It has been envisaged that by 2025, the number of connected heterogeneous smart devices will reach seven billion over cellular IoT technologies. This shows that IoT connectivity will grow faster compared to legacy mobile broadband connections. This is a clear indication that some cell stations will have more densely connected number of devices. Therefore, it is hoped that LPWA IoT connectivity solutions should be able to handle most of these connected smart devices simultaneously.

III. EXISTING IoT COMMUNICATION TECHNOLOGY

Although there is still no unified solution for IoT at this point, there have been a number of different communication technologies that have been proposed and are currently in operation, having been deployed in a number of devices worldwide. Both fixed and short-range communication standards will be utilized for most connections to achieve both Massive IoT and Critical IoT connectivity through either traditional cellular IoT or Low Power Wide Area Networks (LPWAN). LPWA technologies are for IoT applications because of their unique features which include wide-area coverage, high energy efficiency, channel bandwidth, data rate, and low power consumption. This technology is a representation of the various technologies which are currently being used in connecting both sensors and controllers to the Internet without the intervention of existing traditional Wi-Fi or cellular networks. Among these promising technologies are SigFox, Ingenu RPMA, and LoRa. Current future demand of Internet connectivity of "Things" has motivated the cellular technology to introduce their own IoT device connectivity landscape solutions such as LTE Cat-M1 (also known as eMTC), EC-GSM-IoT, and NB-IoT (also called LTE Cat-NB1) that will enhance and enable future IoT use cases. LPWA networks are currently being deployed for IoT applications including smart cities, building management system, asset monitoring, smart agriculture etc. This section briefly discuss the main features of currently prominent technologies for IoT and categorizes them into long-range networks, short-range networks and cellular technology.

A. LONG-RANGE NETWORKS

LPWA technologies are among the promising technologies to provide low-power and long-range connectivity solution for IoT applications. This section discusses some of the popular LPWAN to support long-range MTC such as SigFox, LoRa, Ingenu RPMA, Weightless, and DASH7 which are relevant to achieve MTC use cases for the IoT.

1) LoRa

LoRa is a physical layer protocol [30] that has emerged as a promising technology for low-cost, low-power and long-range communication. LoRa wireless technology is based on LoRaWAN, a media access control (MAC) layer protocol based on ALOHA [61] for wide coverage area network. LoRa network are based on a star-to-star network topology where each node (i.e. end device) has a direct single-hop connection to a LoRa gateway. The LoRa architecture consists of end devices (nodes), server, a gateway and a remote terminal as depicted in Fig. 2. LoRa's unique modulation scheme uses a proprietary Chirp Spread Spectrum (CSS) with different bandwidths 7.8 kHz, 10.4 kHz, 15.6 kHz, 31.2 kHz, 41.7 kHz, 62.5 kHz, 125 kHz, 250 kHz, and 500 kHz [62], and provides bi-directional communication. To mitigate the effect of interference, LoRa uses a Frequency Hopping Spread Spectrum (FHSS) which enables access to available channels. It has

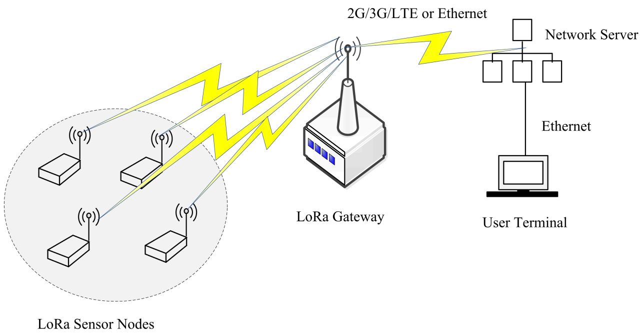

FIGURE 2. Architecture of a LoRa network.

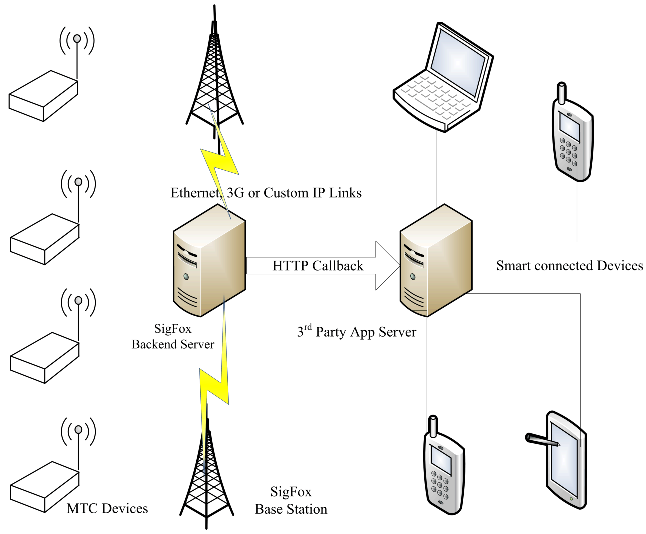

FIGURE 3. Overview of SigFox MTC network [67].

been shown that long communication ranges (15 km+) are achievable in urban environments (i.e. with no clear line-of-sight) [63]. LoRaWAN is based on LoRa and adds a network layer to handle network congestion between connected end-devices (i.e. nodes) and central nodes. It uses the 868 and 915 MHz bands for communication at a maximum data rate of 50 kbps, which is sufficient for most IoT applications. LoRa is aimed specifically at IoT applications. Possible data rates with LoRa are dependent on channel bandwidth and spreading factor, where the ALOHA medium access scheme enables multiple devices to communicate using different spreading factors.

2) SigFox

SigFox [29] low power wide area network technology offers a complete end-to-end connectivity solution which is based on their patented technologies by using ultra-narrowband (UNB). Since M2M communications requires a small amount of data to be transferred efficiently on a low bandwidth, SigFox suits such type of communication. This technology is deployed by using proprietary base stations which are configured with cognitive software-defined radios by connecting them to backend servers utilizing IP-based network infrastructure as depicted in Fig. 3. SigFox end devices connect to the network base stations by using a unique modulation scheme called Binary Phase Shift keying (BPSK) [64] in an ultra-narrowband of 100Hz Sub-GHz Industrial, Scientific and Medical (ISM) band carrier. With UNB, SigFox technology provides higher sensitivity, ultra-low power consumption and long ranges by efficiently utilizing its bandwidth at the expense of limited data rates, which is adequate for IoT since most applications do not require high throughputs. SigFox networks use the unlicensed ISM band and as such its frequency of operation varies accordingly between 868 MHz and 915 MHz and enables wide coverage using line-of-sight communication. For instance, in rural areas, range up to 30-50 km and beyond can be achieved through frequency hopping, and this range is reduced to 3-10 km in urban locations due to the presence of obstacles. The SigFox network supports up to 12 bytes of packet size for each message using typical modulation including Gaussian Frequency-Shift Keying (GFSK) for downlink and Differential Binary Phase Shift Keying (DBPSK) for uplink transmission respectively. Uplink messages are restricted/limited to 140 12-bytes messages per day which on the other hand conform to the regional regulations which states no use of license-free spectrum [65], while allowing 4 8-bytes messages per day for downlink transmission from the base stations to end connected devices. However, ultra-narrowband signals are susceptible to any aggressive bursts exceeding the duration of a bit (i.e. 10 ms), causing devices in a SigFox network to retransmit frames a number of times [66]. This in turn increases the traffic load.

3) INGENU-RPMA

Unlike other LPWA technologies which have been previously mentioned that use the 2.4 GHz ISM band for communication, Ingenu-RPMA is a proprietary LPWA technology with more flexible regulations on the use of spectrum across different regions [28], [65]. This means that higher throughput and more capacity can be achieved when compared to other technologies which are also operating in SUB-GHz band. At the core of the wireless technology, Ingenu uses Random Phase Multiple Access (RPMA) [68] Direct Sequence Spread Spectrum (DSSS), which is used for uplink communication, and allows multiple transmitters to share a single timeslot as a variation to Code Division Multiple Access (CDMA). This is achieved by adding a random offset delay to each transmitter within the timeslot, consequently reducing overlapping between transmitters [69], and thereby increasing the signal to interference ratio for each individual link. Ingenu also provides bi-directional communication. For downlink communication, signals are continuously being spread by base stations to individually connected end devices and broadcast such signals using CDMA. Ingenu RPMA is capable of achieving up to −142 dBm receiver sensitivity and a link budget of 168 dB [28]. This technology is made compliant to legacy IEEE 802.15.4k specifications.

4) DASH7
DASH7 is a long range low-power wireless technology that operates in the 433 MHz ISM band and is an extension of active Radio-frequency Identification (RFID) based on the ISO/IEC 18000 standard [70], where communication can take place directly between devices and they can be used for non-RFID applications. DASH7 employs narrow band modulation using two-level GFSK in SUB-GHz bands. This technology is aimed at low-rate applications with bursty nature, and offers data rates up to 167 kbps. It also supports multi-hopping, albeit limited to 2 hops by default, but can be extended to more hops. Ranges up to 2 kilometers are possible with DASH7 [71].

5) WEIGHTLESS
Weightless is a new wireless technology which was introduced by the Weightless Special Interest Group (SIP) [72] with three open LPWA standards known as Weightless-W, Weightless-N, and Weightless-P, which operate in both license-free and licensed spectrum for different ranges and low power consumption. This technology uses cognitive radio and TV white-spaces which enable devices to utilize these bands as opportunistic users without causing interference to the primary user devices as licensed owners. Fig. 4 depicts the architecture of a Weightless Network.

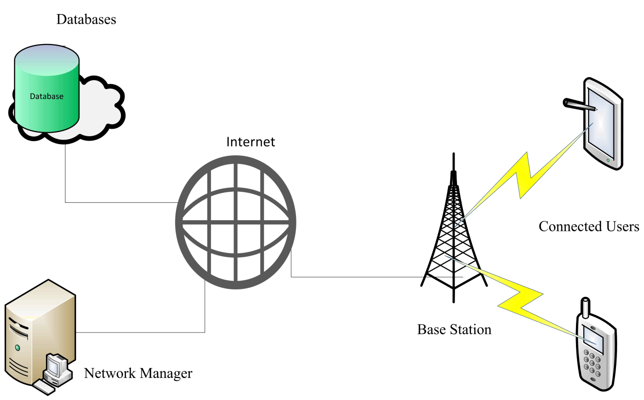

FIGURE 4. Architecture of a weightless network provider [36].

a: *WEIGHTLESS-N*
This is a UNB standard which supports only one-way communication (i.e. from end devices to the base station) using DBPSK modulation scheme. It exploits TV white-space (SUB-1GHz) in the region of 470 to 790 MHz.

b: *WEIGHTLESS-W*
This standard supports different modulation schemes such as Differential -BPSK and 16-Quadrature Amplitude Modulation (16-QAM) with a data rate up to 10 mbps which depends on the link budget [73]. In order to improve energy consumption, end devices are enabled to transmit at a lower power level to the base stations in a narrow band.

c: *WEIGHTLESS-P*
This standard, on the other hand, uses GMSK and QPSK modulation and achieves data rates of 100 kbps using narrow channels (12.5 KHz). The main drawback of Weightless-N is that it supports one-way communication, therefore limiting the number of IoT applications it can be used for. However, the fact that bidirectional communication is not supported extends the battery life for several years more than both Weightless-P and Weightless-W.

B. SHORT-RANGE NETWORKS
This subsection presents some legacy short-range wireless network technologies which are currently being used to support short-range M2M communication applications including Bluetooth, ZigBee and low power Wi-Fi. These technologies are viable and best-fit for consumer use cases of the IoT, but may not be able to support for civic, industrial and other related IoT applications for which the demands are beyond the capacity of their characteristic features.

1) BLUETOOTH
Bluetooth was designed based on the IEEE's 802.15.1 wireless personal area communication standard [74] to be used for short-range ad-hoc communication (i.e. Master and Slave configuration) between devices operating in the 2.4 GHz ISM bands with achievable data rates in the low mbps. Bluetooth technical specifications and developments are currently being managed by Bluetooth Special Interest Group (SIG) [75]. Bluetooth Low Energy (BLE) [Smart Bluetooth Low Energy], which is also called Bluetooth 4.0 was introduced to improve energy consumption. The most recent amendment to the standard uses 40 channels with a width of 2 MHz channel spacing. The modulation scheme used is Gaussian Frequency Shift Key (GFSK) modulation. To make it more robust to interference, and multi-path fading [76], Bluetooth uses a frequency hopping spread spectrum (FHSS) scheme where the signal switches carriers over a predetermined pattern of channels [76]. Although, Bluetooth was originally aimed as a replacement for wires in mobile devices, it has evolved to be used in many different applications. However, one of the drawbacks is the restriction of only one-to-one communication between only two devices at a time. The Bluetooth Smart Mesh working group was proposed by the Bluetooth Special Interest Group in order to define and standardize a new architecture for mesh networking for Bluetooth Low Energy which will enhance the communication coverage and enable deployments of Bluetooth Low Energy for IoT. Bluetooth Low Energy is envisaged as a connectivity solution for short-range communication in the IoT applications including smart energy, healthcare, and smart home applications [77].

2) IEEE 802.15.4 AND ZigBee
This standard is currently the *de facto* standard for low-rate wireless personal area networks (LR-WPAN). Three different frequency bands can be used with IEEE 802.15.4: 868 MHz, 914 MHz and 2.4 GHz supporting 1, 10 and 16 channels,

TABLE 2. Summary of current IoT wireless technologies.

Technology	Frequency Band	Range	Maximum Data Rate	Channel Bandwidth
LoRa	868 MHz and 915 MHz	15 km	50 kbps	125, 250 or 500 kHz
SigFox	915 to 928 MHz	20 km +	100 bps	100 Hz
ZigBee	868 MHz, 915 MHz and 2.4 GHz	Typically less than 1 km	250 kbps	2 MHz
DASH7	433, 868, 915 MHz	0 – 5 km	167 kbps	Up to 1.75 MHz
Wi-Fi	2.4 GHz; 5 GHz	100 m	54 Mbps	22 MHz
Ingenu-RPMA	2.4 GHz	15 km	20 kbps	1 MHz
Weightless	Multiple bands in the sub-GHz	5 km	100 kbps	200 Hz to 12.5 KHz
Bluetooth	2.4 GHz	50 m	2 mbps	2 MHz

respectively, each with a 2 MHz bandwidth. The maximum supported data rate is 250 kbps [78]. Direct Sequence Spread Spectrum (DSSS) is used as a modulation scheme for IEEE 802.15.4. This standard only defines physical (PHY) and data link layers (DLL). ZigBee uses the PHY and DLL as defined by IEEE 802.15.4, and builds on it by adding a network layer. A drawback of the original version of IEEE 802.15.4 is the fact that a single static channel is used for communication when the network is established, which is susceptible to interference. It uses Carrier sense multiple access with collision avoidance (CMSA/CA) for channel access. This is one particularly important from the IoT perspective, given that a massive number of connected devices might attempt to communicate concurrently. More recent amendments (i.e. 802.15.4e) of the standard have incorporated frequency diversity to counter the impact of interference. The main differences between ZigBee and LoRa are the communication ranges and topology options, as the latter supports star, mesh and cluster tree topologies [79]. Figure 5 shows the different topologies - star, peer-to-peer and cluster tree – of a ZigBee network.

