Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues

Machine-to-Machine Wireless Communication Technologies for the Internet of Things: Taxonomy, Comparison and Open Issues

Federico Montori, Luca Bedogni, Marco Di Felice, Luciano Bononi

Department of Computer Science and Engineering (DISI)
University of Bologna, Italy
Email: {federico.montori2, luca.bedogni4, marco.difelice3, luciano.bononi}@unibo.it

Abstract

Machine-to-Machine (M2M) communication technologies enable autonomous networking among devices without human intervention. Such autonomous control is of paramount importance for several deployments of the Internet of Things (IoT), including smart manufacturing applications, healthcare systems and home automation just to name a few. As a result, several M2M technologies are nowadays available on the market as either proprietary solutions or the effort of standardization initiatives, each targeted for a specific class of IoT applications and characterized by unique features in terms of achievable performance, frequency in use and supported network topologies. In this paper, we aim to organize the existing M2M approaches and technologies into a consistent framework that provides an in-depth vision of the main trends, future directions and open issues. We provide three main contributions in this survey. First, we identify the main use cases and requirements of M2M scenarios and we introduce a multi-layer taxonomy for M2M solutions, taking into account both deployment types and PHY/MAC characteristics. Second, in light of such characteristics, we provide an in-depth review of the existing M2M wireless technologies, considering both proprietary and open/standardized solutions for proximity-based, short-range and large-scale networks. Finally, we perform a critical comparison of the surveyed solutions over different M2M use cases and requirements, and we identify the research directions and open issues that still have to be addressed.

Keywords: Machine-to-Machine (M2M) communication, Internet of Things (IoT), wireless technologies, Medium Access Control (MAC) protocols

Table 1: Summary of the acronyms used throughout the paper.

3GPP	3rd Generation Partnership Project
ASK	Amplitude Shift Keying
BFSK	Binary Frequency Shift Keying
BPSK	Binary Phase Shift Keying
CDMA	Code Division Multiple Access
CIoT	Cellular IoT
CSMA/CA	Carrier Sense Multiple Access for Collision Avoidance
CSS	Chirp Spread Spectrum
DBPSK	Differential Binary Phase Shift Keying
DLL	ISO/OSI Data Link layer
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IoT	Internet of Things
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Medium Access Control sublayer
MTC	Machine Type Communication
OFDM	Orthogonal Frequency Division Multiplexing
OQPSK	Offset Quadrature Phase Shift Keying
PHY	ISO/OSI Physical layer
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RPMA	Random Phase Multiple Access
S-CSMA/CA	Slotted CSMA/CA
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UMTS	Universal Mobile Telecommunications System
UNB	Ultra Narrow Band

1. Introduction

Hardware miniaturization, device pervasiveness and ubiquitous connectivity are three of the main technological enablers of the novel paradigm of the Internet of Things (IoT). The disruptive impact of such paradigm on both ICT and

non-ICT contexts is proved by the following estimations: 3.5 connected devices per capita by 2021 [1] and 3.5 billion IoT connections using cellular connectivity by 2023 [2], a total volume of data exceeding the 600 ZB per year by 2020, a global spending on IT of more than 3.7 trillion in 2018 and projected to grow by 2.7% in 2019 [3]. Although no global consensus exists on the IoT definition, and hence several different deployments have been proposed so far, the rationale of the IoT paradigm is straightforward: make the physical objects able to access the digital ecosystem by generating, processing and exchanging data with other objects and with humans. Moreover, since objects are everywhere, the applications of IoT are almost unlimited and involve all the human activities, from industrial production (i.e. smart manufacturing and the Industry 4.0) and agriculture to healthcare and daily life within cities and private buildings (i.e. smart city and smart home applications) [4].

The IoT paradigm cannot be considered a novel technology, rather a combination of approaches taking advantage from the research advances in the fields of semiconductors, networking and information processing. If we consider a data-centric perspective, the IoT is made of devices – being both novel devices as well as physical objects augmented with sensing and processing capabilities – which are able to generate context-aware data and to convey it to other devices and to the cloud, where it is stored and mined in order to extract hidden knowledge [5]. Such knowledge can then enable novel services and applications. The Machine-to-Machine (M2M) communication technologies play the crucial role to enable wireless data exchange among the IoT devices and the gateway, and then from the gateway to a remote repository via the Internet. Clearly, the energy efficiency of the wireless communication is of paramount importance given the battery-constrained nature of the IoT devices: duty cycling algorithms as well as energy harvesting solutions are being deeply investigated [6, 7]. At the same time, heterogeneous IoT deployments might prioritize different qualitative or quantitative metrics that are required by the applications on top. For instance, healthcare scenarios might prioritize qualitative metrics such as reliability, low

latency and security [8], whereas industrial scenarios, concerning automation and process control, might also consider the operational costs, the data-rate and real-time behaviors as main requirements [9]. Consequently, a great number of M2M communication technologies are nowadays available on the market, with orthogonal features in terms of system performance, frequencies, Medium Access Control (MAC) scheme, and standardization process (open vs proprietary solutions).

The aim of this paper is to review the state-of-the-art of the M2M wireless technologies for the IoT by classifying the existing solutions according to a multi-layer taxonomy that allows clarifying the technical features of each approach. Open issues and future research directions are discussed as well. Despite the overwhelming number of survey papers on IoT, our work can be considered a missing piece of the puzzle, since:

- it focuses on the existing wireless technologies and on the PHY/MAC layers, hence it differs from generic surveys like [5], [10] or [11], which describe the IoT protocols at each layer of the network stack;
- at the same time, it is not restricted to any specific stack or infrastructure like [12], [13] or [14], rather it provides an in-depth review of the existing solutions, considering both open standards and proprietary solutions, short-range, long-range and cellular-based solutions.

Three main contributions are provided. First, we introduce a novel multi-layer taxonomy, which allows classifying the existing M2M wireless technologies according to the deployment characteristics (i.e. network size and topology), and the application requirements (i.e. data-rate, frequency bands, power consumption, reliability and MAC layer access method). Second, based on the classification criteria defined above, we review the existing technologies, distinguishing between short-range and long-range solutions. Finally, we discuss the mapping between the enabling M2M communication technologies and the IoT use cases, and we identify the research challenges that are still not completely addressed

by the existing solutions. We think that our work can be useful for researchers willing to acquire knowledge on M2M for IoT through a comprehensive tutorial, as well as for practitioners who need to understand strengths and weaknesses of the available alternatives.

The rest of the paper is structured as follows. Existing surveys on M2M for IoT are described on Section 2, and the novelties of our approach are also highlighted. The classification criteria used within the taxonomy are introduced in Section 3. The wireless technologies are described in detail in Sections 4 and 5. A critical discussion on the mapping between technologies and application requirements is reported in Section 6. A review of the research challenges can be found in Section 7, while Section 8 concludes the paper.

2. Related works

The term IoT was first coined by Kevin Ashton – executive director of the Auto-ID Center – in 1999 [15]. From there, a huge number of IoT applications and enabling technologies have been proposed and an entire scientific literature has risen on the topic. Just to give an idea, according to [16], the number of IoT-related articles published between 2008 and 2013 has exceeded the 10000 units. At the same time, several surveys on IoT and M2M have been proposed so far, with the goal of analyzing, classifying and comparing the existing research studies. Since the IoT bundles different technologies, from wireless communication to cloud computing and data analytics, the existing surveys usually follow one of these two approaches, i.e. they either provide a *broad* vision of the IoT paradigm, or investigate a specific research issue in *depth*. We cite works like [5], [9], [10], [17], [18], [19], [20], [21], [22] and [23] as main representatives of the first category (i.e. general surveys). In [5], the authors propose a five-layer architecture for IoT applications, and give a general overview of the main IoT enabling technologies, protocols and applications. A broad illustration of the IoT and M2M standards focusing on the activities of the main standardization bodies (ITU, ETSI) is provided in [10]. The survey in [17] presents the state-

of-the-art of IoT smart systems, considering seven application domains (cities, homes, grid, building, transportation, health, industry). A similar approach is also followed in [9], where the authors review the main IoT applications in industries and identify main challenges and future trends. A brief discussion of IoT visions and challenges can be found both in [18] and in [19], which, however, do not delve into the different existing technologies. In [20], the authors describe the state-of-the-art and the research challenges for LPWAN technologies and, in [21], such technologies are compared against their actual deployments in the real world. In [22], the authors discuss the current trends in the IoT with a focus on technologies and paradigms at different layers (perception, network and application) with specific stress on Fog and Edge Computing. The survey in [23] is the most similar to our work, although addressing a slightly different theme, since it mainly focuses on cellular technologies and discusses in detail the state-of-the-art with respect to the 5G requirements; compared to it, our work provides a more general categorization of the M2M scenario (e.g. by considering also short range and capillary technologies), and includes actual data on how recent technologies are being deployed in different countries and regions of the world. About the second category (i.e. issue-specific surveys), large attention is devoted to sensor data management and knowledge extraction [24] [25] [26] [27] [28] [29] [30]. In [24] the authors review the main data mining algorithms for classification, clustering and association problems and identify the potentials and unique issues of data analytics techniques for IoT scenarios. When large IoT datasets are available, context information can be inferred from sensor data and possibly returned to users through mobile devices. In [25] the authors review the fundamentals of context awareness (acquisition, modeling and reasoning) and list more than twenty middleware frameworks enabling data fusion and service provisioning. Industrial context-aware technologies and applications, ranging from localization to manufacturing and health-care, are extensively analyzed and classified in [26]. The integration between IoT, context-aware computing techniques and mobile devices is surveyed in [27], focusing on crowdsensing techniques. Similarly, economic and pricing aspects of IoT are discussed in [28], analyzing the

existing strategies aimed to maximize revenues and provide users' incentives for data sharing. The role of mobility is also discussed in [29], where M2M technologies are reviewed with a specific eye on how mobile devices (e.g. smartphones) could be used as relays in constrained resource networks. Performances of M2M-based architectures are discussed in [30], where a new architecture, based on the ETSI M2M standards, is proposed with the goal of enhancing traffic latency. As further examples of issue-specific IoT surveys, we cite the study in [31], which reviews the main IoT middlewares focusing on the aspects of service discovery and composition, and the work in [32], which investigates security for IoT systems. In the latter, the main protocols for securing wireless communications at the MAC, routing and application layers are briefly presented and the open research challenges at each layer are identified.

The present paper focuses on existing M2M communication technologies for the deployment of small-scale and large-scale IoT systems. The most similar survey papers on M2M networking are [11], [12], [13], [14] and [33]. The work in [12] reviews the state-of-art of IoT protocols standardized by the IETF, considering PHY/MAC layer solutions (IEEE 802.15.4), routing (RPL) and application (CoAP). Beside these solutions, Zigbee and Z-Wave technologies are described in [11]. MAC Layer protocols for M2M communication are evaluated and compared in [33], classifying them into three different groups, i.e. contention-based protocols, contention-free protocols and hybrid protocols. Traffic issues of M2M communication, in terms of control and data channel overloads for LTE networks, are discussed in [13]. A comprehensive evaluation of the random access mechanism of LTE for M2M communication is conducted in [14]. Compared to these studies, our paper provides the following key differences and novelties:

- Differently from [10], [11], [12], [22] and [23], it focuses on wireless communications at the PHY layer, considering the open standards as well as the proprietary solutions and the emerging approaches which are still under investigation (e.g. dynamic spectrum access based solutions), instead of taking into account the full protocol stack.

- Differently from other surveys on M2M networking like [13], [14], [33], [20] and [21], it presents technologies for capillary communications as well as for medium and long range communications (based on cellular bands), covering in this way all the solutions currently available on the market, rather than focusing only on one class.

- Besides listing the available technologies, it identifies the unique challenges and requirements of M2M communication on several different deployments and discusses the strengths and the weaknesses of each solution in light of such requirements.

3. M2M Technologies' Requirements and Taxonomy

The purposes for which IoT architectures are designed are conceptually different from the ones that traditional network systems and platforms have always been intended to cope with. From the lowest to the highest layer of the ISO/OSI stack, IoT solutions are committed to satisfy a set of requirements that assure efficiency and suitability. In particular, here we aim to analyze those involving M2M communication technologies (Section 3.1) as well as the axes upon which we intend to pursue our categorization (Section 3.2). Finally, we outline the common use cases for IoT scenarios with a particular focus on the weight, for each use case, attributed to the different requirements (Section 3.3).

3.1. M2M Requirements

In this subsection we report a list of features for M2M technologies universally considered to be strong requirements, to which all the technologies presented in this paper adhere in different measures.

3.1.1. Low power consumption

Low power consumption is clearly one of the key features that devices must satisfy, since, in several cases, networked sensors and actuators need to be powered by means of batteries, due to their extremely distributed physical topology,

as the availability of power sources is usually limited or absent and, especially in wide area deployments, the replacement of batteries is time consuming and implies substantial costs in the long run. Network activity is the main source of energy depletion, since connectivity has been shown to be more energy-consuming than computation by two to three orders of magnitude [34]. Hence, whenever a scenario hosts a number of devices with limited or no access to constant power sources, energy-saving optimizations take place both at the PHY and the MAC layer. More in detail, collisions and the exchange of configuration messages have a deep impact on battery depletion, thus MAC strategies focus on the effective throughput of transmission, which should be as close as possible to the physical throughput. Contention-based mechanisms are highly affected by collisions, which can happen frequently in crowded scenarios; on the other hand, contention-free ones should focus on reducing as much as possible control overheads and beaconing [33]. Furthermore, solutions like duty cycling, a technique that allows the device to turn on and off its radio interface, and energy harvesting can be adopted in order to maximize the battery duration [6] [7]. In particular, duty cycling algorithms may be based on the time coordination between the nodes of a network or dynamically upon a configuration received by the master node or on several other policies [7]. Such algorithms always imply a "deep sleep" time window, in which the radio interface is turned off and the power consumption is close to null. The frequency of the wakeup periods depends on the use case, however, the technology is responsible for part of the preprocessing duration. There are several other methods that can be adopted in order to increase the energy efficiency of M2M communication. According to [35], they can be divided in five main categories, i.e.: radio optimization, data reduction, sleep schemes, energy-oriented routing and battery repletion. We redirect the readers to [35] for further details on the topic.

3.1.2. Low Cost

Due to the high number of devices in an IoT ecosystem, end devices necessarily need to satisfy a low cost per unit, minimizing the amount of hardware and, as a consequence, making the device extremely specialized on its task. Hence, when possible, a per-device single chip solution without including expensive circuitry is imperative [36]. Furthermore, low cost and low power solutions are highly linked; in fact, manual battery replacement is a costly process, especially when repeated for a huge number of units. The cost factor highly impacts the choices made at the MAC layer, especially in the channel access techniques. For instance, in contention-free environments, TDMA is the most viable option, since CDMA-based approaches are not suitable for low power and low cost deployments, primarily due to their complexity. Furthermore, pure FDMA approaches are not used in M2M application due to the high cost of the high-performing frequency filters in the radio hardware of each unit. An exception is given by OFDMA-based systems, due to their easy and low cost implementation of the FFT in chips as well as the lack of necessity for filters for each sub-channel. With such approach, the simultaneous access for a large number of devices can be supported [37].

3.1.3. Scalability

With the advent of massive IoT deployment for new use cases, scalability is a necessary feature. Typically, a high number of nodes brings issues regarding collisions, load balancing, deployment cost and data fusion; for such reasons, a high scalability always implies reconfiguration to be efficient as well as support for a high number of devices per gateway. Scalability also impacts the channel access method, since in dynamic scenarios – i.e. with a non-static number of participants and with dynamically entering and leaving nodes – contention-based methods face an increase of collisions, whereas contention-free ones need to deal with a time-consuming reconfiguration [38].

