Review

The Internet of Things vision: Key Features, Applications and Open Issues

Eleonora Borgia

PII: S0140-3664(14)00316-8
DOI: http://dx.doi.org/10.1016/j.comcom.2014.09.008
Reference: COMCOM 5011

To appear in: *Computer Communications*

Please cite this article as: E. Borgia, The Internet of Things vision: Key Features, Applications and Open Issues, *Computer Communications* (2014), doi: http://dx.doi.org/10.1016/j.comcom.2014.09.008

The Internet of Things vision: Key Features, Applications and Open Issues

Eleonora Borgia

Institute of Informatics and Telematics (IIT)
Italian National Research Council (CNR)
via G.Moruzzi 1, 56124 Pisa, Italy
Phone: +39 050 315 2407; Fax: +39 050 315 2593
Email address: eleonora.borgia@iit.cnr.it

Abstract

The Internet of Things (IoT) is a new paradigm that combines aspects and technologies coming from different approaches. Ubiquitous computing, pervasive computing, Internet Protocol, sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbiotic interaction. The smart object is the building block of the IoT vision. By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and interact/control the physical world, but also to be interconnected, to each other, through Internet to exchange data and information. The expected huge number of interconnected devices and the significant amount of available data open new opportunities to create services that will bring tangible benefits to the society, environment, economy and individual citizens. In this paper we present the key features and the driver technologies of IoT. In addition to identifying the application scenarios and the correspondent potential applications, we focus on research challenges and open issues to be faced for the IoT realization in the real world.

Keywords: Internet of Things (IoT), RFIDs, sensors, Machine-to-Machine (M2M) communications, standardization

1. Introduction

Due to the huge advancements in the fields of electronics and the deployments of wireless communication systems, mobile devices and ubiquitous services (providing anytime-anywhere connectivity to the users) spread rapidly over the past decade. Today, however, the role played by devices is no longer limited to connect users to the Internet, but it has been expanding becoming an opportunity to interlink the physical world with the cyber world [1], leading to the emergence of Cyber-physical systems (CPS) [2, 3]. The notion of CPS refers to a next generation of embedded ICT systems where computation and networking are integrated with physical processes and they control and manage their dynamics and make them more efficient, reliable, adaptable and secure [4–9]. Information about physical processes, for example gathered through sensors, are transferred, processed, and used in the digital world, but they may also affect physical processes through feedback loops, for example by using actuators [1]. The peculiarity of CPS is that the ICT system is designed together with the physical components to maximize the overall efficiency, thus being in contrast with classic embedded systems where the goal is to include electronics/computing/communication/abstraction in an already operating physical world.

CPS will have a great impact on the future society and humans, and their social networks, will play a central role in bridging the cyber, physical and social worlds [10–13]. Through their interactions with ICT devices, they will

gain access to the virtual world affecting the way information is distributed and they will give their contribution to build/modify the cyber infrastructure.

The economic value associated with the CPS will also be large. In the 2013 report[1], McKinsey Global Institute has identified twelve technologies that, by 2025, will have massive, economically disruptive impact, driving profound changes in many dimensions: in citizens' lives, in business and across the global economy. Specifically, four technologies fall within CPS: *i)* automation of knowledge work, *ii)* Internet of Things, *iii)* advanced robotics, and *iv)* autonomous/near-autonomous vehicles. Among them, the Internet of Things (IoT), with an estimated value of 36 trillion of dollars, is considered the CPS paradigm with the highest economic impact [14].

IoT refers to an emerging paradigm consisting of a continuum of uniquely addressable *things* communicating one another to form a worldwide dynamic network. The origin of IoT has been attributed to members of the Auto-ID Center at MIT, the development community of the Radio-Frequency Identification (RFID), around 2000 [15]. Their idea was visionary: they aimed at discovering information about a tagged object by browsing an Internet address or a database entry corresponding to a particular RFID. To address the above idea, they worked on the development of the *Electronic Product Code (EPC)*, i.e., a universal identifier that provides a unique identity for every physical object [16], with the aim of spreading the use of RFID in worldwide networks. Today, the concept of *thing* is more general and is not limited to RFID only. A *thing* can be any real/physical object (e.g., RFID, sensor, actuator, spime[2], smart item[3]) but also a virtual/digital entity, which moves in time and space and can be uniquely identified by assigned identification numbers, names and/or location addresses. Therefore, the *thing* is easily readable, recognizable, locatable, addressable

[1] http://www.slideshare.net/brandsynapse/mgi-disruptive-technologiesfullreportmay2013?related=1

[2] Spimes are objects that can be tracked in space and time and during their entire lifespan univocally through an identifier and the use of technologies such as RFID, GSM. They are very economical and eco-friendly (i.e., they can be recycled) and can be improved over time. For example, the recording of their entire life cycle can be used to revise and modify the object itself or some specific behavior.

[3] Smart items have very advanced features such as to adopt autonomous and proactive behavior. For instance, they are able to generate traffic autonomously for certain purposes, or execute data processing or perform communication in a collaborative form.

Figure 1: The emerging IoT scene.

and/or controllable via Internet. Moreover, this new generation of devices is *smart* thanks to the embedded electronics allowing them to sense, compute, communicate, and integrate seamlessly with the surrounding environment. The association "one device/one function" disappears, but the whole set of objects becomes the place where the function is activated, resulting all widely distributed. The emerging IoT scenario is depicted in Figure 1 [17]. Smart devices will form the so-called *sensory swarm* and will be the majority of the system. They will be extremely heterogeneous in terms of resource capabilities, lifespan and communication technologies. They will exceed classic devices such as smartphones and tablets, which, on the contrary, will form a way for accessing Internet [18]. At the core, instead of having traditional computation systems, the *Cloud* will provide the abstraction of a set of computers and will offer computation and storage services. It is envisaged that the number of connected things[4] will exceed 7 trillion by 2025 [19], with an estimate of about 1000 devices per person. A part of them will be wearable [20], but the majority will be in the infrastructure. In this vision, humans will be completely immersed in the world of technology, leading to the so-called *Immersed human*.

To make the concept of IoT more concrete, let's consider the city ecosystem as an example and how the city of the future will look like [21]. The city is the economic and social life core of a nation. Today, half of the global population is concentrated in the cities and consume its resources (e.g., light, water) every day. Urban population is constantly increasing and this implies an inevitable increase in the resource consumption that undermines the environment. Quality, sustainability and security are crucial and unavoidable issues for the city. The realization of sustainable and secure cities requires intelligent solutions that ensure the efficiency at multiple levels aiming to: *i)* a more aware and optimized usage of the offered resources, *ii)* a minimization of environmental impact, for example by reducing CO_2 emissions, and *iii)* a tangible increase in the life quality in terms of safety, health, and wellness. Indeed, a smart city is a city that operates simultaneously on two levels: one physical and one virtual. The smart city provides a management of its services (e.g., transport, energy, lighting, waste management, entertainment) through the widespread usage of ICT technologies. Such technologies provide a logical/virtual infrastructure that controls and coordinates the physical infrastructure in order to adapt the city services to the actual citizen needs, while reducing waste and making sustainable the city [21]. IoT will be essential to turn a traditional city into a *smart city* and the traditional

[4]From now on we will use the terms *thing* and *object* interchangeably.

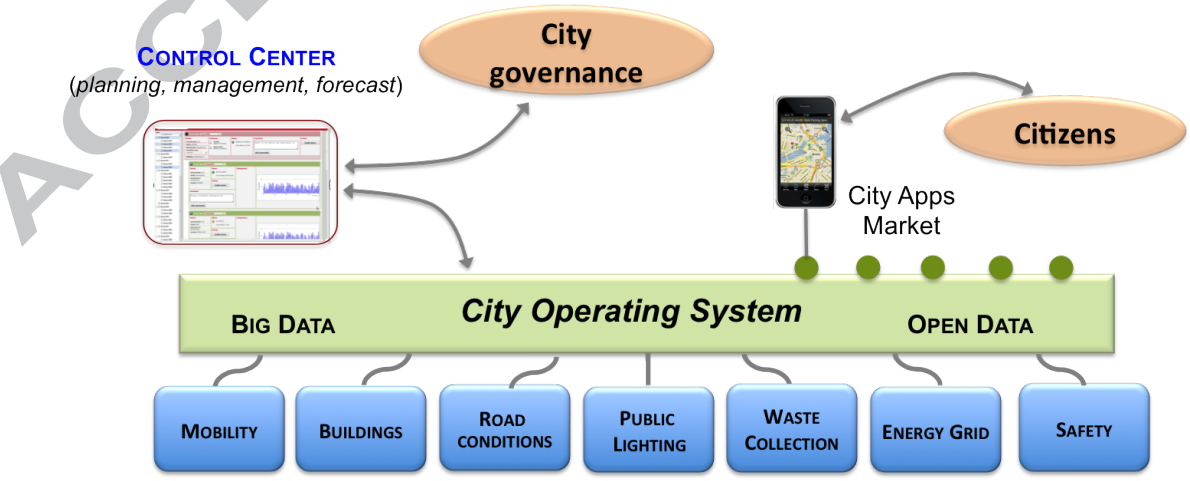

Figure 2: Schematic representation for smart city.

and more emerging sectors such as mobility, buildings, energy, living, governance will also benefit of it. For example, smart mobility services will be created to provide effective tools to the citizens to accurately plan their journeys with public/private transportations, bike/car/van sharing services or multi-modal transport systems. Intelligent traffic lights and static/mobile sensors spread in the city can be used to automatically manage the traffic, to monitor/predict situations of traffic jam and to warn drivers about the presence of critical situations, also proposing them alternative routes/means in real time. At the same time, data gathered by sensors [22, 23] will help municipalities to monitor the condition of the roads (e.g., presence of potholes, slippery, not draining roads), to plan the waste collection service (e.g., volumetric sensors may measure filling level of trashcans and report to sanitation headquarters when full/close to full), to perform environmental monitoring and territorial prevention by measuring water level, air pollution, presence of a certain component (i.e., percentage of allergenic pollen or radiation in the air) [24]. Energy management will also be optimized by using a smart grid for monitoring and modify consumes in town and buildings through actuators and by using renewable energies for the production [25–28]. Figure 2 provides a schematic representation of the smart city. It will be equipped with a network of sensors, cameras, screens, speakers, smart meters, and thermostats that will collect information. The gathered information, the so-called "Big Data" (the name refers to its large volume and its heterogeneity in terms of content and data representation), will not be used for the improvement of just a single service/application, but it will be shared among different services [15]. To this aim, a common platform for operational management of the city - a sort of City Operating System - will be responsible for managing, storing, analyzing, processing, and forwarding it where needed within the city to improve services and adapting to human needs. This management layer, no longer vertical but horizontal, will ensure interoperability, coordination, and optimization of individual services/applications through the analysis of information flows. Citizens/authorities will access the services offered by the platform through their applications, will consume them and will actively participate by creating additional content that will be provided as further input to the City Operating System.

As also highlighted by the above example, IoT will bring tangible benefits to the environment, the society, individuals and business with the creation of new intelligent applications, services and products in various domains whilst ensuring the protection and privacy of information and content exchanged [29]. The economic value associated with IoT will be large and the benefits enormous: for example, it is envisioned a US GDP increase by 2%-5% by 2025 with a faster productivity growth and an increase of job creation [30]. IoT will offer a potential to affect the economic activity across industries, influencing their strategic decisions, their investments and their productivity. Currently, about 20% of the GDP comes from industries working in the digital, while the majority of the GDP (about 80%) comes from primarily physical industries. IoT will bring those industries that are primarily physical (i.e., agriculture, construction, manufacturing, energy, transportation, healthcare) closer to the cyber world and will radically change their way of making business. At the same time, thanks to IoT, the largest software companies will make a shift to the physical world. For instance, recently Google acquired a company producing thermostats to enter its trademarks in the smart home world. Another example is IBM that is interested in intelligent solutions for traffic management and smart grid. Future business and marketing strategies of Google, Facebook, Apple, IBM are clearly delineated: the future market is the IoT, where capital investments are focused and where it is essential to be present and make great effort not to be left behind and lose its own competitiveness.

From the above description it is clear that, for the IoT vision to successfully emerge, a number of different technical challenges need to be faced and solved. They range from hardware, architecture, communication, discovery, data processing, data and network management, power and energy storage, security and privacy to cite a few of them. The main purpose of this paper is to draw a picture of the IoT paradigm. We will focus on the technologies enabling

the underlying IoT fabric, and on the current IoT research activities, highlighting the most significant contributions and solutions proposed over the recent years. Emphasis is also put on standardization activities, which represent a central pillar for the IoT realization. Indeed, it is a common understanding that an effort is required to design standard solutions thus avoiding their excessive fragmentation. The industrial perspective has also a very important role in the success of the IoT paradigm. We will discuss the key strategic industrial priorities providing an overview of the main sectors where industries are making significant investments for the mid- and long- term.

The remainder of the paper is organized as follows. Section 2 introduces the concepts at the basis of the IoT paradigm and the different visions expressed over the years by different bodies. Section 3 is devoted to the presentation of the key technologies involved in IoT. Section 4 explores the impact of IoT on the economy and on the society by providing an overview of the potential IoT applications. In Section 5 we analyze the IoT requirements, focusing also on those specific features needed to support the IoT traffic, while Section 6 identifies the major milestones and challenges for the IoT deployment in the real world. In Section 7, we give an overview of the growing number of initiatives connected with the IoT domain, while in Section 8 we provide a brief summary of other emerging aspects that revolve around the IoT world. Finally, Section 9 concludes the paper.

2. IoT: different visions for a novel paradigm

The growing interest that scientific research as well as marketing and sales strategies raises onto the IoT paradigm has the inevitable consequence that there is not a clear and unambiguous definition of IoT. This is mainly due to the different underlying visions with which standards organizations and research centers, enterprises and various alliances (each one with a different background and driven by specific interests and purpose) look at this paradigm. The meaning of the term continuously evolves also because technology and the ideas behind it change themselves over time.

The term was coined by Kevin Ashton, one of the founders of the original Auto-ID Center at MIT, who introduced it in 1999 during a presentation held at Procter&Gamble (P&G). He imagined a world where Internet is connected to the physical world through ubiquitous sensors and a platform based on real-time feedbacks, which have a huge potential to enhance comfort, security and control of our lives. A few years later, members of the same MIT group used again this concept, defining IoT as: "*an intelligent infrastructure linking objects, information and people through the computer networks, and where the RFID technology found the basis for its realization* [31]".

However, only in 2005, when the International Telecommunication Union (ITU) published its first report on the subject, the term "Internet of Things" began official and relevant to researchers, industries and end-users. In [32], ITU explains its vision: "*a new dimension has been added to the world of information and communication technologies (ICTs): from anytime, any place connectivity for anyone, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks - an Internet of Things*". Here the emphasis is on the fact that not only RFIDs, but also a high number of different objects - univocally addressable - constitute the underlying fabric of IoT.

From 2005 on, the number of IoT definitions, and the related activities, have run up depending on the type of organization looking at this paradigm. In [33], authors report a number of IoT visions proposed over the past years. Specifically, they distinguish three categories: *i) Things oriented*, where the focus is on the "objects" and on finding a paradigm able to identify and integrate them, *ii) Internet oriented*, where the emphasis is on the networking paradigm and on exploiting the IP protocol to establish an efficient connection between devices, while simplifying IP so that it can be used on devices with very limited capacity, and *iii) Semantic oriented*, which aims to use semantic technologies, describing objects and managing data, to represent, store, interconnect, and manage the huge amount of information

provided by the increasing number of IoT objects. Authors conclude that IoT is the result of the convergence of these different visions.

Another definition comes from the Cluster of European Research projects on the Internet of Things (CERP-IoT), which proposed its IoT vision in 2009. According to CERP-IoT, IoT blends together different concepts and technical components that come from Pervasive Computing, Ubiquitous Computing and Ambient Intelligence, and enhances them. IoT is seen as: *"a dynamic global network infrastructure with self capabilities based on standard and interoperable communication protocols where physical and "virtual" things have identities, physical attributes, virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network"* [34]. Hence, the real and physical world is in symbiotic interaction with the digital and virtual world. Physical objects have virtual counterparts representing them, and that become themselves active parts of the process. In addition, IoT enable people and things to be connected not only "Anytime" "Anywhere" with "Anyone" and "Anything", but also use any type of location or network and any available service. Hence, two additional concepts, i.e., "Any path/network" and "Any service", are introduced to complete the picture forming the so-called *6A vision*.

The CERP-IoT vision has been recently extended in [35, Chapter 1] by incorporating two different concepts: *i)* the Web 2.0, as a massive user-interaction is expected, and *ii)* the self-sustainability, especially in respect of possible benefits for individual participants. In particular, regarding the Web 2.0 technology, its primary advantage is the use of simplified and intuitive interfaces to enable users to provide web contributions, regardless of their technical expertise. This is fundamental as the interaction between things and users will be one core issue in the future Web of Things. Combining then the various concepts, authors have summarized their own IoT vision as: "*the future Internet of Things links uniquely identifiable things to their virtual representations in the Internet containing or linking to additional information on their identity, status, location or any other business, social or privately relevant information at a financial or non-financial pay-off that exceeds the efforts of information provisioning and offers information access to non-predefined participants. The provided accurate and appropriate information may be accessed in the right quantity and condition, at the right time and place at the right price. The Internet of Things is not synonymous with ubiquitous/pervasive computing, the Internet Protocol (IP), communication technology, embedded devices, its applications, the Internet of People or the Intranet/Extranet of Things, yet it combines aspects and technologies of all of these approaches* [35, Chapter 1]".

In addition to smart objects, another fundamental component for the realization of the IoT vision is represented by Machine-to-Machine (M2M) communications. The term M2M is deliberately general to emphasize that it does not refer to any specific communication technology, but rather to a number of both wired and wireless technologies that allow devices to communicate. This vagueness has given rise to an intense debate about how much actually innovative is such communication paradigm, resulting in two contrasting schools of thought. On the one hand, the more conservative and cautious vision does not consider M2M completely novel, but rather the natural extension of embedded systems. On the other hand, the more looking-forward vision looks at M2M as a completely revolutionary technology able to radically change the world, as it has been in the past with the era of computer first, and Internet then. Regardless of the paradigm prospective, M2M communications essentially deal with combining electronics, telecommunication and information technologies in order to connect from billion to trillion of devices and remote systems, and are characterized by low power, low cost and low human intervention. The following definition was provided by the ETSI Technical Committee on Machine-to-Machine Communications (ETSI TC M2M) [36]: "*Machine-to-Machine (M2M) communication is the communication between two or more entities that do not necessarily need any direct human intervention*". The novelty of the paradigm does not lie in the technology used for communication, rather in

the environment, where runs consisting in a number of devices that grow quickly, and in the way of interaction, which does not require any form of human intervention.

3. IoT Driver Technologies

The realization of the IoT vision described above goes through an inevitable evolution in the network and services' infrastructure. The approach largely used by current systems is called "silo" or "stove-pipe" because of its vertical approach: each application is built on its proprietary ICT infrastructure and dedicated devices (see Figure 3). Similar applications do not share any features for managing services and network, resulting in unnecessary redundancy and increase of costs. As explained in the smart city example, this totally vertical approach should be overtaken by a more flexible and horizontal approach, where a common operational platform will manage the network and the services, and will abstract across a diverse range of data sources to enable applications to work properly. As shown by Figure 4, applications will no longer work in isolation, but will share infrastructure, environment and network elements, and a common service platform will orchestrate on behalf of them [15]. Figure 4 also shows the three different phases with which the physical-cyber world interaction takes place. Specifically, they are: *i)* collection phase, *ii)* transmission phase, and *iii)* process, management and utilization phase. Each phase is characterized by different and interacting technologies and protocols and has different purposes and functions as discussed below:

i) Collection phase: it refers to procedures for sensing the physical environment, collecting real-time physical data and reconstructing a general perception of it. Technologies such as RFID and sensors provide identification of physical objects and sensing of physical parameters, while technologies such as IEEE 802.15.4 or Bluetooth are responsible for data collecting.

ii) Transmission phase: it includes mechanisms to deliver the collected data to applications and to different external servers. Methods are therefore required for accessing the network through gateways and heterogeneous technologies (e.g., wired, wireless, satellite), for addressing, for routing (e.g., LEACH, RPL, Trickle).

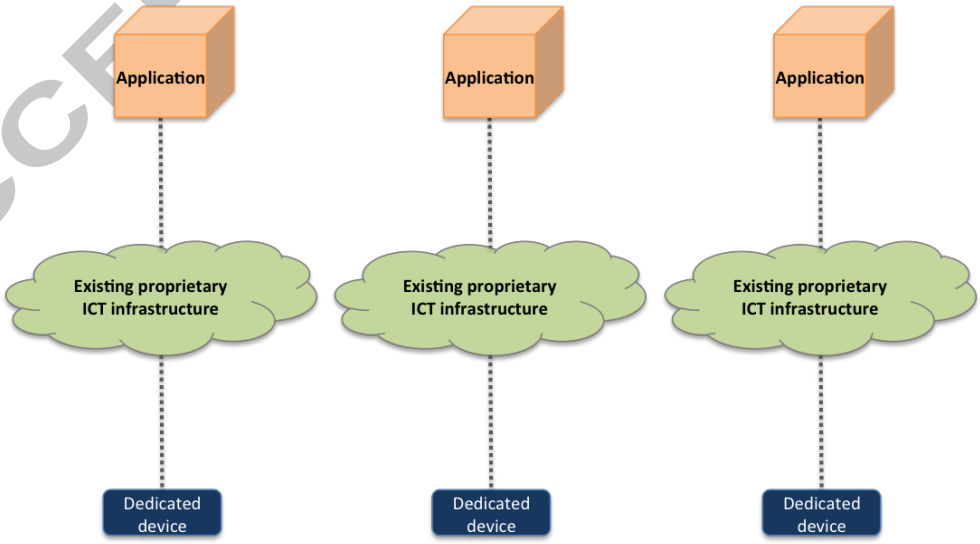

Figure 3: Classic representation for applications seen as vertical silos.

iii) Processing, managing and utilization phase: it deals with processing and analyzing information flows, forwarding data to applications and services, and providing feedbacks to control applications. In addition, it is responsible for critical functions such as device discovery, device management, data filtering, data aggregation, semantic analysis, and information utilization.

The remaining of the section is devoted to describe each phase and the main features of major IoT technologies. The interested readers may refer to specific standards and references herein for further information.

3.1. Collection phase

The first step towards IoT is the collection of information about the physical environment (e.g., temperature, humidity, brightness) or about objects (e.g., identity, state, energy level). Data acquisition is encompassed by using different sensing technologies attached to sensors, cameras, GPS terminals, while data collection is generally accomplished by short range communications, which could be open source standard solutions (e.g., Bluetooth, ZigBee, Dash7, Wireless M-BUS) as well as proprietary solutions (e.g., Z-Wave, ANT).

A fundamental role is covered by the RFID technology [37, 38]. RFID allows to identify objects, people or animals, store information about them and transfer it via wireless communication to other electronic devices. The RFID system consists of two main components: the tag and the reader. The tag is directly applied to an object and identifies it through the Electronic Product Code (EPC), while the reader is the element that collects data from the tag and transmits it to the Internet world. There are two main types of RFID tags: passive and active. The former has no power supplies and can transmit data by using the energy that the reader emits during its passage. Passive tags are very affordable since they are very small, inexpensive and have potentially long life. Their main drawback is that the area in which the tag-reader transmission may take place is very limited (3 m [39]). On the contrary, active tags are equipped

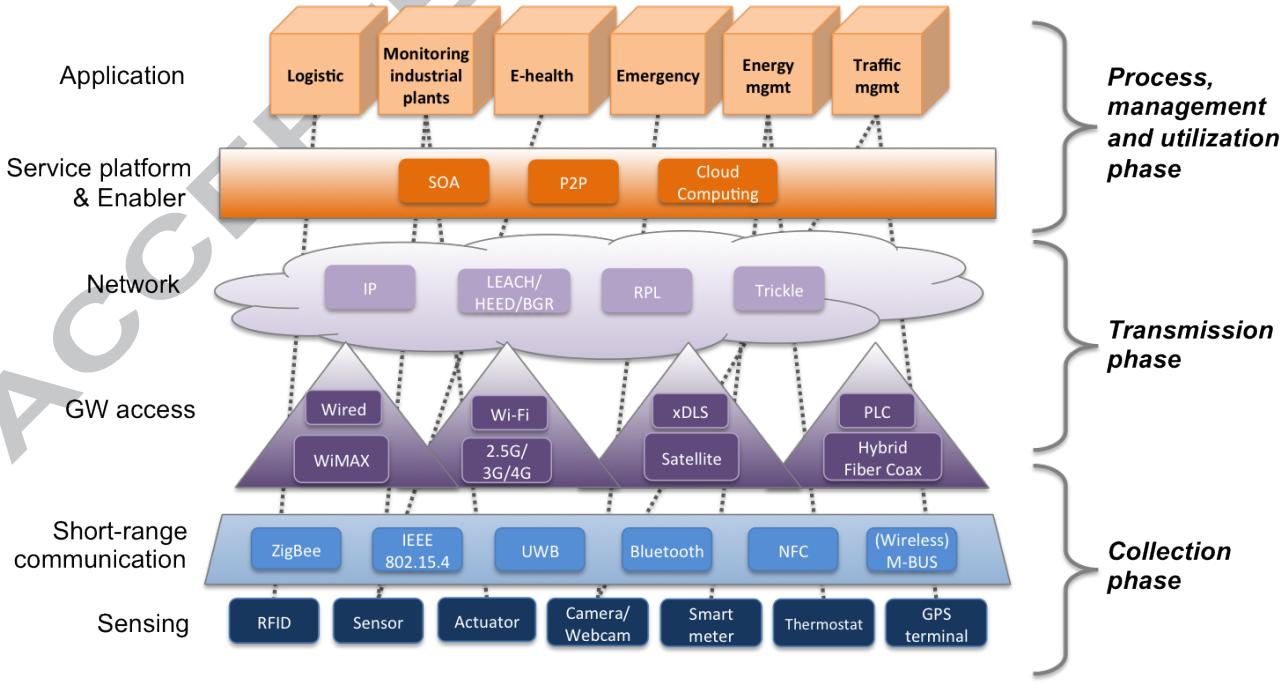

Figure 4: Horizontal representation for IoT applications. A non-exhaustive list of technologies and protocols is shown.