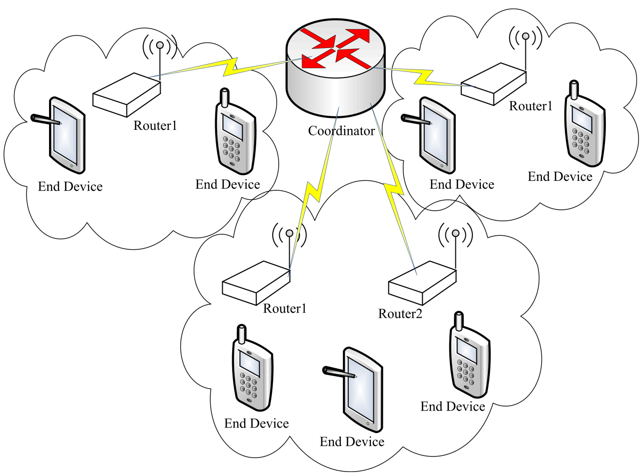

FIGURE 5. ZigBee mesh network [27].

3) Wi-Fi

The early version of Wi-Fi was proposed by the IEEE for local area wireless communication which was released without considering the application of modern IoT connectivity. This technology was intentionally designed for high bandwidth communication between devices which are located within a short-range with the basic aim of providing high throughput connectivity. This technology is also called wireless local area network (WLAN) and belongs to the IEEE 802.11 standard series [80]. In order to provide Internet connectivity through wireless network access points, the network operates within 5 GHz and 2.4 GHz ISM spectrum bands. The access points operate within a coverage area of up to 1 Km, which can be increased by using multiple overlapping hotspots. To improve the network performance and throughput while considering dense and congested areas [81], [82] enhanced features were introduced into the 802.11ac release. In order to extend the Wi-Fi network applications to meet the need and requirements of modern IoT connectivity (which are basically a large number of smart connected devices, enhanced coverage area, and energy constraints), the IEEE proposed and established Low-power Wi-Fi, which is also called IEEE 802.11ah [83] as an amendment to the legacy standard. This newly introduced standard aims to achieve a low energy consumption down to 100's of milliwatts which is suitable for IoT based devices, provides large coverage area, and can achieve a data rate up to 347 Mbps. Research has shown that further enhancements are being introduced into low-power Wi-Fi by the Wi-Fi alliance called Wi-Fi HaLow for M2M smart city [84]. Wi-Fi network can provide M2M/IoT applications including parking metering, autonomous lightning, smart security, smart home thermostats, etc., [85].

4) SUMMARY

Considering the various attributes analyzed for low-power wide area wireless technology for MTC use cases, it is observed that each of these technologies, given the trade-offs, is only able to optimize certain parameters including battery life-time, data rate, operating frequency band, possible achievable range, scalability and channel bandwidth etc. Table 2 summarizes some of the existing alternatives which are currently available and wireless network technologies for IoT applications. Based on these attributes, application developers can easily assess which alternative will be best-fit or viable for deploying IoT use cases.

C. CELLULAR TECHNOLOGY

Future requirements of IoT applications are a major key drive towards enhanced growth in cellular technology. Cellular LPWA technologies are expected to ensure that various services or applications such as Vending Machines, Smart Metering, Automotive Systems (i.e. smart traffic, fleet management, security surveillance and reporting, real time traffic information to the vehicle), Secure/Smart home (Smart heat, Smoke detector, smart appliances) etc., are provided. This section presents the various paradigm shifts that have evolved in the new mobile generation which has been extensively used to enhance the quality of voice communications as well as enabling the opportunity for a new global connectivity solution for end-users with the objective of ensuring that ubiquitous communication is achieved with new service requirements.

1) 2G CELLULAR NETWORKS

Second Generation (2G) digital cellular systems were introduced because of their low-band digital data signaling [86]. Global System for Mobile Communications (GSM) remains one of the most popular technology of 2G wireless systems. This technology was designed to use 25 MHz frequency spectrum in the available 900 MHz band with Frequency Division Multiple Access (FDMA), which allows the operation of multiple users to access available radio frequency band and eliminate the occurrence of interference of message traffic by splitting the available 25 MHz bandwidth into a total of 124 carrier frequencies of 200 kHz each. With the implementation of Time Division Multiple Access (TDMA), each of these frequencies were further divided into eight time slots, which allows for eight simultaneous voice calls to be accessed within the same frequency band. This technology allows for a massive number of subscribers to be connected to a single radio frequency and to allocate time slots to multiple users at the same time. Because of its global ecosystem deployment, GSM networks operate within the 900 MHz and 1800 MHz bands across the universe except in the American Continent where it uses 1900 MHz for its operation. With the development of GSM technology in Europe, North America introduced Code Division Multiple Access (CDMA) technology which uses spread spectrum to identify each caller and to optimize the capacity of wireless carriers network, improve quality of service (QoS) required for wireless messages, and to ease the accessibility of the wireless airwaves to users [86]. TDMA breaks down users' calls by time, whereas CDMA does same on a "signal by codes" basis. These technologies were both introduced to enhance the network capacity for the wireless carrier as well as to prevent the level of interference to the users.

2G cellular technologies were designed based on circuit-switched system, digitalized and to extend the coverage of applications beyond the normal voice services. This technology can be used for services including short message applications and fax systems which can support a data rate of about 9.6 kbps, which makes it not reliable for applications such as multimedia and web browsing. In order to mitigate some of the limitations of wireless GSM, 2.5G networks were introduced to improve the data capacity by adding packet data capability to existing GSM networks. These technologies are General Packet Radio Service (GPRS) and Wireless Application Protocol (WAP).

The all-IP network in 3GPP standardization is based on the GPRS technology which was developed for the provision of Packet services to the GSM networks [87]. With this technology, it is possible to achieve a higher data bandwidth through aggregation of radio channels and additional servers which are required to off-load packet traffic on existing GSM circuits, and support up to 171.2 kbps data rate. WAP, on the other hand, determine the procedure through which web pages and related data are delivered through limited bandwidth wireless channels over small screens in mobile phones [86]. GSM cellular network is an enabling technology because of its global deployment that will aid with the deployment of IoT use cases in cellular networks.

2) 3G CELLULAR NETWORKS

The third generation (3G) cellular evolution started when it was foreseen that one of the most useful applications was the Internet, as this would lead to massive connectivity of things beyond its initial focus on multimedia applications such as video conferencing for smart connected devices such as mobile phones. With the massive increase of personal wireless smart devices (mobile phones, tablets, Ipads etc.), it is clear that there will be need for Personal Wireless Internet Access (PWIA) that will ease the broadband connectivity of smart devices wherever mobile users roam to. However, the tremendous growth of the Internet (smart connected devices) affects both wired and wireless communications, and there is a need for evolution to support the rapid growth of the mobile communication industry.

The International Mobile Telecommunications-2000 (IMT- 2000) [88] which is the official International Telecommunication Union (ITU) name given to 3G systems with the intention of providing wireless accessibility to the globally connected telecommunication infrastructure, utilizing both terrestrial and satellite systems for serving connected users either through private or public network operators [86]. Its objective was to ensure that a globally harmonized system was created for mobile communication that could be used to facilitate global interoperability between different network providers and for the provision of lower cost. Based on these, the following data rate requirements were proposed by the ITU:

- 144 kbps for Moving users in a wide area
- 384 kbps for Pedestrian users or in Urban region
- 2 Mbps for Stationary or fixed users.

The GSM proponents introduced Universal Mobile Telecommunication System (UMTS) as an evolution of GSM for 3G systems for IMT- 2000. UMTS Release 99 Standard was officially released by the 3GPP [89] as a collaboration between six regional telecommunications Standard bodies across the world as the first 3G UMTS Standard. As of January 2012, research has shown that global connectivity to the 3GPP family of 3G/IMT-2000 mobile networks has reached over a billion connected users across the world [90]. The UMTS network utilizes Wide-band Code Division Multiple Access (W-CDMA) as its radio technology which uses a

TABLE 3. Transport technologies evolution (adapted from [98].

Technology	Access Technology	Description	Typical Use/Data Rate	Pros/Cons
2G	TDMA	Time Division Multiple Access	It supports Voice and Data with about 9.6 kbps	+ Level of battery consumption is low - One-way communication with slow speed
	GSM	Global System for Mobile Communications	Mainly for Voice and Data. Operates within 900 MHz and 1.8 GHz frequencies: United States uses 1.9 GHz PCS band with about 9.6 kbps	+ This is globally established with roaming - It transmits only in one-way with a maximum of 160 characters
	CDMA	Code Division Multiple Access, which was introduced by Qualcomm	TIA/EIA IS-95 (Telecommunications Industry Association / Electronic Industries Association Interim Standard – 95) which specify the first CDMA. Voice and data are supported up to 14.4 kbps.	+ It can support massive capacity than TDMA - Fewer subscribers than TDMA
2.5G	GPRS	General Packet Radio Service – for data packets	Data can be supported up to 115 kbps, while the AT & T wireless GPRS will support up to 40 kbps – 60 kbps.	+ Its message characters are not limited as compared to GSM SMS.
3G	EDGE	Enhanced Data Rates for Global Evolution	This system supports up to 384 kbps of Data	+ It will serve as an alternative for network operators who do not have access to W-CDMA licenses; supports high speed mobile data access, and accommodate more voice traffic
	W-CDMA (UMTS)	Wideband CDMA (Universal Mobile Telecommunications System)	It supports voice and data with speed of about 144 kbps to 2 Mbps, initially. It was expected to achieve 10 Mbps by 2005, according to designers.	+Expected to be dominant outside United States, and to support roaming globally. Less commitments from U.S. network operators.
	CDMA2000 1xRTT	1xRTT, represents phase 1 of CDMA	Voice and Data services are supported up to 144 kbps	+Proponents suggest that the migration process from TDMA to CDMA2000 is easier than to W-CDMA, and with efficient use of spectrum. W-CDMA deployment is likely to be more accessible in Europe.
	CDMA2000 1xEV-DO	This ensures that data services are delivered on a different channel	It supports data services up to 2.4 Mbps	(Same as stated above for CDMA2000 1xRTT)
	CDMA2000 1xEV-DO	This supports the integration of both voice and data on a single channel	Supports Voice and Data services up to 2.4 Mbps	(Same as stated above for CDMA2000 1xRTT)

wider band when compared to CDMA [91]. This radio technology has enhanced its transfer rate and increased the system capacity and quality of service (QoS) by employing statistical multiplexing. In order to ensure that it provides a maximum data rate of about 2 Mbps, W-CDMA technology utilizes the entire allocated radio spectrum for efficient communication. With the current demand of Massive connectivity of IoT, the entire Circuit-based backhaul network has to be changed significantly. 3G systems are IP-centric and will justify an all – IP infrastructure [86]. Table 3 gives a detailed summary of the various wireless technologies developed prior to fourth generation (4G) and beyond which could be used in aiding future IoT connectivity.

IV. 3GPP CELLULAR SOLUTIONS FOR THE INTERNET OF THINGS

Cellular technologies such as 3G, 4G and most especially the legacy 3rd Generation Partnership Project Long-Term Evolution (3GPP LTE) networks are among the current and promising technologies which are being considered as a major landscape connectivity solution to achieve modern IoT applications [92]. These promising and appealing technologies are capable of offering wide coverage area, relatively low cost of deployment, high security, dedicated spectrum allocation and efficient management system. However, having been deployed for the interest of optimized broadband networks, they are not suitable for current MTC.

The current IoT landscape comprises different solutions of connectivity which need to be harmonized among the various key industry players in order to ensure that the requirements of IoT technical key performance indicators (KPIs) are achieved. 3GPP in its desire to ensure that M2M applications are efficiently supported on 4G broadband networks including UMTS, and LTE have been working tremendously to make sure that M2M communications are efficiently evolved in future and promising 5G New Radio systems which is being envisaged for Massive IoT applications. 3GPP in its current standardization of Release-13, recently introduced three main key standards that will enable and enhance the deployment of massive smart connected devices and services such as smart cities, smart grid, wearable devices and connected homes. These introduced features are: EC-GSM-IoT [93], eMTC [94] which are expected to enhance the effective communication of existing cellular technologies such as the GSM [95], the LTE [96] networks, and the NB-IoT [97]. It is hoped that with these newly introduced LPWA solutions for the IoT, the connectivity profile and basic requirements for the IoT will be achieved when compared to existing cellular networks.

These technologies were introduced in order to provide extensive coverage area, User Equipment (UE) complexity reduction, efficient long battery lifetime, and backward compatibility with existing cellular networks. However, the end goal of the newly emerging standards is to maximize the re-use of legacy cellular networks infrastructure which will enhance and support the massive connectivity of IoT applications. In this section, we briefly discuss the emerging and promising technologies which are envisaged as future technology for Massive deployment of the IoT use cases.

A. ENHANCED MACHINE-TYPE COMMUNICATIONS

The eMTC, also called LTE Cat-M1, or Cat-M, is a promising cellular LPWA technology introduced in the 3GPP Release-13 standardization which intends to minimize modem complexity and cost, power consumption, and extended coverage over existing legacy handset modems, such as category 0 user equipments (UEs) from Release-12 specification for MTC. This technology is an enhancement for LTE networks to support MTC for the IoT.

Cat-M1 UE operates within a limited bandwidth of 1.08 MHz out of the available 1.4 MHz, allowing Cat-M1 UE to use only six physical resource blocks (PRBs) out of the eight available 180 kHz LTE physical resource blocks, which coexist in a broader, general legacy-purpose LTE system (5G Americas, 2016). In order to mitigate the interference level, the two remaining PRBs are used as guard bands. With the support for 1.08 MHz band (narrowband channel) for both radio frequency and baseband, Cat-M1 devices are further reduced in complexity, cost and power over Cat-0 devices. Cat-M1 devices are expected to achieve a maximum throughput of up to 1 Mbps in both uplink and downlink operations for massive IoT. For common control messages, the maximum Transport Block Size (TBS) is further reduced to 1000 bits from the 2216 bits of Cat-0 devices which is an equivalent of unicast data traffic, allowing further processing and memory savings in Cat-M1 devices over the legacy Cat-0 UE.