3.1.4. Reliability

Reliability is a strict requirement for many use cases. There are several ways of estimating reliability in networks, which, in general, include the probability that a certain node in the network will get the message upon the failure of a certain set of links [39] [40]. Now, as lack of reliability depends primarily on link failures and lack of controlling mechanisms that would put a burden onto the data packets, network topology (see also Section 3.2.2) and management have a central role in addressing it. The failure of a communication link is a damage to the system reliability that can be alleviated by the usage of mesh redundant topologies. Networks organized in plain stars, a common topology used in long range deployments, support reduced reliability, in fact a single link failure results in a single node exclusion. In some use cases this is tolerable, however, in many situations, node or gateway redundancy has to be supported, which results in a cost growth. Lastly, tree networks are, reliability-wise, the worst topologies as any link failure results in the exclusion of the whole subtree.

3.1.5. Low Latency

Low latency is often a highly desirable feature and it is unavoidably bound to other aspects that can influence it. There are physical deployment dependencies such as the link strength between the endpoints and the number of hops in an average communication path as well as the number of nodes in the network. PHY layer mechanisms such as spread spectrum techniques, modulation and coding schemes, frequency and spatial diversity also greatly affect latency [41]. The choice of the MAC layer channel access method (i.e. contention-free vs. contention-based) in relation with the network topology is also crucial, as it can introduce unexpected delays [33]. In general, contention-based protocols used in MTC communications suffer from idle listening and dramatically high delays for large networks. This is the case of CSMA/CA, which is widely used in some technologies due to its possibility to scale efficiently with no need for reconfiguration in small networks. Contention-free protocols are more suitable for large

networks, since they offer algorithms capable of exploiting well the available resources without waste, although they do not scale efficiently due to the need for global reconfiguration anytime a node joins or leaves the network. This is the case of TDMA networks, which are largely used in different adaptations in IoT.

3.1.6. Enhanced Communication Range

A wider range of radio communication means a wider area deployment, which is the current trend in future generation IoT deployments targeting the market of monitoring and public welfare. For many use cases, such feature is a must-have, being aware that the nominal range is often not enough in order to calculate how wide a deployment can be. Indoor scenarios, obstacles and the spatial coexistence with other technologies often put the range in correlation with the spectrum frequency bands and modulation encoding schemes. The 2.4 GHz frequency bands, besides being designed for relatively consistent data transfer, has a list of non-negligible drawbacks for IoT long range scenarios. Due to its nature, it supports more easily a high data rate, however it suffers more from obstacles, indoor deployments and it requires more power in order to be pushed to long distances. Furthermore, the recent overcrowding of such frequency bands does not help in scenarios with high network population. For such reasons, technologies deployed in sub-GHz bands are gaining more and more interest in IoT [42]. Almost all the long-range technologies exploit either unlicensed bands like the 868 MHz, or the licensed bands around 800 MHz, in coexistence with other cellular technologies such as LTE, UMTS and GSM. Furthermore, enhanced range is typically chosen in contrast with the power consumption at the price of a reduced data rate. Many future generation applications require very low consumption and not much data rate, for which arising narrowband long-range solutions designed for wide area deployments appear to be convenient [36].

3.1.7. Security

Security is also a challenging issue due to the nature of M2M deployments, which makes them vulnerable to attacks such as denial of service (DoS) and might compromise confidentiality, authentication, integrity, authorization, and availability. In fact, many aspects of M2M solutions unfortunately open up new vectors for DoS, e.g. packet fragmentation (which may involve long cryptoblocks). For this reason M2M devices and gateways must be able to detect unusual events and implement different solutions for end-to-end security, especially in IP-based interactions [43]. An example on how dangerous a lack of security can be in a crowd on small devices is given by the Mirai botnet, which in September 2016 used more than 400,000 devices to perform DDoS attacks generating more than enough traffic to knock several services offline [44] Although it is important to mention security, it is being discussed in the present paper mostly as an open issue. Furthermore, many other works address specifically the problem [32] [43].

3.2. Technology Classification

M2M technologies for the IoT are various and diverse, their characteristics make them compliant for different purposes; a macro set of features characterizing the plethora of possibilities can be found in [45], in which the existing solutions are distinguished by means of:

- Deployment, which can be incremental or one-time.
- Homogeneity and heterogeneity, meaning that many things in the same ecosystem might be devoted to – and built upon – separate tasks (this is typically the case of industrial deployments) or, on the other hand, considered as general-purpose units.
- Mobility, which might be total, sporadic or absent.
- Minimum lifetime of each node, which might span from hours to years.

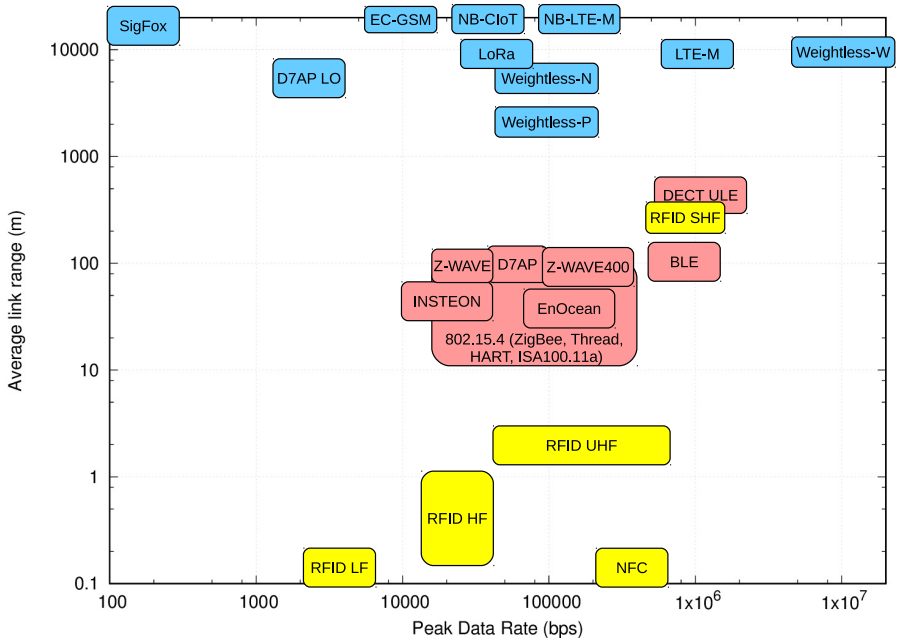

Figure 1: Diagram showing at a glance all the technologies included in the present review work. We consider Spatial Range as the main discriminant, in relation with data rate, that can determine what a defined technology is developed for. Capillary technologies are identified in red boxes and LPWAN technologies in blue. We also include the representation of RFID-based proximity technologies in yellow boxes for the purpose of comparison.

In our case, we consider of paramount importance the differences brought by the range and the data rate of each communication technology, as well as the topology adopted in their deployment. Since such characteristics determine the suitability of the technologies for specific purposes and the network size, we chose to classify each technology using these discriminants. As they are orthogonal, we believe that their combination gives an efficient way to categorize each technology.

3.2.1. Range and Data Rate

M2M communication technologies are used in network types that span, depending on their communication range, from Wireless Body Area Network

(WBAN) to Wireless Personal Area Network (WPAN), to Wireless Local Area Network (WLAN) to even Wireless Wide Area Network (WWAN). According to this, we separate IoT communication technologies in Proximity, Short Range and Long Range. Proximity technologies, such as RFID and NFC, have typically a range of very few meters and are used for identification purposes or small data transfers. Although they are the main pillars on which IoT rose, we do not extensively deal with them in this paper as we do not consider them as strictly M2M technologies; however, for the sake of completeness we report them as a term of comparison. Short Range technologies, often referred to as "Capillary" and outlined in Section 4, have a communication range of some meters up to a maximum of a hundred and are typically suitable for WBANs, WPANs and WLANs. For such reason, their deployment is typically restricted to a certain limited area (e.g. a room, a small building, a house). Finally, Long Range technologies, considered the rising star in the future IoT, are suitable for big WLANs and WWANs, covering areas of few kilometers. This means that a single network is able to serve a big building, a factory or even a rural area, depending on the amount of direct LoS links. Such technologies, outlined in Section 5, can be further divided in proprietary Low-Power Wide-Area Network (LPWAN) and Cellular-IoT technologies (CIoT), depending on the frequency bands, unlicensed for proprietary LPWAN and licensed for CIoT. Figure 1 gathers nearly all the technologies addressed in this paper, using spatial range as discriminant and putting it in orthogonal relation with data rate. The separation between proximity, capillary and long-range solutions is evident as well as their clustering around certain areas of interest.

3.2.2. Topology

Network topology is also a determining feature in relation with the purpose of a certain deployment. A small recall to the existing network topologies is shown in Figure 2. The star topology is the most common network type, in which a central node acts as the sink, while the peripheral nodes are connected

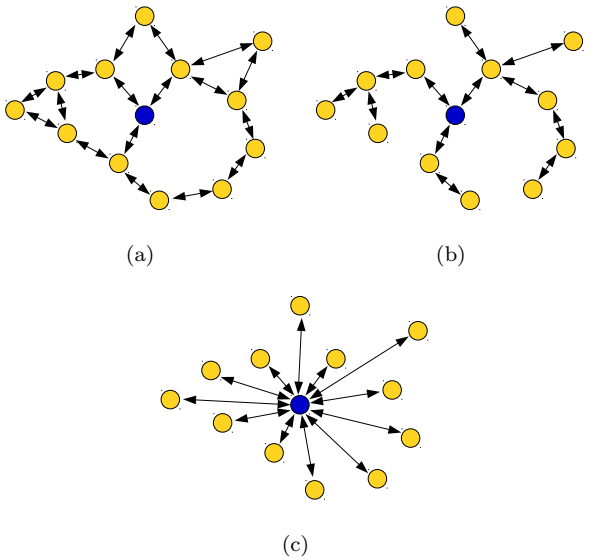

Figure 2: Schemes showing the differences among topologies. (a) Mesh topology, (b) Hierarchical tree topology, (c) Star topology.

to it via a direct link without being connected to each other. In general, the sink is the gateway to the outer world or it is connected directly to such gateway. The latter happens when, for instance, different stars are coexisting and somehow related, in such case we consider it a star-of-stars. The mesh topology is the dual of the star network, where nodes are connected to each other in a multi-hop fashion with only few of them connected to the sink. Nevertheless, not in all cases such nodes are different from the others in terms of capabilities and features. In the hierarchical tree topology connections are designed as in a tree, in which the root is the sink and peripheral nodes are connected in layers via direct links. Choosing one of such deployments determines a different priority given to a number of aspects and features for which the topology is responsible [46]: reliability, scalability, energy efficiency and latency are among them. On top of such considerations, it is worth noting that, in some cases, one choice or another is driven by the constraints of the physical environment. Especially in smart cities, sometimes nodes have to be physically distributed in a way the

makes the choice univocal. For instance, a smart system based on IEEE 802.15.4 controlling and monitoring streetlights deployed in a grid topology over a wide parking lot is inconceivable as a star network [47].

3.3. Use Cases

Table 2: IoT common use cases and requirements, for each of which the average estimated importance (from low to high) is stated.

Use Case	Scalability	Data rate	Reliability	Low Latency	Low Consumption	Cost	Security	Compatibility
Home Automation [48]	Low	Medium	Medium	High	Medium	Medium	Medium	High
Industry [49]	Medium	Medium	High	High	Medium	High	High	Medium
Environmental Monitoring [50]	High	Low	Low	Low	High	High	Medium	Low
Smart City & Building [51]	High	Medium	High	Medium	High	High	High	High
Healthcare [8]	*Variable*	*Variable*	High	High	Low	Low	High	Low
Smart Grid [52]	High	High	High	High	Low	High	High	High

Use cases determine what is required and what is optional when choosing a specific communication technology for a deployment. In particular, proximity and capillary technologies are normally designed for tasks that may differ from the ones for which LPWAN technologies are designed for [53]. Such differences can involve the deployment size, the required latency, the required reliability, the amount of data to be shared, the availability of power sources, the monetary resources, the security requirements, the compatibility, the business models and, clearly, the purpose [54]. In addition, the final customer using an IoT technology can sort differently the requirements in importance due to his or her nature which unavoidably drives and gives shape to the use case itself.

3.3.1. Home Automation

A common citizen, who deals with problems related to home automation and everyday life monitoring purposes, rarely would care about a scalable network or a wide deployment. Conversely, features such as compatibility with preexisting infrastructures and cost would be much more preferred. Low latency is also something appealing in home automation scenarios, since the interaction between sensors and actuators is commonly required "here and now" [48].

3.3.2. Industry

Industrial scenarios, concerning automation and process control, are a completely different reality as they prioritize cost, low latency and reliability over all the other possible metrics [49], giving in some cases secondary importance to scalability and compatibility depending on the factory/installment physical size and location. Required data rate may vary significantly from case to case, while the security is also a central issue, since a malign agent can have devastating consequences [55].

3.3.3. Healthcare

Healthcare scenarios highly prioritize the qualitative metrics such as reliability, the low latency and the security [8], while most of the others, such as the cost and the power consumption are (or should be) of secondary importance. The scalability strongly depends on the installment size which may span from very small (a specialized hospital ward) to very wide (remote patient monitoring). Data rate is also highly variable, since it might be high, like in real-time health status and predictive information, or low, like in periodic monitoring.

3.3.4. Environmental Monitoring

Other use cases involve the environmental monitoring, which normally implies huge deployment zones and prioritize scalability. The end nodes are only committed to report periodically data and usually the network involves no actuator, thus, with few exceptions, the use case normally tolerates delays as well as data unreliability, simply by adding more sensing instances. For such reasons the end devices must be extremely cost-effective and, due to the deployment size which implies a significant maintenance cost, they must observe a high energy efficiency [50].

3.3.5. Smart Cities and Smart Buildings

Smart city and smart building scenarios are rather complex deployments, in which all the mentioned metrics are quite important. Such big infrastructures are promoting both monitoring and interaction and information must cover long

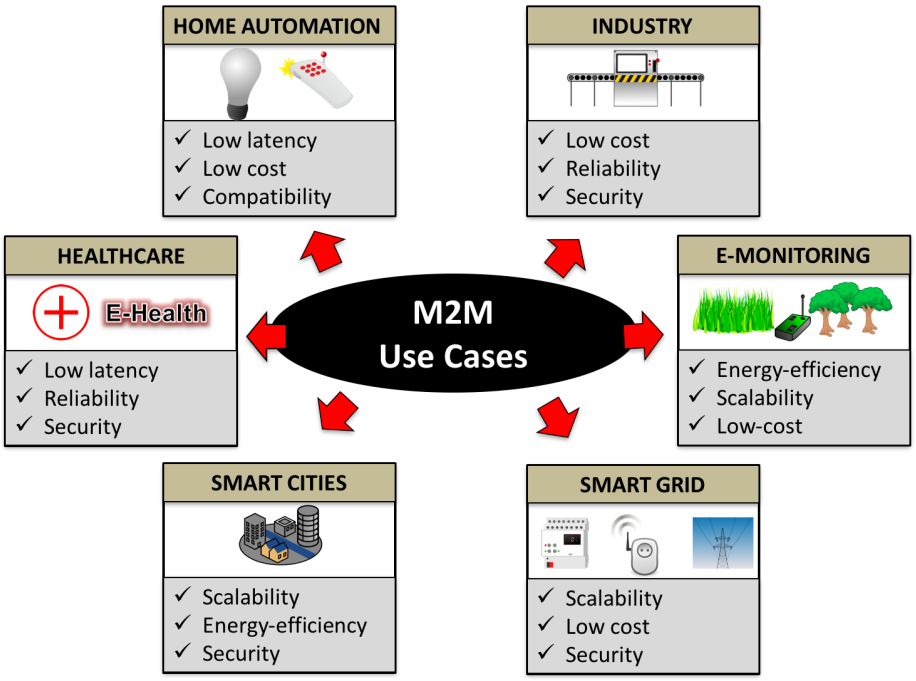

Figure 3: The M2M use-cases and main requirements.

distances. Since actuators are part of the network, data integrity and reliability is also necessary. Cost is another key issue, which can be partially covered whenever the new deployment can coexist and cooperate with legacy systems [51]. One of the most complete examples of Smart City including also features of environmental monitoring is the SmartSantander EU project [56].