Table 1: Characteristics of the main technologies used for collecting data in IoT

Technology	Example of devices	Capabilities	Data rate	Maximum distance	Reference standard	Application
RFID	book/CD/DVD tag, car-sharing cards, RFID passports, RFID badge	Identification, storing, communication	up to 640 kbps	3-10 m	ISO/IEC 18000	transportation, logistics, tracking, animal ID, retail, access control, payment
Sensor	Enviromental monitoring sensors, wearable sensors, digital camera	Sensing, storing, processing, communication	250 kbps	10-100 m	IEEE 802.15.4, ZigBee, Wireless HART, ISA 100	health/environmental/ industrial monitoring, intelligent agriculture, surveillance
NFC	Smartphones, ticket stamping machine, parking meter	Communication	106-424 kbps	$\leq$10 cm	ISO/IEC18092/ECMA-340, ISO/IEC21481/ECMA-352, ISO/IEC14443	sharing/access information, access control, contactless payment

with their own power supply (e.g., a battery), thus covering greater distances when communicating and performing more complex operations (e.g., they may have sensors installed to monitor the environment). Obviously, the duration of the battery affects their lifetime. Transmissions between tags and readers can take place in four different frequency bands, which are generally used for different application scenarios: Low-frequency (LF) operating in the 125/134 kHz and 140/148.5 kHz ranges, High-frequency (HF) operating at 13.56 MHz, Ultra-high frequency (UHF) operating at 915 MHz (US) and at 868 MHz (Europe), 2.4 GHz and higher (Microwave tags).

Another essential technology for the development of IoT is Wireless Sensor Networks (WSNs) [40]. WSNs are a powerful technology for gathering and processing data in a large variety of domains, from environmental monitoring [24] to intelligent agriculture [41]. Traditional WSNs consist in a high number of static and resource constrained sensor nodes deployed in an area to sense a certain phenomenon, e.g., temperature, and humidity. Sensors are usually powered by small battery, have a limited lifetime and scarce computational and memory capabilities. Sensed data is then transmitted wirelessly via multi-hop communications towards one or a small set of sink nodes, which are more powerful devices where the collected information is elaborated. More recently, WSNs with Mobile Elements (MEs) have gained popularity [42–44]. In this case, MEs move in the network and collect opportunistically data from sensors whenever they happen to be in contact [42, 45–48]. As consequence, the network density is reduced to form sparse WSNs (i.e., where sensor nodes cannot communicate directly), the energy consumption is distributed more uniformly in the network, and the network lifetime increases [49, 50]. Independently of the network topology, sensors and sinks mainly operate in the 2.4 GHz band with a rate of 250 kbit/s to exchange data. Predominant standards commonly used in WSN communications include: IEEE 802.15.4, ZigBee [51, 52], Wireless Highway Addressable Remote Transducer Protocol (HART).

In the last ten years, WSNs have triggered intensive research activities which have produced a large body of literature addressing legacy networking such as MAC [53], routing [54] and transport protocols [55], connectivity and topology control [56–58]. However, further works are still expected to increase the energy efficiency of WSN operations [59–62], usage of sensor networks in challenging environments, like underground and underwater [63–68] and intermittently connected networks [69], and to integrate the sensors networks in the IoT world [70]. In the IoT framework, an important role is covered by Low-power wireless personal area networks (LoWPAN) [63, Chapter 3], [71, 72], i.e., networks are made up of sensor nodes which exploit the IEEE 802.15.4 standard for energy-efficient wireless communications [52].

An additional way to collect data is through the Near Field Communication (NFC) technology[5]. NFC is a communication technology that enables devices to share information wirelessly by touching them together or bringing them into proximity. It can be useful for sharing personal data (e.g., contacts/business cards, videos, photos), making transactions, accessing information from smart posters or providing credentials for access control systems with a simple touch. NFC can be considered as an evolution of RFID as it is built upon RFID systems, but, differently from it, NFC allows bidirectional communications. Specifically, when two NFC devices are located at a distance lesser than 4 cm, a peer-to-peer communication between them is created, and both devices are allowed to send and receive data. NFC operates at 13.56 MHz on ISO/IEC 18000-3 air interface with maximum speed of 424kbps.

The Bluetooth technology is also used for sending data among devices located at a short distance. Bluetooth was originally designed for replacing wire communications with low power wireless communications [73]. Basically, devices form specific structures to communicate, named *piconet*. In a piconet, a device assumes the role of master and all the others are slaves, for a maximum of seven slaves. The master decides which slave may access the channel. Bluetooth systems operate in the 2.4 GHz band with original data rate of 1Mbps up to the most recent 24Mbps.

3.2. Transmission phase

Once data is gathered through sensing technologies, it needs to be transmitted across the network so that applications can consume it. Heterogeneous communication technologies form the backbone to access the network [74]. Among the wired technologies, the reference standard is Ethernet (IEEE 802.3), supporting transmissions from 10Mbps to 100Gbps over twisted-pair coppers, coaxial cables, and optical fibers. The main advantage is that transmissions over wired networks are reliable and robust as they are less susceptible to errors and interference phenomenona. However, the need to physically connect devices to allow communications is costly and requires work in case of changes. Therefore, a common way to access the network is through Wireless LAN (WLAN). In this case, wireless devices transmit and receive packets to/from a base station, which is connected to the Internet, within a radius of few tens of meters. There are several wireless technologies with different transmission rates and covering different distances [75]. The WiFi family (IEEE 802.11a/b/g/n) may operate in different frequency bands (2.4GHz or 5GHz) by implementing different modulation schemes. Data communications may reach up to 54Mbps, supporting distances up to 100m. The IEEE 802.11n version includes the possibility of using MIMO (multiple-input multiple-output) antennas to increase the available bandwidth for transmission/reception. WiMAX (IEEE 802.16) is the corresponding wireless communication standard for longer distances (up to kilometers). It operates in a very wide spectrum (i.e., 2-66GHz) with data rate up to 70Mbps. It is a connection-oriented technology, thus a station cannot transmit data until the base station has not allocated a channel for it. This allows also to support QoS [76]. Broadband technologies (i.e., xDSL) are generally used for connecting home end systems to the Internet. They have been conceived to support asymmetrical communications to allow higher data rate from the Internet to home, as home users are more likely to be consumer instead of being producer of information. There exists a variety of transmission rates reaching very impressive speeds: from 12Mbps up to 55Mbps for downstream, and from 1Mbps to 20Mbps for upstream. Cellular networks (GSM, GPRS, UMTS, HSPA+ and LTE) play a central role in the way of accessing the network. Specifically, emerging LTE technologies [77] offer users the possibility to be connected in a dispersed as well highly connected and mobile environment, enabling not only voice exchange but also high value services (e.g., ubiquitous multimedia services [78]) thanks to the allowed high data rate. Satellite communication technologies can also be used as a means to connect to the Internet. They are particularly useful for users located in remote areas that cannot

[5] http://nfc-forum.org/what-is-nfc/

Table 2: Characteristics of the main access networks in IoT

Technology	Reference standard	Transmission medium	Frequency bands	Data rate	Maximum distance	Limitations
Ethernet	IEEE 802.3 u/z	twisted-pair copper wire, coaxial cable, optical fiber	—	10 Mbps, up to 100 Gbps	100 m, up to 50-70 km	shared medium, physical connection among devices
WiFi	IEEE 802.11 a/b/g/n	wireless	2.4 GHz, 5 GHz	1-54-600 Mbps	up to 100 m	sensitive to the presence of household appliances, interference among WiFi communications
WiMAX	IEEE 802.16 a/d/e/m	wireless	2-66 GHz	up to 70 Mbps	up to 50 - 80 km	low practical data rate, sensitive to weather conditions, high installation and operational costs
xDLS	ADSL, ADSL 2+, VDSL	twisted-pair copper wire, coaxial cable	up to 2.2 MHz	12-55 Mbps (d) 1-20 Mbps (u)	5.4-1.3 km	asymmetrical communication
Cellular	GSM,GPRS, UMTS, HSPA+, LTE	wireless	900-1800 MHz 2100-1900 MHz 800-2600 MHz	9.6 kbps, 56-114 kbps, 56 Mbps (d)/22 Mbps (u), 300 Mbps (d)/75 Mbps (u)	macro/micro/pico/ femto cells (10 m - 100 km)	limited wireless spectrum
Satellite	BSM, DVB-S, DVB-TS	wireless	4-8 GHz (C band), 10-18 GHz (Ku band), 18-31 GHz (Ka band)	16 kbps-155 Mbps	GEO sat.: 35786 km MEO sat.: 500-15000 km LEO sat.: 200-3000 km	280 ms propagation delay, huge launching cost, almost impossible repairing
PLC	HomePlug AV, IEEE 1901	electrical power system	1-30 MHz	>100 Mbps	up to 1500 m to the premise, up to 100 m between devices	mutual interference with other technologies

access to broadband connections, where deploying terrestrial connection is costly, or as a way to cross the sea/ocean. Basically, a satellite receives a transmission on a frequency band, regenerates the signal, and transmits it over another frequency. The main drawback is that, due to the large Earth-satellite distances, a propagation delay of 280ms is introduced in the communication.

Wireless technologies, due to their flexibility, will be the main communication paradigm for the IoT. However, the limited wireless spectrum available for cellular networks constitutes a major constraint in the widespread use of these wireless technologies. To overcome this limitation, several approaches are under active research: cognitive radio networks, opportunistic networking, and heterogeneous networks (possibly) with offloading. The research on cognitive radio networks is aimed at exploiting the wireless spectrum in an efficient way by dynamically allocating the spectrum to secondary users when the primary users (who hold the spectrum license) are not using it [44, 79, 80]. Effective spectrum sensing algorithms [81], to verify the presence of primary users [82, 83], and the assignment of the spectrum to the users [84, 85] are key components of a cognitive radio network. This is a very active research area but several challenges are still to be addressed to solve the vulnerabilities of these networks [83, 86]. Opportunistic networks [87] exploit, whenever possible, direct device-to-device communications (e.g., by exploiting WiFi of Bluetooth) to optimize the usage of the spectrum by using short-range wireless links to reduce the interference on the radio channels and the usage of scarce spectrum available for cellular networks. Opportunistic networks be-

long, together with WSN, to the class of mobile multi-hop ad hoc networks [88]. This class of networks includes other self-organizing and infrastructure-less networking paradigms that can be worth using in the IoT world such as wireless mesh networks [89] and vehicular networks [90], which are still under active development [91, 92]. The availability of several medium/short range wireless technologies, which can help to optimize the use of the scarce wireless medium, represent an interesting opportunity for offloading the traffic from congested cellular networks and to make a more efficient use of the scarce spectrum. Therefore, designing effective mechanisms for guaranteeing seamless handovers among these technologies is a very important and hot research issue [93, 94] that is triggering intense research activities [94–98].

Another important technology to gain access to Internet is the Power Line Communications (PLC) that carries data by exploiting the electrical power system as transmission medium [99]. Generally, it is used for smart meters as well as Home Area Networks (HAN), but can be used as alternative to xDLS providing asymmetrical transmissions (i.e., 256 kbps in upload and 2.7 Mbps in download). The main drawback is the mutual interference among PLC and other technologies, e.g., radio interference with signals on frequencies used by amateur radio groups.

3.3. Processing, managing and utilization phase

In this phase, information flows are processed and then forwarded to applications. The Service Platform & Enabler covers a fundamental role for managing the above operations. It is crucial for hiding the heterogeneity of hardware, software, data formats, technologies and communication protocols characterizing IoT [100]. It is responsible for abstracting all the features of objects, network, and services, and for offering a loose coupling of components. Additional features are service discovery and service composition.

To address the above challenges, the Service-Oriented Architecture (SOA) concept can be inherited and applied to IoT [15]. As SOA standards were originally designed for connecting programs running on static computers, their direct application to IoT devices is not feasible but requires an adaptation to this context. Basically, the SOA approach relies on three layers, each responsible for different functionalities. The first layer is responsible for objects abstraction, i.e., each object or single functionality implemented by the object is abstracted and represented as "service". In addition, it offers semantic and procedures to access objects. The second layer is responsible for the management of objects and services, providing a way to automatically and dynamically discover them, monitor them, and make public their status. Additional responsibilities are to remotely manage services, and to maintain a correspondence between objects and the available services on them. Finally, the third layer provides all the mechanisms for the service and objects composition, i.e., it manages how to dynamically and real-time form new services from a single or set of basic services. In addition, the presence of a repository ensures to maintain an updated view of all currently connected service instances.

For the full realization of IoT, cloud computing can also be adopted. The term *cloud* refers to virtualized resources of computation and storage, which can be dynamically allocated by applications and without human intervention, allowing the digital world to efficiently and flexibility work. The cloud seems to be the natural home for IoT applications [101]. Indeed, data collected by objects is mainly streamed online, and IoT applications may use it if it is available in the cloud. To this aim, IoT objects need to be connected to the cloud for storing and retrieving required data. The cloud could be used for handling the high volume of data and its high generated speed thanks to tailored mechanisms for dynamically and automatically provisioning storage resources [102–104]. It also provides efficient mechanisms to access virtual storage, either through cloud database clusters and virtualized physical storage, greatly increasing the local storage capacity, which is very limited in most cases. Finally, the cloud may resolve efficiently several issues such as the semantic description of cloud services (e.g., the OSGi specification supports a lightweight

description of services and their dynamics for resource-constrained devices), the data processing problem for instance by allocating/deallocating dynamically processes, and the extraction of useful information for example by leveraging on specific solutions from the Big Data context.

The current Internet architecture (based on host-to-host connectivity) was designed for sharing resources rather than data. It addresses content by location and hence it is not suitable for IoT which is based on sharing data. Therefore, the research on novel information-centric Internet architecture ([105–110]), protocols [111] and mechanisms ([112, 113]) is a relevant research area for the IoT community, as well. Peer-to-Peer (P2P) systems [114] represent one of the most important types of content-centric Internet technologies that can be used in IoT, for example to implement efficient mechanisms for discovering available resources and capabilities in IoT. Among the two classes of P2P systems, the structured ones, based on Distributed Hash Tables (DHT), are the most promising due to a set of properties they exhibit. They are scalable, efficient, resilient to node failures, and distribute responsibility and load among peers deterministically by highly controlling the overlay network topology and by placing content on specified locations, which make subsequent queries performed by lookup service more efficient. Due to the environmental heterogeneity, service discovery for IoT will also be able to support flexible identification scheme, multi attribute query, or range query, and Prefix Hash Tree (PHT) [115], Mercury [116], MAAN [117], or Squid [118] can be contributing solutions to handle such a complex queries.

4. Application domains

IoT has huge potentialities for developing new intelligent applications in nearly every field. This is mainly due to its double ability to perform situated sensing (allowing for instance to collect information about natural phenomena, medical parameters, or user habits), and to offer them tailored services. Irrespective of the application field, such applications aim at enhancing the quality of every-day life, and will have a profound impact on the economy and society. They will also cover different aspects: personal, social, societal, medical, environmental, logistics to cite a few. The various applications can be grouped in three major domains: *(A)* industrial domain, *(B)* smart city domain, and *(C)* health well-being domain. Each domain is not isolated from the others but it is partially overlapped since some applications are shared. An example is the tracking of products, which is in common between the industrial and the health well-being domains as it can be used for monitoring cargos or foods, but it is also able to monitor the delivery of pharmaceutical products.

Figure 5 shows the subdivision in the aforementioned domains and provides a non-exhaustive list of IoT applications for each of them. Note that not all IoT applications have currently the same level of maturity. Some applications, typically the simplest and the most intuitive for the user, are already part of our daily lives. Many others are still in an experimental phase as they require greater cooperation between the various actors. Finally, others are more futuristic and are at an early stage. The remaining of the section provides the description of the most prominent applications for each domain.

4.1. Industrial domain

The IoT can be exploited in all industrial activities involving commercial or financial transactions between companies, organizations and other entities. Indicative examples are logistics, manufacturing, monitoring of processes, service sector, banking, financial governmental authorities, intermediaries, etc.

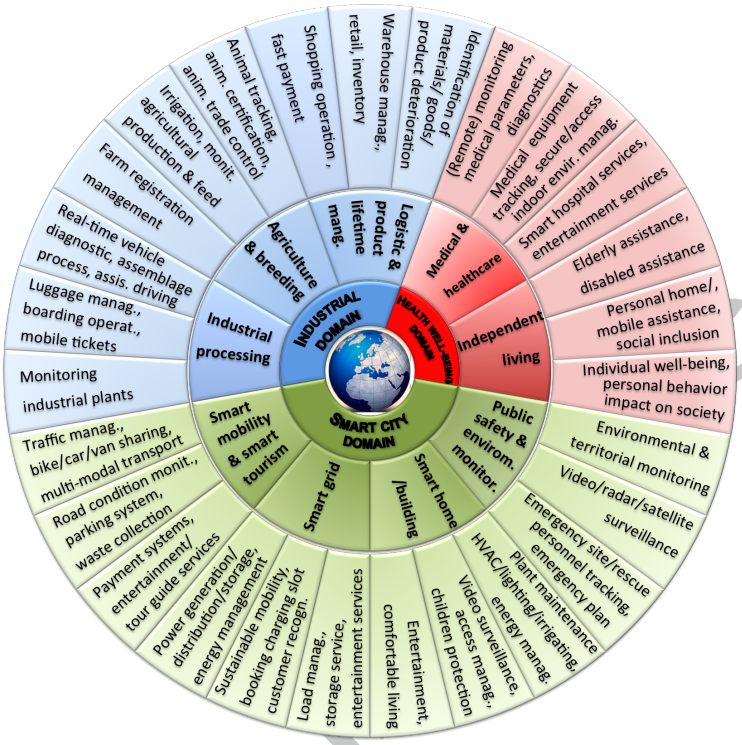

Figure 5: IoT application domains and related applications.

4.1.1. Logistic and product lifetime management

A first relevant example of an industrial IoT application is the logistics and supply chain management. RFIDs can be attached to objects and used to identify materials and goods, be they garments, furniture, equipment, food, and liquids [119]. Their use help to manage efficiently warehouses and retails, and to simplify the inventory by providing accurate knowledge of current inventory, while reducing inventory inaccuracies. The entire lifecycle of objects can be tracked too [120]. For example, RFID readers installed along the production plant allow to monitor the production process, while the label can be traced throughout the entire supply chain (e.g., packaging, transportation, warehousing, sale to the customer, disposal). Advanced IoT systems, composed of RFID-equipped items and smart shelves tracking items in real time, may help to reduce material waste, thus lowering costs and improving profit margins for both retailers and manufacturers. For example, it has been estimated an approximate 8.3% reduction on sales if shelves remain partially free of merchandise [121]. Underproduction and overproduction may reduce drastically by having a correct estimate of needed items, which can be inferred by analyzing data collected by smart shelves. In addition, the real-time analysis by sensors allows to identify product deterioration events, which is of vital importance for food and liquids. For example, to ensure the freshness of perishables (e.g., fruits, vegetables, frozen food), sensors may monitor continuously temperature and humidity inside storages or cold storages, and actuators may modify them to make optimal the conservation of contained food. Additionally, product integrity may be guaranteed by using RFID-based authentication processes. Other interesting IoT applications are intelligent shopping systems. Such systems monitor users' purchasing habits by tracking their mobile phones and guide them in shops/supermarket/mall suggesting discounted products or helping in fast payment operations (e.g., automatic check-out using biometrics).

4.1.2. Agriculture and breeding

IoT may assist in agriculture and breeding. Indeed, regulations for traceability of animals require a continuous monitoring of animals and of their movements in order to report promptly to the appropriate authorities any relevant events, e.g., diseases. Usage of IoT identification systems (e.g., RFID, sensors) allows to identify and monitor animals [122], and to isolate any infected animals from the healthy ones, thus avoiding the spread of contagious disease. Advanced microchips may store information about the status of the animal (e.g., demographic information, veterinary check, contracted diseases, vaccines performed) [122] or transmit information about the animal's body health (e.g., temperature) to streamline animal health certification, to control trade and imports, and to avoid possible frauds. By analyzing collected data, authorities may verify the actual number of livestock reported by local breeders and provide subsidies, accordingly. Monitoring and controlling agricultural production and feed (e.g., presence of OMGs, additives, melanin) by using advanced sensor systems are further applications of IoT [41, 123]. Such systems will ensure the health of plant origin products intended both for human and animal consumption [124]. Advanced IoT services may speed up the management for the registration/modification/closing of farms, their monitoring and the issuance of health authorizations. By using IoT, single farmers can break the long chain of producer-consumer sales, which employs freight or large companies to reach consumers, and will be in direct relationship with consumers. For example, they can provide a publicity window of their farm, real-time showing their offered products to allow customers to order them by using suitable mobile applications [125].

4.1.3. Industrial processes

IoT can offer advanced solutions in the automotive industry. Real-time vehicle diagnostic is a key application. Everything can be monitored by specific sensors: tire pressure, motor data, fuel consumption, location, speed, distance from other vehicles, driving time, stops, driver presence. The sensed data is then reported to the center system [126]. The wireless identifiable technologies attached to vehicle parts can maintain the history of specific automotive components and be used to improve the assembly process by automatically finding missing pieces. The application of IoT technologies enables advanced transportation systems for people and goods. Fare collection, safer luggage management based on automated tracking and sorting, intelligent screening of passengers, are some examples. Smart industrial management systems, based on IoT technologies, allow to monitor industrial plants, for instance to reduce the number of accidents, especially in case of high-risk plants (e.g., oil plants, gas plants). For example, sensors attached to containers transporting hazardous goods may emit different signals to announce the chemical component contained and the maximum level of that component. In case of critical situations (e.g., being close to the maximum level of a chemical component in a specific geographical area, or incompatibility among chemical components within containers in proximity), sensors may automatically send alarms to control centers that, in turn, manage promptly such dangerous situations.

4.2. Smart city domain

IoT may help to increase the environmental sustainability of our cities and the people quality of life. Emphasis is on energy and how to manage it efficiently, and on seeking smart solutions to enjoy the personal stay.

4.2.1. Smart mobility & smart tourism

As explained in Section 1, IoT will transform a traditional city into a Smart City. Indeed, IoT technologies, consisting of networks of sensors, cameras, screens, speakers, smart grid, will collect information, and the operational platform will process it to tune the different services/infrastructures of the city. IoT can be very useful for several

purposes. For example, mobile sensors directly attached to vehicles or integrated in smartphones of car occupants can collect information about the roads (e.g., about traffic density or surface conditions) with finer granularity with respect to fixed sensors [127]. At the same time, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications may be used to convey collected data to the control center. Smart parking systems may guide drivers to the nearest available parking slot according to drivers' location or personal preferences (e.g., free parking space, parking slot located in proximity of a camera), hence saving time and fuel, and thus reducing the carbon footprint [128]. Sensors placed on parking slots may also help municipalities to detect vehicles parked illegally (e.g., in parking spaces reserved to individuals with disabilities), and send tow trucks for towing away. Moreover, payment systems may become simpler and faster. Instead of the traditional coins, drivers may use NFC technology enabled mobile phones to pay for parking, and electronic RFID-based system for toll collection or public transport/ticket payment [129]. Additional applications include smart services for entertainment and tourism. For example, by taking pictures of monuments and other tourist landmarks, the users may obtain pertinent information on the personal smartphone and be guided to discover the heritage of the city [130].