The eMTC devices have been designed to support either 23 dBm or 20 dBm power classes unlike the MTC Cat-0 devices which were designed to support a maximum transmission power of 23 dBm, which is approximately 200 mW for uplink (UL). The maximum transmission power of 20 dBm enable the Power Amplifier (PA) to be integrated as opposed to using a dedicated Power Amplifier. Consequently, this enables and supports the achievement of lower device cost

Considering the current LTE numerology, eMTC technology can be deployed within the regular LTE network up to 20 MHz of operation and also to co-exist with other available LTE network services. Due to the reduced bandwidth for Cat-M1 devices, eMTC requires that a new set of logical control channels, MTC Physical Downlink Control Channel (MPDCCH) is used to replace the existing logical control channels such as Physical Downlink Control Channel (PDCCH), Physical Control Format Indicator Channel (PCFICH), and Physical Hybrid Automatic Retransmission Request (ARC) Indicator Channel (PHICH), which are no longer suitable within the new narrower bandwidth for eMTC technology. With the deployment of eMTC network, series of multiple narrowband regions can be configured. That is, it is possible to configure 6 PRBs each within the LTE carrier for narrowband Physical Downlink Shared Channel (PDSCH) and MPDCCH for data scheduling purposes [99]. It is also important to note that eMTC is designed with an increased link budget of 15 dB with a Maximum Coupling Loss (MCL) of 155.7dB which exceeds the legacy LTE baseline of 140.7dB in order to ensure that coverage is extended for IoT devices which are deployed in remote regions or locations.

eMTC is standardized to ensure that for Massive IoT deployment and coverage, it supports long battery life of about 10 years with a 5 Watt-Hour battery system for effective utilization. This technology uses power savings management (PSM) and extended discontinuous reception (eDRX) as its power savings mechanisms to achieve long battery life for Cat-M1 devices.

B. NARROWBAND-INTERNET OF THINGS

The NB-IoT, also known as LTE Cat-NB1, is a new and promising cellular low power wide area technology introduced in the 3GPP Release-13 specification as an evolution to LTE Cat-M1.

NB-IoT technology is expected to ease the Massive deployment of the IoT by allowing an existing operator to introduce NB-IoT within its small portion of existing network and available spectrum. This technology is designed to ensure that ultra–low end IoT applications including remote sensors, smart buildings and smart meters are supported. LTE-Cat-NB1 (NB-IoT) is designed for optimal co-existence performance with legacy GSM, GPRS and with LTE technologies. Cat-NB1 operates within a minimum system bandwidth of 180 kHz for both the downlink and uplink operations, respectively. Because of its choice of operation, it is possible for a GSM operator to replace one GSM carrier of 200 kHz with an NB-IoT application. On the other hand, an operator of the LTE network can as well deploy NB-IoT applications into an LTE carrier by means of allocating one of its PRBs of 180 kHz to Cat-NB1. The NB-IoT air interface is well optimized to ensure harmonious coexistence with

TABLE 4. Complexity reduction summary for LTE IoT user equipments (UEs).

Device Category	LTE-Cat-1	EC-GSM-IoT	LTE Cat-M1 (eMTC)	LTE Cat-NB1 (NB-IoT)
3GPP Release	8	13	13	13
Peak Data Rate [99]	DL: 10 Mbps UL: 5 Mbps	For DL & UL: 74 kbps (GMSK), 240 kbps (8PSK)	DL: 1 Mbps UL: 1 Mbps	DL: 170 kbps UL: 250 kbps
Duplex Mode [99]	Supports Full duplex FDD/TDD	Supports Half duplex FDD only	Supports Half duplex FDD/TDD	Supports Half duplex FDD only
Bandwidth [99]	20 MHz	0.2 MHz	1.08 MHz (1.4 MHz carrier bandwidth|)	180 kHz (200 kHz carrier bandwidth)
MCL [100]	140.7 dB	Support for:164 dB (33dBm), and 154 dB (23dBm)	155.7 dB	164 dB
Rx Antenna [99]	Supports double Rx	Supports single Rx	Supports single Rx	Supports single Rx
Coverage Support	Complementary to Cat-M1 & NB-IoT	20 dB	+15 Db	+15 Db
Battery Life	Less than 10 years	Supports within +10 years	Supports within +10 years	Supports within +10 years
Max Transmit Power [99]	23 dBm	33 dBm or 23 dBm	20 dBm or 23 dBm	20 dBm or 23 dBm
PSM [100]	PSM	PSM, ext. I-DRX	PSM, ext. I-DRX, C-DRX	PSM, ext. I-DRX, C-DRX
Security	It supports 3GPP (128-256bit)	It supports 3GPP (128-256bit)	It supports 3GPP (128-256bit)	It supports 3GPP (128-256bit)
Spectrum	Supports licensed LTE Bands In-band	Supports licensed GSM bands	Supports licensed LTE Bands In-band	Supports licensed LTE in-band, guard-band & stand-alone

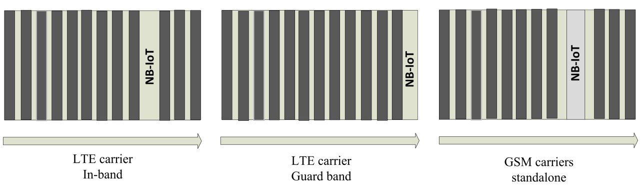

FIGURE 6. Cat-NB1 (NB-IoT) Flexible Deployment Modes [101].[1]

LTE, which means, when an NB-IoT is deployed inside an LTE carrier, the performance of LTE or Cat-NB1 cannot be compromised.

Thus, NB-IoT enables flexible deployment of Massive IoT to network providers as:

- In-band, which is integrated as part of the resource regularly used for the eNB communication
- Guard band, which makes use of the unused frequency band of 180 kHz which is between the last PRB used and the channelization edge
- Standalone system, which is based on a re-farmed channel (i.e. reusing GSM carrier frequencies) of a legacy GSM/GPRS system which is being operated by the service operator. Figure 6 shows the flexible deployment options for NB-IoT systems when considering In-band, Guard band and Standalone deployment options.

In order to ensure that the device complexity and cost of NB-IoT technology are limited, the peak data rates for downlink were further reduced considering 32 kbps for in-band scenario, and 34 kbps for standalone deployment, while the uplink peak data rates are limited to 66 kbps and 16.9 kbps for both multi-tone and single-tone transmissions respectively [99].

[1]Republished with permission of IEEE, from NB-IoT Deployment Study for Low Power Wide Area Cellular IoT, Mangalvedhe, N., Ratasuk, R., and Ghosh, A., PP 2, 2017 Copyright.

Cat-NB1 technology is designed to reuse the existing LTE design structure, which includes the numerologies, Uplink Single-Carrier Frequency Division Multiple Access (SC-FDMA), downlink Orthogonal Frequency Division Multiple Access (OFDMA), rate matching, Channel Coding, and Interleaving, which reduces the time required to introduce a new system specification for NB-IoT [101]. The first normative phase for introducing NB-IoT in 3GPP started sometime in September 2015 with its core complete specification in June 2016 [97]. It is expected that the commercial launch of Cat-NB1 products and services commences towards the end of 2016 and in the early year of 2017. It is forecasted that IoT traffic will compound to an annual growth rate of 23% between 2015 and 2023. Therefore, it is envisioned that the introduction of NB-IoT should have an optimal capacity to accommodate and support such growth at the same time in near future. Some of its key performance indicators to support such are coverage extension, peak data rates, and high capacity to support Massive IoT, latency, device complexity and battery lifetime. Table 4 gives a detailed summary of the high level complexity differences evolved between newly introduced LTE IoT UE Categories.

Finally, the NB-IoT (Cat-NB1), is a pioneer technology towards building the 5G New Radio Network which is intended to enable new use cases for the IoT. It is foreseen that NB-IoT will continue to evolve towards 5G future requirements.

C. EXTENDED COVERAGE GSM FOR THE INTERNET OF THINGS

GSM is one of the most dominant and compelling cellular technologies for the deployment of IoT applications because of its extensive and established global and broad ecosystem. 3GPP standardization in its Release-13 specification introduced EC-GSM-IoT as a standard-based LPWA emerging technology which was designed for high capacity, long range coverage, low energy and low complexity cellular system based on enhanced General Packet Radio Service (eGPRS) for the IoT [93].

Existing GSM Networks can be upgraded using a software application in order to ensure that extensive coverage and accelerated time of deployment are determined through optimization techniques which have been deployed in EC-GSM-IoT and for efficient battery life of about 10 years for a wide range of use cases. EC-GSM-IoT technology is standardized to ensure that its enhancements support extended Discontinuous Reception (eDRX) which improves the power efficiency of devices, minimized idle mode procedures and admission control in terms of QoS. With this technology, GPRS/EGPRS Packet Switched Channels are fully enabled for multiplexing. For effective deployment of Massive IoT applications, new Logical Channels which were introduced to support extended coverage in EC-GSM-IoT technology are called EC–Channels. These include EC-Shared Channel (EC-SCH), EC-Access Grant Channel (EC-AGCH), EC-Broadcast Control Channel (EC-BCCH), EC-Packet Data Traffic Channel (EC-PDTCH), EC-Paging Channel (EC-PCH), and EC-Packet Associated Control Channel (EC-PACCH). These new logical channels can be incorporated into legacy GPRS spectrum to accommodate EC-GSM devices for IoT services. In order to reach the 20 dB extended coverage which is required when compared to existing legacy GPRS networks, repetitions such as L2 (16 times) and L3 Hybrid Automatic Retransmission reQuest (HARQ) (4 times) are required for effective extended coverage while considering effective utilization of spectrum, blind repetitions and incremental redundancy (HARQ type II) used for data traffic channels [99]. EC-GSM-IoT is designed with two different modulation schemes which are Eight Phase Shift Keying (8PSK) and Gaussian Minimum Shift Keying (GMSK) for variable data rates. Figure 7 depicts the extended coverage for EC-GSM-IoT technology indicating the various newly introduced logical channels.

Finally, considering GSM as one of the most widely wireless standard networks which has been deployed globally, EC-GSM-IoT technology has enhanced legacy GSM networks to ensure that it supports the global cellular network and deployment of Massive IoT applications into the future which requires low data rates services.

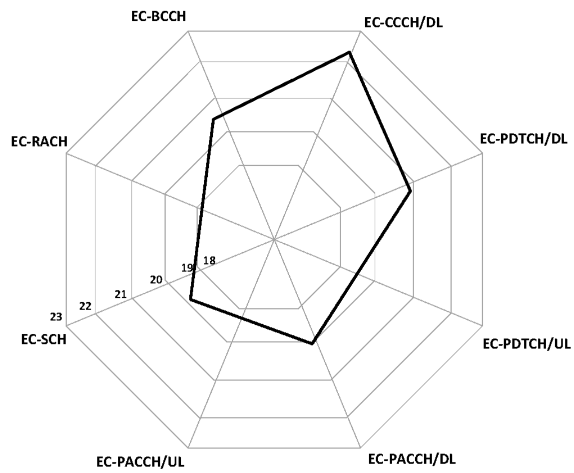

FIGURE 7. Showing EC-GSM-IoT Extended Coverage [99].

The possibility of deploying LPWAN anywhere around the world depends on the choice and availability of the frequency band to be used without going through any process of modification. One major and noticeable difference is that promising LPWA cellular technologies such as eMTC, NB-IoT, and EC-GSM-IoT are defined by the current 3GPP standardization and operate within the licensed frequency band including existing LTE bands and GSM carriers, which offer a high level of security, interference-free collision and quality of service (QoS) guarantees. LPWA cellular-based connectivity solutions will support massive IoT applications by allocating spectrum resources needed for IoT services with an extended coverage area and reduced complexity and cost as a result of eliminating the complex functional radio by using single antennas and half-duplex mode of communication.

In addition, cellular-based solutions are capable of supporting the trade-offs between network capacity and coverage for LPWAN in terms of lower device and infrastructure cost because of its mature and global ecosystem which supports a massive number of devices, high throughput use cases, as well as the ability to scale down in order to support for low-performance use cases while utilizing the same network infrastructure.

On the other hand, LPWA technologies including SigFox, LoRa, and Ingenu RPMA, are proprietary-based networks that have adopted the universal 2.4 GHz ISM band which operates in unlicensed frequency band and are susceptible to interference from other networks using the same bandwidth. In order to enhance and provide long-range communication, some of these technologies adopted the sub 1 GHz bands which are highly fragmented. Unlike SigFox and LoRa networks, Ingenu RPMA can support a large coverage network because of its receiver sensitivity of −145 dBm which is acceptable worldwide without being restricted based on the policy regulations for the 2.4 GHz band. Consequently, one issue to be addressed is the scalability of these technologies to support massive capacity. In most of these networks, new

D. COMPARISON OF 3GPP CELLULAR LPWA STANDARDS OVER NON-CELLULAR LPWA SOLUTIONS

Having discussed the 3GPP cellular solutions for the IoT which is aimed at fostering the next generation 5G new service requirements, and other non–3GPP LPWA technologies that could also be used for deploying massive IoT use cases, this section presents a comparison analysis between the 3GPP cellular LPWA solutions (eMTC, NB-IoT, EC-GSM-IoT) and non–cellular technologies such as SigFox, LoRa, and Ingenu RPMA to enable connectivity solution for MTC applications.

base-stations would have to be configured in order to scale up capacity when the original capacity of the network has been exhausted.

Finally, the different attributes presented by LPWA technologies are enormous and there is a need to ensure that the appropriate connectivity solution is considered when deploying IoT use cases. Technologies including LoRa, SigFox, and Ingenu RPMA are already been deployed in multiple markets, while the promising cellular-based LPWA technologies such as LTE Cat-M1, NB-IoT, and EC-GSM-IoT are yet to be fully commercialized.

V. 5G NEW RADIO ENHANCEMENTS FOR THE INTERNET OF THINGS

Research has shown that the future 5G mobile networks have to cater for the massive deployment of IoT with billions of connected smart objects and sensors that will be a global representation of the real world and to support the provision of mission critical IoT use cases, which will require real-time responses and automation of dynamic processes across different field of operations including vehicle-to-infrastructure (V2I), high speed motion, vehicle-to-vehicle (V2V), and as well as process control system [99].