3.3.6. Smart Grid

Finally, the Smart Grid is another scenario for which IoT technologies and standards are of paramount importance and, since the continuous energy supply is the main concern of customers, reliability, cost effectiveness and security are the key concept for such systems [52].

The aforementioned use cases and their orientation are summarized briefly in Table 2, and illustrated in Figure 3.

4. Short Range Communication Technologies (Capillary)

Since the beginning of its definition, the concept of IoT has been mainly associated with proximity communication technologies. It started with Radio Frequency Identification (RFID), which was the pioneer technology related to IoT and the first reality that connected things in the real world with their representation though information. RFID is still a widely used standard, its importance in identification-driven deployments is paramount and it has been standardized in a significant number of ways that span from low frequency to high frequency, ultra high frequency (UHF) and super high frequency (SHF), depending on the purpose of use as well as the communication range required [57]. Nevertheless, we do not aim to discuss in depth RFID, since we do not consider it strictly a M2M standard; the same applies for RFID-based standards such as Near-Field Communication (NFC). In this section, indeed, we focus on M2M technologies enabling a communication range spanning from few to above a hundred meters. In most cases, technologies in this category are used to design Wireless Sensor Networks (WSNs), consisting of a set of devices with different tasks, committed to sense or act in the real world, connected through peer-to-peer links and sticking to a set of constraint [58]. Such constraints regard low data rate, low energy consumption and an efficient coordination in order to fulfill their task without hindering others. Most of the times, the more energy constrained and the less powerful (in terms of computing capabilities) a node is, the less responsibilities are assigned to it. Such nodes are commonly given a configuration by the coordinators and are only required to dumbly follow a sequence of tasks, typically sense-transmit-sleep or sleep-receive-act [59]. These networks are suitable for deployment in spatially limited environments, usually within a range of around a hundred meters (it can be more for multi-hop networks), where the interactions between the entities are contextually not separable and require simple and secure communication links [60]. This is the case of home automation scenarios, industrial process control, object identification, body activity monitoring, indoor localization and many others. Most of the

communication technologies used in such contexts are exhaustively reviewed in this section.

4.1. IEEE 802.15.1 Bluetooth Low Energy

The Bluetooth (BT) standard has been introduced as a PHY and DLL specification with the goal of connecting devices in small WPANs, in order to exchange information at high data rates. BT devices are connected in an ad-hoc master-slave star network, called "piconet", capable of hosting up to 8 devices. The union of two piconets, possible thanks to the clock synchronization, is called "scatternet". At the moment, 3 classes of BT are used, which are operating at different communication ranges with respect to the power used [61]. The advantages of the BT are the data rate (up to 3 Mbps) and the low cost of the transceiver; although, as a drawback, such a high data rate involves a high dissipated power. For this reason, pure BT is not appropriate for M2M applications and, moreover, the size of the piconet makes it unsuitable for large networks.

Bluetooth Low Energy (BLE), the core enhancement brought by the BT 4.0 specification and originally known as Wibree [62], is the IoT-oriented version of BT, since it preserves its communication range by reducing the data rate down to 1 Mbps and, consequently, the power dissipated down by 20 to 100 times.

It is highly suitable for small networks based on short distance dedicated communication, such as UriBeacon applications, which allow to periodically check for devices around the owner, useful for context-aware and location-based applications. It operates in the 2.4 GHz frequency bands specifying 40 channels with 2 MHz channel spacing and uses the GFSK modulation scheme [63], as well as a 128 bit AES encryption. Three channels are defined as advertising channels and are used anytime an end device needs to broadcast data, following the typical BT master-slave star topology. However, the Logical Link Control and Adaptation Protocol (L2CAP), which provides multiplexing between the higher layer protocols and deals with the segmentation of large data packets, is significantly simplified in BLE: it is a best-effort version and it does neither support retransmission nor frame segmentation, since each frame is assumed to

fit into the maximum frame size. Another crucial difference is the constraint for piconets to 1-hop communications, since scatternets are not currently implemented in BLE. At the MAC layer, BLE uses (as classic BT does) TDMA with adaptive frequency hopping in order to face interference and wireless propagation issues.

BT technology is nowadays still in continuous development: version 5 has been released in 2016 [64] and it is granted support for mesh networks and significantly increased range and speed. In particular, it can dynamically double the data rate at the price of a decreased range or, specularly, quadruple the range decreasing the data rate.

4.2. The IEEE 802.15.4-based technologies

The 802.15.4 is an IEEE standard [65] specifying the PHY and DLL layers for short range and low bit rate communication. With a range of 10 to 75 meters it falls into the category of WPAN technologies. It has been developed within the IEEE 802.15 Working Group for constrained devices with low computational capabilities and low consumption and it suites applications requiring a multihop network

IEEE 802.15.4 supports all the network topologies mentioned in Section 3.2.2, defining two classes of devices: Full Function Devices (FFD), which can communicate with any other node – one of them is required to be the PAN coordinator –, and Reduced Function Devices (RFD), which only communicate with a FFD. The technology has a maximum data rate of 250 kbps and keeps the power dissipated typically below 1 mW, using the DSSS technique and CSMA/CA to access the physical medium. The maximum packet size is 127 bytes, this means that the remaining space for an upper layer header and for a payload is between 86 and 116 bytes, which constitutes a challenge for some applications. Furthermore, the IEEE 802.15.4 standard implements 16 channels in the 2.4 GHz band, modulated with O-QPSK, with channels numbered from 11 to 26 and a 5 MHz gap between two adjacent channels. Given such setup, it can suffer from possible congestions caused by other networks, for this reason,

802.15.4 might perform poorly in terms of QoS in networks with heterogeneous traffic taking place at the same time [66]. In order to contrast these difficulties, Time Slotted Channel Hopping (TSCH) has been proposed for scenarios having possible data bursts. In the 868 MHz band the protocol has a maximum data rate of 20 Kbps with only 1 channel (active in ITU Region 1), while in the 915 MHz band it can achieve a data rate of 40 Kbps with 10 channels (active for ITU Region 2) [67]. In both the latter cases BPSK is used. More recently, the IEEE 802.15.4m protocol has been proposed, which encompasses some new features to be used in the TVWS bands [68]. The protocol foresees three different PHY: an FSK, a Narrowband OFDM, and an OFDM, with the latter being the highest in terms of data rate. The OFDM PHY is capable of achieving a maximum of 1562.5 kbps, theoretically increased by a factor of 4 if bonding 4 channels together. The FSK PHY can achieve a data rate ranging from 50 to 400 kbps, depending on the mode in use, while the Narrowband OFDM spans from 156 kbps to a maximum of 1638 kbps, although using a 3/4 64-QAM modulation scheme.

Due to its characteristics, several IoT devices have been built with integrated compatibility with IEEE 802.15.4 and many standardization organizations implemented their own low-power protocol stack on it. In such cases, since IEEE 802.15.4 standardizes both PHY and DLL layers, the customized stacks integrate their own logic, often altering the original one. In this section we provide a brief description of the proposed protocols and networks stacks which are top of the IEEE 802.15.4 layers, i.e.: Thread 6LoWPAN, ZigBee, WirelessHART and ISA 100.11a. Since the focus of the paper is on PHY/MAC layer issues, we focus the discussion on the modifications introduced by such solution to the original IEEE 802.15.4 stack.

4.2.1. Thread 6LoWPAN

IPv6 Over Low Power WPANs (6LoWPAN) is a data link adaptation implemented on top of the IEEE 802.15.4 stack, focusing on the adaptation of the IPv6 protocol to MTC. In fact, through the 6LoWPAN Working Group, the

Internet Engineering Task Force (IETF) has tackled the challenge of integrating IPv6 to the IEEE 802.15.4 DLL and PHY layers. The main challenges are due to the IEEE 802.15.4 frame size and MTU [12]. In particular, on the one hand the IEEE 802.15.4 frame size is 127 bytes, thus, considering the IPv6 and DLL headers, the space for the payload is very limited. On the other hand, the MTU for IPv6, specified by RFC 2460, is 1280 bytes, which is too big to be wrapped in a single IEEE 802.15.4 frame. Hence, 6LoWPAN acts as an adaptation layer which fragments the IPv6 packet onto several DLL frames. Furthermore, 6LoWPAN implements a stateless compression of the IPv6 packet in order to reduce the overhead for the lower layer. In particular it uses the Improved Header Compression (IPHC) and the Next Header Compression (NHC) depicted extensively in RFC 4944 and RFC 6282.

The Thread Group (TG) alliance constitutes one attempt of standardization for smart home devices (an IPv6/UDP implementation) [69]. In particular, it tries to establish the closed-documentation Thread protocol as a standard for home automation mesh networks. The TG makes use of the capabilities of the IEEE 802.15.4 MAC layer to forward the frame without passing it up to the IP layer for intra-subnet forwarding through 16-bit MAC addresses. In particular, Thread uses the 6LoWPAN stacked headers Mesh Header (for DLL forwarding), the Fragmentation Header (for the fragmentation of the IPv6 packet) and the Header Compression Header (for the IPv6 header compression, present only in the first 6LoWPAN packet relative to the same IPv6 packet). Thread also supports UDP as a transport layer, for which it shrinks the header by means of the NHC.

6LoWPAN has been also proven to be integrable on top of other M2M MAC protocols, for instance the BLE physical link, which has been shown to be possible for the first time in 2013 [70].

4.2.2. ZigBee

ZigBee is one of the most widely used technologies implemented on top of the IEEE 802.15.4 standard. Its version 1.0 has been released in 2005 by the

ZigBee Alliance, an association of companies working upon low-latency, low-power communication standards [71]. ZigBee is adaptable to other standard higher-layer protocols, since it specifies a custom full stack over the MAC layer. It is designed for star, cluster tree (version 1.0) and mesh (version Pro) networks, as it implements routing algorithms at the network layer. More specifically, each ZigBee network is composed primarily by three different types of device [72]:

- *ZED* (ZigBee End Device), a common RFD, which is normally located at the edge of the network.
- *ZBR* (ZigBee Router), an FFD capable of maintaining a routing table and forwarding packets. It is not present in ZigBee star networks, while, in tree and mesh network, every internal node in a path is a ZBR.
- *ZBC* (ZigBee Coordinator), a unique ZBR, capable also of initializing the network and assigning a 16 bit address to any node performing a join request. For star networks and tree networks, it is identified in the root node.

ZigBee tree and star networks use a straightforward address allocation together with a beaconing mechanism, so that each node knows if the packet should be forwarded to its children or to its parent. The slotted CSMA/CA ensures that the communication between a child and its parent occurs during the parent's Contention Access Period (CAP). Mesh networks are highly reliable due to redundant paths and automatic retries and acknowledgments; routers keep in memory routing tables and use Ad-hoc On-demand Distance Vector (AODV) algorithm when no known route is available. It also grants sequential freshness through a five octet code in the MAC frame in order to prevent replay attacks, default 64-bit message integrity, network layer authentication through a common shared network key and AES-128 encryption with shared key distributed by a trustworthy device called the "security trust centre". It is worth mentioning that ZigBee is one of the most used protocols within the scope of home automation scenarios as well as energy demand-response and load management applications;

standard documents on the adaptation of the protocol to such scenarios have been produced [73] [74].

4.2.3. WirelessHART

WirelessHART is the first open wireless standard designed for M2M wireless process control for industrial automation. It has been released in September 2007 [75] by the Highway Addressable Remote Transducer (HART) Organization[1]. It redefines the MAC layer of the IEEE 802.15.4 in order to adapt the PHY to the requirements of industrial environments, which have strict timing constraints and a strong focus on security [76]. For this reason, the typical contention-based approach adopted by the standard IEEE 802.15.4 has been replaced in favor of a more deterministic and controllable contention-free method. In particular, it implements TDMA with 10s slots in order to provide determinism. WirelessHART makes use of a central and permanent coordinator and each node of the network is committed to a very specific and unique task, therefore it is often irreplaceable by another node. WirelessHART operates in the 2.4 GHz ISM radio band and it is designed for star, tree, and mesh topologies. Due to its constraints, its redefined MAC implements channel hopping and channel blacklisting in order to limit the damage brought by background interference by continuously changing the channel and eliminating the noisiest ones.

The current standard specifications define novel network and transport layers, which include a simplified routing algorithm based on predetermined traces that are forwarded by the network manager to all the nodes during the setup. Security is provided at each layer: hop-to-hop security is guaranteed at the MAC by using MIC with an AES-128 cypher key, while end-to-end integrity and confidentiality is provided at network layer through several keys, explained in detail in [76].

[1] http://en.hartcomm.org/

4.2.4. ISA 100.11a

Like WirelessHART, ISA 100.11a is an open M2M standard protocol designed solely for industrial process control application. It has been developed by the International Society of Automation (ISA) and accepted as a standard in September 2009 [77]. Like WirelessHART, ISA 100.11a relies on the PHY of IEEE 802.15.4, sharing the same frequency bands; however, substantial differences from WirelessHART make such a protocol a competitor in the field of industrial automation. More in detail, ISA 100.11a devices have separate roles: they are either routing devices with forwarding capabilities or I/O devices, while in WirelessHART each device have both the capabilities [78]. From a more technical point of view, differences between the two data link layers implementations are present: WirelessHART commits all the responsibilities beyond the 1-hop communication to the network layer, while, in ISA 100.11a, a part of the original IEEE 802.15.4 is kept as a MAC sublayer with modifications aimed at handling the mesh routing. Furthermore, ISA 100.11a does not specify a standard timer for TDMA, it changes such timer whenever a new device joins the network. On the other hand, it specifies five standard MAC channel hopping schemes (slow and fast hopping, depending on the interferences and the payload size), unlike WirelessHART, in which the network manager is devoted to distribute the hopping scheme. Consequently, the network layers are different: WirelessHART implements at the network layer the routing capabilities, while ISA 100.11a only the routing between subnets (i.e. involving a backbone router). Moreover, since the extra-subnet routing is not specified in ISA 100.11a specification, IETF 6LoWPAN is used, with a translation capability from 128-bit addresses to 16-bit MAC short addresses for subnets.

4.3. Z-Wave

Z-Wave is a proprietary wireless protocol designed solely for the purpose of home automation [79]. It has been developed initially by ZenSys and promoted by the Z-Wave Alliance. The home automation scenarios undertaken by the protocol are focused on the reliable communication from a control unit to pe-

ripheral nodes. It operates in the 868 MHz bands for ITU Region 1 and 908 MHz bands for ITU Region 2, even if the subsequent version, Z-Wave 400, operates worldwide in the 2.4 GHz bands at a data rate up to 200 kbps, while the previous version was designed for a maximum of 40 kbps; each version uses the BFSK modulation scheme. The separation between types of nodes is well defined: there is one controller sending commands to the peripheral nodes, which can only reply to messages or execute physically the command. Such a centralized approach affects also the routing mechanism, which is hard-limited to four hops and stores each path onto the controller [80].