4.2.2. Smart Grid

Energy management is a requirement towards a sustainable environment and the Smart Grid represents a building block for its realization. Indeed, the spread of renewable energy sources has led to a profound modernization of the traditional electrical distribution system and on the way of distributing energy. The *smart grid* is defined as an intelligent electrical distribution system that delivers energy flows from producers to consumers in a bidirectional way [25]. Unlike the traditional power grids, where the energy is generated only by a few central power plants and it is "broadcasted" to the final customers, via a large networks of cables/transformers/substations, in the smart grid the producers may also be the final customers. The energy produced by the customers' micro-grids (e.g., through solar panels, wind turbines) is sent to the grid, which, in turn, manages it appropriately through smart energy control services and stores it in specific energy storages. Monitoring and exchanging information about energy flows are additionally applications of the smart grid. Using smart meters, automatic control devices, smart switches, smart appliances, the grid is able to know in advance the expected demands and to adapt the production and consumption of electricity, consequently avoiding peak loads, eliminating possible blackouts and acting promptly in case of failures/leaks [131]. Information concerning consumed electricity is also delivered to customers in order to increase their personal awareness about energy consumption habits and to led them to a more rational energy usage. The latter can be obtained for instance by using incentives and by offering flexible pricing (e.g., variable rate pricing). The smart grid can also be integrated with the smart city, thereby enabling other intelligent services. Sustainable electric mobility is a typical example. Electric charging stations (e-stations) connected to the grid contribute to the diffusion of electric vehicles (e-vehicles), allowing for e-vehicles' charging in a fast, safe and easily accessible way to all citizens [132, 133]. Smart cards will allow automatic customer recognition and the customization of the charging process. Additionally, future services will include the possibility to book charging slots in advance and to enjoy entertainment services integrated into e-stations. Finally, the energy produced for example by renewable energy plants can be stored in the vehicle battery for an immediate use or sent back to the grid for further utilization via Vehicle-to-Grid (V2G).

4.2.3. Smart Home/Building

Homes/buildings in a smart city will be outfitted with a myriad of sensors and smart devices (e.g., broadband gateways, mobile phones, laptops, PCs, TV, speakers, appliances, plugs, surveillance cameras, lights, window shades, thermostats, and meters) that, integrated with communication technologies within buildings and residential homes,

give rise to a wide range of applications. Home automation systems are certainly attractive since allow to control everything remotely via web applications. Some applications use the simplest capabilities enabled by IoT, such as applications for security purpose (e.g., video surveillance, intrusion detection, access management), for plant management and maintenance (e.g., fault detection, asset management, maintenance), for service automation (e.g., HVAC, lighting, irrigation), and for entertainment systems (i.e., distribution of multimedia throughout the home). Other types of applications are integrated with the smart grid and optimize the domestic consumption [134]. For example, the Home Area Network (HAN) allows appliances to interact also with smart meters in order to reduce costs while ensuring the requested performance. This can be achieved through services that schedule the various activities of household appliances (e.g., washing machine or dishwasher cycles) in a dynamic and intelligent way avoiding the expensive periods and/or peak periods (i.e., with highest power demand). More advanced applications may allow to use the smartphone as the unique remote control to manage all the home devices/appliances (e.g., to turn off some appliances left on heedlessly) and to monitor users' habits [135] by tracking their mobile phones to make more comfortable the home living. For example, from the analysis of the information flows, the system can learn the time when a person arrive at home, hence unlocking the door, turning up the light and powering on the boiler to fill the bath tub. Such automatic operations can be always rescheduled or cancelled by the user at any time.

4.2.4. Public safety and environmental monitoring

Local and national governments aim at creating secure society, by guaranteeing public safety and by planning emergency management accurately. The public security services include the maintenance of public order, the prevention and protection of citizens, and the safeguard of public and private properties. Emergency management assists the society in preparing for and coping with natural or man-made disasters such as chemical leaks, floods, fire, earthquakes, tornadoes, epidemics, electrical outages, etc. IoT offers solutions for monitoring and tackling these emergency scenarios [136]. Data collected by fixed cameras located within the city and on personal citizens' devices allow advanced video surveillance and territorial monitoring services, while helping the police to control public order in case of sport events, musical performances, political meetings. Safety of private and public buildings (e.g., banks, shops) can be reinforced by using sensor technology that will trigger alarms. Emergency operations can be improved and strengthened through the use of IoT technologies. Currently, the emergency system lacks of precise information about the emergency site. Dedicated sensors and intelligent cameras, as well as GPS and wireless technologies providing real-time localization [137, 138] and tracking [139, 140], can be used to form a complete map of the event [141], to forecast its trends (e.g., direction and/or speed of fire spread, major risk areas), and thus to establish a dynamic emergency plan to coordinate the rescue operations. Let's consider a fire outbreak in a building where the access is controlled through e-cards. If persons have to swipe their personal e-cards to enter the building, the firefighters will know the exact number of people inside the building and where they are located (if the building has a localization system), and are able to guide people toward the nearest escape route or to guide firemen to save trapped people. In addition, data from wireless video camera and other equipment installed on the firemen helmets will provide real-time information on the fire evolution to calculate the best escape routes, and/or building collapse time. Alarms generated by wearable sensors on firemen (e.g., due to fast or irregular heartbeat) may also provide a reliable way for monitoring the health status of rescue persons.

4.3. Health well-being domain

IoT will play an essential role to develop intelligent services for supporting and improving people's and society's activities. These range from enabling citizens and communities to get involved in administration and government

decisions (e.g., e-participation), allowing people to live independently (e-inclusion) or to maintain their social relationships, to improve the health and social care.

4.3.1. Medical and healthcare

The medical and healthcare sector will be strongly affected by IoT. Advanced sensing devices allow real-time monitoring of medical parameters and vital functions (e.g., temperature, blood pressure, heart rate, cholesterol level). The gathered data is then transmitted via standard or specific communication technologies (e.g., Bluetooth, ZigBee, WirelessHART, ISA100) and made available to medical personnel for diagnosis and control of the patients' health. Body Area Networks (BANs), formed by wearable devices connected to each other, allow doctors to continue the remote patient's monitoring out of the hospital [142]. Other relevant applications are related to the identification of materials and medical instrumentations. For example, the application of smart labels will ensure to accurate tracking objects to prevent equipment to be lost or stolen, or that material is left inside a patient during an operation (for example gauze or other small objects). The use of smart labels is also important to facilitate the inventory of medical equipment. Efficient hospital management services include energy optimization and HVAC systems (similar to those discussed in Sections 4.2.2 and 4.2.3) and safety access systems. The latter refer to the digital control of accesses enabled by smart badges (e.g., equipped with RFIDs) to limit the access of some hospital areas to authorized personnel only. The hospital will also be fit out with a number of Internet access points ("totem") - representing a mean within the hospital to book exams or to check where/when the medical exams will be performed. Beds will be equipped with smart touchscreen terminals, allowing patients to access to entertainment services, TV channels, Internet, and to communicate with their families. In addition, young patients may used them to participate in school educational services (e.g., virtually class, accessing to archived lessons).

4.3.2. Independent living

IoT may also provide several advantages for improving the quality of life of citizens, for example supporting independent living (e-inclusion) and proving lifestyle suggestions for well-being. The e-inclusion focuses mainly on specific categories of people, such as aging or disabled population (see for example the Ambient Assisted Living (AAL) Joint Programme by European Commission), allowing them be active in society. Monitoring of condition/status of elderly and emulating the medical consultation at home are key applications. By monitoring real-time physiological signals captured through sensors, the system will be able to set off medical alarms (e.g., in case of detected falls [143]), to suggest possible hospitalization, to diagnose dementia (e.g., Parkinson, Alzheimer) in the earliest stage by observing deviations from normal behaviors. Personal assistants available on PC screens or TV will stimulate persons to do exercise [144], and guiding them in searching objects in the house. In addition, as elderly people often have limited mobility and may be housebound, social networks will allow elderly to connect, communicate and exchange status, feelings and ideas, and participate in debates and discussion groups [145]. Obviously, simplified and customized interfaces and the system's ability to acquire and anticipate actions will be key requirements. Mobile assistants are other fundamental services. They will provide elderly a secure way to move confidently in town or use public transportations safely. By combining data gathered by personal mobile devices (equipped with e.g., position sensors, orientation sensors, movement obstacle detection sensors, video camera) and data gathered by sensors located in the city, the mobile artificial-intelligent-based system will reconstruct perceptions of the environment, which will be verbalized to persons by synthesized voice. Similar applications will be exploited by visual impaired persons to increase their ability to move in the city [146, 147]. Wellbeing and lifestyle services will also be important. Such services will capture users' habits to provide them suggestions to improve their quality of life. Positive feedbacks, for

Table 3: IoT general requirements

Requirement	Requirement description
Heterogeneity	managing the variety of devices/technologies/services/environments
Scalability	avoiding the explosion of resources/exchanged data/operations
Cost minimization	optimization of development/maintenance costs and energy consumption
Self-*	self-configuration, self-organization, self-adaptation, self-reaction to events and stimuli, self-discovering of entities and services, self-processing of Big Data
Flexibility	dynamic management/reprogramming of devices or group of devices
QoS	observance of QoS guarantees (e.g., bandwidth, delay) to services/applications
Secure environment	robustness to communication attacks, authentication, data transfer confidentiality, data/device integrity, privacy, trusted secure environment

example notifying the number of kilometers (calorie) covered (burnt) during a walk, and the positive impact on their health, will motivate people to repeat daily the same activity. In addition, information derived from the user's habits could measure the impact of the individual behavior on the urban environment and increase the user's awareness of each single action on the environment sustainability [127].

5. Key IoT features

As discussed in the previous section, IoT can open new opportunities to create innovative applications. Some applications strictly belong to a specific domain and exhibit characteristics peculiar of that domain. Conversely, others applications exhibit characteristics cross-cutting multiple domains. In this section we discuss the most significant IoT characteristics. Firstly, we look at the IoT general features, then we focus on traffic features characterizing the M2M communications, which may dependent on the specific application.

5.1. General features & requirements

Table 3 summarizes the IoT general requirements. *Heterogeneity* and *scalability* will be of primary importance in a complex and dynamic system as the IoT. Solutions to cope with the above requirements must be sought at architectural level, at naming/identification/addressing level, at communication level, and at level of object name/code mapping services. *Minimizing costs* can be guaranteed by optimizing the operational costs (i.e., development, installation, maintenance), as well as by developing from scratch energy-efficient solutions. In addition, As IoT will exhibit a low human intervention (if not completely absent), objects should offer *self-* capabilities*. Among the offered self-* capabilities, notable are: *i)* high degree of configuration autonomy, *ii)* self-organization and self-adaptation to various scenarios, *iii)* self-reaction to events and stimuli to which objects are subjected, and *iv)* self-processing of the huge amounts of exchanged data, which can also be used by third parties. Observance of *Quality of Service (QoS)* is mandatory for those services and applications characterized by sensitive inelastic (real-time) traffic. Finally, IoT should also guarantee a *secure environment* in terms of security of communication/authentication, integrity of data and devices, privacy of users and personal data, and trustworthiness of the environment and of the involved parties.

5.2. Communication requirements

In addition to the general requirements discussed above, there exist a number of specific requirements related to the traffic generated and transmitted by IoT devices, i.e., communication requirements. However, not all communication requirements need to be supported by each IoT device. Specifically, we can identify some general communication

Table 4: IoT communication features

Feature	Feature description
Different underlying networks	abstraction of the different underlying networks (e.g., wired, wireless, cellular), support for different communication modes (e.g., access point-based, p2p fashion)
Addressing modes	support of anycast/unicast/multicast/broadcast transmissions, dynamic replacing of broadcast with multicast/anycast to reduce network load
Massive device transmission	handling simultaneous or nearly simultaneous transmissions from huge number of devices (i.e., efficient MAC protocols)
High reliability	guarantee of connectivity/reliable transmissions based on different solutions (e.g., link adaptation protocols, modulation/coding schemes, multi-path establishment)
Enhanced access priority	management of priority levels of services and communications services (e.g., preemption mechanisms)
Path selection	optimization of communication paths based on different policies (e.g., network cost, delay, transmission failures), dynamic metric selection
Mobility	seamless roaming and mobility, communication management towards stationary and low-mobile devices
Sleeping devices	managing communication towards sleeping devices
Low power consumption	include mechanisms for reducing energy consumption
Notification and interaction	functions for supporting data acknowledgement, failure notifications, and interaction mode
Traffic profile	management of data traffic with different traffic profiles (e.g., continuous transmissions, long periods between two data transmissions, small amount of transmitted data, burst of data, bidirectional/unidirectional transmissions)
Time-dependent traffic	support of data traffic with different time requirements (e.g., time-controlled traffic, delay-tolerant traffic, extremely low-latency traffic)
Location reporting support	report the device/gateway location to other devices/applications continuously/upon request
Secure connections	integrity of communications and timestamps, anonymity of identity and location, detection of abnormal events

requirements that should be met by each IoT device, while others are peculiar of specific services, and hence should be provided only by those devices offering that service. Table 4 summarizes the main communication features that are necessary for the correct establishment of M2M communications [36, 148].

The backbone of the IoT network will be composed of heterogeneous communication technologies (e.g., wired, wireless, cellular, hybrid). This implies that communication protocols should be able to interface with the different underlying networks, to support different addressing schemes, and to dynamically adjust them when needed in order to reduce the network load. Fundamental will also cope with the concurrent or almost concurrent transmissions from an extremely large number of devices towards the same access point, for instance through efficient MAC protocols. In addition, high reliability of communications should be ensured regardless the operating environment (e.g., mobility, quality of the channel). In some cases, communications should manage different levels of priority and ongoing communications may be interrupted in order to serve flows with higher priority. As well known, mobility greatly affects wireless communications. Therefore it will be essential to support seamless mobility and roaming, but also to operate efficiently in environments composed of stationary or low mobility devices. The IoT environment consists in devices with limited resource capabilities that, to save energy, may temporarily disconnect from the network and wake on demand. Communication protocols should handle transmissions towards such nodes, reducing also the overall energy consumption. Different traffic profiles and time-requirements should be also handled. Finally, communication protocols should be invulnerable to various attacks. Preventing the compromise of credentials or configuration, being

robust to network attacks (e.g., hacking and DoS), securing the integrity of communications and timestamps, ensuring anonymity where necessary by masking identity and location of the requestor, and identifying any abnormal events are example of how to guarantee security.

5.3. Mapping applications/traffic features

To conclude here we report an example of mapping between the communication features discussed above and a subset of the applications described in Section 4. As shown by Figure 6, some requirements are in common with multiple service applications, while others belong to only a few. For example, the management of simultaneous transmissions is a characteristic shared by several applications such as video surveillance and public safety. On the contrary, priority access is a prerogative of surveillance systems and security, where alarm messages must have a higher priority with respect to other active flows. Furthermore, some services must satisfy simultaneously more than one requirement, e.g., smart grid. Healthcare applications are, on the other hand, characterized by massive device transmissions that have to be highly reliable and have to respect extremely stringent delays when delivering medical data.

6. Milestones and challenges

As described in Section 3, IoT is the result of many different technologies used to gather, process, infer, and transmit data. It is apparent that an extraordinary effort is required to combine all these different "forces" as well as to address all the correspondent challenges. In this section we focus on the most important research areas discussing the main issues and showing the major milestones achieved so far. More specifically, aspects related to architecture, addressing and mobility of objects are discussed in Sections 6.1, 6.2 and 6.3, respectively. Networking and gateway access issues are the objectives of Sections 6.4 and 6.5, respectively. We analyze problems arising with the management of the huge number of devices in Section 6.6 and of the huge amount of data in Section 6.7. Traffic characterization issues are discussed in 6.8. Finally, Section 6.9 covers security aspects.

	IoT Application	Security & surveillance	Smart Metering	Tracking	Healthcare	Remote payment
Communication Feature	Mass device transmission	X		X	X	
	High Reliability				X	X
	Access priority	X				
	Very low power			X		
	Small data burst		X			
	Low/no mobility		X			X
	Monitoring & security					X
	Extremely Low Latency				X	

Figure 6: Example of mapping among IoT applications and communication features.

6.1. Network architecture and system design

Finding a scalable, flexible, secure and cost-efficient architecture, able to cope with the complex IoT scenario, is one of the main goal for the IoT fast adoption. A number of different architectural solutions have been proposed in the past years [149–153]. In addition, some proposals are tailored for specific applications (e.g., healthcare [154], meter reading [152], enterprise services [155]), while others for specific technologies [35, 156]. However, an excessive multitude of technical solutions makes interoperability difficult, slowing down the IoT development process. Therefore, developing an IoT reference architecture is an objective that recently has found a great support within the IoT community. To this aim, the major standards bodies (e.g., 3GPP, IEEE, ETSI) started working for its realization, and their effort resulted in the design of two network architectures: *i)* a hierarchical network architecture for *scalable connectivity* [157], and *ii)* a hierarchical network architecture for *high capacity* [148, 158]. Both solutions are based on a hierarchical organization of the network that allows to satisfy the IoT requirements. In the first case, the emphasis is on the network scalability, ensuring a reliable and efficient connection between the multitude of devices. In the second case, the emphasis is on the efficient management of the high traffic load to which the network is expected to be subjected. In the remainder of this subsection, we present a quick overview of the two proposed architectures, examining their main features.

Hierarchical network architecture for scalable connectivity

The promoter of this architecture is the ETSI Technical Committee for Machine-to-Machine communications (ETSI TC M2M), established in 2009 with the specific purpose of developing and maintaining an end-to-end (e2e) network reference architecture for M2M. The idea is to realize an IP-based architecture relying on existing technologies that: *i)* is scalable, *ii)* is easily developed, *iii)* has low complexity, *iv)* is efficient and interoperable, *v)* uses standardized interfaces and protocols, *vi)* hides the complexity of underlying networks to applications developers, and *vii)* fosters the development of new services [157, 159].

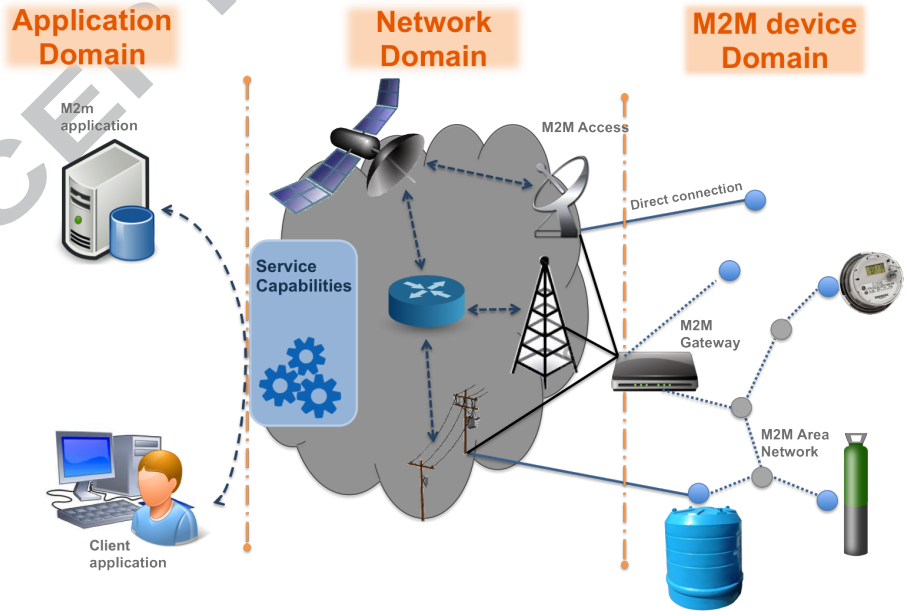

Figure 7: The high-level ETSI M2M reference architecture (Source: ETSI M2M).

Figure 7 shows the high-level architecture, which is composed of three domains (i.e., the Device & Gateway domain, the Network domain, and the Application domain) and several elements. Specifically:

- **Device & Gateway domain:** it consists in a high number of M2M devices, one or more gateways (*M2M GWs*), and one or more *M2M Area Networks*, which provide the physical/MAC connectivity between M2M devices and M2M GWs. A M2M device runs the applications and may connect to the remote server (outside this domain) in two ways: *i)* establishing a direct connection with the *Access Network* if advanced features (e.g., capabilities for managing registration, authentication, authorization) are supported by the M2M device, or *ii)* passing through the M2M Area Network and the M2M GW (or multiple M2M GWs). Any of the short-range technologies listed in Section 3.1 can be used within M2M Area Network. The M2M GW acts as a proxy between M2M devices and the network domain by forwarding data to/from the remote server. It may also run M2M applications and has local intelligence to gather data and make further processing.

- **Network domain:** it consists in *Access Networks* and *Core Networks*, and provides connectivity between the M2M GW(s) and M2M application(s). Access Networks include xDSL, HFC, PLC, W-LAN, WiMAX, satellite, UWB technologies, while Core Networks include 3GPP GPRS and 3GPP EPC for example. The Core Network provides additional features such as IP connectivity, network control and management (e.g., provisioning, supervision, fault management), roaming, interconnection with other networks, etc.

- **Application domain:** applications (both on the client side and on the server side), middleware, and other common features ensuring interactions between applications and devices (i.e., *M2M Service Capabilities (SC)*), reside in this domain. The *M2M Server* resides also here, and stores all data gathered by M2M devices, making data available to applications after further elaborations.

The ETSI M2M Architecture is based on the *REpresentational State Transfer (REST)* [160] architectural style, where any logical and physical entity is represented as a *resource* that has a particular *state* which can be *manipulated* (e.g., a sensor is a resource that can be read and configured). Resources are uniquely addressable, and can be accessed as web links by using web browsers via HTTP. Specifically, each resource is represented as an instance of a M2M SC, and M2M applications and network entities exchange information and handle them by using standardized procedures, which are based on CRUD (i.e., Create, Retrieve, Update, Delete) operations. To standardize these procedures, a number of interfaces have been defined, as well as the operations allowed on them for the communication [157]. Specifically, these interfaces are: *i)* device application interface (dIa), used by applications on devices and gateways to communicate with the local SC, *ii)* M2M to device interface (mId), used for the intra-SCs communications, and *iii)* M2M application interface (mIa), used for communicating with the SC on the network. In addition, each Service Capability instance is responsible for a subset of resources that are modeled and structured as a recursive hierarchical tree.

Hierarchical network architecture for high capacity

In this case, the focus is on providing an architecture able to efficiently support high traffic loads, resulting not only from voice/audio/video exchange services, but also from the presence of a high number of transmitting devices. 3GPP is the principal investigator of an architecture for high capacity based on cellular to support **Machine-Type Communication (MTC)**. The term MTC has been coined by 3GPP to highlight that M2M communications may consist also on interactions between machines and humans (i.e., M2H communications or H2M communications).

The 3GPP activity on the network architecture aims principally at optimizing LTE to support MTC traffics and applications. At the same time, it aims to: *i)* lower operational costs of network operators when offering MTC services, *ii)* reduce the impact and effort of handling large MTC groups, *iii)* optimize network operations to minimize impact on device battery power usage, and *iv)* stimulate the development of new MTC applications [148, 161].

Figure 8 depicts an overview of 3GPP MTC architecture, highlighting also the basic elements: MTC device, MTC server, and MTC Interworking Function, which is in charge of authorizing the communications and triggering the devices. As in the previous case, three different domains can be distinguished: the **MTC device domain**, the **communication network domain**, and the **MTC application domain**. The peculiarity of this architecture lies in the communication network that in this case is a 3GPP mobile network. Specifically, since the dominant technology is LTE-Advanced [162], a multi-tier connectivity can be offered. Indeed, *macrocells* with LTE's base stations (eNBs) can provide a large and ubiquitous coverage to the MTC devices as well as manage their high mobility [94, 163]. In contrast, *cells* with relay nodes (RNs), *picocell* with eNBs, and *femtocells* with home eNBs (HeNBs), bring link connectivity close to MTC devices, increasing reliability and the overall system capacity [164].

Two different communication models are envisaged. On the one hand, an MTC user can access and control the MTC devices through one or more MTC servers. In this case, the MTC server is provided by an operator, and the user accesses the server through APIs specified by the operator itself. The MTC server location does not modify the access modality. MTC servers can be positioned in the operator domain or placed outside the operator domain, but the access procedure is the same. On the other hand, the MTC devices can communicate with each other directly, without the help of intermediaries, regardless of the operator to which are connected.

6.2. Addressing and Naming

Finding efficient mechanisms to retrieve all content produced by (and available on) the various objects is another important IoT topic. Indeed, it is fundamental that users, regardless of their position, may access and use the data generated by objects. In other words, in this section we try to answer to the following questions: *i)* how can we identify and interact with the huge number of IoT objects?, and *ii)* how can we make it efficiently if IoT objects are heterogeneous for characteristics and technologies?