The 5G new radio network which is currently under consideration is expected to cater for both Massive and Critical IoT use cases as the demand for machine communications continue to grow extensively for connecting a massive number of smart devices with the benefits of using cellular networks. In light of this, further enhancements are currently being introduced in M2M and NB-IoT systems as specified in the current 3GPP Release-14 for cellular IoT, being the first normative phase for 5G standards. Currently, 3GPP standardization is working towards ensuring that further enhancements of KPIs are introduced into existing 4G networks to ensure that the 5G mobile network is designed from scratch in order to accommodate the growing span of the IoT use cases into the market, and minimizing the cost of developing new networks.

In 3GPP Release-14, some of the expected key performance features and enhancements for M2M and NB-IoT systems highlighted for Massive and Critical IoT applications to be considered for discussion are briefly introduced as follows:

- General Enhancements to MTC
- Enhancements of NB-IoT
- NB-IoT RF requirement for co-existence with CDMA networks
- Release- 14 extensions for Cellular Internet of Things (CIoT)
- New band support for Release- 14 NB-IoT
- New services and Markets Technology Enablers

A. REL-14 EXTENSIONS FOR CELLULAR INTERNET OF THINGS

The need to ensure that a massive number of MTC user equipments are efficiently supported and to also address related issues to mission critical MTC applications are part of the expected enhancements to 5G radio access technology. The future paradigm shift of MTC connectivity solutions in next generation cellular networks is to ensure that mission critical MTC applications including industrial automation, mobile healthcare system, which require ultra-high reliability, diverse range of data throughput, and extremely low latency performance are well supported. The ''moving ambulance'' use case for instance is expected to ensure that life-critical treatment is given to patients while reducing the delay when transporting patients from the incident scene to the hospital for medical attention. This use case requires that such ambulances are well connected to the hospital with immediate transmission of medical analysis that may include high resolution images and/or video transmissions [99]. Consequently, the need for real-time response updates is important from the hospital unit when providing medical treatment inside the ambulance. For Cellular IoT applications, 3GPP Release-14 has considered the following capability requirements as enhancements to Cellular IoT (CIoT): Authorization of use of Coverage Enhancement, GPRS support for Non-IP small data through services capability exposure function (SCEF), Re-use of legacy multicast/broadcast system, effective communication service between user equipment (UE) and service capability exposure function (SCEF), Inter-RAT mobility to and from NB-IoT. It is clearly observed that in 3GPP earlier Release-13, Coverage Enhancement (CE) was addressed, but Release-14 introduces this capability only to subscribers who are fully subscribed to this service of Coverage Enhancement and effective communication between UE and SCEF as an enhancement for acknowledgements of messages sent and delivered in order to detect message loss in the process of transmission.

In conclusion, a lot of progress has been made in the Cellular IoT domain through the LTE enhancements of low complexity devices which have been introduced for MTC applications. However, there is a need to embark on further research and development that will establish and enhance connectivity solutions which are based on 5G mobile network for MTC use cases. This will surely aid the IoT concept and ubiquitous connectivity for heterogeneous devices across verticals such as smart healthcare system, industrial automation system, public safety and electronic commerce.

B. ENHANCEMENTS TO MTC

Even though Cellular Internet of Things (CIoT) is a promising technology that supports the provision of MTC to end-users and facilitates an opportunity for mobile service operators in terms of revenue generation, there is a need to further improve and enhance LTE devices for MTC. Considering this, the 3GPP standardization proposed further complexity reduction schemes than can be used to achieve MTC. In Release-14, enhancements are currently been considered to support multicast downlink transmissions which will extend Release-13 Single Cell Point-to-Multipoint (SC-PTM) in order to support multicast transmission for eMTC and enhanced coverage area. For various IoT applications, it is important that the position of device is known. Therefore, there is need to evaluate and enhance MTC related to reception and transmission of time difference measurements. This will also ensure that the UE complexity and power consumption for the Observed Time Difference of Arrival (OTDOA) are considered [99]. To improve higher data rates for enhanced eMTC, further consideration include increasing the Transport Block Size, support HARQ-ACK bundling and up to 10 DL HARQ processes and finally ensuring that Voice over LTE (VoLTE) enhancements for eMTC devices will be achieved. The aim of these improvements is to ensure that coverage of Voice over LTE for half-duplex FDD and TDD UEs are efficiently enhanced and supported.

C. ENHANCEMENTS OF NB-IoT

NB-IoT has emerged as 3GPP standard-based cellular solution in Release-13 for improved indoor coverage, low delay sensitivity, support for large number of low throughput devices, ultra-low device cost, low device power consumption and optimized network systems able to support non-real-time voice and consequently to facilitate ultra-low cost for the current demand of IoT. Common use cases for NB-IoT include applications such as asset tracking, smart cities and buildings, and environment control system etc. This further enhancements into the 3GPP-LTE features for NB-IoT is to extend support to location positioning, multi-cast, mobility and link adaptation enhancements, and new power class(es) which are expected to be considered in Release-14 for 5G New Radio (NR) network in order to ensure that the market-driven demand of MTC is achieved efficiently.

1) MULTICAST

Single Cell Point–to–Multipoint (SC-PTM) which was considered in Release-13 is to be extended in order to enable multicast downlink transmission (either software upgrade or firmware, group message delivery) are supported for enhanced NB-IoT (eNB-IoT).

2) MOBILITY AND SERVICE CONTINUITY ENHANCEMENTS

These enhancements to NB-IoT enable connected mode mobility, which at the same time enhances service continuity, prevents Non-Access Stratum (NAS) recovery when considering the Control Plane (CP) and User Plane (UP) solutions without compromising the power consumption of the user equipment (UE).

3) NEW POWER CLASS(ES)

New Classes which might lead to the introduction of New User Equipment with a power level of 14dBm have to be evaluated. Based on the final evaluation, a signaling system will be developed for lower maximum transmit power which will be convenient for small form-factor batteries for wearables. It also intended to increase maximum transport block sizes by considering 1352 bits for downlink and 1800 bits for uplink which will enable UE in this release to support maximum data rates, reduced delay and power consumption.

In 3GPP Release- 13, high prioritized bands were officially allocated for NB-IoT including 1, 2, 3, 5, 8, 12, 13, 17, 18, 19, 20, 26, 28, and 66. Since NB-IoT is a promising technology for future applications, there is a need to ensure that issues related to coexistence with other deployed technologies are prevented. Based on this, special consideration is being given to NB-IoT radio frequency (RF). 3GPP currently reviewed the coexistence structure of operation between technologies like CDMA and IoT to ensure that about 49 dB Adjacent Channel Leakage Ratio (ACLR) can be achieved with 385 kHz edge separation, which is a clear indication of coexistence between CDMA systems and NB-IoT UE. This shows that no additional requirements are needed for coexistence with other legacy technologies which are currently deployed for future NB-IoT use cases. In addition, to enhance MTC applications, NB-IoT support has been introduced into the following bands: 25 (US), 70 (US), Bands 11 (Japan) and 31 (SA and Europe) for effective utilization.

D. NEW SERVICES AND MARKETS TECHNOLOGY ENABLERS

The 5G mobile network is being considered as the future telecommunications system that promises to provide the opportunity to design a 3GPP network that can be easily optimized to support connected devices and services. 3GPP is currently reviewing Rel-14 towards potential 5G service requirements which are expected to cover over 70 use cases under the New Services and Markets Technology Enablers (SMARTER) as promising opportunities for next generation telecommunications networks [102]. These newly introduced use cases cut across a wide range of new service markets from the IoT to vehicular communications and control, drone control systems, tactile internet, and industrial automation as well as catering for new services such as device theft prevention and recovery. In as much as some of the applications for the IoT will be supported by current systems, there is a need for improvements in terms of efficient resource utilization, adequate support for different access technologies, network flexibility, and network slicing that needs to be implemented into the future 5G radio network which is not readily retrofitted into already functional and existing networks. According to different industry white papers [99], the objective of the future 5G mobile network is a new network system that is expected to ensure that multiple service dimensions are efficiently and effectively supported. These proposed use cases are further being categorized as follows:

1) MASSIVE MACHINE-TYPE COMMUNICATIONS (mMTC)

This proposed Feasibility Study on New Services and Markets Technology Enablers for mIoT covers different applications (use cases such as smart utilities, smart buildings and cities, e-health systems, smart wearables and inventory control systems) with massive connected number of heterogeneous devices including wearables, actuators and sensors etc., with variety of characteristics and demands, which are specifically of importance when considering these new vertical services [103]. For instance, smart wearables are envisaged to ensure that human clothing is integrated with a number of ultra-light, low power, waterproof sensors which will be used to evaluate and determine environmental and health conditions (attributes) including temperature, pressure, heartbeats, blood pressure, body temperature, etc. However, it is important that a management system is put in place to control these devices as well as the data generated and applications for effective deployment of mMTC.

2) ENHANCED MOBILE BROADBAND (eMBB)

This proposed Feasibility Study on New Services and Markets Technology Enablers - Enhanced Mobile Broadband, envisaged that users are provided with accessibility of mobile broadband services anywhere - anytime, including constrained areas in terms of extended coverage (such as moving from urban to suburban and rural areas). Use cases to be considered in this category are relevant to higher data rates, high density, deployment and coverage (ultra-low cost networks), higher user mobility, and fixed mobile convergence [104]. For instance, network infrastructure as well as its cost of terminals are not readily deployed by network operators due to the very-low average revenue per user (ARPU) in rural areas (low population density distribution). With this new service requirement, 5G mobile network is envisaged to be more flexible for deployment under ultra-low cost requirements in order to provide Internet access to such areas, enabling new business models and avenues in underserved regions to be globally connected for efficient IoT applications.

3) CRITICAL COMMUNICATIONS

This proposed Feasibility Study on New Services and Markets Technology Enablers for Critical Communications, use cases such as industrial control applications (Drone/Robot/Vehicle), and tactile Internet are to be considered. This family of use cases require strong demand of real-time interaction with enhancements to be focused on mobility, latency (high throughput), critical reliability and availability which can be achieved through improved radio interface and optimized network architecture [105]. Use case such as tactile interaction, requires a typical tactile control signal and audio or visual feedback system where real and virtual devices can be controlled wirelessly by humans. For instance, considering running software applications on the cloud such that the end user interacting with such environments is not aware of the difference between the local and remote content. However, it is also challenging because of the real-time reaction which is expected to be within sub-millisecond in tactile Internet use cases. (For Critical MTC use cases with Ultra-Reliable and Low Latency Communications (URLLC).

4) NETWORK OPERATION

This proposed Feasibility Study on New Services and Markets Technology Enablers - Network Operation, use case scenario is expected to look into functional system requirements such as network slicing, flexible functions and capabilities, routing, migration and internetworking, optimizations and enhancements, and security [106] to enable connectivity of heterogeneous networks as a unique feature of 5G mobile network.

5) ENHANCEMENT OF VEHICLE-TO-EVERYTHING (eV2X)

These proposed use cases include autonomous driving, safety and non-safety aspects (which are associated with vehicles), requiring provision of ultra-reliable communication based on real-time response in order to prevent occurrence of road accidents. It is hoped that emerging 5G mobile networks will be able to provide low latency, high reliability, higher accuracy positioning and mission critical services which are required for future safety applications to mitigate the occurrence of road accidents, enhance traffic efficiency and enable the mobility of emergency vehicles including fire trucks, ambulances etc. Enhancement of Vehicle-to-Everything (eV2X) is foreseen to not being applicable to only vehicle-to-vehicle (V2V) or vehicle to infrastructure communication, but to be also applicable to other vulnerable road users.

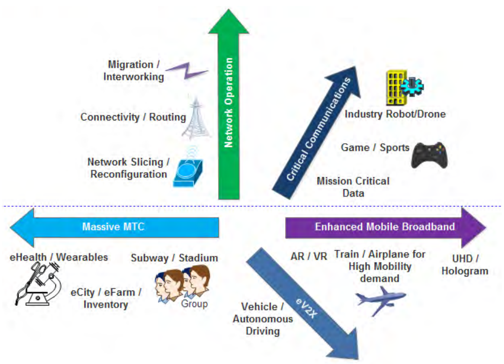

FIGURE 8. **FS_SMARTER New Service Dimension [102].**

The proposed use cases highlighted above as specified in 3GPP, are the basis of normative requirements which are currently under consideration as service requirements for the future 5G next generation network. Figure 8 depicts the proposed new enhancements for service requirements for 5G mobile networks that can efficiently and effectively support multiple service dimensions. Finally, we conclude that with further research on the 3GPP New Radio (NR) (Release-13/14) for the emerging IoT standards, 5G mobile network aim at enabling the basic requirements and KPIs which are required for future 5G new service requirements to enable the IoT use cases.

E. PERFORMANCE ANALYSIS OF MTC/IoT USE CASES

Considering the various use cases and new services envisaged for the 5G mobile network with their wide range of requirements are the main design principles for the future next generation communications technology for enabling the IoT. Some of the requirements to enable these use cases are extended coverage, reliability, battery life, low latency, mobility support, SLA support among others as mentioned in Table 8. Depending on the use cases to be deployed, some applications may only require a single KPI while others may demand for multiple KPIs for optimized performance. A major challenge for 5G mobile network is to be able to effectively support the various envisioned use cases in a more efficient and reliable way. For the interest of this survey, we have grouped the various use cases and new services from a business point of view and their probability to be exploited into the following generic applications such as fleet management sector, automotive sector, smart society, connected consumers and industrial automation.

In fleet management use case, some of the possible applications to be considered are route optimization, smart surveillance system, driver monitoring and management system, and operation management etc., to manage and control the running cost, ensure the safety of drivers and passengers and quality of experience (QoE). These use cases require reliable connectivity, seamless extended coverage to support geographical and remote areas, and location support for efficient deployment with evolving cellular technologies which promises new service improvements in fleet management system. Automotive applications will include new use cases considering mobile communications to support vehicles where on-board passengers will be entertained continuously with high capacity and high mobility mobile broadband irrespective of their current location. This use case also promises to ensure that future communications are established between connected vehicles, exchange of vital information between connected vehicles and infrastructure support base systems between vehicles and other related connected devices either Vehicle-to-Pedestrian (V2P). The emerging cellular-based LPWA solutions and the envisaged 5G mobile networks, will therefore further enhance the capability functions of connected vehicle and enable a speedy transmission and massive data that would be created by these use cases. Smart society includes use cases such as smart cities and smart buildings which are embedded system of wireless intelligent sensor networks that will be able to identify and specify the required cost and energy efficient systems that can be deployed to maintain connected cities and homes. It is envisaged that with the promising 5G mobile network, such diverse connected "things" will be properly integrated for efficient network management. The connected consumers use case includes application across smart transportation such as traffic congestion in urban areas. Emerging cellular IoT technologies will aid the collection of real-time and huge data that will be generated from vehicles, drivers, connected road sensors and cameras to control and manage the rate of traffic flow. In industrial, use cases include smart metering, maintenance monitoring, smart grid, and oil and gas pipeline etc., which are expected to have low delay and minimal error of probability as part of the promising new service requirements to be considered with 5G mobile networks.