4.4. INSTEON

INSTEON is a proprietary home automation protocol designed by SmartLabs and promoted by the INSTEON alliance[2] [81]. It is claimed to support data rates up to 38.4 kbps using FSK-based modulation on the 904 MHz bands. It has been implemented as a pure peer-to-peer mesh approach, in which power line devices and wireless devices can communicate simultaneously using 24-bit unique addresses. Power line devices use a time slotted retransmission scheme, while wireless devices can retransmit the message simultaneously using an approach called "simulcast", which relies on the very low probability of having colliding messages at the receiver. More in detail, wireless devices transmit the same message at the same time in order to achieve a stronger signal at the receiver, therefore message cancellation occurs only when two sources are using the same frequency with phase shifting of around 180 degrees, which is highly infrequent in such a small subnet when the data rate is low enough. In both cases, wired and wireless, the retransmission is always triggered in case the receiver is not the recipient and it is limited to four hops.

4.5. EnOcean

EnOcean is a proprietary solution originated from a spin-off from Siemens. It is based on the odd concept of getting rid of both batteries and wires, feeding

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

its devices using exclusively energy harvesting [82]. It is claimed to be highly compatible with renewable resources such as solar panels, since the energy required by devices is low enough to work during multiple days in absence of the primary source. From the wireless protocol point of view, EnOcean operates in sub-GHz bands and has a range of typically 30 meters, which can be extended up to 300 meters in LoS; however, no further technical documentation is provided.

4.6. DASH7 Alliance Protocol (D7AP)

The DASH7 Alliance Protocol (D7AP) is a full stack open source protocol for low-power M2M communications promoted by the DASH7 Alliance, for which the 1.0 specification version has been released in 2015 [83]. It has been designed with respect to the RFID technology defined in the ISO/IEC 18000/7, inheriting its asynchronous MAC and its air interface for the 433 MHz bands. Its key concepts are often referred to with the acronym BLAST (Bursty, Light, Asynchronous, Stealth and Transitional) in order to emphasize the protocol features: low power, duty cycling, support for seamless mobility and ad-hoc non-periodic synchronization [84]. D7AP is implemented in the sub-GHz bands at 433 MHz, 868 MHz in ITU Region 1 and 915 MHz in ITU Region 2 and it is very flexible depending on the spatial requirements and the available bandwidth. In particular, it is designed for medium data rate (about 166 kbps) in short distances or low data rate (9.6 kbps) in long distances, making it a technology exploitable both in WPANs and LPWANs (see Tables 3 and 4). In both cases it uses the 2-(G)FSK modulation scheme. The protocol supports nominally tree topologies, however, due to the wide range of communication the technology can provide, only shallow topologies featuring at most two hops are normally deployed.

The protocol specifies each layer of the ISO/OSI stack, including the Presentation and the Application layer, implementing a highly structured distributed file system able to store data and configuration files with which a D7AP network can be set up simply invoking scripts. In practice, this means that the communication between entities in a D7AP network happens through the actions

of reading from and writing to a remote file. This respects the RFID standard from which D7AP originates, because it is built on top of a request-response paradigm without the use of a address-based communication. The schedule is driven by an ad-hoc wakeup scheme received by each endpoint from the gateway. The tree is composed by different entities: endpoints, which are devices devoted to sense or actuate and designed for low power operations and duty cycling; gateways, which are constantly in listen mode and can send packets to each node in their subtree; sub-controllers, which implement all the D7AP functionalities and are normally located as middle nodes in large tree networks and can act as relays for packets, even though they have a sleep period.

4.7. DECT ULE

Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE) is the last version of the already well-known ETSI DECT standard, launched in 1987 and used widely in the home telephony cordless technology. DECT ULE is a protocol extension proposed in 2011 by Dialog Semiconductor as an open standard for wireless technology featuring low power and low cost. It is claimed to be an ideal choice for home security and automation as its range is normally enough to cover an average household [85]. Indeed, it is deployed in star topologies and can reach a hop range of around 70 meters indoors, suffering little the interferences as it uses the 1.8 GHz frequency bands in ITU Region 1 and the 1.9 GHz in ITU Region 2. Another advantage is given by the ease of upgrade from the legacy DECT gateways to the new DECT ULE ones as the upgrade is exclusively software. It has already been specialized over several use cases such as energy monitoring, remote control for energy and climate, smart plugs, time-driven applications, baby monitoring, surveillance, smoke detectors, and voice-enabled panic buttons.

Even if its use is normally restricted to indoor scenarios, it is claimed to reach up to 600 meters range outdoors. Its features make it suitable for IoT applications: the low cost, the low latency, the data rate (1 Mbps), the link budget (which is higher than the one in BT and IEEE 802.15.4), the built-

in security and authentication, the single-chip solution and the duty cycling. DECT ULE hosts 5 (ITU Region 2 and 3) or 10 (ITU Region 1) different channels and uses dynamic channel selection in order to avoid interferences. The evaluation study conducted in in [86] demonstrates that the DECT ULE technology can represent an efficient solution for WSN deployments.

Table 3: Capillary IoT technologies. Some of the data were cross-checked with [87].

Name	Spectrum	Bandwidth	Peak DR	Range	Topology	PHY Modulation	MAC Access
BLE	2.4 GHz	2 MHz	1 Mbps	100 m	Star	GFSK (FHSS)	TDMA
Thread 6LowPAN	2.4 GHz	5 MHz	250 kbps	10-75 m	Mesh	OQPSK (DSSS)	CSMA/CA
ZigBee	2.4 GHz	2 MHz	250 kbps	10-75 m	All	OQPSK (DSSS)	S-CSMA/CA
ZigBee	915 MHz	1.2 MHz	40 kbps	10-75 m	All	BPSK (DSSS)	S-CSMA/CA
ZigBee	868 MHz	600 kHz	20 kbps	10-75 m	All	BPSK (DSSS)	S-CSMA/CA
WirelessHART	2.4 GHz	3 MHz	250 kbps	30-90 m	Mesh	OQPSK (DSSS)	TDMA
ISA 100.11a	2.4 GHz	5 MHz	250 kbps	30-90 m	Mesh	OQPSK (DSSS)	TDMA
Z-Wave	868/908 MHz	200 kHz	9.6 - 40 kbps	30-100 m	Mesh	FSK	TDMA
Z-Wave 400	2.4 GHz	-	200 kbps	30-100 m	Mesh	FSK	TDMA
INSTEON	908 MHz	-	38.4 kbps	45 m	Mesh	FSK	TDMA
EnOcean	868/315 MHz	62.5 kHz	125 kbps	30 m	Mesh	ASK, FSK	TDMA
D7AP Hi-Rate	433/868/915 MHz	200 KHz	166.67 kbps	10 m	Tree	GFSK	CSMA/CA
D7AP	433/868/915 MHz	200 KHz	55.55 kbps	100 m	Tree	GFSK	CSMA/CA
DECT ULE	1.8/1.9 GHz	1.728 MHz	1152 kbps	70-300 m	Star	GFSK	TDMA

5. Long Range Communication Technologies (LPWAN)

Nowadays, the common interest in IoT technologies is shifting from capillary scenarios, in which object clusters are enclosed in a LAN (or a PAN), to wide area scenarios, already envisioned as a key component of the future 5G deployments [88] [20] [21] [23] and now starting to hit the market. Several companies already working on proprietary IoT wireless protocols for the purpose of home automation and monitoring scenarios are now focusing more and more on wide area technologies. An example is given by the Wavenis technology [89], implemented by Coronis Systems, which had been distributed as a short range technology until few years ago, while now it shifted to an LPWAN implementation. The architectures for long range technologies follow the principles of the cellular deployments, therefore mesh networks are not an option, since the high capacity of the gateway and the wide communication range make any node capable to reach the gateway in one hop. Existing cellular networks, based

on 2G, 3G and 4G technologies, already meet some of the MTC requirements, while some others, such as low power and low battery consumption, are still a challenge and, in some cases, not addressable (i.e. low power consumption for UMTS due to the MAC channel access policy). Several solutions have been proposed and can be subdivided into two main categories: proprietary LPWAN solutions deployed in unlicensed spectrum bands and solutions integrated with the existing cellular infrastructure sharing licensed bands with the current cellular deployment. We will refer to the latter solutions as Cellular IoT (CIoT).

Wide-area M2M technologies are envisioned to be applied to many use cases requiring a spread node distribution, such as Smart Traffic management, street light control, smart city facilities, GPS asset tracking, smart farming, environmental metering and so on so forth. Although they are still a rising star, several deployments are already available nationwide and Machina Research forecasts that in a decade a great part of the radio traffic will be occupied by small devices and around a quarter of it will be using LPWAN technologies [90]. It is also predicted that wide area technologies will have the chance to replace the existing solutions for at least the half of the M2M market.

We introduce the proprietary LPWAN technologies in Section 5.1; CIoT approaches are reviewed in Section 5.2.

5.1. Proprietary LPWAN

The Low Power Wide Area Network (LPWAN) architectures aim to exploit IoT over a wide area deploying small devices' connections in unlicensed spectrum bands [20]. This enables stringent requirements, such as a low per-device cost, a long battery life, a low deployment cost, a high coverage (which is granted by the long range transmission) in all scenarios (e.g. indoor and outdoor) and a high scalability. Proprietary LPWAN technologies also can rely on immediate deployment, since they do not need to coexist with legacy cellular standards due to the different frequency bands. They are also considered a hot research theme, since LPWAN connected objects are expected to be 3.6 billions by 2024, according to Machina Research forecasts [91], an impressive slice of the market.

They are currently competing with 3GPP cellular technologies operating in licensed bands, outlined in Section 5.2, which, however, are 1 to 3 years away from providing a competitive solution and a significant deployment. Furthermore, 3GPP solutions suffer from a cost disadvantage due to the intellectual property of LTE and other leading technologies, indeed, a significant part of the device cost (5% to 10%) is covered by royalties [92].

5.1.1. SigFox

SigFox[3] is a proprietary M2M communication technology that uses unlicensed frequency bands for radio communication. It has been developed by the homonym company, founded in 2009 in France, which has been the first proposing a LPWAN solution [93] and had grown very fast since then, operating now in more than 30 countries and currently registering several millions connected devices that produce petabytes of data everyday [94] [95]. It has been, until few years ago, the world's leader private provider of LPWA connectivity, now surpassed by LoRa.

In particular, it is based on UNB (Ultra Narrow Band) wireless modulation (the same used in WWI by submarines) based on BPSK in uplink and GFSK in downlink, however, as a proprietary technology, no public documentation is available about the network layer. It is suitable for very small messages (8-12 bytes in size), small bandwidth (around 100 Hz) and low data rate (100 bps), hence achieving a wide area coverage with little energy consumption has been quite easy, also due to the UNB-based radio access that enable very low signaling overhead. The average area coverage has been identified in 13 km, however SigFox claims that it is possible to achieve an area coverage of 30-50 km for rural areas and a million connected objects per gateway [93]. In fact, the technology is mostly oriented to rural scenarios, in which messages are small and infrequent and require a long transmission range. The disadvantage is that, in

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

order to send and receive SigFox messages, a device must integrate respectively a compatible modem and an integration with the SigFox servers, i.e. it must be a SigFox device.

5.1.2. LoRa

LoRa is a proprietary technology supported by LoRa Alliance[4], a project started in 2015 and highly discussed nowadays as it is one of the major candidates for the LPWAN technologies. It has been patented by Semtech Corporation [96] and relies upon PHY Chirp Spread Spectrum (CSS) technology, according to which each symbol is encoded in a longer sequence of bit, thus increasing the resulting SINR [97]. Apart from the PHY layer, which is proprietary, each part of the stack built on top of it, better known as LORAWAN (Long Range Wide Area Network) [98], is open source and it is currently developed by LoRa Alliance. Its topology is designed as a star-of-stars, which means that each LoRa end device communicates in a single hop with one or more LoRa gateway and each gateway, in turn, communicates with a central node, namely a LoRa NetServer, through the backhaul. Each end device, however, never directly associates with the gateway; the association happens against the NetServer, thus all the complexity is moved from the gateways to the central node, simplifying the network access and making the devices in fact unaware of the presence of the gateways. This makes the gateway behaving as a relay, which simply forwards messages adding only some information about, for instance, the reception quality. Therefore, the NetServer is totally in charge for the removal of duplicates, making mobility implicitly supported and tracking applications simpler, since handover is no longer required. Furthermore, without the need to perform network association at each wakeup, the battery lifetime is significantly longer, claimed to be 3 to 5 times more a typical wireless technology [99]. In Europe, LORAWAN defines 10 channels, 8 of which are multi data rate, from

[4] https://www.lora-alliance.org/

250 bps to 5.5 kbps, one is a high throughput channel and the other is a FSK channel which allows a data rate up to 50 kbps. LoRa nodes use a maximum Tx and Rx power of 14 dBm, according to the ETSI restrictions. The use of the unslotted ALOHA channel access ensures a low power consumption, and the MAC sublayer resembles the IEEE 802.15.4 MAC, including the authentication mechanism, based on MIC (Message Integrity Code) [93], in order to be able to support protocols running on top of the same MAC, such as 6LoWPAN.

The behavior of LoRa devices is determined by the class they belong to, which is assigned according to the power resources they can afford:

- Class A (All): supported by all LoRa things, for which downlink is only available after transmission. It is suitable for power efficient end devices.
- Class B (Beacon): it is a class A with scheduled receive slots. The device is allowed to open the receive window through the synchronization with a time server (receiving a time beacon). It is suitable mainly for actuators.
- Class C (Continuously listening): class A things which listen continuously and do not need energy efficiency. It is suitable for devices powered by constant sources instead of batteries.

LoRa features also native localization capabilities without the need of a GPS chip, which is considered too power hungry. This topic is still under debate, however, the current implementation is sufficient to achieve an acceptable precision, using Time Difference Of Arrival (TDOA) and multi-gateway perception. This enables a lot of new applications such as rescue trackers, location-based environmental monitoring, tracking of pets and objects and so on.

5.1.3. Weightless

Weightless is a set of LPWAN communication technologies proposed by Weightless Special Interest Group (SIG)[5], all of them relying on well known

[5] http://www.weightless.org/

PHY technologies adapted to the IoT requirements. All such technologies were initially developed by a group of partners, among which we cite Neul, and resulted in three different Weightless standards, designed for different use cases [100]. *Weightless-N*, based on narrow band technologies and DBPSK digital modulation scheme with frequency hopping, is suitable for low data rate applications in very challenging scenarios. It uses the 868 MHz ISM frequency bands and has a predicted data rate of 30-100 kbps reaching a range of 5 km even in urban scenarios, however it is used for one-way communications only. *Weightless-P* is a modification of Weightless-N for bi-directional communications, possible through acknowledgment protocols. It operates in 12.5 kHz narrow bands, using TDMA and FDMA, implying the time synchronization with the BSs. Such enhancements determine a loss in the transmission range from 5 km to 2 km in urban scenarios. *Weightless-W*, relying on the TV white spaces spectrum bands, is a technology designed for higher data rate scenarios. It supports modulations from DBPSK to 16-QAM and it uses TDD to guarantee uplink and downlink pairing. It supports communication range up to 10 km in outdoor scenarios and 5 km in indoor scenarios. In general, TVWS can be foreseen as a viable option indoor, mostly thanks to the shadowing that shields them from the primary signal and thus might offer better signal separation [101]. Weightless is proprietary and some features are known only to the SIG members, furthermore, to our knowledge, there is a lack of public documentation and of possibility of performing tests.