Addressing is the mechanism commonly used to identify objects (e.g., computers, laptops, routers, switches, small devices) within a network. In IP-based networks, IPv4 and IPv6 represent the two possible choices. However, as IPv4 relies on 32-bit addresses and IANA (Internet Assigned Numbers Authority) allocated the last blocks of IPv4 addresses in July 2011, IPv6 is the only feasible solution. IPv6 provides a huge address space as relies on 128-bit addresses, and it will be certainly able to identify all IoT objects. However, even if the premises of using IPv6 are encouraging, finding a unique solution is extremely challenging for the heterogeneity of the identifier lengths used by the different technologies.

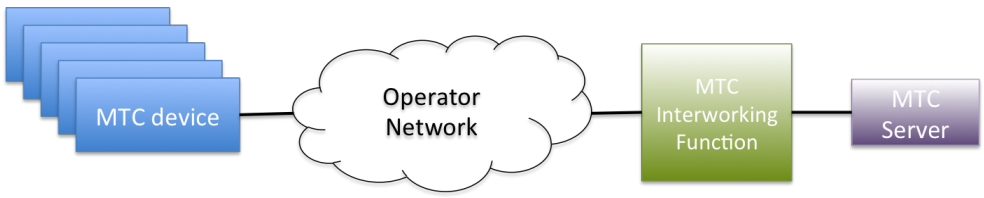

Figure 8: The high-level 3GPP MTC reference architecture.

In the sensor context, IETF IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) working group focuses on solutions to make IPv6 compatible with IEEE 802.15.4, and defines an intermediate layer, named *adaptation layer*, between the 802.15.4 data link layer and the IP network [165], whose objective is to map IEEE 802.15.4 addresses on IPv6 addresses, and vice versa. A PAN refers to a group of IEEE 802.15.4-based sensor devices physically close. Each PAN is identified by an address directly mapped on a specific IPv6 link. IEEE 802.15.4 devices may have a local address (but unique within a PAN) of 16 bits, or a global unique address of 64 bits. Hence, the IPv6 address associated with the single sensor node is obtained by concatenating the address of the PAN and the address of the sensor node. The adaptation layer is also in charge of providing mechanisms (e.g., encapsulation, header compression, fragmentation, reassembly) allowing IPv6 packets to be sent/received correctly over IEEE 802.15.4 based networks. Specifically, header compression techniques reduce the IPv6 header from 48 bytes to 6 bytes through a process that eliminates redundant information, which can, however, be retrieved from the link layer or the contest application. To fragment IPv6 datagrams to fit into 127-byte fragment (i.e., the IEEE 802.15.4 MTU), each fragment stores additional information for its correct identification: *i)* the size of the original IPv6 packet, *ii)* the offset indicating the position of the payload carried by the fragment in the original IPv6 packet, *iii)* the information to distinguish the first fragment from the others, and *iv)* a random number to distinguish different fragments belonging to different IPv6 packets.

In the RFID context, as RFIDs rely on different addressing schemes with variable lengths (i.e., 64 bits, 98 bits), a number of different research solutions have been proposed during the past years. A first approach is to use directly the EPC. For example, in the 64-bit case, in [166] the IPv6 address associated with an RFID tag is obtained by concatenating the ID of the GW connecting the RFID system to the Internet (first 64 bits) with the identifier of the RFID tag (second 64 bits). Therefore, the GW has also to manage and handle messages to and from the RFID. Specifically, for each message generated by a RFID, an IPv6 packet is generated where the source address is obtained as described earlier and the RFID message is encapsulated in its payload. A reverse process is executed to handle messages from the Internet and intended to RFID reader. Conversely, for 96-bit addresses, the mapping between the RFID identifier and IPv6 address is performed by an *agent*, a dedicated element within the RFID reader [167]. Specifically, the agent generates a virtual physical address by using the RFID tag ID and, by using such virtual address, asks for an IPv6 address to the DHCP server. It also maintains updated the mapping in a table, which is checked every time it needs to forward packets generated from RFID to the outside world or vice versa. Recently, alternative solutions are proposed, which are independent from the RFID addressing scheme, and do not require any address-translation mechanism. For example, in [168] each RFID network is connected to the IP network via the so-called RFIPv6 gateway and nodes outside the RFID network can find information on a specific tag via the RFIPv6 gateway.

Another important research challenge is connected with the address retrieval: how can we retrieve the address associated with an object starting from the available information about that object? In addition, how can we determine which is the object associated with a given address? Essentially, these issues are similar to those solved, in the legacy Internet architecture, by the classic Dynamic Name Service (DNS). Within the RFID context, this role is played by the Object Name Service (ONS) [169, 170], which implements a simple lookup service that resolves the EPC number in the EPCIS server address of the manufacturer of the searched tag. To ensure scalability and to maintain separate information related to different object classes, ONS is organized as a hierarchy of lookup services. Basically, the lookup process consists in the following steps: *i)* a first check in the Root OSN, which contains the Local ONS addresses for each EPC Manager Number; *ii)* a second check in the Local ONS, which identifies the address of the EPCIS server associated with the specific EPC, and *iii)* a direct access to the EPCIS server where the

desired information is stored. Unfortunately, ONS can not be used for the reverse process, i.e., retrieving information associated to a specific EPC number. To this aim, the Object Code Mapping Service (OCMS) has been proposed. To improve the scalability of OCMS service, both in the storage and search capabilities, authors of [171] propose a web service where the repository of tag description is implemented as a P2P network. Major open issues consist in the lack of knowledge about the robustness of services such as OCMS, when used in large-scale systems. Furthermore, ONS and OCMS work only within the RFID environment. Solutions for different technologies, such sensors and other devices, are missing.

6.3. Objects' mobility

A large part of IoT objects are not fixed, but have a certain degree of mobility (e.g., products in an assembly line and transported by containers). As a consequence, supporting and managing efficiently the mobility of this large amount of objects is of paramount importance.

A feasible solution is the use of MobileIPv6 [172], where, to each mobile node (the mobile object in IoT context) are assigned a permanent address on its home network (*home address*) and a temporary address on each network who is visiting (*Care-of Address (CoA)*). Two different agents storing the information about mobile nodes' location are used: the *home agent* stores the permanent address, while the *foreign agent* is used when the node visits a foreign network, to announce the CoA. One of the main home agent tasks is to intercept packets destined to a mobile node, and redirect them to the mobile node using the CoA announced through an IP tunnel. However, recently, it has been shown that these approaches may not be sufficiently scalable in IoT environments due to a huge amount of signaling traffic to discover devices and to maintain updated their positions. To deal with the above issues, in [173] authors exploit a natural phenomenon, named *object group mobility (OGM)*. According to OGM, objects usually move in group and aggregate around a carrier (e.g., a person, a vehicle, a box), named *group master (GM)*. GM is the entity that takes care of assigning addresses to objects that belong to its *home network*, and keeps continuously updated their CoA, without the need of generating management traffic between the object and its *home agent*. This approach also reduces the uncertainty in objects' localization. Indeed, an object, which can not be located for example because its access technology does not cover a given area, can be localized, with a low approximation degree, by using those objects belonging to the same group, whose locations are known.

6.4. M2M communications

The nature of IoT scenarios presents a high number of technical challenges related to communication protocols. Among these, significant research efforts have been devoted to addressing the routing issues and the e2e reliability.

6.4.1. Routing

Routing is one of the key network functionalities for IoT environments as it selects the multi-hop paths that data packets follow from the source to reach the destination. Several technical challenges make the design of routing protocols for M2M communications complex. First, most of the communicating objects are resource-constrained devices in terms of computation, memory and energy capacity. In addition, the routing protocol must operate in very large networks. Finally, communication technologies typically used for M2M communications are characterized by low data rates, frequent packet losses and time-varying channel conditions. Accordingly, suitable routing solutions for M2M communications should be scalable, reliable and minimize resource consumption. Existing routing protocols designed for mobile ad hoc networks are inadequate for this context. Conversely, solutions for wireless sensor networks (WSNs) are a promising starting point. Various categories of protocols exist: *i) clustering routing protocols* (e.g., LEACH [174], HEED [175]) organize the network into hierarchical structures [62, 176, 177], which can

be problematic to create and maintain; *ii) geographical routing protocols* (e.g., greedy solutions [178], EtE [179], BGR [180], VCCSR [48]) use nodes positions to build network paths, but geographical information is difficult to maintain in mobile networks; and *iii) protocols with mobile sinks/data collectors* [42, 181] use additional mobile elements (e.g., robots) to facilitate data collection. In addition, some solutions exploit cross-layer optimizations to automatically adjust protocol parameters in order to minimize power consumption [182]. Others are based on an efficient combination of multi-hop protocols and duty cycling [183]. Finally, in application scenarios characterized by very low duty cycle (0.1%), solutions where control overhead is minimized are preferred [184]. For instance, in [185] nodes do not maintain persistent information about the networking state, which is on the contrary stored by the gateway. As a consequence, the overhead for the storage of state information is significantly reduced, as well as the code running on sensors is simplified. The proposed solution uses an approach similar to AODV to establish route and commands nodes along the selected route to switch channel before downloading large amount of data. Recently, the IETF Routing Over Low power and Lossy networks (ROLL) working group has focused on designing a routing protocol specific for IP smart object networks. Based on a careful analysis of routing requirements of several IoT applications (e.g., smart grid, industrial automation, home networks, building automation), the WP has defined the RPL routing protocol [186, 187], able of operating in large-scale networks composed of tiny devices communicating over low-power and lossy networks (LLNs) technologies and incorporating some of the above approaches. RPL has been designed to work efficiently with traffic flows from RPL nodes towards an aggregation point (named *root* or LoWPAN Border Router (LBR)), but it supports also the traffic in the reverse direction (although less efficiently), and some basic functionality for point-to-point flows. Basically, RPL builds Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics. In contrast with traditional networks, in LLNs node and link metrics change over time, and it is important that the routing protocol adapts dynamically to these changes [188, 189]. The DODAG formation process starts at the root that announces its presence by sending DIO messages and ensures that DODAGs do not overlap (i.e., each node belongs to only one DODAG). From the above discussion, it emerges that many general routing issues still need to be addressed, for example how to cope with the heterogeneity of devices' capabilities (and communication technologies) that affect the amount of information that can be stored and used for computing optimal paths.

6.4.2. End-to-end reliability

Other fundamental features are those implemented by the transport protocol that should guarantee e2e reliability and perform e2e congestion control in the network. Intuitively, TCP, which is used in Internet networks, is unsuitable for M2M communications because: *i)* it produces a too high overhead during connection setup and termination phases, which is unacceptable for M2M short-lived connections, and *ii)* it is based on a congestion control mechanism ill-suited for connections which transmit small amount of data. Conversely, the UDP protocol can be used in many resource-constrained connections thanks to its low overhead and its connectionless property. The downside, of course, is lack of reliability. Very few works exist in literature aiming at designing efficient M2M transport protocols. One solution is SCTP [190], a lightweight TCP variant specifically optimized for multi-streaming and multi-homing. Specifically, the multi-homing SCTP feature guarantees to support mobility without the need to use any special router agents in the network. Another approach adds the reliability mechanisms at the application layer (e.g., CoAP [191], MQTT [192]), even though this is generally less efficient. The Constrained Application Protocol (CoAP) has been designed with IoT requirements in mind, targeting at resource-constrained devices and at the REST paradigm for objects addressing. It is a one-to-one protocol for transferring state information between client and server. It is characterized also by low overhead and low parsing complexity. Reliability of communications are guaranteed by QoS

mechanisms based on acknowledgements. When the reliability of transmissions is fundamental (e.g., in scenarios of public safety and emergency), the Message Queuing Telemetry Transport (MQTT) protocol [192], proposed by OASIS open standards consortium, is a viable solution. MQTT employs a publish/subscribe mechanism to support energy-efficient one-to-many message distribution in a reliable manner. Moreover, the integration of sensor applications with other existing applications is guaranteed by MQTT-S [193]. MQTT-S, extension of MQTT, has been designed keeping low-end and battery-constrained sensors/actuators in mind. However, novel reliable transport protocols are needed to cope with congestion issues that may arise due to the scale of the network, while taking into account that M2M communications are short-lived and involve the transmission of few bytes per message.

6.5. Flexible GWs

The gateway (GW) is another key component of the IoT architecture as it interconnects smart devices to the network core. GW has to be extremely versatile and flexible, managing efficiently many aspects (e.g., access, resources, QoS, security, multimedia conversion), and catering for the different characteristics of devices. The design of flexible gateways, incorporating all the above characteristics, is extremely challenging. A good example of heterogeneous environment where the choice of the gateway is important is the Home Area Network (HAN). The HAN will in fact be outfitted with a variety of applications (e.g., HVAC systems, lighting control systems, smart grid systems, medical systems, entertainment systems) and, consequently, with numerous body/personal/local subnetworks. The key issue is to avoid that each system has its own gateway, but to converge toward a unique and integrated solution representing the only contact point used by the homeowner to interact with the home environment. Moreover, as devices on HAN are generally characterized by low power constrains, GW should be able to understand which processes and energy resources are available, and to disseminate data by means of smart routing and caching techniques to minimize the usage of resources. A number of solutions have been proposed. For example, in [194] the gateway exhibits self-configuration and advanced cognitive capabilities. The *Software Defined Radio (SDR) technology* can also be used [195]. The SDR technology [196] allows to develop the operating radio functions via software, thus ensuring flexibility and interoperability. Therefore, SDR-based gateways can be multi-carrier and multi-band, allowing the interoperability between different communication protocols, on different frequency bands, and on different frequencies. SDR-based solutions have been proposed also for the vehicular environment [197], where the gateway supports cellular, Bluetooth, and ZigBee technologies, as well as communication between vehicles' internal components (e.g., audio, diagnostic, and navigation systems). Additional GW solutions based on user-space programmable software are proposed in [198, 199], and allow a flexible plugging of protocols. Moreover, benefits can also be obtained by GW solutions that provide cross-layer interactions involving all levels [198].

6.6. Device management

Management of objects is of paramount importance for the development of the IoT. IoT applications require, not only that objects are connected and communicate over a wide number of communication technologies, but also that devices and appliances are remotely managed. The management process is complex, and includes a lot of different actions, such as switching on/off the device, configuring the device/network, updating firmware/software, recovering from errors, monitoring the device/network, gathering data and connectivity statistics, etc.

Solutions for an efficient device management should take into account the heterogeneity of devices and of their available resources. Indeed, typical IoT devices are resource constrained, thus they do not provide much memory, processing and power capabilities. Standardized device management solutions, such as TR-069 [200], SNMP [201], and NETCONF [202], are generally used for the management of resource-rich devices and appliances such as routers,

switches, and smartphones. It is a common understanding that such solutions are not particularly useful for the management of a large number of constrained devices, also because they generate a high volume of traffic to send control commands and a high footprint on the device. However, in [203] authors demonstrate the feasibility of implementing the above existing device management protocols also on resource-constrained devices. Specifically, authors consider the Atmel AVR Raven device (equipped with 16KB RAM and 128KB program memory) and analyze a number of performance figures such as the memory usage of each component and the time taken for transferring and processing SNMP and NETCONF requests. Their results show that using these protocols is beneficial, especially in those scenarios where it makes sense to deploy existing management protocols because they are already in usage by the other devices. In addition to the classic device management protocols, newer solutions may be used. For example, OMA Device Management (OMA-DM) [204] is a device management protocol targeting mobile devices (e.g., mobile phones, PDAs), but, due to its design characteristics (i.e., small footprint device, constraints on communication bandwidth, security mechanisms), can be extended to resource-constrained IoT mobile devices. Its peculiar feature is the usage of SMS for wake up and bootstrapping operations. Recently, the OMA Lightweight M2M (LWWM2M) management protocol [205] has also been proposed. It is considered the successor of OMA-DM and has been designed targeting constrained devices. It is built on top of COAP and features REST-based architecture. SMSs are used for wakeup operations but also for other management operations (i.e., GET, PUT, POST).

6.7. Data management

Managing Big Data is extremely challenging due to the different data properties. IoT data will be sampled by a variety of objects and sensors, each having different methods for data representation and semantic. Moreover, the large number of IoT devices will lead to a rapid explosion of the scale of collected data (petabytes and more). Collected data will have often a time-space relationship (i.e., position and time information) to describe the dynamics of the objects' location (i.e., the so-called pervasive location information). In contrast with today's applications, where data is usually consumed by single applications, data will be shared among different IoT applications, thus requiring a greater interoperability. The last data property is connected with the data multi-dimensionality, i.e., the integration of different type of sensor data to monitor simultaneously a number of indicators, such as temperature, pressure, light.

IoT data properties generate new data management issues that change the way the system works. Indeed, IoT data management moves from being a classic "offline" system, where storage/query processing/transaction operations are managed offline, to be an ""online/offline" system, where processing and analysis are also real-time.

Scalability of data is an important problem. Efficient indexing methods need to be developed in order to find a specific data item easily. Suitable representation schemes are also needed to capture the heterogeneity of objects and metadata, and to enable their self-description. In addition, interoperability among different data is also important. Approaches introducing an abstraction level may solve them. Ontologies and semantics look to be promising. For example, Web Ontology Language (OWL) [206] is a family of language for representing ontology in the web that can be adapted to IoT. Effective methods should be also developed for filtering redundant data or events. For example, an efficient RFID data filtering solution has been proposed in the supply chain context [207]. The research attention should be also devoted to finding suitable languages for accessing data. Structured Query Language (SQL) is the most popular language for querying structured data. However, data in IoT will be mainly semi-structured, hence alternative solutions should be considered. The XML Query (XQuery) language [208] seems a suitable choice allowing to query structured data as well as less structured data. For what concern data process modeling and data interoperability issues, the SOA approach can provide suitable solutions. For instance, in [209], a SOA-based scheme has been proposed for managing heterogeneous data from different devices. Specifically, the proposed scheme is implemented

as Web Service. Features implemented by devices are encapsulated into services, and a common interface for invoking services is defined. However, even though SAO-based approaches are encouraging, several other issues need to be solved, e.g., to guarantee the respect of the ACID (Atomicity, Consistency, Isolation, Durability) properties.

The data archiving is another important problem coverings a number of correlated challenges. Firstly, as time passes and data may become obsolete, suitable policies to retain or not data are required. Inadequate policies may lead to loss of data, inaccurate recording, or missing of information. Solutions relying on semantic continuity of data elements by using timestamps can be adapted to solve the aforementioned issues [210]. Secondly, suitable models for storing Big Data are also challenging. Several models have been proposed, but they are tailored for specific technologies. For example, the RFID-Cuboids model [211] manages efficiently massive RFID data, achieving a significant data compression and speeding up the analysis process. Finally, understanding the optimal location for storing data is also challenging. IoT data storage can be local, distributed, and centralized. A set of researchers focuses on centralized solutions as they assume this approach more suitable for an environment with huge data, intensive queries, and data shared among different applications [212]. Among the proposed solutions, the Sea-Cloud-based massive heterogeneous data management (SeaCloudDM) system is based on relational database and uses key-value store combination [213]. The main drawback of SeaCloudDM lies in its inability to support concurrency due to the distributed lock mechanism. The solution in [214] overcomes such an issue by proposing a centralized solution based on Not Only SQL (NoSQL [215]) systems. A second set of researchers proposes localized and data-centric storages for storing data as near as possible to its production points (i.e., objects). To this aim, the ideas at the basis of the Mobile Cloud Computing (MCC) [102, 216, 217] can be exploited too. Specifically, MCC refers to the extension of Cloud Computing into the mobile environment with the goal to reduce the mobile device load. Resources external to the mobile devices (i.e., group of mobile devices in proximity, local servers) form the so-called *Mobile Cloud*, and can be exploited by mobile devices to execute applications and store data. By applying such concepts, data may be stored and retrieved from: *i)* a *virtual resource cloud*, made up of mobile devices in proximity [218], or *ii)* a local *cloudlet*, which is composed of several multi-core computers connected with the remote cloud servers [219]. MCC shared concepts also with the area of Opportunistic Computing, where mobile devices avail of each other's resources (e.g., computational capabilities, connectivity, storage), which are abstracted as services, to opportunistically invoke services [220–222]. Finally, a third set of researchers propose to dynamically adjust the data storage position according to specific conditions. For example, in [223] authors determine the optimal storage position in different WSN topologies (i.e., tree structure, linear, grid, mesh) by taking the geographical location of producers and data rate of exchanged queries into consideration.

6.8. Traffic characterization

Currently, the characteristics of the traffic generated in IoT scenarios are unknown. There exists very few works in literature that focus on analyzing the actual characteristics of M2M traffic, and the majority aims at understanding the traffic characteristics in Home Area Network (HAN) scenarios. A part of them relies on real experiments to measure and characterize the traffic through the access network, such as [224, 225]. Others focus on the characterization of exchanged traffic within the HAN. For example, in [226] authors analyze the individual effect of the most common home services (e.g., phone calls over Internet, TV streaming, data upload and download) on e2e performance in a controlled HAN environment. Such analysis provides a better understanding of HAN performance and of traffic profiles within the HAN, allowing to identify when the HAN itself is the main cause of performance disruptions. In addition, when feedbacks and incentives about the HAN utilization are sent back to users, they may also be further

motivated to a more intelligent and rationale use of the HAN network, and consequently improving the overall network performance [227].

Capturing realistic M2M traffic characteristics, as well as collecting information about IoT users habits, are still open issues. Their collection is extremely important. By exploiting the statistical representations of IoT traffic flows, it will be possible to design services tailored on users' needs and requirements.

6.9. Security

Security issues are central in IoT as they may occur at various levels, investing technology as well as ethical and privacy issues. To ensure security of data, services and entire IoT system, a series of properties, such as confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy, must be guaranteed [228, 229]. This is extremely challenging due to the IoT environmental characteristics. The scarce of objects' resources limits computation and transmission operations, while the use of short-range low-data rate protocols greatly affects packets size, resulting in a fragmentation of packets affect the security protocols. For example, an excessive fragmentation may simplify network attacks (DoS attacks), while lowering the overall system performance. Finally, devices' heterogeneity makes necessary to define a minimum set of functions implemented by all the objects to support interoperability between devices and different solutions.

We split the remaining subsection in four parts, each corresponding to a different set of security requirements, and we discuss possible solutions in order to meet them. The four identified requirements are:

i) secure authentication and authorization,
ii) secure bootstrapping of objects and transmission of data,
iii) security of IoT data,
iv) secure access to data by authorized persons.

Depending on the application, a part of or all the above requirements should be satisfied. For example, let us focus on an application to monitor the medical parameters of a patient. The monitoring activity starts when the patient arrives at the hospital and wearable devices are used to monitor her status. The monitoring activity is performed during her stay in the hospital and for a control period after her return at home. First of all, there must be a correct identification and mapping between the wearable devices and the monitored patient, and personal data must be stored safely on the device (requirement *i)*). The device has to securely join IoT, and the transmission of collected data has to ensure integrity and confidentiality (requirement *ii)*). Data is then maintained on a remote server where secure storage mechanisms are essential (requirement *iii)*). Finally, data access should be guaranteed only to authorized people such as doctors, who use it to monitor the patient's condition (requirement *iv)*).

Secure authentication and authorization

SIM cards, and the most recent MIM cards (M2M SIM cards), which have been designed specifically for IoT applications, are elements that may deal efficiently with security concerns. Among the implemented features, they secure the identity of communicating devices, perform secure data storage, and guarantee secure authentication and authorization operations by using for example PIN, PUK and Public Key Infrastructure (PKI).

Secure bootstrapping of objects and transmission of data

Bootstrapping operations refer to processing operations required before the network becomes active and available. These include installing and configuring credentials, keys, and certificates on the devices. In [230, 231], authors

investigate how constrained devices can securely bootstrap into a system. The order in which objects are bootstrapped is also important. For example, in [231] constrained devices can only be bootstrapped in circle starting from a predefined point.

Security issues affecting data communications span over three layers: network, transport, and application. The Internet Protocol Security (IPSec) protocol [232] is the standard way to secure data exchange at network level. However, it can not be directly applied to the IoT environment for several reasons: *i)* the negotiation phase, which is based on the Internet Key Exchange (IKE) protocol [233], is computationally heavy to work on small constrained devices, *ii)* the data overhead is high, even though it could be partially alleviate with suitable header compression techniques [234], and *iii)* dynamic configurations are also difficult. An alternative approach is the Host Identity Protocol (HIP) protocol [235], which uses cryptographic identifiers to allow enhanced accountability, and provides easier build up of trust. The most used secure Internet transport protocols are Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS), which run over TCP and UDP, respectively. Intuitively, TLS is unsuitable for IoT for all reasons highlighted in Section 6.4, while DTLS seems to be the solution toward which the security community is moving. Obviously, even though it is a promising starting point, some modifications are required: *i)* the introduced overhead must be reduced for example by using some specific packet optimizations or header compression techniques [236], and *ii)* e2e security issues must be solved in case of presence of intermediate nodes (e.g., proxies, application level GWs). An alternative way to create e2e security is by enforcing it at the application level. Again, standard Internet solutions (e.g., S/MIME, STRP) are inadequate because too resource expensive, but currently no solutions exist. Finally, other solutions can foresee cross-layer interactions among protocols to avoid duplicating security mechanisms at different layers.