Table 5 summarizes the possible use cases in each generic application with the LPWA technologies which are likely to meet the demand of the use cases based on outstanding KPI requirements. Each use case is linked to the LPWA technologies which are likely to meet the basic requirements of such use case. In addition, not in all scenarios that the unlicensed LPWA solutions such as SigFox, LoRa, and Ingenu RPMA will be able to meet such use case demands because of their KPI requirements.

In summary, this shows that in deploying MTC use cases, there is no one-fit-for-all technology as the attributes for each LPWA technology differs and therefore, in deploying such use cases, one must ensure that the appropriate technology is selected based on the use case's KPI requirements. However, it is envisaged that the emerging cellular-based LPWA standards such as eMTC, EC-GSM-IoT, NB-IoT and the 5G mobile network will definitely enhance and enable the deployment of mission–critical services, and also provide major improvements to the system in terms of reliability, availability and secure end-to-end communication because of their global eco-system establishment and further enhancements which have been introduced into existing networks.

VI. NETWORK ENABLER FOR THE INTERNET OF THINGS

5G mobile networks are envisaged as a promising next generation technology to support the massive deployment of simultaneously connected heterogeneous devices with new service requirements based on wearable things, improved better coverage edge, low latency, high versatility and scalability for efficiently enabling the Massive to Critical IoT applications. However, it is obvious that the conventional network infrastructure is continuously becoming outdated to support these features for the IoT architecture with the existing conventional networking system. Consequently, the network management complexity continue to increase because of the manual process which is used in network configurations owing to the limitations of conventional hardware-based networking. Moreover, a network system should be able to enable the ever-evolving networking technologies for future network infrastructure. In addition, the current traditional networks cannot enable the ever-growing networking technologies demand for future next generation networks. To achieve these objectives, emerging technologies including Software-Defined Wireless Sensor Networking (SDWSN), Network Function Virtualization and Cognitive Radio (CR) are among the few network enablers to be discussed briefly in this section to overcome such limitations of the legacy networks by 5G mobile network for the IoT.

A. SOFTWARE-DEFINED WIRELESS SENSOR NETWORK

Cellular technology which is currently deployed for wireless communications and most especially for the rapid growth and requirement of the IoT applications, are hardware-based designs and as such require that emerging technologies for future next generation network are introduced to ease the flexibility of the network infrastructure to accommodate and process the massive inflow of data for the IoT use cases. SDWSN is a new promising paradigm to achieve Low-Rate Wireless Personal Area Networks (LR-WPAN) [107]–[109].

TABLE 5. Performance analysis for MTC/IoT use cases.

Application Domain	Common Use Cases	LPWA Technologies	Outstanding Requirements
Fleet Management	Route Optimization	Cellular-based LPWA	Reliability, enhanced Coverage, SLA Support, Data rates
	Smart Surveillance	Cellular-based LPWA	Reliability, enhanced Coverage, SLA Support, Data rates
	Driver Monitoring System	Cellular-based LPWA	Reliability, enhanced Coverage, SLA Support, Data rates
	Operation Management	Cellular-based LPWA	Reliability, enhanced Coverage, SLA Support, Data rates
Automotive	Vehicle-to-Infrastructure (V2I)	Cellular-based LPWA	Mobility, Coverage, Cost, SLA Support, Reliability, Security
	Vehicle-to-Vehicle (V2V)	Cellular-based LPWA	Mobility, Coverage, Cost, SLA Support, Reliability, Security
	Vehicle-to-Cloud (V2C)	Cellular-based LPWA	Mobility, Coverage, Cost, SLA Support, Reliability, Security
	Vehicle-to-Pedestrian (V2P)	Cellular-based LPWA	Mobility, Coverage, Cost, SLA Support, Reliability, Security
Smart Society	Smart Cities	Unlicensed LPWA, Cellular-based LPWA	Coverage, SLA Support, Reliability
Connected Consumers	Smart Buildings	Unlicensed LPWA, Cellular-based LPWA	Coverage, Indoor, SLA Support, Reliability, Security
	Smart Transportation	Cellular-based LPWA	Coverage, Mobility Support, SLA Support, Reliability, Network Scalability
	Smart Automatic Driving	Cellular-based LPWA	Coverage, Mobility Support, SLA Support, Reliability, Network Scalability
Industrial Automation	Smart Metering	Unlicensed LPWA, Cellular-based LPWA	Capacity, Security, Bandwidth
	Maintenance Monitoring	Unlicensed LPWA, Cellular-based LPWA	Capacity, Security, Bandwidth
	Smart Grid	Unlicensed LPWA, Cellular-based LPWA	Capacity, Security, Bandwidth
	Oil and Gas Pipeline	Cellular-based LPWA	Mobility, SLA Support, Capacity, Security, Reliability, Bandwidth

Technology Compatibility Mode	
Unlicensed LPWA – SigFox, LoRa, RPMA	Cellular-based LPWA - EC-GSM-IoT, eMTC, NB-IoT

This network paradigm is achieved by the infusion of Software-Defined Networking (SDN) model into existing Wireless Sensor Networks (WSNs). SDN was primarily intended to be used in wired communication systems such as data centers and for next-generation Internet connectivity [110]–[112] but has recently emerged in most wireless communication networks [113], and is envisaged as a future technology enabler for the next generation 5G mobile networks [114], [115]. This intelligent network paradigm provides a centralized network abstraction for programmability of the entire network.

The primary purpose for introducing SDN is to decentralize the control logical plane from the network device, e.g., switch and to enable an external network controller to define the nature and behaviour of the network forwarding infrastructure (i.e. routing and major management processing). SDN also makes it easier for the introduction and deployment of new application services, and enables the flexibility of network management that would support the exponential traffic growth of the envisaged 5G mobile networks [116] as a major network enabler for the IoT. WSNs are expected to be a vital enabler for IoT systems since the majority of the sensor nodes are the main entity for this concept [117]. It is hoped that SDWSN will be a key network enabler technology to address the issue of flexibility and interoperability of future multi-vendor infrastructure in 5G mobile network for the IoT. With the massive increase of connected devices through Massive to Critical IoT, traditionally deployed network architectures, which are hardware-based, will need to be enhanced to accommodate, manage, and control the large amount of heterogeneous devices and inflow of data into the network.

Therefore, there is a need to introduce SDWSN into next generation cellular networks that will simplify the entire network infrastructure, manage and control the entire system requirements and maintain the heterogeneity of the networked environments to enable future IoT use cases.

B. NETWORK FUNCTION VIRTUALIZATION

Network Function Virtualization (NFV) is highly complementary to SDN, envisaged as an enabling network technology for next generation service requirements for the IoT applications but are both not dependent on each other. This means that NFV can be successfully implemented without considering SDN and vice–versa. In addition, it is possible that both solutions can be combined to achieve optimal performance output.

According to [118], NFV technology can be used to virtualize a set of network functions which can be further implemented into software packages to be configured in order to efficiently provide related service requirements like existing network infrastructure. The concept of NFV came into reality from the perspective of Virtual Machines (VM) which can be installed to run on various operating systems on the same server machine. With the rapid growth and increase of connected heterogeneous devices for Massive to Critical IoT applications towards new service requirements for 5G mobile networks, there is a need for a key technology enabler in 5G technology to efficiently enable the massive deployment of MTC devices.

By network functions (i.e. by relocating the routing decision making from local hardware and to be implemented into general purpose computing and other storage devices such as servers and cloud), NFV technology would ensure that the deployment of heterogeneous MTC devices to achieve Critical and Massive IoT applications are well managed and controlled. According to [119], NFV is currently being considered in the context of virtualizing core networks, and centralizing base band processing within Radio Access Networks (RAN). In addition, by virtualizing network functions in any deployed network infrastructure, system scalability and flexibility of connected heterogeneous devices, reduction in Capital Expenditure (CAPEX) and Operational Expenditure (OPEX), as well as power consumption can be achieved efficiently which will at the same time aid the market deployment of IoT use cases.

C. COGNITIVE RADIO NETWORKS

The current demand for MTC ensuring that everything is connected, anywhere and at any-time, has resulted in drastic changes which are evolving in currently deployed cellular networks and next generation network such as the 5G mobile network. Interconnectivity of heterogeneous devices with diverse service requirements poses a huge opportunity and challenge to cellular network operators to massively deploy future IoT applications. The current service requirements for IoT applications from both Massive to Critical IoT will definitely result in an increased average revenue per user (ARPU) which would be a result of newly introduced services. On the other hand, the massive demand for connected "things" leads to overloading of certain cellular geographical areas which is a result of limited spectrum resources which have been licensed to cellular network operators. Research has shown that a deficit in broadband spectrum was likely to have approached 300 MHz in 2014, and the provision of additional spectrum to be considered for mobile broadband would also lead to an excess increase of $100 billion [120].

Cognitive Radio (CR) technology is a key network enabler for 5G mobile networks to utilize the limited and scarce spectrum resources in order to support the increasing and high demand for new service requirements of emerging and promising IoT applications. CR supports the capability of using or sharing the licensed spectrum in an opportunistic manner [121]. Dynamic spectrum access techniques allow the CR to operate in the best available channel. CR technology enables the identification of available free spectrum and also enables the detection of licensed users present in the system (spectrum sensing), the ability to select the best available channel (spectrum management), the ability to coordinate accessibility to the available channel with other users (spectrum sharing) and finally the ability to vacate the accessed channel on arrival of the licensed or primary user (spectrum mobility) [121].

CR technology can be used to augment next generation cellular networks (such as LTE, WiMAX and future 5G mobile network) to dynamically access newly introduced spectrum (such as TV White Space) which has been officially released by the Federal Communications Commission (FCC) for "unlicensed operation in the TV Broadcast Bands" [122]. This can be achieved by introducing a spectrum coordinator in the non-access stratum (NAS) which will enable cellular network technology to dynamically lease or access spectrum markets and to determine/identify secondary license exempt spectrum opportunities which can be used in deploying IoT applications for a period of time in a given location. Another major consideration where CR technology can be an enabler to achieve the massive deployment of the IoT vision is the rural geographical area, which is generally known to have poor coverage. Since licensed spectrum is limited and scarce, cellular network operators in most cases prefer not to deploy their networks in rural areas due to low population density distribution which is typically not cost effective due to the limited number of network subscribers. With CR technology, white space spectrum which has been proposed and made available for unlicensed use, can be explored for backhaul by cellular network providers in order to ensure that their cell towers are connected to their backbone networks, thereby providing and deploying connectivity solutions for IoT applications in unserved and underserved geographical areas which will aid the vision of connecting more MTC devices for the IoT.

VII. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

The current demand for MTC connectivity to provide the various new services and applications for both the industrial and societal need has introduced new challenges to satisfy the current requirements for the IoT vision. It is important to ensure that special considerations are given in order to address these challenges to support MTC devices, such that the security and quality of service (QoS) for both MTC devices and human-to-human (H2H) users that utilize the same network infrastructure are not being compromised. In this section, we try to describe some of the challenges based on IoT requirements, while aligning them for future research consideration.

A. SCALABILITY

Network scalability can be seen as a major issue to be addressed, specifically when considering LTE systems for MTC. IoT scalability refers to the ability of introducing new heterogeneous devices, applications and functions for the interest of end users without compromising the quality and provision of existing services. According to [24], legacy LTE cellular technology will have to manage the small message size packets of M2M devices with large transmission intervals effectively. This poses a major issue due to the envisaged ultra-dense deployment of connected devices in future, and managing the state information of massive number of connected devices is also an issue that needs to be considered [108], [109].

A generic IoT system was presented in [123] with an IoT daemon which consists of three different layers including Composite Virtual Object, Virtual Object and Service layer, which are expected to guarantee scalability as well as interoperability between heterogeneous networks. In order to ensure that massive deployment of IoT is achieved, networks which are deployed and currently in use must be optimized for scale efficiently [124]. Hence, this ensures that network capacity is scalable to accommodate as much connected devices as possible. In particular, the use of IPv6 makes available more than enough addresses for IoT devices currently deployed and devices that will be deployed in the near future. Hence, there is need for a holistic system that will maintain, manage and control the state information generated as a result of massive connection of devices.

B. NETWORK MANAGEMENT

Network management solutions (NMS) are basically deployed to ensure that network equipment, services, and devices are properly managed. However, considering the IoT concept, the need for management goes beyond the traditional networked society and their services, but to also ensure that everything is entirely considered. The massive number of connected things and their wide range in diversity pose a major management requirements in the IoT for Fault, Configuration, Accounting, Performance and Security (FCAPS). Thus, in conventional network environments, management functionalities including monitoring, remote control, and maintenance are considered to be very important in the operation of connected devices in the IoT. Because of the heterogeneity-nature of the IoT, these management capability functionalities would have to be re-engineered to the specific management functionalities which are required to control, manage and cater for the unique features of the IoT. Therefore, it is important to ensure that new lightweight management standards are developed to provide efficient management of the networked IoT environments. For instance, functionalities like network reconfiguration and self-configuration are very important management requirements to be considered in the IoT. Consequently, for conventional networked environment, network management solutions (NMS) are expected to provide required management information within a minimal time frame. However, due to the constrained-nature of IoT devices, network management solutions should be able to provide such required management information in a comprehensive format while minimizing energy consumption [125].

Nevertheless, in the IoT, the characteristics of data which are generated are quite distinct when compared to the conventional network [126] because of the constrained-nature of the IoT networks. Therefore, the need for management functionalities in the IoT is significant as this will help network administrators to carry out their managerial tasks remotely through the Internet and across heterogeneous interconnected networks. With such functionalities deployed by the management system, the rate of inaccuracy will be reduced to minimal, thereby improving the response time of the network. In addition, such an efficient system would aid in diagnostic/troubleshooting of IoT devices and real-time remote control monitoring, thereby minimizing the cost of operations and enhancing maintenance tasks which are to be managed by system managers. In [127], a conceptual framework to manage IoT through the concept of intercepting intermediary was introduced for managing heavy device tasks on designated edge routers of constrained-networks. A lot of research is on-going to specify standards and mechanisms that could be used to manage mobile devices and services in terms of resource constrained-networks such as the Open Mobile Alliance (OMA) Device Management working group.