5.1.4. Ingenu's Machine Network

Ingenu[6] is a company, headquartered in San Diego, rebranded from On-Ramp Wireless in 2015. During the same year it released its Machine Network [102], a LPWAN technology based on proprietary Random Phase Multiple Access (RPMA), running on the 2.4 GHz and designed for being compatible with

[6] http://www.ingenu.com/

IEEE 802.15.4k. Despite the high frequency, it is claimed to be able to operate in the most challenging RF environments and at long distances [93]. The company deployed the technology in several US cities in 2017, leading the idea that M2M technologies based on 2G are likely to have no upgrade path. Ingenu claims that its technology will cover areas of around ten times more the ordinary cellular technologies and guarantees 10 to 20 years of battery life to its compatible devices.

Table 4: LPWAN technologies operating in unlicensed bands. Some of the data were cross-checked with [87].

Name	Spectrum	Bandwidth	Peak DR UL	Peak DR DL	Range	PHY Modulation	MAC Access
D7AP Lo-Rate	433/868/915 MHz	25 kHz	9.6 kbps	9.6 kbps	∼5km	GFSK	CSMA/CA
SigFox	868-915 MHz	192 kHz	∼100 bps	∼100 bps	>20 km	GFSK/DBPSK (UNB)	ALOHA
Ingenu MN	2.4 GHz	1 MHz	∼30 kbps	∼30 kbps	∼15 km	FSK, PSK (DSSS)	RPMA
LoRa	868-915 MHz	125 kHz	∼50 kbps	∼50 kbps	∼11 km	CSS	ALOHA
Weightless-N	868 MHz	200 Hz (?)	∼100 kbps	-	∼5 km	DBPSK (UNB)	S-ALOHA
Weightless-P	868 MHz	12.5 kHz	∼100 kbps	100 kbps	∼2 km	GMSK, OQPSK (UNB)	FDMA,TDMA
Weightless-W	470-790 MHz	6-8 MHz	∼10 Mbps	∼10 Mbps	∼10 km	DBPSK/QPSK /16-QAM (DSSS)	FDMA,TDMA

5.2. CIoT

Cellular IoT (CIoT) technologies represent the second facet of long range M2M technologies; their distinction lies in their deployment in licensed bands alongside with existing cellular technologies, whereas proprietary LPWAN technologies use unlicensed spectrum. As a matter of fact, CIoT technologies are proposed and led by telecommunication companies. Ericsson Mobility Report forecasts that there will be around 1.5 billion of M2M CIoT connected devices by 2021; therefore such set of technologies, despite being still in its testing phase, is considered already to have a prospective critical impact on the future of IoT. The term CIoT was first approved by 3GPP in GERAN [103] and 3GPP is now seeking for new proposals with regards to the following aspects [104]: improved indoor coverage (where RF signal penetration is limited), support for a massive number of low throughput devices in limited bandwidth and delay sensitivity (in particular, a delay of at most 4 seconds is considered appropriate for the

uplink traffic).

5.2.1. EC-GSM

One of the first attempts to exploit the licensed frequency bands in the cellular infrastructure is given by Extended Coverage GSM (EC-GSM). It is part of a recent initiative supported by Ericsson and Orange and standardized by 3GPP, public since 2015 and previously expected to be operative in 2017 [105], however, it has currently been demonstrated in a use case and still far from being deployed.

It is based on the fact that GSM is still a predominant market solution, since many devices are GSM-enabled and use GPRS/EDGE technologies for cellular connection. Due to its diffusion, GSM is likely to be still one of the pillars of IoT cellular connectivity, since the infrastructure is stable, ready-to-use and grants a global coverage and immediate access to the market. Due to the well known requirements demanded by the Cellular IoT ecosystems, an improvement of the GSM coverage has been undertaken in 3GPP Rel. 13 [106]. The use of a new PHY technique onto one of the GSM carriers in the 900 MHz frequency band for low data rate communications leads to an improvement of the GSM coverage up to seven times more the current deployment [107]. The balance between data rate and coverage is achieved through the definition of multiple service classes. Furthermore, techniques such as repetition and signal combining on the one hand and new control channels on the other are being added to the legacy communication in order to reach the edges of the coverage area. The expected number of devices supported by one BS is 50,000 on a single transceiver.

Battery life has been significantly increased in 3GPP Rel.12 through the introduction of a PSM (Power Saving Mode), in which the constrained device requires the network access for a limited time slot according to a TAU (Tracking Area Update) time window. This, according to the regular DRX (Discontinuous Reception) cycle, determines the whole duration of the duty cycle. During the TAU, the device stays reachable for updates and switches to PSM until the TAU

expires, being still registered with the network, but not checking for updates. 3GPP Rel. 13 introduced eDRX (Extended Discontinuous Reception), which shortens the length of the TAU and the reachability time window, negotiating them prior to the data transfer.

EC-GSM brings significant advantages since the ecosystem is in place and a software upgrade on legacy systems is likely to be sufficient in order to achieve compliance. The stability of the technology and the absence of requirements for new hardware makes the overall cost extremely low and the access to the market very fast.

5.2.2. LTE-M

OFDM-based LTE has been the first reason why Cellular IoT has gained interest after a big black hole of very little development because of CDMA-based 3G systems not being suitable for MTC [88]. With the advent of such technology, some important documents have been produced, such as TS 22.368 [108] and TR 23.888 [109], specifying requirements, challenges and improvements for cellular MTC. In particular, 3GPP Rel.13 introduced the latest features for LTE-M, a version of LTE optimized for constrained devices [110]. LTE-M is often referred to as LTE Cat-M1, LTE Cat-M or eMTC (standing for enhanced Machine-Type Communication). Such technology has been introduced firstly in Rel. 10, however, only in Rel. 13 specific requirements have been satisfied. The solution is based on concentrating LTE traffic in narrow bands in order to improve scalability. The deployment will be carried out onto existing LTE guard bands or through refarming one of the GSM carriers. The great advantage is given by the reuse of the LTE technology, thus no additional hardware is required by legacy components and coexistence is not an issue, furthermore basic LTE services such authentication, security, policy, tracking and charging are totally supported [111].

In LTE, each PRB (Physical Resource Block) already fitted in 180 kHz. Some of the LTE channels need to be modified in order to fit into the same

bandwidth, as shown in [111]. Basically, an LTE-M channel comprehends 12 subcarriers with 15 kHz spacing and shares the same LTE numerology, thus it is possible to multiplex LTE-M traffic without mutual interference, sharing the same PRB through time. This allows to increase the number of LTE-M channels dynamically as more M2M devices join the network. In particular, LTE-M operates in a 1.4 MHz carrier using up to 6 PRBs at consecutive locations. In order to keep the BoM (Bill of Materials) low enough, LTE features have been considerably limited, achieving an estimated reduction in the cost of the modem of 75% compared to the regular LTE UE [112]. Half-duplex transmission for FDD instead of full duplex is one of the key features, introduced since Rel. 12 and the UE has only one receiving antenna compared to a minimum of 2 for regular LTE UE. The receive bandwidth is reduced to 1.4 MHz, being still able to operate in the 20 MHz LTE system bandwidths. The power class of the end device is reduced to 20 dBm, allowing the integration of the amplifier in one chip [113]; consequently, peak data rate is reduced to 1 Mbps both in uplink and downlink compared to 10 Mbps downlink and 5 Mbps uplink for the regular LTE UE [112].

LTE-M coverage analyses have been performed [113]. It is shown that a test environment passed the Minimum Coupling Loss (MCL) requirement for LTE-M, achieving a 15 dB coverage extension. Such test has been performed both in uplink and downlink for each channel, showing that some of them, such as PDSCH and all the uplink channels require the use of repetition in order to achieve a coverage bonus. It is shown that LTE-M coverage can be pushed until reaching 11 km, however likely only 10% of the devices will need more than 10 dB additional coverage. From theoretical consideration it is stated that generally only one LTE-M channel is needed to support thousands smart meters. More specifically, this result has been achieved considering the area of Washington D.C., taking into account the fact that, by specifications, an LTE-M channel can support up to 83,000 devices (7,600 considering 15 dB penetration loss with all meters deployed in the basement).

Rel. 13 LTE-M devices support the eDRX cycle, evolved from the DRX in

Rel. 12, the same already outlined for EC-GSM (see Section 5.2.1). Such approach is suitable whether the transmission is not delay-tolerant or in scenarios requiring high coverage, when transmission is repeated many times. Theoretically, using this approaches, the battery is suitable to last around 36 years (with a daily update of 200 B), however, due to current leakage and battery self-discharge, an estimation of 10 years appears more realistic [114].

5.2.3. NB-LTE-M

The extension of LTE for constrained low power devices required a narrowband solution, namely narrowband LTE-M (NB-LTE-M) to cope with battery constraints when significant data rate is not required. In fact MTC traffic, for many applications, may be very latency tolerant: according to Nokia White Paper, the MTC broadband traffic is expected to cover only 0.01% of the mobile traffic and presents different (or no) traffic peaks, also in some cases it is possible to schedule the traffic overnight. For this purpose, NB-LTE-M solution has been introduced in Rel. 13 [110] with the following changes over LTE-M [114]:

- Reduced device bandwidth both in uplink and downlink to 200 kHz as in EC-GSM and reduced throughput due to a single PRB operation.
- Link budget increased by 5 dB over LTE-M, thus a 20 dB total increase over legacy LTE.
- UE transmit power increased to 23 dBm instead of 20 dBm for regular LTE-M UE.

Apart from such alterations, with the purpose of generating a different bandwidth category, NB-LTE-M preserves the same characteristics of LTE-M regarding battery consumption, duty cycle, use of PSM and repetition for increased coverage and hardware low cost solutions. The single PRB approach allows the NB-LTE-M carrier to be deployed in a single 200 kHz refarmed GSM carrier or within LTE-M ordinary channels. Such approach is carried out through

time multiplexing of the 6 LTE-M PRBs with the possibility to integrate the NB-LTE-M communication stack within any LTE-enabled device without any hardware upgrade. This is a key concept from which the NB-LTE-M proposal takes advantage, since it implies a significant reduction in the deployment costs. Furthermore, since the LTE channel numerology is kept, the integration does not generate any coexistence issue and the introduction of LTE for M2M communications is as simple as a software upgrade. NB-LTE-M is also known as LTE Cat-NB1 or, more commonly, simply as NB-IoT.

After the 3GPP Rel. 14, finalized in early 2017, it is clear how NB-LTE-M has been designed as the IoT pillar technology for the cellular ecosystem. Many improvements have been finalized in order to meet the requirements of the future 5G networks, such as the coexistence with CDMA, the support for multicast downlink transmission, a new UE power class with a level of 14dBm and localization support. The latter will be achieved through the use of Observed Time Difference Of Arrival (OTDOA). More information on the recent Rel. 14 improvements are reported in [115], whereas Rel. 15 will be completed in late 2018 and will include mobility support.

5.2.4. Clean Slate NB-CIoT

Other CIoT approaches not based on legacy technologies are arising. In particular, Vodafone, Huawei and Neul support a "clean slate" solution, claiming that the new requirements for a fully connected CIoT environment are likely to be achieved through a dedicated cellular technology. The concept is based on the statement saying both that a licensed cellular solution is crucial in order to avoid proprietary LPWAN technologies to absorb the long range IoT market, and solutions trying to adapt existing ecosystems (such as LTE) to M2M communications will be likely unsuccessful. The latter is mainly due to the fact that the starting point of existing technologies is the high data rate [116].

The proposed technology, namely NB-CIoT, is deployed in 180 kHz bandwidth channels both in uplink and in downlink, which offer plenty of deployment options and a high capacity per gateway. Each downlink channel is modulated

through BPSK, QPSK, 16QAM, reaching a data rate between 375 bps and 36 kbps. In uplink the individual modulation uses (D)QPSK, (D)BPSK or GMSK and is pulse-shaped in order to minimize the interference between UEs, reaching a data rate between 200 bps and 45 kbps. The resource blocks are split into 12 downlink channels (spaced by 15 kHz) or 36 uplink channels (spaced by 5 kHz) that support frequency hopping, making the receiver equalization simple. One of the downlink channels is reserved for broadcast acquisition [117]. It is deployable in two different ways:

- As a single re-farmed pulse-shaped GSM sub-carrier, implemented as FDD.
- Within both the LTE guard bands, providing frequency diversity. Again, pulse-shaped and individually modulated carriers help to avoid coexistence issues and side-lobes, however it is more challenging than the coexistence with GSM.

The coverage enhancement is claimed to be 20 dB over GSM standard coverage and the power consumption varies according to the distance from the gateway. For instance, for a device submitting on the average 4 reports per hour the battery life is expected to be over 10 years when relying in the standard GSM range, while it falls down to half a year whether it requires the range enhancement. In addition, the technology supports both scheduled and event-driven traffic, still using duty cycling. Finally, the estimated cost of each device, based on the 2016 standard costs, is claimed to be around 4$ per unit.

Table 5: Cellular IoT technologies operating in licensed bands. Some of the data were cross-checked with [87].

Name	Spectrum	Bandwidth	Peak DR UL	Peak DR DL	Range	Modulation	Access
EC-GSM	700-900 MHz	200 kHz	∼10 kbps	∼10 kbps	∼15 km	GMSK	TDMA
LTE-M	700-900 MHz	1.4 MHz	∼1 Mbps	∼1 Mbps	∼11 km	QPSK, 16-QAM, 64-QAM	OFDMA
NB-LTE-M	700-900 MHz	200 kHz	∼144 kbps	∼200 kbps	∼15 km	QPSK, 16-QAM, 64-QAM	OFDMA
NB-CIoT	800-900 MHz	180 kHz	∼36 kbps	∼45 kbps	∼15 km	BPSK, QPSK, 16-QAM	OFDMA

6. Discussion

In this Section, we examine horizontally the technologies that we presented in Sections 4 and 5, focusing primarily on the metrics and the use cases we introduced in Section 3. In particular, we discuss the use of all the technologies targeting each specific use case in Section 6.1 as well as examining the status of LPWAN technology deployments in the real world in Section 6.2, as this will give a footprint of the market direction of the future 5G scenarios.

6.1. Scenario Specific Discussion

We now discuss research challenges and scenario specific possibilities using the technologies presented so far and related to the use cases introduced in Section 3.3.

Clearly, short range communication is more suited for networks that do not need to span across considerable distances. Rather, their characteristics make them useful for networks in need of local control, which may rely on other technologies to bring the data at longer distances through the Internet. Long range communication technologies enable M2M devices to communicate at longer distances, enabling novel possibilities for services requiring communication over different places located farther apart.

Concerning *Home Automation* scenarios, short range technologies are certainly those which are better suited and more widespread in the current deployments [118]. Typically, *Home Automation* systems require energy efficient communication through devices and, possibly, communication either to a user device (e.g. a smartphone) or to the fog/cloud layer, thus requiring an Internet connection. While intra-network communication may leverage specific technologies tailored for the specific device and communication requirements, such as Zigbee and Z-Wave, the latter requires a shared technology between the *Home Automation* devices and the smartphone, like BLE. Typically, a bridge device, generally main powered, acts as a central gateway which is equipped with multiple technologies (i.e. the ones suited for the intra-network communication

and the ones for communicating with the user device or with the home router), which makes the communication possible. The main research challenge here resides on making the communication efficient between different technologies, which is typically realized in the gateway through a middleware which handles the heterogeneity between the connections, a challenge tackled in the Fog Computing paradigm. In less critical scenarios, end devices may be all equipped with both technologies, thus reducing energy efficiency, while cutting the need for an additional device. In contrast, long range technologies are not the best suitable option for *Home Automation* due to the limited space in which the network is deployed. However, they may still be viable for specific scenarios, such as connecting parts of the building that are either far apart from each other or need different features not offered by short range technologies in order to overcome obstacle shadowing (e.g. more transmitting power or lower frequencies). Another option for long range technologies is to be used as backups or load balancing on the router, useful in case of problems on the main Internet connection. Nonetheless, there are companies relying entirely on LPWAN deployments for their smart home products. One of the first examples was KingTing, a company that relies on LoRa for its home automation solutions[7].