Secure data transmissions consist also in the use of cryptographic algorithms to ensure the integrity of data traveling through the network. Conventional approaches as Advanced Encryption Standard (AES) [237] are inadequate. Conversely, lightweight cryptography (LWC) algorithms seem the most promising for this environment [238] as they are mainly tailored to constrained devices by introducing trade-offs between security levels, cost, and performance. Examples are Scalable Encryption Algorithm (SEA) [239], and PRESENT [240] for symmetric cypher, and the Elliptic Curve Cryptography (ECC) [241] family for asymmetric cipher. The latter is able to reach the same security level of the standard RSA requiring shorter keys and lighter operations [242, 243]. Another essential part for any protocols that use cryptography is hash functions. Their main duties are to provide message integrity check, digital signatures, and fingerprinting. Recently, some solutions have been proposed keeping in mind constrained devices in general [244], or specific device categories such RFIDs [245, 246].

Security of IoT data

Data aggregation is an important operations to efficiently handling IoT data. Specifically, it refers to the process that guarantees that only significant information is stored and transmitted inside the IoT environment. Aggregation is generally executed at intermediate network nodes to minimize the amount of data transmitted. Some forms of encryption (and the corresponding decryption) are usually implemented to achieve confidentiality, authenticity and integrity. However, in networks with high constrained devices, this may lead to an increase of nodes' complexity to share keys, and a higher computation and energy consumption due to need of decrypting incoming messages. A possible solution is to use homomorphic encryption schemes, which consist in aggregating directly encrypted data avoiding intermediate and unnecessary decryptions. A consequent advantage of using similar approaches is to increase the overall security, as only source and destination are capable of accessing to real data. Equally important

is to guarantee integrity and persistence to sensitive information stored in the cloud, being piece of personal data or keys used by cryptographic algorithms. Possible solutions may use on-chip ROM memory, on-chip One-Time-Programmable (OTP) technology, and off-chip flash memory.

Secure access to data by authorized persons

Security mechanisms should also guarantee that only allowed users can access some given data, defining which operations each single user or group of users are allowed to perform on the data. In general, mechanisms to avoid unauthorized accesses are very simple but efficient. For example, data could be protected by some passwords/passcodes, and a user may access sensitive data only when he generates a request carrying the right password/passcode. In some cases, solutions based on Sign-On (SSO) mechanisms could be useful. Basically, SSO refers to a unified login system that allows users to login only once, and with which users may access a group of applications associated with the login point (i.e., all the mutual trusted applications) without further authentication processes [247, 248].

7. IoT initiatives

As IoT is gathering its momentum, the number of initiatives around the world taken by research organizations, industries, standardization bodies, and governments to bring IoT to a mass market, is significant. In this section we discuss the most representative ones. More specifically, first we look at the major past and still ongoing IoT projects aimed at investigating novel solutions (e.g., architectures, platforms, communication protocols, and tools). Then, we discuss the main directions followed by industries as well as those industrial sectors considered attractive for the envisaged profit margin increase. Finally, we focus on standardization activities, which are of primary importance to remove the technical barriers and ensure the interoperability among IoT applications, services, and networks.

7.1. IoT projects

The number of funded projects worldwide aimed at investigating the IoT challenges is rapidly increasing. Starting from 2009 the European Commission launched the IoT initiative within the 7^{th} Framework Programme (FP7) focusing on the development of architectures and optimized technologies for supporting the multitude of novel IoT-based applications and services. This research line continued under the "Internet-connected object" initiative, focused on developing context-aware, reliable, energy-efficient and secure distributed networks of cooperating sensors, actuators and smart devices. A wide range of EU research and application projects have been launched within these two initiatives, supported and coordinated by the European Research Cluster on Internet of Things (IERC). IERC aims at promoting a common vision of the IoT paradigm, facilitating also the knowledge sharing and the secure IoT deployment at world level [249]. The US government started funding projects on IoT almost in the same years. Specifically, four research projects have been funded since 2010 as part of the "National Science Foundation's Future Internet Architecture (NSF FIA)" program, which aims at designing and validating comprehensive new architectures for the next-generation Internet. China, Korea and Japan have also started research programs about IoT. In Korea, only recently the National Research Foundation of Korea (NRF) decided to support projects specifically on IoT. Japanese investments on IoT started when the New Generation Network Promotion Forum (NWGN) was established in 2007. In addition, after the 2011 Tohoku earthquake, the IoT interest converged on specific sectors such as energy saving and renewable energy. As far as China, the focus on IoT has grown considerably since 2009 and it has been supported by several research and development programs, such as: the "National Basic Research Program of China" (973 program), the "National High Technology Research and Development Program of China" (863 program), and the "National Natural Science Foundation of China".

In the remainder of this section, we quickly overview various IoT projects - in progress or already completed - around the world. For the sake of clarity they are grouped in three main categories according to the main objectives (see Figure 9). Interested readers may refer to projects' website for further information.

The first group of IoT projects focuses on the development of IoT architectures that ensure interoperability between vertical application solutions and different technologies. A subset of them focuses on business services and on the development of SoA-based architectures and dynamic environments to semantically integrate services into IoT (e.g., EBBITS [250], IoT.est [251]). Another subset focuses on cloud computing architecture to meet the challenges of flexibility, extensibility and economic viability of IoT (e.g., NEBULA [252], BETaaS [253]). Theoretical models of the IoT architecture and the definition of an initial set of key building blocks are key objectives of [254] and IoT-A [255], respectively. Furthermore, the main goal of iCORE [256] and COMPOSE [257] is to develop an open network architecture based on objects' virtualization that encompasses the technological heterogeneity, while BUTLER [258] and MobilityFirst [259] aim at developing open architectures providing secure location and context-aware services, transparent inference of users' behaviors and needs, and actions on their behalf to improve their quality-of-life. The IoT6 project [260] is an example of researching the potentiality of IPv6, and related standards, within a high-scalable SoA-based architecture in order to integrate smart and heterogeneous things components.

The second group of IoT projects deals with the design of innovative communication protocols for IoT. For example, SNAIL [261] proposes a network platform fully compatible with the IETF standards, enabling smart objects to communicate seamlessly one another, while EPCSN [262] aims at developing wireless sensor networks like EPC systems. The ICSI project [263] focuses on Intelligent Transport Systems (ITSs) and proposes intelligent solutions for communication protocols, advanced sensing, and distribution of context-data to enable advanced traffic and travel management strategies. A subset of projects deals with cross-layer communication challenges. For example, CALIPSO [264] focuses on energy efficiency and network lifetime increase by proposing solutions spread at the network, routing and application levels. Conversely, other projects focus on a single network layer, such as GAMBAS [265], OPENIOT [266] and SmartIoT-SSC [267]. Specifically, GAMBAS focuses on open source and adaptive middlewares for enabling utilization of behavior-driven services, OPENIOT on the dynamic formulation of self-managing cloud environments, and SmartIoT-SSC on spontaneous service composition for smart IoT.

The last group of projects aims to develop software frameworks that can be directly used and tested by users. This is the case of ELLIOT [268], where users/citizens can test the platform and join in the creation, exploration,

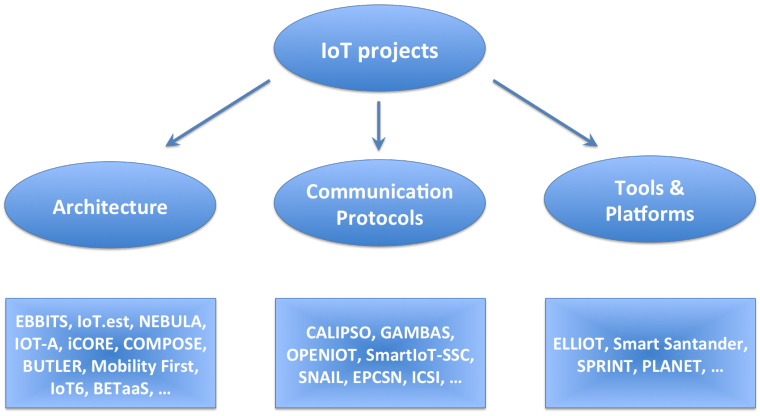

Figure 9: Taxonomy of IoT projects - active and completed - all around the world.

experimentation of novel IoT ideas, applications and services. Similarly, SmartSantander [269] focuses on creating an experimental facility for a smart city in order to research and test architectures, key enabling technologies, services and applications (e.g., control and management of environmental/building parameters, of gardens, of parks, of different sensors and mobile devices). SPRINT [270] provides a platform to connect the software tools used by the industrial companies within the project and to allow integration of different sub-systems at the design level. Conversely, the platform developed in PLANET [271] is designed for maintaining and testing heterogeneous and large-scale networks, with particular attention to biological reserves and airfield scenarios.

7.2. Industrial perspective

As explained in Section 1, the potentialities of IoT are limitless and the economic value associated with IoT is expected to produce a fast GDP increase. Therefore, industrial and business priorities are deeply affected by this emerging paradigm. This section aims at providing an overview of the industrial perspective on the IoT, highlighting those areas considered the most attractive and where industrial companies are making significant capital investments[6]. In Section 4 we have seen the huge variety of envisioned IoT applications, spanning in nearly every field. However, the emerging trend indicates that, in the medium term, the industry will focus its effort mainly in one sector: the Smart City domain (see Section 4.2). Indeed, industry believes that the development of innovative and practical solutions promoting sustainable and secure cities is the key to be competitive in the market. Specifically, the three main areas of interest are: *i)* smart grid, *ii)* smart building, and *iii)* smart home. Figure 10 summarizes the main industrial priorities and provides some examples of commercial solutions for each area.

7.2.1. Smart grid

As discussed in Section 4.2.2, a number of technological transformations changed radically the energy distribution system in the last decade. The electric grid, conceived at the beginning as a centralized unidirectional system, is now turning into a high distribution system, referred to as *smart grid*, where users can consume but also generate the power. Such process is leading to a significant increase of efficiency in the electricity transmission-distribution-control chain,

[6]Contributions for this section come from a number of different IoT workshops (e.g., ETSI M2M Workshops, IEEE-SA IoT Workshops, M2M Forum).

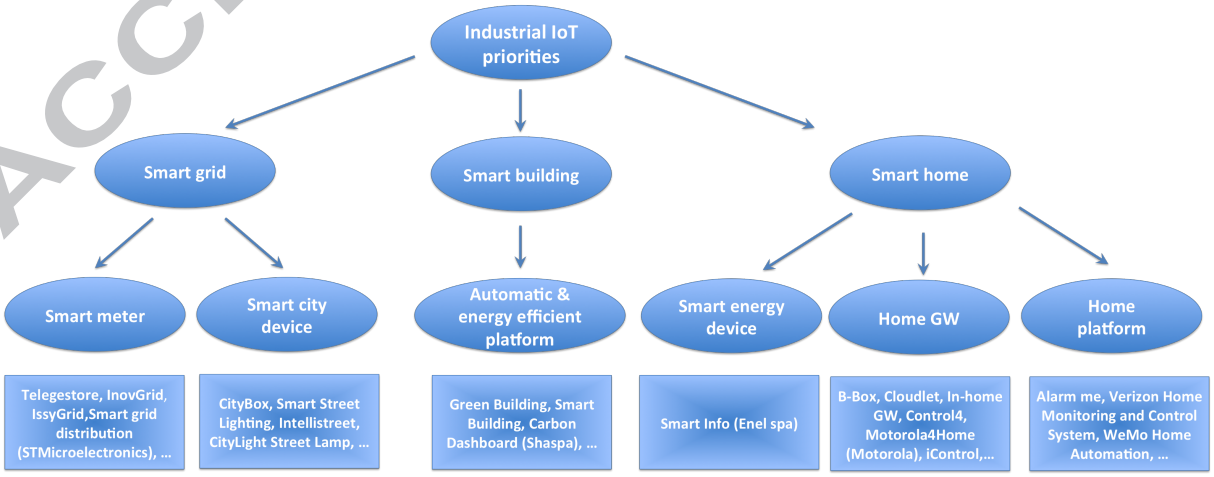

Figure 10: Key industrial IoT priorities and examples of commercial products.

as well as to a reduction of CO_2 emissions. For example, it is envisaged that a 5% improvement of the US grid is equivalent to cut CO_2 emission of 53 millions cars [272]. To meet the performance targets set by major countries, under their research and development plants on smart grids (see, for example, Europe 20-20-20[7] [273, 274], and US DoE Smart Grid Research and Development Program[8] [275]), major industries are making massive investments to allow the convergence of three different networks: *i)* the energy network (e.g., electricity, gas, heat), *ii)* the physical network (e.g., roads, train tracks, water), and *iii)* the communication network (e.g., fiber, wireless, 4G). Examples of developed Smart Grids are available, worldwide. Among them, it is worth remembering the earliest (and still largest) example of a smart grid that is installed by Enel S.p.A. of Italy, named Telegestore[9]. The project started in 2001, when the company replaced old electromechanical meters with electronic smart meters, installing 32 million of them in only five years. Today, the Enel smart grid is composed of smart meters, data concentrator devices and a remote metering management system. Telegestore can count on such large infrastructure to perform bidirectional communication to remotely read the consumption of its customers, remotely manage contractual operations and monitor the quality of service. InovGrid[10] by EDP Distribuição is a project with the target to equip the first urban area in Portugal with a smart grid. In addition to automate grid management, to improve service quality, and to reduce operating costs, the project boosts the penetration of micro generation and electric mobility. Another ambitious initiative will be realized in the city of Issy-les-Moulineaux, where nine major industrial groups will create IssyGrid [276], the first district smart grid in France. IssyGrid will consist in a large-scale smart grid able to measure energy consumption in homes and buildings, to manage renewable energy productions (e.g., solar panels, co-generation units, windmills) and energy storage devices, and to use information about consumption in order to identify incentive polices for energy optimization. Additional services will be offered to citizens. Street lamps will be equipped with sensors and smart devices to efficiently manage the street lighting (thus consuming one third less than traditional lamps), and the public street lighting network will be turned into a digital network connected with Internet to provide new urban services, such as public loudspeaker, CCTV, assistance for the visually impaired, pollution readings, traffic control, parking tolling, charging for e-vehicles. Examples of such commercial products are CityBox[11] by Bouygues, Smart Street Lighting[12] by Echelon, Intellistreet[13] by Wired.

7.2.2. Smart building

The industry commitment towards sustainable building construction is another strategic industrial priority. This can be achieved by working at two distinct levels: *i)* making buildings more energy-efficient, through a better control of their actual power consumption and innovative technologies to produce energy and reduce consumption, and *ii)* creating automated buildings where all services (e.g., fire detection, HVAC, light, power, access control, elevators) are connected and managed efficiently through an IP-based backbone. For example, the Green Building, the new headquarters building in Turkmenistan by Bouygues Construction, is a notable example. A smart ceiling lighting fixture, composed of an IP-based network of luminance and temperature sensors, is used to reduce energy and light pollution. Moreover, the presence of motorized shutters, which open automatically according to inside/outside tem-

[7] The "20-20-20" EU objectives for 2020 are: *i)* a 20% reduction in EU greenhouse gas emissions from 1990 levels, *ii)* a 20% improvement in the EU's energy efficiency, and *iii)* a 20% of EU energy production from renewable resources.

[8] The US objectives for 2030 are: *i)* a 20% reduction in the US peak energy demand, *ii)* a 100% availability for manage critical loads, *iii)* a 40% improvement in system efficiency, and *iv)* a 20% of energy capacity coming from renewal sources.

[9] http://www.enel.com/en-GB/innovation/smart_grids/smart_metering/telegestore/

[10] http://www.inovcity.pt/en/Pages/inovcity.aspx

[11] http://www.bouyguesenergiesservices.com/solutions/citybox.php#citybox

[12] https://www.echelon.com/applications/street-lighting/

[13] http://intellistreets.com/index.php

perature, guarantees a comfortable permanence also in area without air conditioning systems. A building management system could centralize metering of real time water and energy consumption (e.g., heating, cooling, ventilation, lifts, lighting) enabling to detect and adjust unusual consumption. Another relevant example of smart building is the Smart Building Solution by Echelon. Basically, it is composed of smart transceivers embedded in building automation devices (e.g., sensors, thermostats, motion detectors, air handlers, and chillers), a smart server controller connecting devices and controlling networks through open protocols (e.g., LonWorks, BACnet, Modus), and an open operating system (OpenLNS) that facilitates resource management. Important examples of buildings relying on such a platform are the Louvre museum at Paris and Beijings Bird's Nest stadium.

7.2.3. Smart home

Another important area is the Smart Home: the term "home" refers to an eco-system of devices, home appliances and sub-systems, all interconnected and interacting one another. The main challenge within this research area is to facilitate the communication between all heterogeneous devices and applications running on them. Industry proposes new solutions and products that include simple home energy monitoring, home automation, home media services, home security and comfort to cite a few. Many solutions focus on fostering a more rational electricity consumption at home, which in Europe accounts for 29% of the overall energy consumption [277]. To achieve this, the interaction with the grid becomes fundamental. The Smart Info device, developed by Enel S.p.A. within the Energy@Home initiative [14], represents a good example of a solution to efficiently interface the smart grid and the electric home appliances. Such innovative device can be plugged in every domestic appliance allowing their communication to make them work only when their energy consumptions are low, and allowing users to consult information available on the smart meter. Other solutions focus on the development of smart gateways that, in addition to maximize the home efficiency, provide entertainment services. The main challenge here is to design a solution to limit the number of "smart boxes" within the home. To active this, the smart gateway, if possible based on an open platform, has to implement a number of different features within the same device and it has to interface with many different communication technologies. Shaspa Bridge by Shaspa, In-home gateway by STMicroelectronics, Control4 by Control4 are examples of gateways that allow users to have a clear view of the energy home consumption. In addition, they allow to interact and manage remotely any home devices and appliances. Although, currently, the gateway represents a fundamental IoT building block and the enabler for new IoT services, in a long term view it will lose its importance and will disappear, because everything will be connected though *virtualization* in the cloud. Each each physical object will be virtualized in the cloud, so that the IoT will be seen as a *virtual continuum* of real objects and their representations, and the cloud will facilitate users to access resources and create their own applications.

Security is a hot topic in IoT industries. The focus is mainly on data privacy and how to guarantee robustness and integrity of the IoT system. The robustness and the integrity are a complex problem because the system can be under attack at different levels. For example, concerning the hardware level, it has been shown that open OS platforms are subject to malware (e.g., Android is the target of 92% of detected malware [278]). Moreover, many attacks are possible to software failures. In the industry vision, usage of SIM cards represents a valid starting point. SIM is turning into a Secure Element (SE) where hardware and software are designed to be robust and secure. For example, the new SIM generation is composed of a MCU (ARM Secure Care) and a Crypto Co-processor to crypto data, assuring highly stability to SE platforms. A usability example is the Octo Telematics project[15], where SEs offer services for

[14] http://www.energy-home.it/
[15] http://www.octotelematics.com/en

car insurance (e.g., pay-as-you-drive, "green" car insurance, whose policy depends on the personal CO_2 emissions), for real traffic monitoring, for smart vehicle tracking. Advantages of using SEs in IoT are manifold. Among them, notable are: *i)* secure connection (e.g., at routing level, at e2e level), *ii)* data security (i.e., message cryptography, data integrity), *iii)* secure remote management (e.g., application verification, application loading, remote management), and *iv)* safe storage.

Another important issue for industries is to understand how monetizing IoT services. A common understanding is that the main value resides in data and not in the connection. Data opens opportunities for business. Indeed, IoT data is owned by users, who decide to share it or not. Therefore, traditional business models are not directly applicable, but novel ones should be proposed.

Standardization is another key IoT topic. There is a general industrial agreement that, for a massive spread of IoT, a lot of standardization challenges need to be solved. Issues about data format, data interfaces, protocols, service platform, and architecture are some examples. In Section 7.3 we will carefully discuss the main standardization activities.

7.3. Standardization

The past years are characterized by an intense increase of standardization activities connected with IoT. Indeed, the main effort is to avoid excessive fragmentation of solutions, and to define standards for interoperable solutions. To this aim, a number of bodies and alliances have launched standardization activities on IoT. Some of them (such as EPCglobal Inc™, IEEE, IETF, 3GPP, IPSO Alliance, ATIS, CCSA, OMA, NIST) are focused on technologies, addressing sensing and communication issues, while others (such as ETSI, IEEE-SA, and the just launched global oneM2M initiatives) consider IoT as a whole, addressing standardization of the service architecture, of its components, and the related interactions. Tables 5 and 6 provide a list of the main standardization activities, which will be presented in the remainder of this section.

7.3.1. RFID standardization

Concerning to RFID technologies, the joint-venture organization between GS1 and GS1 US, named EPCglobal Inc™, leads the EPC standardization to spread the use of RFIDs. Specifically, EPCglobal Inc™ has defined a number of standards related to RFID data (e.g., TDS [16], TDT [279]), which oversee the EPC representation and the rules to include data on the EPC tag itself, and the security functions distributed across the EPCglobal Network using the X.509 certificate [280]. Further activities cover location service standards. For example, Object Name Service (ONS) [169] represents a system to locate metadata and services associated with a given EPC, while EPC Information Services (EPCIS) [281] is used to enable all the enterprises involved in the EPCglobal Network to know the EPC-objects position and to share the EPC-related data. Other specifications address the standardization of communication protocols at low frequency (13.56MHz) [282] and at high frequency (860 MHz-960 MHz) [283]. Standards on discovery services are currently under development.

In Europe, RFID standardization activities started as a result of mandate M/436 issued by European Commission in 2009 to the three major SDOs (i.e., CEN, CENELEC, and ETSI), who set up a Specialist Task Force (STF), named STF 396, to develop common guidelines for RFID implementation. The mandate addresses data protection, privacy and information security aspects of RFID. In addition, CEN TC 225 WP 5 mainly focuses on RFID privacy issues, while ETSI ERM TG 34, TG 28 and TG 37 focus on several RFID aspects including a more efficient spectrum usage in the range [9kHz - 40GHz], the coexistence among RFID devices and E-GSM-R, and the interoperability among tags manufactured by different vendors.

Table 5: Standardization activities

Standardization area	Organization	Main objectives
RFID	EPC global	data representation/storage, interface, communication protocols, discovery services
	STF 396 (CEN/CENELEC/ETSI)	data protection, information security, privacy
	CEN TC 225 WP5	privacy issues
	ETSI ERM TG 34, TG 28, TG 37	spectrum usage, tag interoperability
	ISO/IEC JTC1/SC31 WG4, WG6	data protocol, mobile RFID
	ITU SG13, SG16	communication protocols, architecture, multimedia information access
Sensors	IETF 6LoWPAN	adaptation layer for the IPv6-IEEE 802.15.4 interoperability
	ISO/IEC JTC1 WG7, WG4	architecture, application protocols, interoperability in hybrid RFID-sensor environment
	ITU-T SG13, SG16	USN, architecture for USN, service description for USN middleware, USN automatic location identification capabilities
NFC	ISO/IEC JT1 SC 06, 17	signaling interface, data protocol, NFC communication mode, security aspects
	ECMA TC47	same objects of ISO/IEC JT1 SC 06, 17
	NCF Forum	architecture, data exchange protocol, logical link protocol
	GSMA NFC WG	mobile NFC integrated with SIM, handset and SIM requirements, interface
Communication protocols	IEEE	VLC optical communication, broadband power line communication, multiple home networking technologies
	3GPP	architecture, signaling congestion, network overload
	IETF	IP interoperability, routing/application protocols for constrained resources
	W3C EXI WG	efficient XML-based solutions

ISO and IEC formed two working groups within the subcommittee 31, named WG4 and WG6, respectively. The former develops a data protocol between RFID reader and RFID tag [284, 285], while the latter investigates Mobile RFID technologies (e.g., mobile phones equipped with RFID interrogator). Specifically, the main WG6 objective is to extend existing methodologies and protocols for static RFIDs to the mobile RFIDs (i.e., MAC protocols, collision avoidance/arbitrary schemes, security, and privacy aspects) [286, 287].

ITU SG13 and ITU SG16 are responsible for studying networking aspects, architecture and multimedia information access for the support of applications and services using tag-based identifications [288–292].