Finally, the magnitude of connected networks and the level of data which are associated with the IoT presents more challenging issues confronting the IoT in terms of data and service management including data acquisition and aggregation, service provisioning and control as well as system performance of connected things. Therefore, it is very important to have an efficient management solution that would be used to determine the performance level of connected things as well as the IoT network. The benefits of having an efficient management solution are enormous to enable general management of connected things in the IoT. However, there are some management challenging issues which confront the IoT and need to be addressed. Table 6 summarizes some of the key management issues in the IoT.

C. INTEROPERABILITY AND HETEROGENEITY

A major challenge to be addressed when considering MTC for the IoT - which aimed at connecting everything, anywhere and at any-time - is the seamless end-to-end interoperability between the different network technologies which have been presented in the earlier sections and heterogeneous IoT devices. This will enable the connectivity of multiple devices across the various communication networks, and perhaps the realization of the IoT concept which enables heterogeneous devices to be connected through a communication technology to communicate, disseminate, and collect vital information with other related smart devices or applications [128]. To achieve this, elusive interoperability must be deployed across devices among all network technologies considering their model, network provider, as well as the vendors that manufacture said network infrastructure. This means that for massive IoT deployment, connectivity of devices must be enabled irrespective of hardware infrastructure and application programming interface (API) being used. The current

TABLE 6. Summary of management issues in the IoT [128].

Management Issues	Brief Description
System Configuration Management	Configuration to be included include: - Connectivity of the network - Self-configuration functionality - Process of setting up devices and who is in control? - Network reconfiguration
System Monitoring	It is important to know the operation and position of connected thing either their running system, sleep condition (mode), down-time, etc. in order to identify their current position of service. These include: - Discovery of network topology - System notification - Network condition monitoring
Maintenance of Connected Devices	Considering the heterogeneity of the IoT that involve massive number of connected things, it is important to monitor and detect the presence of failure. Therefore, there is need for a software defined system that will be used for detecting and controlling the presence of failure in connected things. Other maintenance issues to be looked at are updating software, protocol version detection and patches for updates.
Performance of Connected Devices	It is important to ensure that appropriate monitoring solutions are introduced for system performance evaluation as this will prevent the occurrence of any failure in future. This become very important when considering applications which are installed in remote regions.
Energy Efficiency Management	This ensure that the energy consumption level of the networked devices are efficiently monitor including: - Adequate statistics on the energy level such expected life-span of connected devices. - Management of energy resources.
Security and Privacy in Networked society	Considering the resource-constrained nature of IoT, basic security challenges that need to be considered are authentication, authorization, and access control. Other security related issues to be dealt with are end-to-end communications. For example, considering the situation where connected devices will have to be accessed by running applications and software without human intervention, therefore, there is need to ensure that strict security policy are enforced to prevent connected things from revealing vital and private information to unauthorized devices or being used mischievously. Therefore, strict privacy must be enforced.

situation on ground is a fragmented system that does not support interoperability between heterogeneous devices. For massive IoT applications to be achieved, interoperability and standardization between the various communications technologies is of great importance in meeting consumers' requirements that must be addressed.

However, the presence of various protocols and standards which are being implemented by different organizations in order to address the competitive nature of the IoT pose a major challenge for interoperability [129]. Finally, the heterogeneous nature of the IoT is also a major issue that makes interoperability between different devices more difficult and complex to achieve, especially with the emergence of new communication technologies which introduce many integration challenges including common practices, service descriptions, standards and discovery mechanisms which need to be adequately addressed in order to ensure that an enabling interoperable environment is established between the IoT heterogeneous networks.

D. SECURITY AND PRIVACY

The paradigm shift of wireless technologies and M2M communications has led to the massive number of devices connected to communication networks in the IoT and increase in security threats which pose new security issues. Security issues include malicious code attacks (such as worms), inability to receive security patches, hacking into smart meters, eavesdropping, sniffing attacks and Denial of Service (DoS) attacks [130]–[133]. Security is a fundamental challenge confronting the vision of the IoT because of the heterogeneity of devices, physical accessibility to actuators, sensors and objects, and most especially the openness of the systems which are connected to the Internet through a wireless communication medium. Heterogeneity of devices in the IoT inherits the security threats of present day computer devices. However, the degree of impact of such threats could be significantly different from each other. This gives a major reason why a lot of research is focused on threat analysis [134] and risk assessment of such security challenges. Therefore, key security requirements such as authorization, authentication, trust, confidentiality, data security, and non-repudiation must be carefully addressed in the future IoT networks.

One of the most fundamental components which is required in securing any IoT network is based on the device identity and the mechanisms to deploy. Since the processing capability of MTC devices is limited due to their resource-constrained nature, these devices may not be able to activate existing security schemes which are currently used on the Internet. Most commonly used strong encryption and authentication schemes such as Advanced Encryption Suite (AES), which is used for confidential data transport, Diffie-Hellman (DH) to implement key exchange and management, and Rivest-Shamir-Adleman (RSA) to implement digital signatures and key transport are based on cryptographic suites with robust protocols and as such require a very high performance platform which is not suitable for future IoT resource-constrained devices [135]. In addition, authentication and authorization will require appropriate re-engineering in order to accommodate the concepts of future IoT networks.

In order to overcome these challenges and ensure that secure end-to-end communication is guaranteed for IoT networks, there is a need to investigate and design new authentication schemes which can be developed based on current strong encryption and authentication algorithms for resource-constrained devices. In addition, the inability to incorporate a shared infrastructure and unique security protocols is a challenging issue confronting the security of the IoT communication networks.

E. NETWORK MOBILITY AND COVERAGE

Network mobility, coverage and reachability remain open research areas for the IoT that needs to be addressed for effective deployment of Massive to Critical IoT use cases as performance metrics because most of the IoT services are expected to be delivered to mobile users. This is an important premise of the IoT to ensure that users are connected anywhere and provided with their service requirements while on the move. Smart connected mobile devices experience service interruption as a result of device mobility (i.e. moving from one specific gateway to another).

An efficient mobility management mechanism is needed to manage and control the enormous growth of smart connected devices in the IoT networks. In [136], a feasible approach was presented in which a leader is assigned to manage group mobility based on some peculiar metric analysis which is a function of the mobility pattern of devices. Considering the massive number of IoT devices, current cellular networks will have to deploy more base stations in order to effectively and efficiently connect all the networks together. Moreover, the promising new service requirements of 5G mobile networks for the IoT needs unique attention when considering the mobility issue in the IoT.

F. NETWORK CONGESTION AND OVERLOAD

Network congestion and overload is a major challenge that needs to be addressed in the evolution of the IoT because the smart connected devices play a vital role in driving up the signaling load in the mobile network when compared to the traditional human-to-human (H2H) traffic in cellular networks. Network congestion degrades the IoT performance and quality of service (QoS). A challenging issue which is pertinent to MTC is the ability to accommodate the huge traffic that would be generated as a result of the massive number of MTC devices that would create congestion problem in the networks. Thus, the Internet Protocols (IP) will have to deal quite efficiently with the network congestion problem. Most networks provide a stable Internet connection, irrespective of the massive connection of devices using Transmission Control Protocol (TCP) in the transport layer. However, the existing TCP implementations are not suitable for the IoT application scenarios, and fail to cope with the IoT traffic pattern since the traffic pattern of the IoT network is entirely different from the conventional networks.

The Constrained Application Protocol (CoAP) was developed by the Internet Engineering Task Force (IETF) and as a lightweight protocol for resource-constrained devices and lossy communication networks [137]–[139]. CoAP, being considered as an IP must be able to handle congestion control in order to maintain the network backbone. Enabled IoT networks would have to use different protocols to enable communication. There are different existing application protocols for the IoT. These protocols are designed to perform for different application scenarios. A lot of research is ongoing from both the academics and industrials on congestion control mechanism. Hence, without incurring high overhead, there is a need for an efficient handling of network congestion and bit error rate (BER) to trade-off the packet loss and delay in the IoT environment. In addition, the congestion control mechanism in IoT should be capable of assuring a safe network operation with efficient network resource utilization. Table 7 summarizes some of the related application protocols that can be used with different performance features for the IoT.

G. SUMMARY

The IoT will continue to be more pervasive in future use cases, which are expected to positively impact the everyday-life of the end users' community. However, the massive number of connected things and the heterogeneous nature of communication networks in the IoT pose many research challenges.

Although the IoT paradigm has been the focus of research, there is a need for more intense research work to ensure that the vision of the IoT is globally achieved as projected. The continuous contribution and attention which has been given by academia, industries, and governments has definitely led to great achievements in terms of research projects towards achieving new service requirements for the IoT. Some of the IoT challenges including security, extended coverage, low device cost, low power consumption and network architecture, have been given some considerations over time while others including network management, heterogeneity and interoperability, traffic congestion and control - which automatically guarantee the availability of network information and QoS over specific time - are still broadly open for more intense research. With the current emerging cellular-based LPWA solutions for the IoT including eMTC, EC-GSM-IoT, and NB-IoT, there is a need to research into network positioning of smart connected things and context-aware services considering the new service requirements for next generation mobile telecommunications. Table 8 presents a summary analysis of 5G KPIs [140] of the various existing and emerging technologies which have been presented in detail, considering their modern connectivity characteristics to address the IoT requirements in terms of extended coverage, availability of dedicated spectrum, low deployment cost, battery lifetime, and scalability etc., for the new service requirements.

TABLE 7. Summary of some related application protocols for the IoT.

Applicable Protocol	Supported Architectures	Applicable Transport	Lossy nature	Available Compute Resources	Security Requirement	Developer
CoAP	Request/Response	UDP/IP	Very excellent	10Ks/RAM Flash	Medium – not compulsory	IETF
MQTT	Publish/Subscribe	TCP/IP	Fair enough	10Ks/RAM Flash	Medium – not compulsory	IBM (OASIS)
MQTT-SN	Publish/Subscribe	UDP/IP	Fair enough	10Ks/RAM Flash	Medium – not compulsory	
AMQP	Publish/Subscribe	TCP/IP	Fair enough	-	Very High - compulsory	John O'Hara (JP Morgan)
XMPP	Publish/Subscribe Request/Response	TCP/IP	Fair enough	10Ks/RAM Flash	Very High - compulsory	Jabber Open Source
Continua HDP	Publish/Subscribe Request/Response	UDP/IP	Fair enough	10Ks/RAM Flash	-	Continua Health Alliance
DDS	Publish/Subscribe	UDP/IP	Fair enough	100Ks/RAM Flash	Very High – not compulsory	OMG

TABLE 8. Key performance indicators (KPIs) analysis for modern IoT connectivity solutions.

KPI	ZigBee	BLE	Wi-Fi	SigFox	LoRa	EC-GSM-IoT	eMTC	NB-IoT
Extended Coverage	x	x	x	✓	✓	✓	✓	✓
Reliability	x	✓	✓	x	x	✓	✓	✓
Low Deployment Cost	✓	✓	✓	✓	✓	✓	✓	✓
Long Battery-Life	✓	✓	✓	✓	✓	✓	✓	✓
Low Latency	x	✓	✓	x	x	✓	✓	✓
Network Scalability	x	x	✓	x	x	✓	✓	✓
Mobility Support	x	x	x	x	x	✓	✓	✓
SLA support	x	x	x	x	x	✓	✓	✓
Support for Roaming	x	x	x	x	x	✓	✓	✓
Dedicated Spectrum	x	x	x	x	x	✓	✓	✓

VIII. LESSONS LEARNED

This paper reviewed the current state-of-the-art of the IoT from various perspectives. The IoT paradigm promises to provide a conducive networking environment through connected heterogeneous things. These things (devices) are systems of embedded sensors and actuators which are networked to communicate through a wireless communication medium. The applications of the IoT and the related KPI requirements to fully realize the IoT concept were presented. From this analysis, it is obvious that there is no one-fit-for-all solution that could be used to deploy the IoT use cases, since different application domains require different service provision.

The IoT concept envisioned that massive heterogeneous devices will be connected through enterprise networks, optical networks as well as mobile wireless communication networks. LPWA networks are novel communication technology that is expected to fully complement the conventional cellular and short range wireless networks to meet the IoT diverse application requirements. These technologies promise to offer some specific features to enable MTC including wide-area solutions for low power and low data rate devices, which are not currently available through the existing wireless technologies. Moreover, it is worth mentioning that to achieve the IoT vision for massive deployment of MTC use cases, enabling cellular-based LPWA connectivity solutions such as EC-GSM-IoT, eMTC, and NB-IoT is no doubt a major breakthrough for Massive to Critical IoT use cases, since this technology has been globally deployed and offers different service requirements which would be needed for the diverse applications of the IoT within a single network.

The paper also delved into 5G mobile network as the future telecommunications system for new services and market technology enablers (SMARTER) for next generation networks. Key performance enhancement features for M2M and NB-IoT systems for Massive to Critical IoT use cases were discussed. Moreover, it is also envisaged that the 5G mobile networks will be software driven. Network functions including SDWSN, NFV, and CR are expected to simplify the entire IoT network, provide flexibility and scalability of connected heterogeneous devices and to ensure connectivity for the IoT applications in unserved and underserved geographical regions.

TABLE 9. Definitions of all acronyms used in the paper.

Abbreviations	
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
ARPU	Average Revenue Per User
AR	Augmented Reality
BPSK	Binary Phase Shift Keying
CACC	Context-Aware Congestion Control
CAPEX	Capital Expenditure
CSS	Chirp Spread Spectrum
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
Cat	Category
CRN	Cognitive Radio Network
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
DBPSK	Differential – Binary Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
DSS	Data Distribution Service
DL	Downlink
EC-GSM-IoT	Extended Coverage Global System for Mobile Communications for the Internet of Things
eMTC	Enhanced Machine-Type Communications
eDRX	Extended Discontinuous Reception
eV2X	Enhancement of Vehicle-to-Everything
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance & Security
eMBB	Enhanced Mobile Broadband
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile Communications
GPS	Global Position System
GPRS	General Packet Radio Service
GFSK	Gaussian Frequency Shift Keying
H2H	Human-to-Human
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IIoT	Industrial Internet of Things
IP	Internet Protocol
ISM	Industrial, Scientific, and Medical band
IMT	International Mobile Telecommunications
ITU	International Telecommunication Union
ITS	Intelligent Transportation System
KPI	Key Performance Indicator
LPWA	Low Power Wide Area
LPWAN	Low Power Wide Area Network
LR-WPAN	Low-Rate Wireless Personal Area Network
LTE	Long-Term Evolution
LTE-A	Long-Term Evolution-Advanced
M2M	Machine-to-Machine
MTC	Machine-Type Communications
MAC	Medium Access Control
MCL	Maximum Coupling Loss
MQTT	Message Queuing Telemetry Transport
MQTT-SN	Message Queuing Telemetry Transport for Sensor Networks
mMTC	Massive Machine-Type Communications
NB-IoT	Narrowband-Internet of Things
NFV	Network Function Virtualization
NMS	Network Management Solutions
OPEX	Operational Expenditure
OMG	Object Management Group
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Open Mobile Alliance
OTDOA	Observed Time Difference of Arrival

TABLE 9. *(Continued.)* Definitions of all acronyms used in the paper.