Industry 4.0 nowadays heavily relies on short range communication technologies, mainly due to energy efficiency and reliability. Among the possible scenarios which *Industry 4.0* face, such as *Predictive Analytics* and *Machine Internal Control*, all of them need long operational life, and resilience to malfunctions. For such reason, in the vast majority of deployments, TDMA-based protocols (such as WirelessHART and ISA 100.10a) are chosen over others, due to their efficiency in time and the fact that industrial scenarios are rarely subject to topology change. BLE has been taken into account as well due to recent developments in its mesh real-time variant [119]. Here the challenge is the number of devices that can occur in a limited space, since such technologies may not

[7] http://www.yosmart.com/

allow high numbers of connections, and will possibly need to form independent networks. This is the case for the countless sensors installed inside different kind of industrial appliances, which communicate between them to report the device behavior. While some of these may be connected through wires, others may be more convenient to be connected wirelessly. Hence, control at the PHY or MAC layer have to be efficient, always maintaining energy efficiency. Although *Industry 4.0* does not normally rely on long range technologies, since the majority of the nodes tend to be close to each other in the network, long range technologies may be used for scenarios in which different buildings have to be connected or separate entities can be cut off from the network. In fact, the use of unlicensed spectrum, as in LPWAN, has reliability issues, due to the lack of guarantee of service availability, mainly because of duty cycling and Listen-Before-Talk (LBT) regulations. The coexistence problems introduced doubts on cellular solutions as well [120]. For such reason, a union between short range and long range technologies is required and, again, the challenges are on the optimization and on the efficiency for using technologies with different requirements, characteristics and constraints together. A practical study on large deployments has been performed in [121], where a hybrid topology is taken into account and local networks are interconnected by means of SigFox.

Healthcare is a broad scenario that makes large use of short range communication technologies. Apart from hospital devices, which form networks on their own, more recent wearable computing devices also leverage these technology, for continuous monitoring of the vital signs of human beings. These devices need a gateway to report data to the user, being it the user's smartphone, hence generally using BLE, or a different gateway, hence using 802.15.4 [122]. Usually networks are composed by a reduced number of devices, hence the challenges are rather on the upper layer optimization, reducing communication between the end devices and the gateway to reduce battery consumption. For *Healthcare*, long range technologies are mainly used to report patient monitoring data to a central aggregator. This is particularly useful for recent scenarios such as

those in which, instead of monitoring patients in hospitals, the monitoring takes place remotely. The foremost challenge is the resilience of the communication; long range communication technologies are mandatory, since it should not be assumed to be always in the home router range, however, for many of them, the reliability of the connection is not always granted. In order to reduce the possibility of unavailable connections, novel mechanisms that prioritize urgent communications have to be designed as well as a possible combination of long range communication technologies. In fact, practical studies have been conducted, stressing the current unsuitability of LPWAN technologies for critical monitoring use cases [123].

Environmental monitoring usually requires to span over large distances. Hence, short range communication technologies are not the most suitable option, although, using multi-hop short range communication technologies may still be viable, clearly with increased battery consumption due to the increased volume of communications. The latter is also the main challenge, and the use of short range technologies have to provide considerable advantages compared to longer range technologies. To this purpose, in [124] the authors compare the performance of ZigBee, BLE and Wi-Fi technologies for data intensive monitoring applications, and demonstrate that the choice of the optimal technology in terms of energy consumption strongly depends on the application rate to support. Long range technologies are much more suitable for *Environmental monitoring*, as the area to monitor may be large. Standards like LoRa and SigFox are already used depending on the scenario requirements and, in the future, cellular technologies are also desirable. Energy efficiency is the most important focus here, in contrast with reliability, as a longer battery duration turns out in a huge monetary saving. In particular, NB-LTE-M and LoRa appear to be suitable options, with more than 10 km range outdoors. NB-CIoT is another alternative too, although it slightly penalizes the data rate, favoring the number of devices supported per BS. For wider distances, SigFox, which is currently in use in Europe, grants a high coverage for environmental or remote monitoring

applications (in open air environments [20] states that it reaches up to 50 km), however, the extremely low data rate make it suitable for a restricted set of employments.

Wireless technologies have been a fundamental building block in environmental monitoring and remote sensing scenarios, such as water management [125] and ecology [126], always relying on traditional WSNs. Nowadays most of such paradigms are shifting to long-range technologies, although their adoption is slow due to the interdisciplinarity of such areas, for instance within the scope of monitoring in conservation biology [127]. In fact, through the recent blend of such areas, the field of "*conservation technology*" had recently arisen, which leverages wireless remote monitoring for conservation purposes [128].

In *Smart cities and Smart buildings* there are many different use cases, such as the *Smart grid*. Clearly, there is and there will be a merge of different telecommunication technologies, therefore, the main challenge is making those interactions efficient and resilient to different problems. Energy efficient routing algorithms and software optimization such as caching, along with self healing capabilities for both the devices and the bridge are needed. A specific technology is hard to predict, as each of those is built according to specific constraints and can suit better a specific use case compared to others. Again, the interaction between different networks and at different layers of the network architecture is the key challenge and, in the commonly shared future IoT vision, such ecosystems will necessarily make extensive use of long-range technologies as well. Finally, as already pointed out, *Smart cities and Smart buildings* is a wide use case, in which both short range and long range technologies are used. Short range is currently in use in local networks, however, to achieve city-wide optimization and monitoring, long range technologies have necessarily to be employed. Depending on the size of the city, and on the layer of optimization, different standards may be well suited. For instance, the authors of [129] compare the coverage of GPRS, NB-IoT, LoRa, and SigFox technologies via a simulation study over a realistic, large-scale city scenario; the experimental results show that the NB-

IoT technology provides the largest coverage, however they also reveal the need of additional measurements and research studies in order to identify the best trade-off in presence of multiple requirements (e.g. scalability and deployment costs on dense populated urban areas).

Focusing on the *Smart Grid*, again longer range technologies are needed to connect local networks to the utility aggregator. Short range technologies are only needed to achieve energy efficiency by load balancing the longer communication effort between devices, with frameworks like [130]. The main challenge in such contexts is given by the heterogeneous traffic balance, since, especially with the future vision of the 5G, the M2M traffic will coexist in cities with the legacy cellular traffic sharing the same medium. This also affects reliability, which has to be addressed. As an example, in LoRa star-of-star topology the aggregation happens at the backhaul, thus, a single node can be supported by multiple gateways. In such cases few more gateways can cope with the issue, this is the common case of big smart building coverage [131]. It is also worth mentioning that the multiple gateway solution releases the system from the Single Point of Failure (SPOF) problem, an important achievement with respect to reliability.

6.2. Current M2M Deployments

In this Section, we discuss the existing deployments of M2M technologies worldwide, by identifying current trends and future initiatives. We mainly focus on LPWAN-based deployments, since most of short range and capillary technologies constitute consolidated approaches and are less preferable for large-scale installations, particularly when these are sparse. Instead, LPWAN technologies are, according to several sources [20] [132], expected to occupy a huge part of the IoT market, to the point in which one fourth of the skyrocketing 30 billion devices connected to the internet will use LPWA technologies. This is not surprising, due to the new requirements that characterize use cases like smart cities, healthcare and remote monitoring, in which end devices are expected to be arbitrarily deployed and moved anywhere without connectivity conse-

quences [53]. To this end, proprietary LPWAN technologies are already hitting the market in several countries, while the efforts to bring CIoT technologies to an active state on the market are still at their beginning. In fact, apart from few testbeds aimed to compare CIoT technologies under similar environmental circumstances, the actual studies are still limited to analytics [133] [134] and simulations [135]. Technologies like SigFox and LoRa are still under rollout worldwide, however, they have been adopted as a local network in different measures. SigFox, at the time of writing, covers officially 20 countries in Europe, 10 in Asia, 11 in South America, 2 in North America, 4 in Oceania and 3 in Africa [95], although the numbers are changing incredibly fast. It was first deployed to cover nationally France in 2014 and it fastly reached coverage in 5 countries in 2015. In the same year SigFox deployments had been established in the United States, making it a worldwide adopted technology, although not standardized. The number of countries has rose significantly in only 4 years and many companies are establishing their own SigFox network in order to provide coverage to whole countries. LoRa is a big competitor to SigFox and slightly more common. It is operating actively in 43 countries through 76 different network operators giving a public network access [136]. At the time of writing, LoRa is also present in Canada, China, India and Russia, whereas SigFox is not. If we do not consider only the public networks, LoRa deployments are operating in more than 100 countries. The Netherlands started to deploy LoRa gateways in 2015 through the company KPN as well as the French telecom company Orange, which covered rapidly 4,000 cities in France and it reached nationwide coverage in only one year. These numbers reveal about how such market is rising rapidly and reaching an enormous quantity of connected devices. Although SigFox and LoRa tend to be concurrent deployments, they have different features and, in a sense, they are complementary, thus coexisting deployments can serve easily different types of market and use cases [21], e.g. LoRa grants more payload length, more latency performance and more deployment flexibility thanks to the hierarchical network topology, whereas SigFox offers more coverage (only three SigFox base stations can offer coverage to the whole Belgium). Ingenu is

stated to be deployed officially in 29 countries: 3 in North America, 13 in Asia, 7 in South America, 3 in Africa, 1 in Oceania while in Europe it is deployed only in Italy (used by the Italian telemetry company Meterlinq in its smart metering services) and Portugal [137]. The technology is rising rapidly as a competitor of LoRa and SigFox, however its deployments are typically limited to single use cases rather than providing an actual nationwide coverage, this is due probably to a higher cost of the infrastructure, since it guarantees a high range communication, yet ensuring a rather strong link budget.

The other big competitor in the area is LTE-M together with its complementary NB-IoT (or NB-LTE-M), although it comes somewhat late in the big LPWAN party, as currently (to the best of our knowledge) it has no active and publicly available deployment. Nevertheless, its backward compatibility with the current cellular deployments is a strong point that will give to this technology a central role within the future IoT traffic in the 5G. Moreover, during 2017 and 2018 its rise has been quite impressive, with 41 launches by 23 mobile IoT commercial operators in 26 countries as of 21 February 2018 and currently under rollout [138]. Results for testbeds are expected to be ready by the end of 2018; in the meantime, several LTE-M IoT labs are opened in several countries. Commercial launches of LTE-M and NB-IoT took place quite early in USA and Canada as well as Japan and China, whereas, for Europe it has been adopted later for 14 countries and almost exclusively oriented to the narrowband version. Compared to NB-IoT, other standards by 3GPP received a lot less attention, however, we report a demonstration of an EC-GSM weather station in the US carried out by Groundtruth with the support of Nokia, Orange and Sierra Wireless [139].

7. Research Challenges and Future Directions

The IoT vision demands more and more requirements to be satisfied by the MTC systems, as the industrial and the societal ecosystems are evolving, and new opportunities are arising. As indicated in the previous sections, there has

been a significant focus on ensuring IoT-specific features to M2M communication technologies such as low cost, low consumption and extended coverage. Although these may not be directly required by the lower layers, the envisioned scenario for many M2M applications need such characteristics, which are hence primarily tackled at the communication layers. Nevertheless, nowadays M2M technologies still present a plethora of open issues, mainly due to their heterogeneity as well as to the extreme difficulty in managing networks that are changing dynamically in terms of number of devices. We broadly classify these challenges into (i) Interoperability (Section 7.1), (ii) Scalability and overload (Section 7.2), (iii) Security (Section 7.3), (iv) Management (Section 7.4), and (v) Support for Mobility (Section 7.5). Besides that, all the requirements outlined in Section 3.1 are satisfied to some extent by most of the technologies, however, optimized approaches that cope with such requirements are still under study. In fact, any small improvement at MAC and PHY layers can lead to an impressive economic saving. Despite a number of dedicated approaches have been proposed, such as in [140], [141] and [142], still some significant issues remain open. In this section we outline the aspects that have been poorly addressed so far and need the researchers' attention for future research.

7.1. Interoperability

The heterogeneous nature of IoT-based devices and technologies makes the interoperability among them a hard task. In this paper we have observed how many different communication protocols are different in at many levels, however, IoT deployments are more and more in need of being included in a big picture and able to be reachable uniquely, both in MTC and Human to Human paradigms. Nevertheless, the current situation is somehow fragmented, in which IoT ecosystems are deployed in closed islands with little or no interoperability with others, thus many related IoT applications cannot exchange data. With the exponential increase of connected IoT devices, the amount of information available depends strongly on the interoperability among such devices, which is a crucial point and cannot be ignored. This feature is also what distinguishes

mostly IoT scenarios from others: the crucial importance of the availability of shared information and the end-to-end interconnectivity among all the entities. The current deployments gave little or no importance to this aspect, which unavoidably caused the resources to be unreachable or the developers to design costly ad-hoc solutions for each use case. Interoperability is a major challenge that has to be tackled from different points of view. With the establishment of the paradigm of fog and edge computing [22], the data processing tasks can be executed in different aggregation points of the network, balancing properly the battery consumption of the end devices. Designing correctly such layered computation structure, with specific regard to the M2M technologies involved, is a viable option for granting end-to-end interoperability via balancing the loads and ensuring that the requirements of the systems are respected. Furthermore, the heterogeneous nature of the devices combined with the emerging need for massive IoT deployments generates other challenges for interoperability since devices must be enabled with a compatible connectivity regardless of their vendor and their network interface. In order to enable such interoperability, also new service discovery and description standards have to be designed in order to cope with the new set of requirements. There have been many attempts in such direction at many levels: many proposed an integration at the architectural level, while others proposed an approach based on multi technology gateways. For several years, several organization attempted to establish a standard through oneM2M[8] in service architecture design and application protocol bindings for constrained devices (e.g. CoAP and MQTT). Nonetheless, integration and compatibility among M2M technologies is still subject to studies.

7.2. Scalability and overload

MAC protocol scalability is one of the key open problems when end devices in the same network are dramatically increasing in number, thus MAC layer enhancements in simultaneous channel access are highly desired. In [33] the

[8] http://www.onem2m.org

authors suggest that future research directions should involve also a better signal processing at the PHY that facilitates the MAC layer in such direction. In practice, most of the open issues are related to dense networks, where scalability brings along many other challenges, such as QoS management, prioritized access to relevant applications and differentiated support for bursty/periodic traffic types. With specific regards to MTC traffic flows, scalability is foreseen by many researchers as a major research problem for future IoT networks, in particular when dealing with IoT services running over cellular technologies in order to grant the coexistence with the previous services without affecting the QoS. Indeed, legacy LTE deployments will have to manage M2M traffic consisting of small size packets that potentially transmit at large intervals. Given that each cell is expected to cover a massive number of M2M connections over long periods of time, the maintenance of the state information of each connection is another face of the challenge [143]. This can be achieved by the design of a proper architecture that redesigns the connection and communication policies at all layers (e.g. the use of IPv6 at the network layer). Network overload is also a challenge, due to the traffic type of M2M devices and their amount. There is also a huge need for traffic priority differentiation, since many IoT applications have compulsory low latency requirements, such as healthcare remote monitoring and automotive communication. Recent works have shown that the legacy cellular deployment is incapable of addressing the bursty, sporadic and ubiquitous nature of IoT V2X network traffic [144], thus new mechanisms to address such an heterogeneous demand have to be designed. Furthermore, for different scenarios, the balance between the packet loss and the delay have to be tackled at different network layers, including the transport and the application layer, since, clearly, the UDP protocol is the only viable options for M2M traffic, although its unreliability is tackled at upper layers.