7.3.2. Sensor network standardization

The majority of sensor-network standardization activities is carried out within IEEE TC on Sensor Technologies, IEEE WG for WPAN, IETF 6LoWPAN, and ZigBee Alliance. Another part is covered by ISO/IEC JTC1, which formed WG7 in 2009, to standardize a reference architecture for sensor networks (i.e., Sensor Network Reference Architecture - SNRA) able to interface heterogeneous environments (e.g., smart grid systems) and collaborative information processing services. To this end, a number of standards, such as ISO/IEC 29182 [293], ISO/IEC 20005 [294], and ISO/IEC 30101 [295], have been proposed. In addition, ISO/IEC JTC1 WG4 studies rules and functions (mainly application protocols) to manage sensors when operating in conjunction with passive and active RFID tags [296]. ITU

is also working on this area, carrying out several activities on Ubiquitous Sensor Networks (USN). Specifically, ITU-T SG13 and ITU-T SG16 aim at establishing functional requirements and architectures for supporting USN applications and services, service description for USN middleware, and USN automatic location identification capabilities [297–300]. In addition, ITU-T SG 17 contributes to define secure solutions for secure technologies, middleware, and routing [301–303].

7.3.3. NFC standardization

Concerning NFC technology, the major actors are ISO/IEC JT1 subcommittees 06 (SC06), ISO/IEC JT1 subcommittees 17 (SC17), and ECMA TC47. They specify the signaling interface and a set of protocols (i.e., radio frequency interface, initialization, anti-collision and data protocol) for NFC, named NFCIP-1 (see ISO/IEC 18092 [304] and ECMA-340 [305]), and the mechanism to detect and select the NFC communication mode, named NFCIP-2 (see ISO/IEC 21481[306] and ECMA-352 [307]). In addition, they work on security aspects by defining a protocol stack, named NFC-SEC, that enables (application independent) encryption functions on the data link layer, on top of NFCIP-1 (see ISO/IEC 13157-1 [308], ISO/IEC 13157-2 [309], ECMA-385 [310] and ECMA-386 [311]). Another major actor, who drives the NCF standardization, is the NCF Forum. It focuses on NFC specifications for a modular architecture that ensures interoperability between different NFC tag providers and NFC device manufactures. To this aim, a number of technical specifications have been defined: *i)* NFC Data Exchange Format (NDEF), *ii)* Tag Type Operation, *iii)* Record Type Definition (RTD), *iv)* Logical Link Control Protocol (LLCP), and *v)* NDEF Exchange Protocol. In 2006, also GSMA approached the NFC area by forming a NFC Working Group focusing on mobile NFC integrated with SIM. The use of mobile phones, where NFC chips are embedded into SIM cards, enables a set of new digital services, such as ticketing on public transport systems, and payment systems similar to credit-card systems. To this aim, GSMA worked on the definition of handset and SIM requirements to ensure security features, and on common APIs to guarantee portability across many different handsets.

7.3.4. Communication protocol standardization

IEEE is the main contributor for the standardization of physical and MAC layers for IoT.

Recently, with the advances in LED technologies that allow intensity modulating of LED lights, there has been a renewed interest towards optical technologies for short-range. Specifically, IEEE 802.15 TG 7 is in charge of writing standards to transmit data over short-range wireless optical links using the visible light [312]. Visible light communications (VLCs) guarantee high data rate communications at short distance (up to 96Mbps, ~3 m), with ~300 THz of available visible light spectrum at low power and cost. They are also immune to electromagnetic interference and non-interfere with Radio Frequency (RF) systems. IEEE is also involved in developing standards for smart grid and home area networking. For instance, the IEEE 1901 Broadband over Power Line (BPL) standard [313] is designed for a wide range of applications including smart energy, smart transportation and Home Area Networks, allowing rate up to 500 Mbps. Conversely, IEEE 1901.2 [314] refers to power line communications (PLCs) for low frequency and

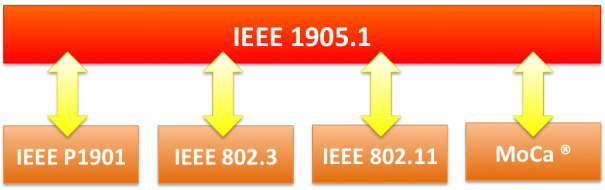

Figure 11: IEEE 1905.1.

low data rate (less than 500kHz, 500kbps). The major use is for smart grid applications (e.g., smart metering) and e-vehicle charging (at the station), but it can be also used in combination with lighting or solar panels. The standard also provides security functions. In 2012, IEEE launched the IEEE 802.24 Smart Grid Technical Advisory Group (TAG), which focuses on the use of IEEE 802 standards in smart grid applications. IEEE 1905.1 [315] is another interesting standard designed specifically for "convergent digital home network". It provides an abstraction layer for multiple home networking technologies to support dynamic interface selection for packets transmission, e2e QoS and secure configurations (see Figure 11). Currently, it works mainly with proprietary technologies (i.e., Powerline communication, Ethernet, WiFi, and MoCA 1.1), but it is extendable to other home networking technologies.

Another major actor in the standardization of communication protocols is 3GPP, which mainly focuses on how cellular networks can support machine-type communications (MTC). Specifically, in Release 10, the 3GPP System Architecture WG 2 addresses the "first and last mile" problem, and defines network improvements in UMTS and LTE core networks by addressing the MTC signaling congestion and network overload (see also Section 6.1).

Significant contributions at higher layers (layer 3 and above) are produced within the IETF 6LoWPAN WG, whose main objective is to allow the IP protocol to efficiently work on smart constrained devices (see Section 6.2). The WG was originally conceived to guarantee the IP interoperability on IEEE 802.15.4. Recently, standardization activities include solutions allowing other technologies (e.g., Wavenis and PLC) to use the same 6LoWPAN mechanisms. Further standardization activities is carried out under IETF ROLL WG, which focuses on routing issues over low power and lossy networks by proposing the RPL routing protocol (see Section 6.4), and under the IETF CoRE WG, whose main objective is to realize the REST architecture to support resource-oriented applications. Specifically, CoRE is currently proposing the Constrained Application Protocol (CoAP) [191] (see Section 6.4). Other interesting standardization activities aim at providing very compact representations of languages that can be described by a grammar (e.g., XML, Java, HTTP, etc.) to simultaneously optimize performance and the utilization of computational resources. For instance, W3C EXI WG investigated alternative XML forms developing the Efficient XML Interchange (EXI) format [316]. EXI uses a grammar-based approach that encodes the most likely alternatives of an XML document in fewer bits and a small set of datatype representations. While it is optimized specifically for XML, it may work also with any other languages.

7.3.5. IoT standardization

The need to look at the IoT paradigm as a whole to speed up its diffusion resulted also in the establishment of a number of new WGs focusing only on IoT, as shown in Table 6. For instance, at the international level, ITU-T launched a Joint Coordination Action (JCA) on IoT with the scope of coordinating the whole ITU-T work on IoT including networks aspects of identification of things, and ubiquitous sensor network (USN) [317–320]. The ISO/IEC JT1 counterpart established WG5 with the purpose of identifying IoT-related market requirements and standardization gaps. At the European level, CEN launched the TC 225 WG6 focusing on identification technologies, data gathering protocols, and communication protocols. Conversely, ETSI is more oriented on M2M standardization activities. To this aim, as deeply explained in Section 6.1, the ETSI TC M2M has been established to develop an e2e architecture and protocols for M2M.

In North America several associations and standard organizations are very active in promoting IoT standards:

* TIA (Telecommunications Industry Association) formed Engineering Committee TR-50 on Smart Device Communication, specifying ubiquitous protocols for communicating with smart devices used in industries and releasing its *Smart Device Communications Reference Architecture* standard (TIA-4940 [321]),

Table 6: Objectives of the most important standardization WGs/initiatives established recently focusing on IoT as a whole

Organization	Objectives
ITU-T JCA IoT	Networking aspects, identification, USN
ISO/IEC JT1 SWG WG5	Identification of IoT-related market requirements, standardization gaps
CEN TC 225 WG6	Identification technologies, data gathering protocols, and communication protocols
ETSI TC M2M	M2M e2e network reference architecture, identification, addressing, security, privacy
TIA R-50	Ubiquitous protocols for industrial smart devices communications
ATIS M2M Committee	Service layer and interfaces towards application and transport layers
IEEE 802.16 M2M TG	IEEE 802.16 improvements to support M2M applications
OMA M2M	Device management extension, location services
CCSA TC10	Green community, vehicle communication systems, e-health monitoring
ARIB M2M Study Ad Hoc Group	Smart grid, smart cities, smart home
TTA M2M PG	Service requirements, data structure, identification
oneM2M	M2M service layer platform, service architecture, resource/data access protocols and management, security, privacy

* ATIS (Alliance for Telecommunications Industry Solutions) launched the M2M committee to define a common service layer for multiple M2M applications and the correspondent interfaces among the application and the transport layer(s),
* IEEE established the IEEE 802.16 WG M2M TG aimed at studying IEEE 802.16 improvements (i.e., IEEE 802.16p, IEEE 802.16b) to support M2M applications. Basically, it investigates efficient ways to support low power consumption at the device, a significant large number of devices at the base stations, small burst transmissions, and improved device authentication,
* OMA (Open Mobile Alliance) is interested in extending the well-established device management protocol to M2M communications (e.g., LWM2M, DM Gateway supporting M2M networks for constrained cellular and other M2M devices, DM security enhancements), and in working on location services for mobile M2M applications.

The standardization of IoT and M2M is an important theme in Asia, too. In China, the IoT standardization is driven by CCSA Technical Committee 10, which works mainly in the areas of green community, vehicle communication systems, and e-health monitoring. The Japanese ARIB established the M2M Study Ad Hoc Group focusing on standardization for smart grid, smart cities and smart homes, while the Korean TTA founded M2M PG (PG708) working at service requirements, data structure, and identification scheme.

As discussed above, a huge number of standardization activities looking at the IoT paradigm as a whole have started, however they still remain highly fragmented among the individual bodies. To boost the global IoT market, a further collaboration effort and an effective interaction of standardization organizations is mandatory. This is required to reduce standardization overlap and the risk of lack of interoperable solutions. An example in this direction is the *oneM2M*[16] initiative, which is considered the evolution of ETSI TC M2M into a global partnership project. In July 2012, seven SDOs (i.e., ARIB, ATIS, CCSA, ETSI, TIA, TTA, and TTC) have agreed to create a global harmonization group to ensuring the most efficient deployment of M2M communications systems. The *oneM2M* objective is to develop e2e specifications for the development of a common M2M Service Layer platform, which works with different hardware and software and is able to connect the myriad of IoT devices. Activities within oneM2M include: a Service

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

Layer platform, a Service Architecture, open/standard interfaces, protocols to access resources, security and privacy enforcement (e.g., authentication, encryption, integrity verification), application discovery services, data collection for billing and statistical purposes, identification and naming of objects, management aspect (i.e., object and data management).

8. IoT emerging research directions

So far we have analyzed and discussed the main challenges that the international community is facing to make the IoT paradigm a reality. We have also provided an overview of the industrial perspective highlighting which are the strategic priorities for industries. Obviously, the above discussion, although extensive, can not be considered exhaustive. In this section, we complement it by providing a brief overview and discussion with two other important networking and computing paradigms: social networks and context-aware computing.

8.1. IoT and Social Networks

The use of the social network paradigm in the IoT context can open new possibilities of interaction among smart objects. The main idea is that objects may have a social consciousness and may exhibit social behaviors allowing them to build their own social network of objects [322]. This social network of objects can be exploited to enhance the trust level between objects that are "friends", to guarantee a higher network navigability, and to make applications and services more efficient. Indeed, if objects share information about their provided services, service discovery may exploit the social network of "friends" to search information, thus becoming manageable and avoiding the usage of those discovery mechanisms - generally used in Internet - that are not able to scale with the envisioned multitude of IoT devices. It is envisaged that the realization of the above vision goes through three different stages, corresponding to the three distinct levels of social involvement of the objects [322]. The first step relies on exploiting humans, and their social network relationships, to share the resources offered by smart things. By using different web protocols and communication paradigms, objects may communicate with the human social network (e.g., posting information about their status) but not with other objects. SenseShare [323] is an example where users may share data gathered by their smart objects with friends through the use of Facebook only, while in [324] several social networks can be exploited for data sharing. Users may choose, for each device, the social network for sharing data and may allow other users to use their devices. In addition, the automatic publishing of device messages on personal profile is allowed. In the second step, objects have interaction with the environment and exhibit pseudo-social behaviors with objects. For example, in [325] devices are allowed to establish temporary relationships, which, however, are still controlled by their owner. Finally, "social objects", i.e., objects that take part and actively form a social network of objects, represent the last step. In [326–328], authors focus on the social relationships that may be established in the social network of objects (named *Social Internet of IoT* (SIoT)). Such relationships are among objects rather than their owners. Objects may become "friends" and may form social groups autonomously, for the benefits of human but without their intervention. Inspired by social human interactions, authors define five types of relationships among objects: *i) parental objects relationship (POR)* - established among similar objects that are produced in the same period and by the same manufacturer, *ii) co-location objects relationship (C-LOR)* - established among objects located always in the same place, *iii) co-work objects relationship (C-WOR)* - established among objects that periodically cooperate for a service/application, *iv) owner objects relationship (OOR)* - established among objects associated to the same user, and *v) social objects relationship (SOR)* - established among those objects that come in contact by chance, mainly because their owners meet for personal reasons. These relationships may be static and not change over time (e.g., POR), or may evolve

towards complex social structures (e.g., C-WOR, SOR). Authors also propose a system architecture that incorporates the features required for the SIoT realization, and analyze the social structure. They observe that statistically exists a correspondence between geographical distance among nodes and the type of relationship that links them. In addition, they investigate which are the social rules and structures that mainly characterize objects in SIoT.

8.2. IoT and Context-aware computing

Context awareness has been exploited since the early 1990s by various computing and communications paradigms (e.g., desktop and web applications, mobile and ubiquitous computing and communications), and refers to any kind of information that can be used to characterize the situation of an entity (e.g., a person, an object, a place) [329]. Context awareness may provide a great support to process and store the Big Data, and to make their interpretation easier [330]. Another advantage associated with the use of context will be the implementation of efficient services, such as service discovery mechanisms. Indeed, IoT services run in a highly dynamic environment composed of trillion of nodes that may move, so that services may suddenly appear or disappear, at any time. To this aim, information about object's features, its status, its geographical location, and security data may be exploited to enrich the knowledge on services and refine for instance the choice of the most suitable provider. For example, in [331, 332], authors propose an efficient solution for distributing and retrieving services in the IoT environment. In the authors' view, the first step needed for a rapid diffusion of the IoT is to decouple the name of the object (i.e., its identifier) from its physical location (i.e., locator), which in the classic Internet approach are instead tightly coupled through the IP address. The next step is then to enrich the locator with context metadata, which can be of any type of information that can be used at any level, forming the so-called *enriched locator (e-locator)*. E-locators allow a better accessibility and exploitation of the provided services. This is achieved by two different services: an e-locator distributing service and a lookup service. The former deals with efficiently distributing the e-locators of service providers, while the latter returns a list containing the e-locators of those peers maintaining that particular service. By checking this list, the subscriber's application may choose the best provider based on characteristics described by the e-locator and according to device capabilities and user preferences. For example, if the e-locator consists in a geographic location, the lookup service may provide the list of the providers in the proximity of the subscriber, according to a desired level of accuracy (e.g., 1 km, 10 km). Both services (i.e., e-locator distribution and lookup) are based on a non-structured P2P network, created and maintained among high-capability devices (e.g., access network devices).

9. Conclusions

The proliferation of a new generation of objects, equipped with embedded intelligence and communicating-actuating capabilities, pushes towards a fast realization of the Internet of Things (IoT) vision. According to this emerging paradigm, everything will be seamlessly connected to form a virtual continuum of interconnected and addressable objects in a worldwide dynamic network. The result will be a solid underlying structure on which users may develop novel applications useful for the entire society.

In this paper, we have defined the fundamental characteristics of IoT, describing the technologies involved in its realization as well as the envisaged applications. In addition, we have discussed the major challenges that need to be faced for supporting the IoT vision, which cover with different research areas: architecture, communication, addressing, discovery, data processing, data management, security and privacy, etc. A number of solutions aimed at solving those challenges has been proposed, however they are not exhaustive and do not cover all the various aspects. As a result, many open issues still wait for suitable solutions. Moreover, we have analyzed the industrial perspective

by providing an overview of the main attractive sectors and where industries are making capital investments for the mid- and long- term. Finally, we have reported some interesting activities that standardization bodies have started recently specifically on the IoT theme. Indeed, standardization is the key enabler for IoT to avoid fragmentation while enabling interoperability of proposed solutions.

As IoT is an emerging paradigm, it is highly dynamic and continuously evolves. Although we have overviewed the main IoT research area as well related IoT challenges, many other research issues can be identified. For example, with the forthcoming advent of nano-technology and the development of nanoscale devices, innovative solutions tackling channel modeling, information encoding, and communication protocols, are also required to allow the integration of these nano devices into IoT [333].

[1] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Tröster, G. Tsudik, F. Zambonelli, Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence , Pervasive and Mobile Computing 8 (1) (2012) 2 – 21.

[2] R. Poovendran, Cyber-Physical Systems: Close Encounters Between Two Parallel Worlds [Point of View], Proceedings of the IEEE 98 (8) (2010) 1363–1366.

[3] K.-J. Park, R. Zheng, X. Liu, Cyber-physical systems: Milestones and research challenges, Computer Communications 36 (1) (2012) 1–7.

[4] I. Lee, O. Sokolsky, Medical cyber physical systems, in: Proc. of 47th Design Automation Conference, 2010, p. 743748.

[5] J. Hur, K. Kang, Dependable and secure computing in medical information systems, Computer Communications 36 (1) (2012) 20 – 28.

[6] K. Sampigethaya, R. Poovendran, L. Bushnell, Secure operation, control, and maintenance of future e-enabled airplanes, Proceedings of the IEEE 96 (12) (2008) 19922007.

[7] S. R. Azimi, G. G. Bhatia, R. Rajkumar, P. Mudalige, Vehicular networks for collision avoidance at intersections, in: Proc. of SAE 2011 World Congress, 2011.

[8] G. Hackmann, F. Sun, N. Castaneda, C. Lu, S. Dyke, A holistic approach to decentralized structural damage localization using wireless sensor networks, Computer Communications 36 (1) (2012) 29 – 41.

[9] S. Barro-Torres, T. M. Fernndez-Carams, H. J. Prez-Iglesias, C. J. Escudero, Real-time personal protective equipment monitoring system, Computer Communications 36 (1) (2012) 42 – 50.

[10] G. Schirner, D. Erdogmus, K. Chowdhury, T. Padir, The Future of Human-in-the-Loop Cyber-Physical Systems, Computer 99 (PrePrints) (2012) 1.

[11] F. Xia, J. Ma, Building Smart Communities with Cyber-Physical Systems, in: Proc. of 1st international symposium on From digital footprints to social and community intelligence (SCI '11), 2011, pp. 1–6.

[12] A. Passarella, R. I. Dunbar, M. Conti, F. Pezzoni, Ego network models for future internet social networking environments, Computer Communications 35 (18) (2012) 2201 – 2217.

[13] V. Arnaboldi, A. Guazzini, A. Passarella, Egocentric online social networks: Analysis of key features and prediction of tie strength in facebook, Computer Communications 36 (10-11) (2013) 1130–1144.

[14] McKinsey Global Institute, Disruptive technologies: Advances that will transform life, business, and the global economy, Executive Summary (May 2013).

[15] K. Gama, L. Touseaui, D. Donsez, Combining heterogeneous service technologies for building an internet of things middleware, Computer Communications 35 (4) (2012) 405–417.

[16] EPCglobal Inc™, GS1 EPC Tag Data Standard 1.6 (2011).
URL `http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf`

[17] A. Sangiovanni-Vincentelli, Lets get Physical:Marryng Physics withComputerScience, keynote speech at Horizon 2020 @DIITET conference, `http://media.src.cnr.it/node/3239` (Rome, May 2014).

[18] M. Conti, Computer communications: Present status and future challenges, Computer Communications 37 (2014) 1–4.

[19] A. Sangiovanni-Vincentelli, Let's get physical: adding physical dimensions to cyber systems, Internet of Everything Summit (Rome, July 2014).

[20] R. Harle, S. Taherian, M. Pias, G. Coulouris, A. Hopper, J. Cameron, J. Lasenby, G. Kuntze, I. Bezodis, G. Irwin, D. Kerwin, Towards real-time profiling of sprints using wearable pressure sensors, Computer Communications 35 (6) (2012) 650660.

[21] F. Calabrese, M. Conti, D. Dahlem, G. D. Lorenzo, S. Phithakkitnukoon, Special issue on pervasive urban applications, Pervasive and Mobile Computing 9 (5) (2013) 614 – 750.

[22] C. Konstantopoulos, P. Bellavista, C.-F. Huang, D. Turgut, Special issue: Reactive wireless sensor networks, Computer Communications 36 (9) (2013) 963–1100.

[23] J. Chen, H. Frey, X. Li, Special issue: Wireless sensor and robot networks: Algorithms and experiments, Computer Communications 35 (9) (2012) 1017–1164.

[24] F. M. Al-Turjman, H. S. Hassanein, M. A. Ibnkahla, Efficient deployment of wireless sensor networks targeting environment monitoring applications, Computer Communications 36 (2) (2013) 135 – 148.

[25] E. Ancillotti, R. Bruno, M. Conti, The role of communication systems in smart grids: Architectures, technical solutions and research challenges, Computer Communications 36 (17-18) (2013) 1665 – 1697.

[26] R. Rajkumar, I. Lee, L. Sha, J. Stankovic, Cyber-physical systems: The next computing revolution, in: Proc. of 47th ACM/IEEE Design Automation Conference (DAC), 2010, pp. 731–736.

[27] A. A. T. Samad (Ed.), The Impact of Control Technology,s, IEEE Control Systems Society, 2011, Ch. Cyber-Physical Systems.