PA	Power Amplifier
PRB	Physical Resource Block
PSM	Power Saving Mode
QoE	Quality of Experience
QoS	Quality of Service
RF	Radio Frequency
RPMA	Random Phase Multiple Access
RFID	Radio Frequency Identification
RAN	Radio Access Network
SCEF	Services Capability Exposure Function
SC-FDMA	Single-Carrier Frequency Division Multiple Access
SC-PTM	Single Cell Point-to-Multipoint
SDN	Software-Defined Networking
SDWSN	Software-Defined Wireless Sensor Network
SLA	Service Level Agreement
SIG	Special Interest Group
TDMA	Time Division Multiple Access
TBS	Transport Block Size
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunication System
UHD	Ultra-High Definition
UNB	Ultra-Narrowband
UDP	User Datagram Protocol
UE	User Equipment
UL	Uplink
URLLC	Ultra-Reliable and Low Latency Communications
VM	Virtual Machines
V2V	Vehicle-to-Vehicle
V2P	Vehicle-to-Pedestrian
VR	Virtual Reality
VoLTE	Voice over Long-Term Evolution
WAP	Wireless Application Protocol
WSN	Wireless Sensor Networks
W-CDMA	Wide-band Code Division Multiple Access
XMPP	EXtensible Messaging and Presence Protocol
2G	Second Generation
3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation Mobile Network

The challenges confronting the IoT vision were presented for future consideration, keeping in mind that there is no one-fit-for-all solution in deploying the IoT use cases. Some of these challenges include; scalability, network management, interoperability and heterogeneity, security and privacy, network mobility and coverage and finally but not the least network congestion and overload. Interoperability and heterogeneity is a vital issue to be addressed due to the heterogeneous-nature of the IoT and various communication networks which will have to be integrated for a unique standardization. Network congestion is essential since with the massive number of connected things, the huge traffic that would be generated result to network congestion and lead to high packet loss rate. Therefore, we believe that this demands for an efficient quality of service (QoS) assurance system as a lightweight context-aware congestion control (CACC) mechanism to manage and handle the network congestion problem and bit error rate in the IoT networks.

IX. CONCLUSION

The current expectation and future evolution of the IoT is promising to enable new services and quality of experience (QOE) across the users community and very challenging at the same time because of the resource constrained-nature of the network which has compelled research community to ensure that the requirements for massive deployment of MTC applications are achieved for globally connected things.

This paper has reviewed the unique features of the current state-of-the-art of IoT standard infrastructure, including the cellular-based LPWA eMTC, EC-GSM-IoT, NB-IoT, and non-cellular LPWA technologies including LoRa, SigFox, and Ingenu-RPMA with main focus on 5G mobile networks as next generation network for enabling the new service requirements. The requirement of 5G mobile network will be massive to enable mission–critical services, and will be software driven including SDWSN, NFV, and CR to support dynamic data control, provide a centralized network system and to enable the adaptation of new service requirements for enabling Massive to Critical IoT use cases with efficient coverage and high capacity targets for lifetime MTC devices.

However, there still exists open research challenges for effective control and management of the IoT networks. For future evolution of the IoT, it is therefore recommended to develop a context-aware congestion control (CACC) scheme for lightweight CoAP/UDP-based IoT network as a multi-objective function that would support the exponential traffic growth pattern of the envisaged 5G mobile networks for MTC applications.

APPENDIX

All the acronyms used in the paper are enlisted in Table 9.

REFERENCES

[1] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.
[2] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Comput. Commun.*, vol. 54, no. 12, pp. 1–31, 2014.
[3] R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," *Computer*, vol. 48, no. 1, pp. 28–35, 2015.
[4] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[6] O. Vermesan *et al.*, "Internet of Things strategic research agenda," in *Internet of Things—Global Technological and Societal Trends*. Gistrup, Denmark: River Publishers, 2011, ch. 2.
[7] *Service Requirements for Machine-Type Communications, Sophia-Antipolis Cedex, France*, document 3GPP TS 22.368 V11.5.0, 3GPP, 2012.
[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[9] *Cellular Networks for Massive IoT: Enabling Low Power Wide Area Applications*, Ericsson, Stockholm, Sweden, 2016, pp. 1–13.
[10] Nokia, "LTE evolution for IoT connectivity," Nokia, Espoo, Finland, White Paper, 2017, pp. 1–18.
[11] E. Berthelsen and J. Morrish. (Apr. 2015). "Forecasting the Internet of Things revenue opportunity." Machina Res., London, U.K., Tech. Rep. [Online]. Available: https://machinaresearch.com/report_pdf/313
[12] S. Horten, "Bringing the smart city to life," *M2M Alliance J.*, no. 24, Dec. 2014.
[13] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 514–519.
[14] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, "A global perspective of smart cities: A survey," in *Proc. IEEE 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2013, pp. 439–444.
[15] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.
[16] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, 1st Quart., 2013.
[17] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014.
[18] A. M. Abu-Mahfouz, T. O. Olwal, A. M. Kurien, J. L. Munda, and K. Djouani, "Toward developing a distributed autonomous energy management system (DAEMS)," in *Proc. IEEE AFRICON*, Sep. 2015, pp. 1–6.
[19] P. Dongbaare, S. P. D. Chowdhury, T. O. Olwal, and A. M. Abu-Mahfouz, "Smart energy management system based on an automated distributed load limiting mechanism and multi-power switching technique," presented at the 51st Int. Univ. Power Eng. Conf., Sep. 2016.
[20] B. Silva, R. M. Fisher, A. Kumar, and G. P. Hancke, "Experimental link quality characterization of wireless sensor networks for underground monitoring," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1099–1110, Oct. 2015.
[21] B. Cheng, L. Cui, W. Jia, W. Zhao, and P. H. Gerhard, "Multiple region of interest coverage in camera sensor networks for tele-intensive care units," *IEEE Trans. Ind. Informat.*, vol. 12, no. 6, pp. 2331–2341, Dec. 2016.
[22] K. S. E. Phala, A. Kumar, and G. P. Hancke, "Air quality monitoring system based on ISO/IEC/IEEE 21451 standards," *IEEE Sensors J.*, vol. 16, no. 12, pp. 5037–5045, Jun. 2016.
[23] A. M. Abu-Mahfouz, Y. Hamam, P. R. Page, K. Djouani, and A. Kurien, "Real-time dynamic hydraulic model for potable water loss reduction," *Procedia Eng.*, vol. 154, no. 8, pp. 99–106, 2016.
[24] J. Jermyn, R. P. Jover, I. Murynets, M. Istomin, and S. Stolfo, "Scalability of machine to machine systems and the Internet of Things on LTE mobile networks," in *Proc. IEEE 16th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2015, pp. 1–9.
[25] S. Cho, B. F. Spencer, Jr., H. Jo, J. Li, and R. E. Kim, "Bridge monitoring using wireless smart sensors," *SPIE Newsroom*, pp. 1–3, Jan. 2012, doi: 10.1117/2.1201201.004043.
[26] BLE. *Smart Bluetooth Low Energy*. Accessed: Feb. 15, 2017. [Online]. Available: https//blog.bluetooth.com/bluetooth-low-energy-it-starts-with-advertising
[27] Taylor, Larry, Alliance, and ZigBee, "Interconnecting ZigBee & M2M networks," in *Proc. ETSI M2M Workshop*, Sophia Antipolis, France, Oct. 2011, pp. 1–18.
[28] "RPMA: Technology for the Internet of Things," Ingenu, San Diego, CA, USA, Tech. Rep., 2016, pp. 1–38. [Online]. Available: http://theinternetofthings.report/Resources/Whitepapers/4cbc5e5e-6ef8-b8cd-f6e3888624cb_RPMA%20Technology.pdf
[29] SigFox. *SigFox*. [Online]. Available: htpp://www.sigfox.com
[30] L. Vangelista, A. Zanella, and M. Zorzi, "Long-range IoT technologies: The dawn of LoRa," in *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*. Cham, Switzerland: Springer, 2015, pp. 51–58.
[31] C. Pereira and A. Aguiar, "Towards efficient mobile M2M communications: Survey and open challenges," *Sensors*, vol. 14, no. 10, pp. 19582–19608, 2014.
[32] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digit. Commun. Netw.*, vol. 1, no. 1, pp. 1–19, 2015.
[33] F. Ghavimi and H.-H. Chen, "M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 525–549, 2nd Quart., 2015.

[34] M. Condoluci, M. Dohler, G. Araniti, A. Molinaro, and K. Zheng, "Toward 5G densenets: Architectural advances for effective machine-type communications over femtocells," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 134–141, Jan. 2015.

[35] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub. (Dec. 2015). "Towards massive machine type cellular communications." [Online]. Available: https://arxiv.org/abs/1512.03452

[36] A. Ali, G. A. Shah, M. O. Farooq, and U. Ghani, "Technologies and challenges in developing machine-to-machine applications: A survey," *J. Netw. Comput. Appl.*, vol. 83, no. 4, pp. 124–139, 2017.

[37] D. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "CASAS: A smart home in a box," *Computer*, vol. 46, no. 7, pp. 62–69, Jul. 2013.

[38] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on smart homes system using Internet-of-Things," in *Proc. IEEE Int. Conf. Comput. Power, Energy Inf. Commun. (ICCPEIC)*, Apr. 2015, pp. 330–335.

[39] M. B. Yassein, W. Mardini, and A. Khalil, "Smart homes automation using Z-wave protocol," in *Proc. IEEE Int. Conf. Eng. MIS (ICEMIS)*, Sep. 2016, pp. 1–6.

[40] C. Talcott, "Cyber-physical systems and events," in *Software-Intensive Systems and New Computing Paradigms*. Berlin, Germany: Springer, 2008, pp. 101–115.

[41] L. Yongfu, S. Dihua, L. Weining, and Z. Xuebo, "A service-oriented architecture for the transportation cyber-physical systems," in *Proc. IEEE 31st Chin. Control Conf. (CCC)*, Jul. 2012, pp. 7674–7678.

[42] J. Markoff, "Google cars drive themselves, in traffic," *New York Times*, vol. 10, no. A1, p. 9, 2010.

[43] O. G. Blog. (2012). *The Self-Driving Car Logs More Miles on New Wheels*. [Online]. Available: http://googleblog.blogspot.com/2012/08/the-self-driving-car-logs-more-miles-on.html

[44] T. Gea, J. Paradells, M. Lamarca, and D. Roldán, "Smart cities as an application of Internet of Things: Experiences and lessons learnt in Barcelona," in *Proc. IEEE 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Jul. 2013, pp. 552–557.

[45] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 112–121, Apr. 2014.

[46] G. P. Hancke, B. de Carvalho e Silva, and G. P. Hancke, "The role of advanced sensing in smart cities," *Sensors*, vol. 13, no. 1, pp. 393–425, 2012.

[47] M. J. Mudumbe and A. M. Abu-Mahfouz, "Smart water meter system for user-centric consumption measurement," in *Proc. IEEE 13th Int. Conf. Ind. Inform. (INDIN)*, Jul. 2015, pp. 993–998.

[48] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[49] V. Ç. Güngör and G. P. Hancke, *Industrial Wireless Sensor Networks: Applications, Protocols, and Standards*. Boca Raton, FL, USA: CRC Press, 2013.

[50] T. Chang, P. Tuset-Peiro, X. Vilajosana, and T. Watteyne, "OpenWSN & OpenMote: Demo'ing a complete ecosystem for the industrial Internet of Things," in *Proc. 13th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2016, pp. 1–3.

[51] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An emerging era in the management of Parkinson's disease: Wearable technologies and the Internet of Things," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 6, pp. 1873–1881, Nov. 2015.

[52] P. A. Laplante and N. Laplante, "The Internet of Things in healthcare: Potential applications and challenges," *IT Prof.*, vol. 18, no. 3, pp. 2–4, 2016.

[53] *Radical-7 Breakthrough Measurements. Radical Monitor, Data Sheet Radical-7*, Masimo Corp., Irvine, CA, USA, 2013.

[54] C. Nay, "Sensors remind doctors to wash up," IBM Res., Armonk, NY, USA, Tech. Rep., 2013.

[55] K. Michaelsen, J. L. Sanders, S. M. Zimmer, and G. M. Bump, "Overcoming patient barriers to discussing physician hand hygiene: Do patients prefer electronic reminders to other methods?" *Infection Control Hospital Epidemiol.*, vol. 34, no. 9, pp. 929–934, 2013.

[56] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[57] 5G Americas. (2015). *Cellular Technologies Enabling the Internet of Things*. [Online]. Available: htpp://www.5gamericas.org/files/6014/4683/4670/4G_Americas_Cellular_Technologies_Enabling_the_IoT_White_Paper_November_2015.pdf

[58] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. Hoboken, NJ, USA: Wiley, 2007.

[59] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient energy management for the Internet of Things in smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 84–91, Jan. 2017.

[60] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017.

[61] "LoRaWAN specification v1.0," LoRa Alliance, Tech. Rep., Jan. 2015.

[62] G. Margelis, R. Piechocki, D. Kaleshi, and P. Thomas, "Low throughput networks for the IoT: Lessons learned from industrial implementations," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 181–186.

[63] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, and M. Pettissalo, "On the coverage of LPWANs: Range evaluation and channel attenuation model for LoRa technology," in *Proc. IEEE 14th Int. Conf. ITS Telecommun. (ITST)*, Dec. 2015, pp. 55–59.

[64] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[65] J. Burns, S. Kirtay, and P. Marks, "Future use of licence exempt radio spectrum," Plum Consulting, London, U.K., Tech. Rep., Jul. 2015.

[66] J.-P. Bardyn, T. Melly, O. Seller, and N. Sornin, "IoT: The era of LPWAN is starting now," in *Proc. IEEE 42nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2016, pp. 25–30.

[67] B. Poller, *Connecting Things to the Internet With SigFox*, May 2013. [Online]. Available: http://www.ekito.fr/people/connecting-things-to-the-internet-with-sigfox/

[68] T. J. Myers *et al.*, "Light monitoring system using a random phase multiple access system," U.S. Patent 8 477 830, Jul. 2, 2013.