7.3. Security

As M2M-enabled devices handle and transmit potentially sensitive data, such as in-home recorded videos or medical data, security has to be addressed.

Security for such devices is still currently a challenge due the heterogeneity of the devices, their limited resources, their reduced ability to add computation layers and their access to entities in the real world (through sensors and actuators). For such reason, there is a need for researchers to focus and assess the different types of threats that may affect massive and heterogeneous IoT deployments and address all the security requirements.

Attacks can be performed on 3 different parts of the network: the *device*, the *remote infrastructure* and the *communication link*. Devices may be target of two different attacks: either an authenticated device is altered, by changing its information or sensing capabilities, or unauthorized devices join the network. While the former has to be avoided by providing security mechanisms on the device, such as anti-tampering solutions, the latter may be realized at the network and protocol level, by including authentication schemes. However, given the reduced processing capabilities an the constrained nature of M2M-enabled devices, existing encryption and authentication schemes such as AES and RSA introduce a high computation overload that is typically not applicable. Hence, the challenge is, while these mechanisms should guarantee security and privacy of the data, they cannot be too much expensive in terms of computation power or adding too much data to transmit. The *Remote infrastructure* could be either at the cloud or at the fog layer. Its security lie outside specific M2M communication, although it should be assured to protect data coming from the devices, by using, for instance, data encryption. The challenge is here given by the absence of a shared infrastructure and, thus, the ability to deal with diverse devices. Finally, attacks can target the *communication link* itself, i.e. when M2M devices transmit, the communication may be target of packet sniffing and man-in-the-middle attacks. The typical solution is to use some sort of encryption (i.e. TLS) when communicating, obviously increasing the computation power needed to decode and encode messages. It is also worth to note that security is a chain. It is totally useless to secure one part of the chain while leaving other parts unprotected, as the security of a whole systems equates to the security of the least-secure of its components, thus all security challenges

need to be tackled efficiently by future IoT systems designers.

7.4. Management

The human intervention in M2M-enabled IoT systems needs to be reduced as much as possible. For such reason, conventional IoT deployments employ a set of management policies for self-organization and self-reconfiguration in order to address faults, link failures, optimization and security. Because of the heterogeneous nature of constrained devices and their number, such solutions need to be reconsidered and redesigned in order to address efficiently the new network paradigms. Indeed, it is imperative to keep such solutions efficient, rapid and, at the same time, lightweight enough in terms of energy consumption. The effective impact of such solution is even more noticeable when considering a huge number of devices, in that network administrators cannot deal with the single entities due to their amount, thus features like fast network diagnostics and troubleshooting are a significant part of the challenge. Localized and hierarchical network structures, such as fog-based paradigms, are currently undertaken by researchers as viable solutions, since they provide more efficient service-driven capabilities, such as service aggregations, service discovery and localized diagnostics.

7.5. Support for Mobility

Due to the entirely different type of traffic given by the M2M devices, legacy systems are currently not able to cope with the reachability of mobile devices that require low latency and continuous support and at the same time display a bursty and sporadic communication behavior. Service interruption due to handover, although being addressed in existing network deployments, has gained little attention so far for IoT deployments, especially when targeting cellular scenarios, in which the coexistence issues introduce yet another layer of complementary challenges. From one side, such challenges are promised to be addressed by the deployment of more dedicated base stations in the future 5G scenarios, however, the design of efficient handover mechanisms remains an open issue.

8. Conclusions

In this paper we provided to the best of our knowledge and research efforts a technical vision on the world of M2M communication technologies. We introduced the general requirements of such paradigms and provided an efficient taxonomy to classify all the technologies relevant to our studies. We also introduced the use cases for which such technologies are designed for and provided a panoramic vision on their MTC applications. As a core part of the paper, we described in detail each technology with a particular focus on the requirements we meant to analyze and, finally we provided a comparative discussion oriented towards several aspects of such technologies.

We foresee the main research efforts to be directed towards the wide area ecosystems, mainly due to the heavy market shift that such technologies caused, for which the chance for LPWAN technologies to take over the legacy ones is consistent. It is worth mentioning that, in general, M2M long-range technologies are still in their "embryonal phase", in which, moreover, proprietary LPWAN and CIoT solutions are competing to absorb this slice of the market [100]. In Sections 5.1 and 5.2 we outlined the advantages that the promoters of such technologies claim, in practice we are still facing a division and none of them acquired supremacy. Proprietary LPWAN technologies are closer to a practical wide area deployment, having several countries already covered, however, CIoT solution promise an integration within the actual cellular infrastructures and, in some cases, a backward compatibility with legacy devices. To the best of our knowledge, the competition is still open and more performance studies, dedicated PHY/MAC strategies and theoretical models are yet to come.

Bibliography

[1] Cisco, Cisco Visual Networking Index: Forecast and Methodology, 2016–2021, Cisco White Paper, 2017.

[2] Ericsson, Ericsson Mobility Report, Ericsson White Paper, 2018.

[3] Gartner, Gartner worldwide IT spending forecast for 2018 (2018).
URL https://www.gartner.com/newsroom/id/3845563

[4] O. Vermesan, P. Friess, Internet of Things From Research and Innovation to Market Deployment, 2014.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys and Tutorials 17 (4) (2015) 2347–2376. doi:10.1109/COMST.2015.2444095.

[6] P. Nintanavongsa, R. Doost-Mohammady, M. Di Felice, K. Chowdhury, Device characterization and cross-layer protocol design for RF energy harvesting sensors, Pervasive and Mobile Computing 9 (1) (2013) 120–131. doi:10.1016/j.pmcj.2012.09.004.

[7] R. C. Carrano, D. Passos, L. C. S. Magalhaes, C. V. N. Albuquerque, Survey and taxonomy of duty cycling mechanisms in wireless sensor networks, IEEE Communications Surveys and Tutorials 16 (1) (2014) 181–194. doi:10.1109/SURV.2013.052213.00116.

[8] N. Bui, M. Zorzi, Health care applications: a solution based on the internet of things, in: Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, 2011, pp. 131:1—-131:5. doi:10.1145/2093698.2093829.

[9] L. D. Xu, W. He, S. Li, Internet of things in industries: A survey (2014). arXiv:arXiv:1011.1669v3, doi:10.1109/TII.2014.2300753.

[10] V. Gazis, A Survey of Standards for Machine to Machine (M2M) and the Internet of Things (IoT), IEEE Communications Surveys & Tutorials (c) (2016) 1–1. doi:10.1109/COMST.2016.2592948.

[11] J. Tan, S. G. M. Koo, A survey of technologies in Internet of Things (2014).

[12] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. McCann, K. Leung, A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities, IEEE Wireless Communications 20 (6) (2013) 91–98. doi:10.1109/MWC.2013.6704479.

[13] K. G. E. Soltanmohammadi, M. Naraghi-Pour, A survey of traffic issues in Machine-to-Machine communications over LTE, IEEE Internet of Things journal (in print) (2015) 1–21.

[14] A. Laya, L. Alonso, J. Alonso-Zarate, Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives, IEEE Communications Surveys and Tutorials 16 (1) (2014) 4–16. doi:10.1109/SURV.2013.111313.00244.

[15] K. Ashton, That 'Internet of Things' Thing, RFID Journal 22 (7) (2009) 97–114.

[16] A. Botta, W. De Donato, V. Persico, A. Pescape, On the integration of cloud computing and internet of things, in: Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014, 2014, pp. 23–30. doi:10.1109/FiCloud.2014.14.

[17] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wireless Communications 23 (5) (2016) 10–16. doi:10.1109/MWC.2016.7721736.

[18] D. Singh, G. Tripathi, A. J. Jara, A survey of Internet-of-Things: Future vision, architecture, challenges and services, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE, 2014, pp. 287–292.

[19] J. A. Stankovic, Research directions for the Internet of Things, IEEE Internet of Things Journal 1 (1) (2014) 3–9.

[20] U. Raza, P. Kulkarni, M. Sooriyabandara, Low Power Wide Area Networks: An Overview, IEEE Communications Surveys & Tutorials.

[21] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, A comparative study of lpwan technologies for large-scale iot deployment, ICT Express.

[22] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal 4 (5) (2017) 1125–1142.

[23] G. A. Akpakwu, B. J. Silva, G. P. Hancke, A. M. Abu-Mahfouz, A survey on 5g networks for the internet of things: Communication technologies and challenges, IEEE Access 6 (2018) 3619–3647.

[24] C. W. Tsai, C. F. Lai, M. C. Chiang, L. T. Yang, Data mining for internet of things: A survey, IEEE Communications Surveys and Tutorials 16 (1) (2014) 77–97. doi:10.1109/SURV.2013.103013.00206.

[25] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: A survey, IEEE Communications Surveys and Tutorials 16 (1) (2014) 414–454. doi:10.1109/SURV.2013.042313.00197.

[26] C. Perera, C. H. Liu, S. Jayawardena, M. Chen, A Survey on Internet of Things From Industrial Market Perspective, IEEE Access 2 (2014) 1660–1679. doi:10.1109/ACCESS.2015.2389854.

[27] A. Kamilaris, A. Pitsillides, Mobile phone computing and the Internet of Things: a survey, IEEE Internet of Things (on print) (2016) 1–13.

[28] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, Z. Han, Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey, IEEE Communications Surveys & Tutorials 18 (4) (2016) 2546–2590.

[29] C. Pereira, A. Aguiar, Towards efficient mobile M2M communications: survey and open challenges, Sensors 14 (10) (2014) 19582–19608.

[30] H. C. Kuo, F. J. Lin, Performance management of IoT/M2M platforms, in: Communications and Electronics (ICCE), 2016 IEEE Sixth International Conference on, IEEE, 2016, pp. 119–124.

[31] A. H. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, M. Z. Sheng, IoT Middleware: A Survey on Issues and Enabling technologies, IEEE Internet of Things Journal X (X) (2016) 1–1. doi:10.1109/JIOT.2016.2615180.

[32] J. Granjal, E. Monteiro, J. S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Communications Surveys & Tutorials 17 (3) (2015) 1294–1312.

[33] A. Rajandekar, B. Sikdar, A survey of MAC layer issues and protocols for machine-to-machine communications, IEEE Internet of Things Journal 2 (2) (2015) 175–186. doi:10.1109/JIOT.2015.2394438.

[34] C. Schurgers, G. Kulkarni, M. B. Srivastava, Distributed on-demand address assignment in wireless sensor networks, IEEE Transactions on Parallel and Distributed Systems 13 (10) (2002) 1056–1065. doi:10.1109/TPDS.2002.1041881.

[35] T. Rault, A. Bouabdallah, Y. Challal, Energy efficiency in wireless sensor networks: A top-down survey, Computer Networks 67 (2014) 104–122. doi:10.1016/j.comnet.2014.03.027.

[36] H. S. Dhillon, H. Huang, H. Viswanathan, Wide-area wireless communication challenges for the internet of things, IEEE Communications Magazine 55 (2) (2017) 168–174.

[37] J. Li, Q. Sun, G. Fan, Resource allocation for multiclass service in IoT uplink communications, in: Systems and Informatics (ICSAI), 2016 3rd International Conference on, IEEE, 2016, pp. 777–781.

[38] K. Zheng, S. Ou, J. Alonso-Zarate, M. Dohler, F. Liu, H. Zhu, Challenges of massive access in highly dense lte-advanced networks with machine-to-

machine communications, IEEE Wireless Communications 21 (3) (2014) 12–18.

[39] M. Rausand, A. Hsyland, System Reliability Theory: Models, Statistical Methods, and Applications, Wescon/96doi:10.1109/WESCON.1996.554026.

[40] A. Shrestha, L. Xing, Quantifying application communication reliability of wireless sensor networks, International Journal of Performability Engineering 4 (1) (2008) 43–56.

[41] M. Weiner, M. Jorgovanovic, A. Sahai, B. Nikolie, Design of a low-latency, high-reliability wireless communication system for control applications, in: 2014 IEEE International Conference on Communications, ICC 2014, 2014, pp. 3829–3835. doi:10.1109/ICC.2014.6883918.

[42] L. Vangelista, A. Zanella, M. Zorzi, Long-range iot technologies: The dawn of lora, in: Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Springer, 2015, pp. 51–58.

[43] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, K. Wehrle, Security challenges in the IP-based Internet of Things, in: Wireless Personal Communications, Vol. 61, 2011, pp. 527–542. doi:10.1007/s11277-011-0385-5.

[44] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, Ddos in the iot: Mirai and other botnets, Computer 50 (7) (2017) 80–84.

[45] D. Bandyopadhyay, J. Sen, Internet of things: Applications and challenges in technology and standardization, in: Wireless Personal Communications, Vol. 58, 2011, pp. 49–69. arXiv:1105.1693, doi:10.1007/s11277-011-0288-5.

[46] A. Shrestha, L. Xing, A Performance Comparison of Different Topologies for Wireless Sensor Networks, 2007 IEEE Conference on Technologies for Homeland Security (2007) 280–285doi:10.1109/THS.2007.370059.

[47] A. Murthy, D. Han, D. Jiang, T. Oliveira, Lighting-Enabled Smart City Applications and Ecosystems based on the IoT, IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings (2015) 757–763doi:10.1109/WF-IoT.2015.7389149.

[48] D. Surie, O. Laguionie, T. Pederson, Wireless sensor networking of everyday objects in a smart home environment, in: ISSNIP 2008 - Proceedings of the 2008 International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2008, pp. 189–194. doi:10.1109/ISSNIP.2008.4761985.

[49] A. Varghese, D. Tandur, Wireless requirements and challenges in Industry 4.0, in: Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, 2014, pp. 634–638. doi:10.1109/IC3I.2014.7019732.

[50] M. T. Lazarescu, Design and field test of a WSN platform prototype for long-term environmental monitoring, Sensors (Switzerland) 15 (4) (2015) 9481–9518. doi:10.3390/s150409481.

[51] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet of Things Journal 1 (1) (2014) 22–32. arXiv:arXiv:1011.1669v3, doi:10.1109/JIOT.2014.2306328.

[52] A. Mahmood, N. Javaid, S. Razzaq, A review of wireless communications for smart grid (2015). doi:10.1016/j.rser.2014.08.036.

[53] X. Xiong, K. Zheng, R. Xu, W. Xiang, P. Chatzimisios, Low power wide area machine-to-machine networks: Key techniques and prototype, IEEE Communications Magazine 53 (9) (2015) 64–71. doi:10.1109/MCOM.2015.7263374.

[54] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation

Computer Systems 29 (7) (2013) 1645–1660. arXiv:1207.0203, doi:10.1016/j.future.2013.01.010.

[55] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE, IEEE, 2015, pp. 1–6.

[56] L. Sanchez, L. Muñoz, J. A. Galache, P. Sotres, J. R. Santana, V. Gutierrez, R. Ramdhany, A. Gluhak, S. Krco, E. Theodoridis, D. Pfisterer, SmartSantander: IoT experimentation over a smart city testbed, Computer Networks 61 (2014) 217–238. doi:10.1016/j.bjp.2013.12.020.

[57] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and near-Field Communication, 2010. doi:10.1002/9780470665121.

[58] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (4) (2002) 393–422. arXiv:1004.3164, doi:10.1016/S1389-1286(01)00302-4.