[28] H. Kim, S. K. Lee, H. Kim, H. Kim, Implementing home energy management system with {UPnP} and mobile applications, Computer Communications 36 (1) (2012) 51 – 62.
[29] O. Garcia-Morchon, D. Kuptsov, A. Gurtov, K. Wehrle, Cooperative security in distributed networks, Computer Communications 36 (12) (2013) 1284 – 1297.
[30] M. Mandel, Can the Internet of Everything bring back the High-Growth Economy?, Internet of Everything Summit (Rome, July 2014).
[31] D. L. Brock, The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects, White Paper (January 2001).
[32] International Telecommunication Union, ITU Internet Report 2005: The Internet of Things, International Telecommunication Union, Geneva, 2005.
[33] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer Networks: The International Journal of Computer and Telecommunications Networking 54 (15) (2010) 2787–2805.
[34] A. K. Jain, L. Hong, S. Pankanti, Internet of Things - Strategic Research Roadmap, Tech. rep., Cluster of European Research projects on the Internet of Things (September 2009).
URL http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf
[35] D. Uckelmann, M. Harrison, F. Michahelles (Eds.), Architecting the Internet of Things, Vol. 1, Springer-Verlag Berlin Heidelberg, 2011, Ch. An Architectural Approach Towards the Future Internet of Things.
[36] ETSI TC M2M, ETSI TS 102 689 v1.1.1 (2010-08) - Machine-to-Machine communications (M2M); M2M service requirements, http://www.etsi.org/deliver/etsi_ts/102600_102699/102689/01.01.01_60/ts_102689v010101p.pdf (August 2010).
[37] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication , John Wiley & Sons, Inc., New York, NY, USA, 2003.
[38] R. Gadh, G. Roussos, K. Michael, G. Q. Huang, B. S. Prabhu, C.-C. P. Chu, RFID - A Unique Radio Innovation for the 21st Century., Proceedings of the IEEE 98 (9) (2010) 1546–1549.
[39] M. Buzzi, M. Conti, C. Senette, D. Vannozzi, Measuring uhf rfid tag reading for document localization, in: Proc. of IEEE International Conference on RFID-Technologies and Applications (RFID-TA), 2011, pp. 115–122.
[40] I. Akyildiz, M. C. Vuran, Wireless Sensor Networks, John Wiley & Sons, Inc., New York, NY, USA, 2010.
[41] S. Li, S. Peng, W. Chen, X. Lu, Income: Practical land monitoring in precision agriculture with sensor networks, Computer Communications 36 (4) (2013) 459 – 467.
[42] M. Di Francesco, S. K. Das, G. Anastasi, Data collection in wireless sensor networks with mobile elements: A survey, ACM Transaction on Sensor Networks 8 (1) (2011) 7:1–7:31.
[43] I. F. Akyildiz, I. H. Kasimoglu, Wireless sensor and actor networks: research challenges, Ad Hoc Networks 2 (4) (2004) 351 – 367.
[44] M. Conti, S. Chong, S. Fdida, W. Jia, H. Karl, Y.-D. Lin, P. Mähönen, M. Maier, R. Molva, S. Uhlig, M. Zukerman, Research challenges towards the Future Internet , Computer Communications 34 (18) (2011) 2115 – 2134.
[45] G. Anastasi, E. Borgia, M. Conti, E. Gregori, A Hybrid Adaptive Protocol for Reliable Data Delivery in WSNs with Multiple Mobile Sinks, The Computer Journal 54 (2) (2011) 213–229.
[46] M. I. Khan, W. N. Gansterer, G. Haring, Static vs. mobile sink: The influence of basic parameters on energy efficiency in wireless sensor networks , Computer Communications 36 (9) (2013) 965 – 978.
[47] K. Ota, M. Dong, Z. Cheng, J. Wang, X. Li, X. S. Shen, ORACLE: Mobility control in wireless sensor and actor networks , Computer Communications 35 (9) (2012) 1029 – 1037.
[48] T.-S. Chen, H.-W. Tsai, Y.-H. Chang, T.-C. Chen, Geographic convergecast using mobile sink in wireless sensor networks, Computer Communications 36 (4) (2013) 445 – 458.
[49] G. Anastasi, M. Conti, M. D. Francesco, A. Passarella, Energy conservation in wireless sensor networks: A survey, Ad Hoc Networks 7 (3) (2009) 537 – 568.
[50] G. Anastasi, M. Conti, M. Di Francesco, Reliable and energy-efficient data collection in sparse sensor networks with mobile elements, Performance Evaluation 66 (12) (2009) 791–810.
[51] 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.
[52] N. Fourty, A. van den Bossche, T. Val, An advanced study of energy consumption in an {IEEE} 802.15.4 based network: Everything but the truth on 802.15.4 node lifetime , Computer Communications 35 (14) (2012) 1759 – 1767.
[53] I. Demirkol, C. Ersoy, F. Alagoz, Mac protocols for wireless sensor networks: a survey, Communications Magazine, IEEE 44 (4).
[54] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks 3 (3) (2005) 325–349.
[55] C. Wang, K. Sohraby, B. Li, M. Daneshmand, Y. Hu, A survey of transport protocols for wireless sensor networks, Network, IEEE 20 (3) (2006) 34–40.
[56] A. Ghosh, S. K. Das, Coverage and connectivity issues in wireless sensor networks: A survey, Pervasive and Mobile Computing 4 (3) (2008) 303 – 334.
[57] J. Yu, N. Wang, G. Wang, D. Yu, Connected dominating sets in wireless ad hoc and sensor networks a comprehensive survey, Computer Communications 36 (2) (2013) 121 – 134.
[58] S. H. Khasteh, S. B. Shouraki, N. Hajiabdorahim, E. Dadashnialehi, A new approach for integrated coverage and connectivity in wireless sensor networks, Computer Communications 36 (1) (2012) 113 – 120.
[59] F. Bouabdallah, N. Bouabdallah, R. Boutaba, Reliable and energy efficient cooperative detection in wireless sensor networks, Computer Communications 36 (5) (2013) 520 – 532.
[60] R. A. Mini, A. A. Loureiro, Energy-efficient design of wireless sensor networks based on finite energy budget, Computer Communications 35 (14) (2012) 1736 – 1748.
[61] L. A. Villas, A. Boukerche, D. L. Guidoni, H. A. B. F. De Oliveira, R. B. De Araujo, A. A. F. Loureiro, An Energy-aware Spatio-temporal Correlation Mechanism to Perform Efficient Data Collection in Wireless Sensor Networks, Comput. Commun. 36 (9) (2013) 1054–1066.
[62] H. Li, Y. Liu, W. Chen, W. Jia, B. Li, J. Xiong, Coca: Constructing optimal clustering architecture to maximize sensor network lifetime,

Computer Communications 36 (3) (2013) 256 – 268.
[63] S. Basagni and M. Conti and S. Giordano and I. Stojmenovic (Editors), Mobile Ad hoc networking Cutting Edge Directions, IEEE Press and John Wiley and Sons, Inc., New York, 2013.
[64] I. F. Akyildiz, E. P. Stuntebeck, Wireless underground sensor networks: Research challenges, Ad Hoc Networks 4 (6) (2006) 669 – 686.
[65] M. C. Domingo, M. C. Vuran, Cross-layer analysis of error control in underwater wireless sensor networks, Computer Communications 35 (17) (2012) 2162 – 2172.
[66] B. Chen, D. Pompili, Team formation and steering algorithms for underwater gliders using acoustic communications, Computer Communications 35 (9) (2012) 1017 – 1028.
[67] M. Ayaz, A. Abdullah, I. Faye, Y. Batira, An efficient Dynamic Addressing based routing protocol for Underwater Wireless Sensor Networks, Computer Communications 35 (4) (2012) 475 – 486.
[68] L. Jin, D. D. Huang, A slotted {CSMA} based reinforcement learning approach for extending the lifetime of underwater acoustic wireless sensor networks, Computer Communications 36 (9) (2013) 1094 – 1099.
[69] S. Cha, E. Talipov, H. Cha, Data delivery scheme for intermittently connected mobile sensor networks, Computer Communications 36 (5) (2013) 504 – 519.
[70] F. M. Al-Turjman, A. E. Al-Fagih, W. M. Alsalih, H. S. Hassanein, A delay-tolerant framework for integrated {RSNs} in iot, Computer Communications 36 (9) (2013) 998 – 1010.
[71] X. Wang, S. Zhong, R. Zhou, A mobility support scheme for 6lowpan, Computer Communications 35 (3) (2012) 392 – 404.
[72] R. Silva, J. S. Silva, F. Boavida, A proposal for proxy-based mobility in {WSNs}, Computer Communications 35 (10) (2012) 1200 – 1216.
[73] R. Bruno, M. Conti, E. Gregori, Bluetooth: Architecture, protocols and scheduling algorithms, Cluster Computing 5 (2) (2002) 117–131.
[74] P. Du, G. Roussos, Adaptive Communication Techniques for the Internet of Things, Journal of Sensor and Actuator Networks 2 (1).
[75] B. Bellalta, A. Vinel, P. Chatzimisios, R. Bruno, C. Wang, Research advances and standardization activities in {WLANs}, Computer Communications 39 (0) (2014) 1 – 2.
[76] S.-J. Wu, S.-Y. Huang, K.-F. Huang, Efficient quality of service scheduling mechanism for wimax networks, Computer Communications 35 (8) (2012) 936 – 951.
[77] I. F. Akyildiz, D. M. Gutierrez-Estevez, R. Balakrishnan, E. Chavarria-Reyes, LTE-Advanced and the evolution to Beyond 4G (B4G) systems , Physical Communication 10 (0) (2014) 31 – 60.
[78] M. Chen, V. C. M. Leung, R. Hjelsvold, X. Huang, Smart and interactive ubiquitous multimedia services, Computer Communications 35 (15) (2012) 1769 – 1771.
[79] J. Mitola III, Cognitive Radio Architecture: The Engineering Foundations of Radio XML, John Wiley and Sons Ltd., 2006.
[80] S. Haykin, Cognitive radio: brain-empowered wireless communications, Selected Areas in Communications, IEEE Journal on 23 (2).
[81] T. Yucek, H. Arslan, A survey of spectrum sensing algorithms for cognitive radio applications, IEEE Communications Surveys Tutorials 11 (1) (2009) 116–130.
[82] W. Ejaz, N. ul Hasan, H. S. Kim, Distributed cooperative spectrum sensing in cognitive radio for ad hoc networks, Computer Communications 36 (12) (2013) 1341 – 1349.
[83] W. Zhang, C. K. Yeo, Joint iterative algorithm for optimal cooperative spectrum sensing in cognitive radio networks, Computer Communications 36 (1) (2012) 80 – 89.
[84] J. Wu, Y. Dai, Y. Zhao, Effective channel assignments in cognitive radio networks, Computer Communications 36 (4) (2013) 411 – 420.
[85] M. H. Rehmani, A. C. Viana, H. Khalife, S. Fdida, SURF: A distributed channel selection strategy for data dissemination in multi-hop cognitive radio networks, Computer Communications 36 (1011) (2013) 1172 – 1185.
[86] S. Bhattacharjee, S. Sengupta, M. Chatterjee, Vulnerabilities in cognitive radio networks: A survey, Computer Communications 36 (13) (2013) 1387 – 1398.
[87] C. Boldrini, K. Lee, M. Önen, J. Ott, E. Pagani, Opportunistic networks, Computer Communications 48 (0) (2014) 1 – 4.
[88] M. Conti, S. Giordano, Mobile ad hoc networking: milestones, challenges, and new research directions, IEEE Communications Magazine 52 (1) (2014) 85–96.
[89] R. Bruno, M. Conti, E. Gregori, Mesh networks: commodity multihop ad hoc networks, IEEE Communications Magazine 43 (3) (2005) 123–131.
[90] H. Hartenstein, K. Laberteaux, A tutorial survey on vehicular ad hoc networks, IEEE Communications Magazine 46 (6) (2008) 164–171.
[91] A. de la Oliva, A. Banchs, P. Serrano, Throughput and energy-aware routing for 802.11 based mesh networks, Computer Communications 35 (12) (2012) 1433 – 1446.
[92] S.-S. Wang, Y.-S. Lin, Passcar: A passive clustering aided routing protocol for vehicular ad hoc networks, Computer Communications 36 (2) (2013) 170 – 179.
[93] X. Yan, Y. A. ekerciolu, S. Narayanan, A survey of vertical handover decision algorithms in fourth generation heterogeneous wireless networks, Computer Networks 54 (11) (2010) 1848 – 1863.
[94] M. Zekri, B. Jouaber, D. Zeghlache, A review on mobility management and vertical handover solutions over heterogeneous wireless networks, Computer Communications 35 (17) (2012) 2055 – 2068.
[95] B. S. Ghahfarokhi, N. Movahhedinia, A survey on applications of {IEEE} 802.21 media independent handover framework in next generation wireless networks, Computer Communications 36 (10-11) (2013) 1101 – 1119.
[96] Y. Zhu, L. Ni, B. Li, Exploiting mobility patterns for inter-technology handover in mobile environments, Computer Communications 36 (2) (2013) 203 – 210.
[97] H. Tuncer, S. Mishra, N. Shenoy, A survey of identity and handoff management approaches for the future internet, Computer Communications 36 (1) (2012) 63 – 79.
[98] V. Ishakian, J. Akinwumi, F. Esposito, I. Matta, On supporting mobility and multihoming in recursive internet architectures, Computer Communications 35 (13) (2012) 1561–1573.
[99] S. Galli, A. Scaglione, Z. Wang, Power Line Communications and the Smart Grid, in: Proc. of First IEEE Smart Grid Communications (SmartGridComm), 2010, pp. 303–308.

[100] M. Chen, V. C. M. Leung, R. Hjelsvold, X. Huang, Smart and interactive ubiquitous multimedia services, Computer Communications 35 (15) (2012) 1769 – 1771.
[101] E.-J. project, Cloud of Things for empowering the citizen clout in smart cities, http://clout-project.eu/ (2013 - 2016).
[102] K. Kumar, Y.-H. Lu, Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?, Computer 43 (4) (2010) 51–56.
[103] J. Baliga, R. Ayre, K. Hinton, R. Tucker, Green cloud computing: Balancing energy in processing, storage, and transport, Proceedings of the IEEE 99 (1) (2011) 149–167.
[104] S.-Y. Chang, C.-F. Lai, Y.-M. Huang, Dynamic adjustable multimedia streaming service architecture over cloud computing, Computer Communications 35 (15) (2012) 1798 – 1808.
[105] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard, Networking named content, in: Proc. of the 5th International Conference on Emerging Networking Experiments and Technologies, 2009, pp. 1–12.
[106] M. Bari, S. Chowdhury, R. Ahmed, R. Boutaba, B. Mathieu, A survey of naming and routing in information-centric networks, Communications Magazine, IEEE 50 (12) (2012) 44–53.
[107] B. Ahlgren, H. Karl, D. Kutscher, L. Zhang, Special section on Information-Centric Networking, Computer Communications, 36 (7) (2013) 719720.
[108] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of information-centric networking, Communications Magazine, IEEE 50 (7) (2012) 26–36.
[109] C. Dannewitz, D. Kutscher, B. Ohlman, S. Farrell, B. Ahlgren, H. Karl, Network of Information (NetInf) - An information-centric networking architecture , Computer Communications 36 (7) (2013) 721 – 735.
[110] D. Trossen, J. Riihijärvi, P. Nikander, P. Jokela, J. Kjällman, J. Rajahalme, Designing, implementing and evaluating a new internetworking architecture, Computer Communications 35 (17) (2012) 2069 – 2081.
[111] M. Amadeo, A. Molinaro, G. Ruggeri, E-CHANET: Routing, forwarding and transport in Information-Centric multihop wireless networks , Computer Communications 36 (7) (2013) 792 – 803.
[112] W. K. Chai, D. He, I. Psaras, G. Pavlou, Cache less for more in information-centric networks (extended version), Computer Communications 36 (7) (2013) 758–770.
[113] G. Carofiglio, M. Gallo, L. Muscariello, D. Perino, Evaluating per-application storage management in content-centric networks, Computer Communications 36 (7) (2013) 750 – 757.
[114] A. Passarella, A survey on content-centric technologies for the current Internet: CDN and P2P solutions , Computer Communications 35 (1) (2012) 1 – 32.
[115] S. Ramabhadran, S. Ratnasamy, J. M. Hellerstein, S. Shenker, Brief announcement: Prefix hash tree, in: Proc. of the 23th ACM Symposium on Principles of Distributed Computing, 2004, pp. 368–368.
[116] A. R. Bharambe, M. Agrawal, S. Seshan, Mercury: Supporting scalable multi-attribute range queries, in: Proc. of ACM SIGCOMM 2004, 2004, pp. 353–366.
[117] M. Cai, M. Frank, J. Chen, P. Szekely, MAAN: A Multi-Attribute Addressable Network for Grid Information Services, in: Proc. of the 4th International Workshop on Grid Computing, GRID '03, 2003.
[118] C. Schmidt, M. Parashar, Squid: Enabling search in dht-based systems, Journal of Parallel and Distributed Computing 68 (7) 962 – 975.
[119] F. Villanueva, D. Villa, F. Moya, M. Santofimia, J. Lopez, Internet of Things Architecture for an RFID-Based Product Tracking Business Model, in: Proc. of 6th Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012, pp. 811–816.
[120] H. Cai, L. D. Xu, B. Xu, C. Xie, S. Qin, L. Jiang, IoT-Based Configurable Information Service Platform for Product Lifecycle Management, IEEE Transactions on Industrial Informatics 10 (2) (2014) 1558–1567.
[121] T. W. Gruen, D. S. Corsten, S. Bharadwaj, Retail Out-of-Stocks: A Worldwide Examination of Extent, Causes and Consumer Responses, Tech. rep. (2002).
[122] A. S. Voulodimos, C. Z. Patrikakis, A. B. Sideridis, V. A. Ntafis, E. M. Xylouri, A complete farm management system based on animal identification using RFID technology , Computers and Electronics in Agriculture 70 (2) (2010) 380 – 388.
[123] J. Ma, X. Zhou, S. Li, Z. Lio, Connecting Agriculture to the Internet of Things through Sensor Networks, in: Proc. of Internet of Things (iThings/CPSCom), 2011, pp. 184 – 187.
[124] D. Yan-e, Design of Intelligent Agriculture Management Information System Based on IoT, in: Proc. of International Conference on Intelligent Computation Technology and Automation (ICICTA), 2011, 2011, pp. 1045–1049.
[125] J. chun Zhao, J. feng Zhang, Y. Feng, J. xin Guo, The study and application of the IOT technology in agriculture, in: Proc. of 3rd IEEE Computer Science and Information Technology (ICCSIT), 2010, 2010, pp. 462 – 465.
[126] P. Hank, S. Müller, O. Vermesan, J. Van Den Keybus, Automotive Ethernet: In-vehicle Networking and Smart Mobility, in: Proc. of the Conference on Design, Automation and Test in Europe (DATE'13), 2013, pp. 1735–1739.
[127] R. Ganti, F. Ye, H. Lei, Mobile crowdsensing: current state and future challenges, IEEE Communications Magazine 49 (11) (2011) 32–39.
[128] E. Polycarpou, L. Lambrinos, E. Protopapadakis, Smart parking solutions for urban areas, in: Proc. of IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'13), 2013, pp. 1–6.
[129] M. Qadeer, N. Akhtar, S. Govil, A. Varshney, A Novel Scheme for Mobile Payment Using RFID-Enabled Smart SIMcard, in: Proc. of International Conference on Future Computer and Communication (ICFCC 2009), 2009, pp. 339–343.
[130] G. Amato, F. Falchi, F. Rabitti, Landmark Recognition in VISITO Tuscany, in: C. Grana, R. Cucchiara (Eds.), Multimedia for Cultural Heritage, Vol. 247 of Communications in Computer and Information Science, Springer Berlin Heidelberg, 2012, pp. 1–13.
[131] E. Ancillotti, R. Bruno, M. Conti, Smoothing peak demands through aggregate control of background electrical loads, in: Proc. of IEEE PES Innovative Smart Grid Technologies Conference (ISGT), 2014, 2014, pp. 1–5.
[132] M. Gharbaoui, B. Martini, R. Bruno, L. Valcarenghi, M. Conti, P. Castoldi, Policies for efficient usage of an EV charging infrastructure deployed in city parking facilities, in: Proc. of 13th ITS Telecommunications (ITST), 2013, 2013, pp. 384–389.
[133] M. Gharbaoui, B. Martini, R. Bruno, L. Valcarenghi, M. Conti, P. Castoldi, Designing and Evaluating Activity-Based Electric Vehicle Charging in Urban Areas, in: Proc. of IEEE Electric Vehicle Conference (IEVC), 2013, 2013, pp. 1–5.
[134] J. Lu, T. Sookoor, V. Srinivasan, G. Gao, B. Holben, J. Stankovic, E. Field, K. Whitehouse, The Smart Thermostat: Using Occupancy

Sensors to Save Energy in Homes, in: Proc.s of the 8th ACM Conference on Embedded Networked Sensor Systems (SenSys '10), 2010, pp. 211–224.
[135] C. Chen, D. J. Cook, A. S. Crandall, The user side of sustainability: Modeling behavior and energy usage in the home, Pervasive and Mobile Computing 9 (1) (2013) 161–175.
[136] E. Sun, X. Zhang, Z. Li, The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines , Safety Science 50 (4) (2012) 811 – 815.
[137] G. Deak, K. Curran, J. Condell, A survey of active and passive indoor localisation systems, Computer Communications 35 (16) (2012) 1939 – 1954.
[138] K. Kaemarungsi, P. Krishnamurthy, Analysis of wlan's received signal strength indication for indoor location fingerprinting, Pervasive and Mobile Computing 8 (2) (2012) 292 – 316.
[139] M. D'Souza, T. Wark, M. Karunanithi, M. Ros, Evaluation of realtime people tracking for indoor environments using ubiquitous motion sensors and limited wireless network infrastructure, Pervasive and Mobile Computing 9 (4) (2013) 498 – 515.
[140] S. Srinivasan, S. Dattagupta, P. Kulkarni, K. Ramamritham, A survey of sensory data boundary estimation, covering and tracking techniques using collaborating sensors, Pervasive and Mobile Computing 8 (3) (2012) 358 – 375.
[141] C.-C. Lo, L.-Y. Hsu, Y.-C. Tseng, Adaptive radio maps for pattern-matching localization via inter-beacon co-calibration, Pervasive and Mobile Computing 8 (2) (2012) 282 – 291.
[142] F. Delmastro, Pervasive communications in healthcare, Computer Communications 35 (11) (2012) 1284–1295.
[143] S. Abbate, M. Avvenuti, F. Bonatesta, G. Cola, P. Corsini, A. Vecchio, A smartphone-based fall detection system, Pervasive and Mobile Computing 8 (6) (2012) 883 – 899.
[144] A. Dias, L. Gorzelniak, R. A. Jrres, R. Fischer, G. Hartvigsen, A. Horsch, Assessing physical activity in the daily life of cystic fibrosis patients, Pervasive and Mobile Computing 8 (6) (2012) 837 – 844.
[145] Ambient Assisted Living Joint Programme - Call2, ALICE - Advanced Lifestyle Improvement system & new Communication Experience, http://aal-alice.eu (May 2012).
[146] AAL-2011-4-099, ALICE - Assistance for Better Mobility and Improved Cognition of Elderly, http://alice-project.eu (2011).
[147] R. Manduchi, J. Coughlan, (computer) vision without sight, Communications of the ACM 55 (1) (2012) 96–104.
[148] 3GPP , 3GPP TS 22.368 v11.0.0 - Service Requirements for Machine-Type Communications (December 2010).
[149] H. Ning, Z. Wang, Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?, Communications Letters, IEEE 15 (4).
[150] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, H.-Y. Du, Research on the architecture of Internet of Things, in: Proc. of 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 5, 2010, pp. V5–484–V5–487.
[151] L. Zhou, H.-C. Chao, Multimedia traffic security architecture for the internet of things, Network, IEEE 25 (3) (2011) 35–40.
[152] D. Guinard, V. Trifa, E. Wilde, A resource oriented architecture for the Web of Things, in: Internet of Things (IOT), 2010, 2010, pp. 1–8.
[153] G. Pujolle, An Autonomic-oriented Architecture for the Internet of Things, in: IEEEE JVA International Symposium on Modern Computing, 2006, pp. 163–168.
[154] A. J. Jara, M. A. Zamora, A. F. G. Skarmeta, An Architecture Based on Internet of Things to Support Mobility and Security in Medical Environments, in: Proc. of 7th IEEE Consumer Communications and Networking Conference (CCNC), 2010, pp. 1–5.
[155] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, V. Trifa, SOA-Based Integration of the Internet of Things in Enterprise Services, in: Proc. of the IEEE International Conference on Web Services (ICWS), 2009, pp. 968–975.
[156] A. P. Castellani, N. Bui, P. Casari, M. Rossi, Z. Shelby, M. Zorzi, Architecture and protocols for the Internet of Things: A case study, in: Proc. of the 8th IEEE Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010, pp. 678–683.
[157] ETSI TC M2M, ETSI TS 102 921 v1.1.1 (2012-02) - Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces, http://www.etsi.org/deliver/etsi_ts/102900_102999/102921/01.01.01_60/ts_102921v010101p.pdf (February 2012).
[158] IEEE 802.16 WG, IEEE C802.16-10/0016r1 - Future 802.16 Networks: Challenges and Possibilities, http://www.ieee802.org/802_tutorials/2010-03/C80216-10_0016r1.pdf (February 2010).
[159] ETSI TC M2M, ETSI TS 102 690 v1.1.1 (2011-10) - Machine-to-Machine communications (M2M); Functional architecture, http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf (October 2011).
[160] R. T. Fielding, Architectural Styles and the Design of Network-based Software Architectures, Ph.D. thesis, University of California, Irvine, http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm (2000).
[161] 3GPP, 3GPP TR 22.888 v1.0.0 - System Improvement for Machine-Type Communications (September 2010).
[162] 3GPP, 3GPP TS 36.300 v10.0.0 - Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN) (June 2010).
[163] S. M. Razavi, D. Yuan, Mitigating signaling congestion in LTE location management by overlapping tracking area lists, Computer Communications 35 (18) (2012) 2227 – 2235.
[164] D. Xenakis, N. Passas, C. Verikoukis, An energy-centric handover decision algorithm for the integrated {LTE} macrocellfemtocell network, Computer Communications 35 (14) (2012) 1684 – 1694.
[165] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, RFC 4944 Transmission of IPv6 Packets over IEEE 802.15.4 Networks, http://tools.ietf.org/html/rfc4944 (2007).
[166] S.-D. Lee, M.-K. Shin, H.-J. Kim, EPC vs. IPv6 mapping mechanism, in: Proc. of 9th International Conference on Advanced Communications Technology (ICACT), 2007, pp. 1243–1245.
[167] D. G. Yoon, D. H. Lee, C. H. Seo, S. G. Choi, RFID Networking Mechanism Using Address Management Agent, in: Proc. of the 4th International Conference on Networked Computing and Advanced Information Management, 2008, pp. 617–622.
[168] Y.-C. Chang, J.-L. Chen, Y.-S. Lin, S. M. Wang, RFIPv6 - A Novel IPv6-EPC Bridge Mechanism, in: Proc. of the IEEE International Conference on Consumer Electronics (ICCE), 2008, pp. 1–2.