[69] R. G. Cid-Fuentes, M. Y. Naderi, R. Doost-Mohammady, K. R. Chowdhury, A. Cabellos-Aparicio, and E. Alarcón, "Leveraging deliberately generated interferences for multi-sensor wireless RF power transmission," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[70] M. Weyn, G. Ergeerts, L. Wante, C. Vercauteren, and P. Hellinckx, "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 12, p. 870430, 2013.

[71] O. Cetinkaya and O. B. Akan, "A DASH7-based power metering system," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 406–411.

[72] *Weightless*. [Online]. Available: http://www.weightless.org/

[73] Wavenis Weightless. *What is Weightless*. [Online]. Available: http://www.elstermetering.com/en/wavenis-technology

[74] IEEE Standard 802.15.1, Bluetooth.

[75] BSIG. *Bluetooth Special Interest Group*. [Online]. Available: https://www.bluetooth.org

[76] 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. 11734–11753, 2012.

[77] 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 *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2012, pp. 232–237.

[78] *Wireless Medium Access Control and Physical Layer Specifications for Low-Rate Wireless Personal Area Networks*, IEEE Standard 802.15.4, IW Group, 2003.

[79] *ZigBee Specifications r13*, ZigBee Alliance, Davis, CA, USA, 2006.

[80] *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, IW Group, 2010.

[81] S. Andreev *et al.*, "Understanding the IoT connectivity landscape: A contemporary M2M radio technology roadmap," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 32–40, Sep. 2015.

[82] U. Raza, P. Kulkarni, and M. Sooriyabandara. (2017). "Low power wide area networks: An overview." [Online]. Available: https://arxiv.org/abs/1606.07360

[83] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11AH: The WiFi approach for M2M communications," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 144–152, Dec. 2014.

[84] A. de Barcelona. *Barcelona Smart City*. Accessed: May 2015. [Online]. Available: http://www.ben.cat/barcelonawifi/en/
[85] S. Dimatteo, P. Hui, B. Han, and V. O. K. Li, "Cellular traffic offloading through WiFi networks," in *Proc. IEEE 8th Int. Conf. Mobile Adhoc Sensor Syst. (MASS)*, Oct. 2011, pp. 192–201.
[86] V. Pereira, T. Sousa, P. Mendes, and E. Monteiro, "Evaluation of mobile communications: From voice calls to ubiquitous multimedia group communications," in *Proc. 2nd Int. Work. Conf. Perform. Modeling Eval. Heterogeneous Netw. (HET-NETs)*, vol. 4. 2004, pp. 4–10.
[87] G. Patel and S. Dennett, "The 3GPP and 3GPP2 movements toward an all-IP mobile network," *IEEE Pers. Commun.*, vol. 7, no. 4, pp. 62–64, Aug. 2000.
[88] *Vision, Framework and Overall Objectives of the Future Development of IMT-2000 and Systems Beyond IMT-2000*, ITU-R, Geneva, Switzerland, 2002.
[89] H. Holma and A. Toskala, *WCDMA for UMTS: Radio Access for Third Generation Mobile Communications*. Hoboken, NJ, USA: Wiley, 2005.
[90] D. Meyer, *A Billion 3G/UMTS Mobile Connections*, UMTS Forum, Zürich, Switzerland, Jan. 2014. [Online]. Available: www.zdnet.com/article/umts-3g-passes-one-billion-connections/
[91] K. Tachikawa, "A perspective on the evolution of mobile communications," *IEEE Commun. Mag.*, vol. 41, no. 10, pp. 66–73, Oct. 2003.
[92] *Study on Provision of Low-Cost Machine-Type Communications (MTC) User Equipments (UEs) Based on LTE*, document TR36.888v12.0.0, 3GPP, 2013. [Online]. Available: htpp://www.3gpp.org/ftp/Specs/archive/36_series/36.888/36888-c00.zip
[93] *Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things*, 3GPP TR 45.820 v13.1.0, 3GPP, 2015. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/45_series/45.820/45820-d10.zip
[94] *Further LTE Physical Layer Enhancements for MTC*, document RP-141660, 3GPP TSG RAN Meeting #65, Ericsson, Nokia, 2014.
[95] P. Stuckmann, *The GSM Evolution: Mobile Packet Data Services*. Hoboken, NJ, USA: Wiley, 2003.
[96] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband*. New York, NY, USA: Academic, 2013.
[97] *Narrowband IoT (NB-IoT)*, document RP-151621, 3GPP TSG RAN Meeting #69, Qualcomm, 2015.
[98] *2G-3G Cellular Wireless Data Transport Terminology Arc Electronics*. [Online]. Available: http://www.arcelect.com/2g-3g_cellular_wireless.htm
[99] 5G Americas, "LTE and 5G technologies enabling the Internet of Things," 5G Amer., Bellevue, WA, USA, White Paper, Dec. 2016. [Online]. Available: htpp://www.5gamericas.org/files/3514/8121/4832/Enabling__IoT_WP_12.8.16_FINAL.pdf
[100] P. Reininger. (2016). 3GPP standards for the Internet-of-Things. Smart Summit, Singapore. [Online]. Available: https://www.slideshare.net/eikoseidel/3gpp-standards-for-the-internetofthings
[101] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "NB-IoT deployment study for low power wide area cellular IoT," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6.
[102] *Feasibility Study on New Service and Market Technology Enablers*, document 3GPP TR 22.891 v14.2.0, 3GPP, 2016. [Online]. Available: htpps://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897
[103] *Feasibility Study on New Services and Markets Technology Enablers for Massive Internet of Things*, document 3GPP TR 22.861 v14.1.0, 3GPP, 2016. [Online]. Available: htpps://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3013
[104] *Feasibility Study on New Services and Markets Technology Enablers for Enhanced Mobile Broadband; Stage 1*, document 3GPP TR 22.863 v14.1.0, 3GPP, 2016. [Online]. Available: htpps://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3015
[105] *Feasibility Study on New Services and Markets Technology Enablers for Critical Communications; Stage 1*, document 3GPP TR 22.862 v14.1.0, 3GPP, 2016. [Online]. Available: htpps://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3014
[106] *Feasibility Study on New Services and Markets Technology Enablers for Network Operation; Stage 1*, document 3GPP TR 22.864 v15.0.0, 3GPP, 2016. [Online]. Available: htpps://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3016
[107] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.
[108] M. Ndiaye, G. P. Hancke, and A. M. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors*, vol. 17, no. 5, p. 1031, 2017.
[109] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Comput. Elect. Eng.*, no. 3, pp. 1–14, 2017.
[110] I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, "A roadmap for traffic engineering in SDN-OpenFlow networks," *Comput. Netw.*, vol. 71, no. 10, pp. 1–30, Oct. 2014.
[111] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 27–51, 1st Quart., 2014.
[112] I. F. Akyildiz, P. Wang, and S.-C. Lin, "SoftAir: A software defined networking architecture for 5G wireless systems," *Comput. Netw.*, vol. 85, no. 7, pp. 1–18, 2015.
[113] F. Granelli *et al.*, "Software defined and virtualized wireless access in future wireless networks: Scenarios and standards," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 26–34, Jun. 2015.
[114] H.-H. Cho, C.-F. Lai, T. K. Shih, and H.-C. Chao, "Integration of SDR and SDN for 5G," *IEEE Access*, vol. 2, pp. 1196–1204, 2014.
[115] A. Hakiri and P. Berthou. (2015). "Leveraging SDN for the 5G networks: Trends, prospects and challenges." [Online]. Available: https://arxiv.org/abs/1506.02876
[116] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun.*, vol. 21, no. 2, pp. 106–112, Apr. 2014.
[117] M. Jacobsson and C. Orfanidis, "Using software-defined networking principles for wireless sensor networks," in *Proc. 11th Swedish Nature Comput. Netw. Workshop (SNCNW)*, Karlstad, Sweden, May 2015, pp. 1–5.
[118] I. F. Akyildiz, S.-C. Lin, and P. Wang, "Wireless software-defined networks (W-SDNs) and network function virtualization (NFV) for 5G cellular systems: An overview and qualitative evaluation," *Comput. Netw.*, vol. 93, no. 12, pp. 66–79, 2015.
[119] Ericsson, "Cloud RAN. The benefits of virtualization, centralization and coordination," Ericsson, Stockholm, Sweden, White Paper Uen 284 23-3271, 2015.
[120] Federal Communications Commission. (Oct. 2010). *Mobile Broadband: The Benefits of Additional Spectrum*. [Online]. Available: www.fcc.gov
[121] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006.
[122] *Unlicensed Operations in the TV Broadcast Bands, Second Memorandum Opinion and Order*, document FCC 10-174, TV Broadcast, Sep. 2010.
[123] C. Sarkar, S. N. A. U. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 508–513.
[124] D. Uckelmann, M.-A. Isenberg, M. Teucke, H. Halfar, and B. Scholz-Reiter, "Autonomous control and the Internet of Things: Increasing robustness, scalability and agility in logistic networks," in *Unique Radio Innovation for the 21st Century*. 2010, pp. 163–181.
[125] M. Welsh and G. Mainland, "Programming sensor networks using abstract regions," in *Proc. NSDI*, 2004, vol. 4. no. 3, pp. 1–15.
[126] Y.-K. Chen, "Challenges and opportunities of Internet of Things," in *Proc. IEEE 17th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan./Feb. 2012, pp. 383–388.
[127] F. Van den Abeele, J. Hoebeke, I. Moerman, and P. Demeester, "Fine-grained management of CoAP interactions with constrained IoT devices," in *Proc. IEEE Netw. Oper. Manage. Symp. (NOMS)*, May 2014, pp. 1–5.
[128] M. Elkhodr, S. Shahrestani, and H. Cheung. (2016). "The Internet of Things: New interoperability, management and security challenges." [Online]. Available: https://arxiv.org/abs/1604.04824
[129] I. Ishaq *et al.*, "IETF standardization in the field of the Internet of Things (IoT): A survey," *J. Sens. Actuator Netw.*, vol. 2, no. 2, pp. 235–287, 2013.

[130] N. Al-Falahy and O. Y. Alani, "Technologies for 5G networks: Challenges and opportunities," *IT Prof.*, vol. 19, no. 1, pp. 12–20, Jan./Feb. 2017.
[131] N. Ntuli and A. Abu-Mahfouz, "A simple security architecture for smart water management system," in *Proc. 11th Int. Symp. Intell. Tech. Adhoc Wireless Sens. Netw.*, Spain, Madrid, 2016, vol. 83. no. 5, pp. 1164–1169.
[132] J. Louw, G. Niezen, T. D. Ramotsoela, and A. M. Abu-Mahfouz, "A key distribution scheme using elliptic curve cryptography in wireless sensor networks," in *Proc. IEEE 14th Int. Conf. Ind. Inform. (INDIN)*, Jul. 2016, pp. 1166–1170.
[133] A. M. Abu-Mahfouz and G. P. Hancke, "Evaluating ALWadHA for providing secure localisation for wireless sensor networks," in *Proc. IEEE AFRICON*, Sep. 2013, pp. 1–5.
[134] *Machine to Machine Communications (M2M); Threat Analysis and Counter-Measures to M2M Service Layer*, ETSI TR103 167 v1.1.1, ETSI, 2011. [Online]. Available: htpp://www.etsi.org/deliver/etsitr/103100_103199/103167/01.01.01._60/tr_103167v01010p.pdf
[135] J. Frahim, C. Pignataro, J. Apcar, and M. Morrow, "Securing the Internet of Things: A proposed framework," Cisco, San Jose, CA, USA, Tech. Rep., 2015, pp. 1–8. [Online]. Available: http://www.cisco.com/c/en/us/about/security-center/secure-IoT-proposed-framework.html#2
[136] H.-L. Fu, P. Lin, H. Yue, G.-M. Huang, and C.-P. Lee, "Group mobility management for large-scale machine-to-machine mobile networking," *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1296–1305, Mar. 2014.
[137] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP)*, document 7252, 2014.
[138] D. Thangavel, X. Ma, A. Valera, H.-X. Tan, and C. K.-Y. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *Proc. IEEE 9th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Apr. 2014, pp. 1–6.
[139] T. Pötsch, K. Kuladinithi, M. Becker, P. Trenkamp, and C. Goerg, "Performance evaluation of CoAP using RPL and LPL in TinyOS," in *Proc. IEEE 5th Int. Conf. New Technol., Mobility Secur. (NTMS)*, May 2012, pp. 1–5.
[140] NGMN Alliance, "Next generation mobile networks (NGMN) 5G white paper," Feb. 2015.

GODFREY ANUGA AKPAKWU received the B.Eng. degree (Hons.) from the University of Pretoria, Pretoria, South Africa, in 2016, the B.Eng. degree (Hons) in electrical and electronic engineering from the Federal University of Agriculture at Makurdi, Nigeria, in 2008, and the M.Sc. degree in electronic communications and computer engineering from the University of Nottingham, Malaysia, in 2011. He is a Graduate Research Candidate with the Department of Electrical, Electronic and Computer Engineering, University of Pretoria. His research interests include Internet of Things, fifth-generation mobile networks, wireless sensor networks, network management, and network security. He received the Bursary for the Department of Research and International Support, University of Pretoria, and Council for Scientific and Industrial Research, South Africa.

BRUNO J. SILVA (S'14) received the B.Eng., B.Eng., (Hons.) and M.Eng. degrees in computer engineering from the University of Pretoria, Pretoria, South Africa, in 2011, 2012, and 2015, respectively. From 2013 to 2014, he was a Visiting Researcher with the ABB Corporate Research Centre, Västerås, Sweden, where he was involved in research on ultrawideband-based localization. He is currently a Junior Research Officer with the University of Pretoria, where he is involved in research on industrial wireless sensor networks and localization for underground mines. His research interests include wireless sensor networks, indoor localization, and mobile computing.

GERHARD P. HANCKE received the B.Eng. and M.Eng. degrees in computer engineering from the University of Pretoria, South Africa, in 2002 and 2003, respectively, and the Ph.D. degree in computer science for the security group from the Computer Laboratory, University of Cambridge, in 2008. He is currently an Assistant Professor with the Department of Computer Science, City University of Hong Kong. He was with the Smart Card Centre and Information Security Group, Royal Holloway, University of London. His main interests are sensing applications and security of embedded systems.

ADNAN M. ABU-MAHFOUZ received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria. He is currently a Principal Research Engineer with the Council for Scientific and Industrial Research. He is also an Adjunct Research and Innovation Associate with the Faculty of Engineering and Built Environment, Department of Electrical Engineering/French South African Institute of Technology, Tshwane University of Technology. His research interests are wireless sensor networks, software-defined wireless sensor networks, network management, network security, localisation systems and low-power wide area networks. He is the Chair of Tshwane Water Resource Management Network.