[59] R. Jurdak, A. G. Ruzzelli, G. M. P. O'Hare, Radio sleep mode optimization in wireless sensor networks, IEEE Transactions on Mobile Computing 9 (7) (2010) 955–968. doi:10.1109/TMC.2010.35.

[60] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecture directions for network sensors, in: Architectural Support for Programming Languages and Operating Systems (ASPLOS), Vol. 35, 2000, pp. 93–104.

[61] Specification Documents. Bluetooth SIG. (2012).

[62] Wibree forum merges with Bluetooth SIG., Nokia, 12 June 2007. (2007).

[63] C. Gomez, J. Oller, J. Paradells, Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology, Sensors (Switzerland) 12 (9) (2012) 11734–11753. doi:10.3390/s120911734.

[64] H. Snellman, M. Savolainen, J. Knaappila, P. Rahikkala, Bluetooth 5, Refined for the IoT, Silicon Labs White Paper.

[65] IEEE Computer Society, IEEE Std 802.15.4-2003 doi:10.1109/IEEESTD.2006.232110.

[66] Y. S. Shin, K. W. Lee, J. S. Ahn, Analytical performance evaluation of IEEE 802.15.4 with multiple transmission queues for providing QoS under non-saturated conditions, in: 2010 16th Asia-Pacific Conference on Communications, APCC 2010, 2010, pp. 334–339. doi:10.1109/APCC.2010.5679712.

[67] I. F. Akyildiz, X. Wang, W. Wang, Wireless mesh networks: A survey (2005). doi:10.1016/j.comnet.2004.12.001.

[68] L. Bedogni, A. Achtzehn, M. Petrova, P. Mähönen, L. Bononi, Performance Assessment and Feasibility Analysis of IEEE 802.15.4m Wireless Sensor Networks in TV Grayspaces, ACM Transactions on Sensor Networks 13 (1) (2017) 1–27. doi:10.1145/3021499.

[69] Thread Group, Thread Usage of 6LoWPAN, White Paper.

[70] Haolin Wang, Minjun Xi, Jia Liu, Canfeng Chen, Transmitting IPv6 packets over Bluetooth low energy based on BlueZ, Advanced Communication Technology (ICACT) (2013) 72–77.

[71] Zigbee Alliance, Zigbee Specification, Zigbee Alliance website (2008) 1–604.

[72] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, Y. F. Hu, Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards, Computer Communications 30 (7) (2007) 1655–1695. doi:10.1016/j.comcom.2006.12.020.

[73] ZigBee Alliance, ZigBee Home Automation Public Application Profile revison 25.

[74] ZigBee Alliance, ZigBee Smart Energy Profile Specification revision 1.

[75] A. N. Kim, F. Hekland, S. Petersen, P. Doyle, When HART goes wireless: Understanding and implementing the WirelessHART standard, in: IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, 2008, pp. 899–907. doi:10.1109/ETFA.2008.4638503.

[76] J. Song, S. Han, A. K. Mok, D. Chen, M. Lucas, M. Nixon, W. Pratt, WirelessHART: Applying wireless technology in real-time industrial process control, in: Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS, 2008, pp. 377–386. doi:10.1109/RTAS.2008.15.

[77] ISA Standard, Wireless systems for industrial automation: process control and related applications, ISA-100.11 a-2009.

[78] S. Petersen, S. Carlsen, WirelessHART versus ISA100.11a: The format war hits the factory floor, IEEE Industrial Electronics Magazine 5 (4) (2011) 23–34. doi:10.1109/MIE.2011.943023.

[79] Z-Wave Alliance, Z-Wave Protocol Overview 4th May.

[80] C. Gomez, J. Paradells, Wireless home automation networks: A survey of architectures and technologies, IEEE Communications Magazine 48 (6) (2010) 92–101. doi:10.1109/MCOM.2010.5473869.

[81] Insteon Alliance, Insteon Whitepaper: The Details, White Paper.
URL http://cache.insteon.com/pdf/insteondetails.pdf

[82] G. Martin, Wireless sensor solutions for home {&} building automation, EnOcean White Paper (2007) 1–7.
URL www.enocean.com

[83] DASH7 Alliance, DASH7 Alliance Wireless Sensor and Actuator Network Protocol VERSION 1.0, DASH7 Alliance Specification (2015) 1–69.

[84] M. Weyn, G. Ergeerts, R. Berkvens, B. Wojciechowski, Y. Tabakov, DASH7 alliance protocol 1.0: Low-power, mid-range sensor and actuator communication, 2015 IEEE Conference on Standards for Communications and Networking, CSCN 2015 (October) (2015) 54–59. doi:10.1109/CSCN.2015.7390420.

[85] B. Buckiewicz, Technical Overview of DECT ULE, LSR White Paper. URL https://www.lsr.com/white-papers/technical-overview-of-dect-ule

[86] K. Das, P. Havinga, Evaluation of DECT-ULE for robust communication in dense wireless sensor networks, in: Proceedings of 2012 International Conference on the Internet of Things, IOT 2012, 2012, pp. 183–190. doi:10.1109/IOT.2012.6402321.

[87] Keysight Technologies, Internet of Things (IoT) (2016). URL http://literature.cdn.keysight.com/litweb/pdf/5992-1217EN.pdf?id=2788751

[88] A. Bartoli, M. Dohler, J. Hernández-Serrano, A. Kountouris, D. Barthel, Low-power low-rate goes long-range: the case for secure and cooperative machine-to-machine communications, in: NETWORKING 2011 Workshops, Springer, 2011, pp. 219–230.

[89] Coronis Systems, Wavenis Technology Plateform, Product Summary.

[90] Machina Research, The need for low cost, high reach, wide area connectivity for the Internet of Things, Neul White Paper.

[91] Machina Research, LPWA Technologies: unlock new IoT market potential, LoRa Alliance White Paper, 2015.

[92] LoRa Alliance, Where does LoRa Fit in the Big Picture?, LoRa Alliance White Paper, 2015.

[93] M. Centenaro, L. Vangelista, A. Zanella, M. Zorzi, Long-Range Communications in Unlicensed Bands: the Rising Stars in the IoT and Smart City Scenarios (2015) 1–7arXiv:1510.00620.

[94] L. Collet, SIGFOX Expanding Internet of Things Network In 100 U.S. Cities to Meet Strong Market Demand, Tech. rep., SigFox (2016).

[95] SigFox Coverage.
URL https://www.sigfox.com/en/coverage

[96] F. Sforza, Communications system (2013).
URL https://www.google.com/patents/US8406275

[97] A. J. Berni, W. D. Gregg, On the Utility of Chirp Modulation for Digital Signaling, Ieee Transactions on Communications 21 (6) (1973) 748–751. doi:10.1109/TCOM.1973.1091721.

[98] LoRa Alliance, LoRa Specification v1.0, Tech. rep. (2015).

[99] LoRa Alliance, A technical overview of LoRa and LoRaWAN, LoRa Alliance White Paper, 2015.

[100] C. Goursaud, J. M. Gorce, Dedicated networks for IoT: PHY / MAC state of the art and challenges, EAI Endorsed Transactions on Internet of Things 1 (1) (2015) 1–11. doi:10.4108/eai.26.

[101] L. Bedogni, F. Malabocchia, M. Di Felice, L. Bononi, Indoor Use of Gray and White Spaces: Another Look at Wireless Indoor Communication, IEEE Vehicular Technology Magazine (2017) XX12–XX12doi:10.1109/MVT.2016.2598414.

[102] J. Cowan, On-Ramp Wireless rebrands as Ingenu and launches US-wide M2M wireless public network (2015).

[103] 3GPP GERAN Documentation (2014).

[104] W. Guibene, K. E. Nolan, M. Y. Kelly, Survey on Clean Slate Cellular-IoT Standard Proposals, in: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, IEEE, 2015, pp. 1596–1599.

[105] Ericsson, Ericsson and Orange trial Internet of Things (IoT) over GSM and LTE, Ericsson Press Release, 2015.

[106] 3GPP, Extended Coverage GSM (EC-GSM) for support of Cellular Internet of Things, Tsg geran wg1 (2015).

[107] Ericsson, Cellular Networks For Massive IoT, Ericsson White Paper, 2016.

[108] 3GPP, Service requirements for Machine-Type Communications (MTC), Tsg geran s1.

[109] 3GPP, System improvements for Machine-Type Communications (MTC), Tsg geran s2.

[110] 3GPP, Standardization of Machine-Type Communications (MTC), v0.2.4, Tech. rep. (2014).

[111] R. Ratasuk, N. Mangalvedhe, A. Ghosh, B. Vejlgaard, Narrowband LTE-M system for M2M communication, in: Vehicular Technology Conference (VTC Fall), 2014 IEEE 80th, IEEE, 2014, pp. 1–5.

[112] R. Ratasuk, N. Mangalvedhe, A. Ghosh, Overview of LTE enhancements for cellular IoT, in: Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015 IEEE 26th Annual International Symposium on, IEEE, 2015, pp. 2293–2297.

[113] 3GPP, Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE, Tsg geran r1.

[114] Nokia, LTE-M - Optimizing LTE for the Internet of Things, Nokia Networks White Paper, 2014.

[115] G. Americas, LTE and 5G Technologies Enabling the Internet of Things. URL http://www.5gamericas.org/files/3514/8121/4832/Enabling_IoT_WP_12.8.16_FINAL.pdf

[116] R. Young, D. Zhang, Introduction to "Clean Slate" cellular IoT radio access solution, Presentation (2014).

[117] 3GPP, New Study Item on Cellular System Suport for Ultra Low Complexity and Low Throughput Internet of Things, Tsg geran 65 (2014).

[118] A. Zaidan, B. Zaidan, M. Qahtan, O. Albahri, A. Albahri, M. Alaa, F. Jumaah, M. Talal, K. Tan, W. Shir, et al., A survey on communication components for IoT-based technologies in smart homes, Telecommunication Systems (2018) 1–25.

[119] G. Patti, L. Leonardi, L. L. Bello, A Bluetooth low energy real-time protocol for industrial wireless mesh networks, in: Industrial Electronics Society, IECON 2016-42nd Annual Conference of the IEEE, IEEE, 2016, pp. 4627–4632.

[120] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial Internet of Things: Challenges, Opportunities, and Directions, IEEE Transactions on Industrial Informatics.

[121] D. Hernandez, G. Peralta, L. Manero, R. Gomez, J. Bilbao, C. Zubia, Energy and coverage study of LPWAN schemes for Industry 4.0, in: Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM), 2017 IEEE International Workshop of, IEEE, 2017, pp. 1–6.

[122] E. Kartsakli, A. S. Lalos, A. Antonopoulos, S. Tennina, M. D. Renzo, L. Alonso, C. Verikoukis, A survey on M2M systems for mHealth: a wireless communications perspective, Sensors 14 (10) (2014) 18009–18052.

[123] J. Petäjäjärvi, K. Mikhaylov, R. Yasmin, M. Hämäläinen, J. Iinatti, Evaluation of LoRa LPWAN technology for indoor remote health and wellbeing monitoring, International Journal of Wireless Information Networks 24 (2) (2017) 153–165.

[124] K. Shahzad, B. Oelmann, A comparative study of in-sensor processing vs. raw data transmission using ZigBee, BLE and Wi-Fi for data intensive monitoring applications, in: 2014 11th International Symposium on Wireless Communications Systems (ISWCS), 2014.

[125] M. Pule, A. Yahya, J. Chuma, Wireless sensor networks: A survey on monitoring water quality, Journal of Applied Research and Technology 15 (6) (2017) 562–570.

[126] D. C. Marvin, L. P. Koh, A. J. Lynam, S. Wich, A. B. Davies, R. Krishnamurthy, E. Stokes, R. Starkey, G. P. Asner, Integrating technologies for scalable ecology and conservation, Global Ecology and Conservation 7 (2016) 262–275.

[127] W. F. Costa, R. Sousa, T. Giannini, B. Albertini, A. Saraiva, New Requirements of Biodiversity Research for Metadata on Models and Sensors on the Internet of Things and Big Data Era, Biodiversity Information Science and Standards 2 (2018) e25653.

[128] O. Berger-Tal, J. J. Lahoz-Monfort, Conservation technology: The next generation, Conservation Letters e12458.

[129] M. Lauridsen, H. Nguyen, B. Vejlgaard, I. Z. Kovacs, P. Mogensen, M. Sørensen, Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km^2 Area, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), 2017.

[130] L. Bedogni, A. Trotta, M. D. Felice, L. Bononi, Machine-to-machine communication over tv white spaces for smart metering applications, in: 2013

22nd International Conference on Computer Communication and Networks (ICCCN), 2013, pp. 1–7. doi:10.1109/ICCCN.2013.6614149.

[131] A. J. Wixted, P. Kinnaird, H. Larijani, A. Tait, A. Ahmadinia, N. Strachan, Evaluation of LoRa and LoRaWAN for wireless sensor networks, in: SENSORS, 2016 IEEE, IEEE, 2016, pp. 1–3.

[132] Nokia, LTE evolution for IoT connectivity, Nokia Networks White Paper, 2017.

[133] Y. Mo, C. Goursaud, J.-M. Gorce, Theoretical analysis of unb-based iot networks with path loss and random spectrum access, in: Personal, Indoor, and Mobile Radio Communications (PIMRC), 2016 IEEE 27th Annual International Symposium on, IEEE, 2016, pp. 1–6.

[134] O. Georgiou, U. Raza, Low power wide area network analysis: Can lora scale?, IEEE Wireless Communications Letters 6 (2) (2017) 162–165.

[135] J. Petäjäjärvi, K. Mikhaylov, M. Pettissalo, J. Janhunen, J. Iinatti, Performance of a low-power wide-area network based on lora technology: Doppler robustness, scalability, and coverage, International Journal of Distributed Sensor Networks 13 (3) (2017) 1550147717699412.

[136] LoRa Alliance, 2017 End of the year report, Tech. rep. (2017).

[137] K. Garvin, Ingenu Expands Global Network, Providing IoT Connectivity to over 29 Countries, and Growing, Ingenu Press Release.

[138] LTE-M and NB-IoT Commercial Launches.
URL https://www.gsma.com/iot/mobile-iot-commercial-launches/

[139] A. Bandeh-Ahmadi, R. Lin, Groundtruth partnership with Orange, Sierra Wireless, and NOKIA to demonstrate how next-generation wireless protocols can help smallholder farmers in the developing world, Groundtruth Press Release.

[140] N. K. Pratas, H. Thomsen, Č. Stefanović, P. Popovski, Code-expanded random access for machine-type communications, in: 2012 IEEE Globecom Workshops, GC Wkshps 2012, 2012, pp. 1681–1686. arXiv:1207.0362, doi:10.1109/GLOCOMW.2012.6477838.

[141] F. V. Azquez-Gallego, J. Alonso-Zarate, I. Balboteo, L. Alonso, DPCF-M: A Medium Access Control protocol for dense Machine-to-Machine area networks with dynamic gateways, in: IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC, 2013, pp. 490–494. doi:10.1109/SPAWC.2013.6612098.

[142] Y. Liu, C. Yuen, X. Cao, N. U. Hassan, J. Chen, Design of a scalable hybrid MAC protocol for heterogeneous M2M networks, IEEE Internet of Things Journal 1 (1) (2014) 99–111.

[143] M. Ndiaye, G. P. Hancke, A. M. Abu-Mahfouz, Software defined networking for improved wireless sensor network management: A survey, Sensors 17 (5) (2017) 1031.

[144] F. Montori, M. Gramaglia, L. Bedogni, M. Fiore, F. Sheikh, L. Bononi, A. Vesco, Automotive communications in lte: a simulation-based performance study, in: Proceedings of IEEE VTC-Fall, 2017.