[169] EPCglobal Inc™, EPCglobal Object Name Service (ONS) 1.0.1 (2008).
URL http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0_1-standard-20080529.pdf
[170] EPCglobal Inc™, EPCglobal Object Name Service (ONS) 2.0.1 (2013).
URL http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf
[171] V. Krylov, A. Logvinov, D. Ponomarev, EPC Object Code Mapping Service software architecture: web approach, MERA Networks publications (2008).
[172] D. Johnson, C. Perkins, J. Arkko, RFC 3775 Mobility Support in IPv6, http://www.ietf.org/rfc/rfc3775.txt (2004).
[173] L. Galluccio, G. Morabito, S. Palazzo, On the Potentials of Object Group Localization in the Internet of Things, in: Proc. of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011, pp. 1–9.
[174] W. B. Heinzelman, A. P. Chandrakasan, H. Blakrishnam, An Application-Specific Protocol Architecture for Wireless Microsensor Networks, IEEE Transaction on Wireless Communications 1 (4) (2002) 660–670.
[175] O. Younis, S. Fahmy, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks, IEEE Transaction on Mobile Computing 3 (4) (2004) 366–379.
[176] T. Liu, Q. Li, P. Liang, An energy-balancing clustering approach for gradient-based routing in wireless sensor networks, Computer Communications 35 (17) (2012) 2150 – 2161.
[177] E. Cañete, M. Díaz, L. Llopis, B. Rubio, Hero: A hierarchical, efficient and reliable routing protocol for wireless sensor and actor networks, Computer Communications 35 (11) (2012) 1392 – 1409.
[178] I. Stojmenovic, S. Oliaru, Geographic and Energy-Aware Routing is Sensor Networks, IEEE Transaction on Mobile Computing (2005) 381–416.
[179] E. Elhafsi, N. Mitton, D. Simplot-Ryl, End-to-End Energy Efficient Geographic Path Discovery with Guaranteed Delivery in Ad Hoc and Sensor Networks, in: Proc. of IEEE 19th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008, pp. 1–5.
[180] H. Kalosha, A. Nayak, S. Rhrup, I. Stojmenovic, Select-and-Protest-basedBeaconless Georouting with Guaranteed Delivery in Wireless Sensor Networks, in: Proc. of IEEE 27th Conference on Computer Communications (INFOCOM), 2008, pp. 346–350.
[181] S. Basagni, A. Carosi, E. Melachrinoudis, C. Petrioli, Z. M. Wang, Controlled sink mobility for prolonging wireless sensor networks lifetime, Wireless Networks 14 (6) (2008) 831–858.
[182] U. M. Colesanti, S. Santini, Andrea, DISSense: An adaptive ultralow-power communication protocol for wireless sensor networks, in: IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), 2011, pp. 1–10.
[183] N. Burri, P. von Rickenbach, R. Wattenhofer, Dozer: Ultra-Low Power Data Gathering in Sensor Networks, in: Proc. of 6th International Symposium on Information Processing in Sensor Networks (IPSN), 2007, pp. 450–459.
[184] W. Pak, S. Bahk, Centralized route recovery based on multi-hop wakeup time estimation for wireless sensor networks with ultra low duty cycles, Computer Communications 35 (11) (2012) 1355 – 1367.
[185] R. Musaloiu-E., C.-J. M. Liang, A. Terzis, Koala: Ultra-Low Power Data Retrieval in Wireless Sensor Networks, in: Proc. of the 7th International Conference on Information Processing in Sensor Networks (IPSN), 2008, pp. 421–432.
[186] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, R. Alexander, RFC 6550 RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, http://tools.ietf.org/html/rfc6550 (2012).
[187] E. Ancillotti, R. Bruno, M. Conti, The role of the RPL routing protocol for smart grid communications, Communications Magazine, IEEE 51 (1) (2013) 75–83.
[188] E. Ancillotti, R. Bruno, M. Conti, Reliable Data Delivery With the IETF Routing Protocol for Low-Power and Lossy Networks, IEEE Transactions on Industrial Informatics 10 (3) (2014) 1864–1877.
[189] E. Ancillotti, R. Bruno, M. Conti, RPL routing protocol in advanced metering infrastructures: An analysis of the unreliability problems, in: Proc. of 2nd IFIP/IEE Conf. Sustainable Internet and ICT for Sustainability (SustainIT 2012), 2012, pp. 1–10.
[190] R. Stewarterf, RFC 4960 Stream Control Transmission Protocol, http://tools.ietf.org/html/rfc4960 (2007).
[191] Z. Shelby, K. Hartke, C. Bormann, IETF Internet-Draft - Constrained Application Protocol (CoAP), http://tools.ietf.org/html/draft-ietf-core-coap-18 (2013).
[192] E. International Business Machines Corporation (IBM), MQTT V3.1 Protocol Specification, http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html (2010).
[193] U. Hunkeler, H. L. Truong, A. Stanford-Clark, MQTT-S - A publish/subscribe protocol for Wireless Sensor Networks, in: Proc. of the International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE), 2008, pp. 791–798.
[194] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, M. Guizani, Home M2M networks: Architectures, standards, and QoS improvement, IEEE Communications Magazine 49 (4) (2011) 44–52.
[195] M. Starsinic, System Architecture Challenges in the Home M2M Network, in: IEEE Long Island Section Systems, Applications and Technology Conference (LISAT), 2010, pp. 1–7.
[196] M. Dillinger, K. Madani, N. Alonistioti, Software Defined Radio: Architectures, Systems and Functions, John Wiley & Sons, Inc., New York, NY, USA, 2003.
[197] B. Gu, J. Heo, S. Oh, N. Park, G. Jeon, Y. Cho, An SDR-Based Wireless Communication Gateway for Vehicle Networks, in: Proc. of the IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1617–1622.
[198] T. Teubler, U. Walther, H. Hellbrück, EZgate-A flexible Gateway for the Internet of Things, Electronic Communications of the EASST 37.
[199] Q. Zhu, R. Wang, Q. Chen, Y. Liu, W. Qin, IOT Gateway: BridgingWireless Sensor Networks into Internet of Things, in: Proc. of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), 2010, pp. 347–352.
[200] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, Broadband Forum - TR-069 CPE WAN Management Protocol, http://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf1.
[201] D. Harrington, R. Presuhn, B. Wijnen, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (2002).
[202] R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman, IETF RFC 6241 - NETCONF Configuration Protocol,

http://tools.ietf.org/html/rfc6241 (2006).
[203] A. Sehgal, V. Perelman, S. Kuryla, J. Schonwalder, Management of Resource Constrained Devices in the Internet of Things, Communications Magazine, IEEE 50 (12) (2012) 144–149.
[204] O. M. Alliance, OMA Device Management V2.0, http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases.
[205] G. Klas, F. Rodermund, Z. Shelby, S. Akhouri, J. Hller, Lightweight M2M: Enabling Device Management and Applications for the Internet of Things, White Paper (February 2014).
[206] W3C OWL Working Group, W3C Recommendation - OWL 2 Web Ontology Language - Document overview (Second Edition), http://www.w3.org/TR/2012/REC-owl2-overview-20121211/ (2012).
[207] T. Ku, Y. Zhu, K. Hu, A Novel Complex Event Mining Network for Monitoring RFID-Enable Application, in: Computational Intelligence and Industrial Application, 2008. PACIIA '08. Pacific-Asia Workshop on, 2008, pp. 925–929.
[208] W3C XML Query Working Group, W3C Recommendation - XQuery 1.0: An XML Query Language (Second Edition), http://www.w3.org/TR/xquery/ (2010).
[209] T. Fan, Y. Chen, A scheme of data management in the Internet of Things, in: 2nd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC), 2010, pp. 110–114.
[210] P. Buneman, S. Khanna, K. Tajima, W. Tan, Archiving scientific data, ACM Transactions on Database Systems 27 (1) (2004) 2–42.
[211] H. Gonzalez, J. Han, X. Li, D. Klabjan, Warehousing and Analyzing Massive RFID Data Sets, in: Proc. of the 22nd International Conference on Data Engineering (ICDE), 2006, pp. 83–83.
[212] H. Zhonglin, H. Yuhua, Preliminary Study on Data Management Technologies of Internet of Things, in: International Conference on Intelligence Science and Information Engineering (ISIE), 2011, pp. 137–140.
[213] Z. Ding, Q. Yang, H. Wu, Massive Heterogeneous Sensor Data Management in the Internet of Things, in: Proc. of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing (ITHINGSCPSCOM), 2011, pp. 100–108.
[214] T. Li, Y. Liu, Y. Tian, S. Shen, W. Mao, A Storage Solution for Massive IoT Data Based on NoSQL, in: Proc. of IEEE International Conference on Green Computing and Communications (GreenCom), 2012, pp. 50–57.
[215] R. Cattell, Scalable SQL and NoSQL data stores, ACM SIGMOD Record 39 (4) (2011) 12–27.
[216] N. Fernando, S. W. Loke, W. Rahayu, Mobile cloud computing: A survey, Future Generation Computer Systems 29 (1) (2013) 84 – 106.
[217] H. T. Dinh, C. Lee, D. Niyato, P. Wang, A survey of mobile cloud computing: architecture, applications, and approaches, Wireless Communications and Mobile Computing 13 (18) (2013) 1587–1611.
[218] E. E. Marinelli, Hyrax: Cloud Computing on Mobile Devices using MapReduce, Master's thesis, Carnegie Mellon University (2009).
[219] M. Satyanarayanan, P. Bahl, R. Caceres, N. Davies, The case for vm-based cloudlets in mobile computing, IEEE Pervasive Computing.
[220] A. Passarella, M. Kumar, M. Conti, E. Borgia, Minimum-delay service provisioning in opportunistic networks, IEEE Transactions on Parallel and Distributed Systems 22 (8) (2011) 1267–1275.
[221] A. Passarella, M. Conti, E. Borgia, M. Kumar, Performance Evaluation of Service Execution in Opportunistic Computing, in: Proceedings of the 13th ACM MSWiM 2010, 2010, pp. 291–298.
[222] V. Arnaboldi, M. Conti, F. Delmastro, CAMEO: A novel context-aware middleware for opportunistic mobile social networks, Pervasive and Mobile Computing 11 (0) (2014) 148 – 167.
[223] Z. Yu, B. Xiao, S. Zhou, Achieving Optimal Data Storage Position in Wireless Sensor Networks, Computer Communications 33 (1) (2010) 92–102.
[224] M. Dischinger, A. Haeberlen, K. P. Gummadi, S. Saroiu, Characterizing Residential Broadband Networks, in: Proc. of the 7th ACM SIGCOMM Internet Measurement Conference, 2007.
[225] G. Maier, A. Feldmann, V. Paxson, M. Allman, On Dominant Characteristics of Residential Broadband Internet Traffic, in: Proc. of the 9th ACM SIGCOMM Internet Measurement Conference, 2009, pp. 90–102.
[226] L. DiCioccio, R. Teixeira, C. Rosenberg, Impact of Home Networks on End-to-End performance: Controlled Experiments, in: Proc. of ACM SIGCOMM workshop on Home networks (HomeNets), 2010, pp. 7–12.
[227] P. Chhabra, N. Laoutaris, P. Rodriguez, R. Sundaram, Home is Where the (Fast) Internet is: Flat-rate Compatible Incentives for Reducing Peak Load, in: Proc. of ACM SIGCOMM workshop on Home networks (HomeNets), 2010, pp. 13–18.
[228] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, K. Wehrle, Security challenges in the ip-based internet of things, Wireless Personal Communications: An International Journal 61 (3) (2011) 527–542.
[229] S. Cirani, G. Ferrari, L. Veltri, Enforcing security mechanisms in the ip-based internet of things: An algorithmic overview, Algorithms 6 (2) (2013) 197–226. doi:10.3390/a6020197.
URL http://www.mdpi.com/1999-4893/6/2/197
[230] B. Sarikaya, IETF Internet-Draft - Security Bootstrapping Solution for Resource-Constrained Devices, http://tools.ietf.org/html/draft-sarikaya-core-secure-bootsolution-00 (2013).
[231] C. Jennings, IETF Internet-Draft - Transitive Trust Enrollment for Constrained Devices (2012).
URL http://tools.ietf.org/html/draft-jennings-core-transitive-trust-enrollment-01
[232] IETF Network Working Group, IETF RFC - Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt (1998).
[233] Harkins, D. and Carrel, D., IETF RFC - The Internet Key Exchange (IKE), http://www.ietf.org/rfc/rfc2409.txt (1998).
[234] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6LoWPAN with compressed IPsec, in: Proc. of IEEE 7th International Conference on Distributed Computing in Sensor Systems, 2011, pp. 1–8.
[235] P. Nikander, A. Gurtov, T. R. Henderson, Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks, IEEE Communications Surveys & Tutorials 12 (2) (2010) 186–204.
[236] S. Raza, D. Trabalza, T. Voigt, 6LoWPAN Compressed DTLS for CoAP, in: Proc. of IEEE 8th International Conference on Distributed Computing in Sensor System Distributed Computing in Sensor Systems, 2012, pp. 287–289.

[237] J. Daemen, V. Rijmen, AES Proposal: Rijndaell (1999).
URL http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf#page=1
[238] T. Eisenbarth, S. Kumar, A Survey of Lightweight-Cryptography Implementations, IEEE Design Test of Computers 24 (6) (2007) 522–533.
[239] F.-X. Standaert, G. Piret, N. Gershenfeld, J.-J. Quisquater, SEA: A Scalable Encryption Algorithm for Small Embedded Applications, in: Proc. of 7th IFIP WG 8.8/11.2 International Conference Smart Card Research and Advanced Applications (CARDIS), Springer-Verlag, 2006, pp. 222–236.
[240] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, in: Proc. of Workshop on Cryptographic Hardware and Embedded Systems (CHES), Springer, 2007.
[241] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation 48 (177) (1987) 203–209.
[242] IETF Network Working Group, IETF RFC - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), http://tools.ietf.org/html/rfc4492 (2006).
[243] D. Fu, J. Solinas, IETF RFC - Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, http://tools.ietf.org/html/rfc5903 (2010).
[244] J. Guo, T. Peyrin, A. Poschmann, The PHOTON Family of Lightweight Hash Functions, in: Proc. of 31st Annual Conference on Advances in Cryptology (CRYPTO), 2011, pp. 222–239.
[245] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, Hash Functions and RFID Tags: Mind the Gap, in: Proc. of the 10th international workshop on Cryptographic Hardware and Embedded Systems (CHES), 2008, pp. 283–299.
[246] A. Shamir, SQUASH — A New MAC with Provable Security Properties for Highly Constrained Devices Such as RFID Tags, in: K. Nyberg (Ed.), Fast Software Encryption, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 144–157.
[247] E. He, Q. Wen, A Single Sign-On Scheme for Cross Domain Web Applications Based on SOA, in: Proc. of International Workshop Internet of Things (IOT), 2012, pp. 581–589.
[248] Y. Wang, Q. Wen, H. Zhang, A Single Sign-On Scheme for Cross Domain Web Applications Using Identity-Based Cryptography, in: Proc. of 2nd International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010, pp. 483–485.
[249] European Union, An action plan for Europe (2009).
URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF
[250] FP7-ICT 257852, ebbits - Enabling the Business-Based Internet of Things and Services (2010-2014).
URL http://datatracker.ietf.org/doc/rfc6750/
[251] FP7-ICT 288385 , IoT.est - Internet of Things Environment for Service Creation and Testing, http://ict-iotest.eu/iotest/ (2011-2014).
[252] NSF FIA CNS-1040672, NEBULA - A trustworthy, secure and evolvable Future Internet Architecture, http://nebula-fia.org (2010-2014).
[253] FP7-ICT 317674, BETaaS - Building the Environment for the Things as a Service, http://www.betaas.eu (2012-2015).
[254] National Basic Research 973 Program of China under Grant No. 2011CB302701, Basic Research on the Architecture of Internet of Things (2011).
[255] FP7-ICT 257521, iot-a - Internet of Things Architecture, http://www.iot-a.eu/public (2010-2013).
[256] FP7-ICT 287708 , iCORE - Internet Connected Objects for Reconfigurable Ecosystem, http://www.iot-icore.eu (2010-2013).
[257] FP7-ICT 317862, COMPOSE - Collaborative Open Market to Place Objects at your SErvice, http://www.compose-project.eu/ (2012-2015).
[258] FP7-ICT 287901, BUTLER - uBiquitous, secUre internet-of-things with Location and contExt-awaReness, http://www.iot-butler.eu (2011-2014).
[259] NSF FIA CNS-1040735, MobilityFirst - A Robust and Trustworthy Mobility-Centric Architecture for the Future Internet, http://www.nets-fia.net (2010-2014).
[260] FP7-ICT 288445, IoT6 - Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability, http://www.iot6.eu (2011-2014).
[261] NRF of Korea 2010-0018859, SNAIL - Sensor Networks for an All-IP worLd (2010).
[262] NRF of Korea, EPCSN - Electronic Product Code sensor networks (2010).
[263] FP7-ICT 317671, ICSI - Intelligent Cooperative Sensing for Improved traffic efficiency (2012-2015).
URL http://www.ict-icsi.eu/index.html#.UbspwJXI9a8
[264] FP7-ICT 288879, CALIPSO - Connect All IP-based Smart Objects IoT6, http://www.ict-calipso.eu (2011-2014).
[265] FP7-ICT 287661, GAMBAS - Generic Adaptive Middleware for Behavior-driven Autonomous systems, http://www.gambas-ict.eu (2012-2015).
[266] FP7-ICT 287305, OPEN IoT - Open Source blueprint for large-scale self-organizing cloud environment for IoT applications, http://openiot.eu (2011-2014).
[267] Korea Communications Agency, Smart IoT-based Spontaneous Service Composition (2011-2014).
URL http://cds.kaist.ac.kr/iotservice/?page_id=2
[268] FP7-ICT 258666, ELLIOT - Experiential Living Lab for the Internet Of Things, http://www.elliot-project.eu (2010-2013).
[269] FP7-ICT 257992, SmartSantander, http://www.smartsantander.eu (2010-2013).
[270] FP7-ICT 257909, SPRINT - Software Platform for Integration of Engineering and Things, http://www.sprint-iot.eu (2010-2013).
[271] FP7-ICT 257649, Planet - PLAtform for the development and operation of heterogeneous NETworked cooperating objects, http://www.planet-ict.eu (2010-2014).
[272] U.S. Department of Energy, The SMART GRID: an introduction (2008).
URL http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf
[273] European Commission, Analysis of option to move beyond 20% greenhouse gas emission reductions and assessing the risk of carbon leakage, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0265:FIN:en:PDF (2007).
[274] European Commission, European Smart Grid Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future,

ftp://ftp.cordis.europa.eu/pub/fp7/energy/docs/smartgrids_en.pdf (2006).
[275] U.S. Department of Energy, Smart Grid Research and Development: Multi-Year Program Plan (MYPP) 2010-2014 (2011).
URL http://energy.gov/oe/downloads/smart-grid-rd-multi-year-program-plan-2010-2014-september-2011-update
[276] Microsoft, Bouygues Immobilier, Bouygues Telecom, Schneider Electric, Total, Alstom, ERDF, ETDE and Steria, The City of Issy-les-Moulineaux and nine major industrial groups create IssyGrid, the first district smart grid in France, http://www.issy.com/index.php/fr/english/issy_a_smart_city/issygrid (2011-2015).
[277] JRC Scientific and Technical Reports, Electricity Consumption and Efficiency Trends in European Union, http://re.jrc.ec.europa.eu/energyefficiency/pdf/EnEff_Report_2009.pdf (2009).
[278] Juniper Networks, Juniper Networks Third Annual Mobile Threats Report, Tech. rep. (2013).
URL http://assets.nationaljournal.com/img/juniperreport062613.pdf
[279] EPCglobal Inc™, GS1 EPCglobal Tag Data Translation (TDT) 1.6 (2011).
URL http://www.gs1.org/gsmp/kc/epcglobal/tdt/tdt_1_6_RatifiedStd-20111012-i2.pdf
[280] EPCglobal Inc™, EPCglobal Certificate Profile Specification (20101).
URL http://www.gs1.org/gsmp/kc/epcglobal/cert/cert_2_0-standard-20100610.pdf
[281] EPCglobal Inc™, EPC Information Services (EPCIS) Version 1.0.1- Specification (2007).
URL http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_0_1-standard-20070921.pdf
[282] EPCglobal Inc™, EPC Radio-Frequency Identity Protocols, EPC Class-1 HF RFID Air Interface Protocol for Communications at 13.56 MHz - Version 2.0.3 (2011).
URL http://www.gs1.org/sites/default/files/docs/epcglobal/epcglobal_hf_2_0_3-standard-20110905r3.pdf
[283] EPCglobal Inc™, EPC Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID, Protocol for Communications at 860 MHz - 960 MHz - Version 1.2.0, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf (2011).
[284] ISO/IEC SC31/WG4, ISO/IEC 15961:2004 Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface (2004).
URL http://www.iso.org/iso/catalogue_detail?csnumber=30528
[285] ISO/IEC SC31/WG4, ISO/IEC 15962:2004 Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions, http://www.iso.org/iso/catalogue_detail?csnumber=30529 (2004).
[286] ISO/IEC SC31/WG6, ISO/IEC 29143 Information technology – Automatic identification and data capture techniques – Air interface specification for Mobile RFID interrogators, http://www.iso.org/iso/catalogue_detail.htm?csnumber=45166 (2011).
[287] ISO/IEC SC31/WG6, ISO/IEC 29176:2011 Information technology – Mobile item identification and management – Consumer privacy-protection protocol for Mobile RFID services (2011).
URL http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45255
[288] ITU-T SG13, ITU-T Y.2213 - NGN service requirements and capabilities for network aspects of applications and services using tag-based identification, http://www.itu.int/rec/T-REC-Y.2213/en (2008).
[289] ITU-T SG13, ITU-T Y.2016 - Functional requirements and architecture of the NGN for applications and services using tag-based identification, http://www.itu.int/rec/T-REC-Y.2016/en (2009).
[290] ITU-T SG16, ITU-T H.642.1 - Multimedia information access triggered by tag-based identification - Identification scheme, http://www.itu.int/rec/T-REC-H.642.1/en (2012).
[291] ITU-T SG16, ITU-T H.642.2 - Multimedia information access triggered by tag-based identification - Registration procedures for identifiers, http://www.itu.int/rec/T-REC-H.642.2/en (2012).
[292] ITU-T SG16, ITU-T H.642.3 - Information technology - Automatic identification and data capture technique - Identifier resolution protocol for multimedia information access triggered by tag-based identification, http://www.itu.int/rec/T-REC-H.642.3/en (2012).
[293] ISO/IEC WG7, ISO/IEC DIS 29182 Information technology – Sensor networks: Sensor network reference architecture (SNRA), http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45261 (2012).
[294] ISO/IEC WG7, ISO/IEC DIS 20005 Information technology – Sensor networks – Services and interfaces supporting collaborative information processing in intelligent sensor networks, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50952 (2012).
[295] ISO/IEC WG7, ISO/IEC WD 30101 Information technology – Sensor networks: Sensor Network and its interfaces for smart grid system, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53221 (2012).
[296] ISO/IEC SC31/WG4, ISO/IEC 24753:2011 Information technology – Radio frequency identification (RFID) for item management – Application protocol: encoding and processing rules for sensors and batteries, http://www.iso.org/iso/catalogue_detail.htm?csnumber=51144 (2011).
[297] ITU-T SG13, ITU-T Y.2221 - Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment, http://www.itu.int/rec/T-REC-Y.2221/en (2010).
[298] ITU-T SG13, ITU-T Y.2026 - Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services, http://www.itu.int/rec/T-REC-Y.2026/en (2012).
[299] ITU-T SG16, ITU-T F.OpenUSN (Draft) - Requirements and reference architecture for open USN service framework (2013).
[300] ITU-T SG16, ITU-T F.USN-ALI (Draft) - Requirements and reference structure for automatic location identification capability for USN applications and services (2013).
[301] ITU-T SG17, ITU-T X.unsec-1 (Draft) - Security requirements and framework of ubiquitous networking (2013).
[302] ITU-T SG17, ITU-T X.unsec-2 (Draft) - USN middleware security guidelines (2013).
[303] ITU-T SG17, ITU-T X.unsec-3 (Draft) - Secure routing mechanisms for wireless sensor network (2013).
[304] ISO/IEC JT1/SC06, ISO/IEC 18092: Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) (2013).

[305] ECMA TC 47, ECMA-340: Near Field Communication - Interface and Protocol (NFCIP-1) (2013).
[306] ISO/IEC JT1/SC06, ISO/IEC 21481: Information technology – Telecommunications and information exchange between systems – Near Field Communication Interface and Protocol -2 (NFCIP-2) (2012).
[307] ECMA TC 47, ECMA-352: Near Field Communication Interface and Protocol -2 (NFCIP-2) (2013).
[308] ISO/IEC JT1/SC06, ISO/IEC 13157: Information technology – Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security services and protocol (2014).
[309] ISO/IEC JT1/SC06, ISO/IEC 13157: Information technology – Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES (2010).
[310] ECMA TC47, Standard ECMA-385 NFC-SEC: NFCIP-1 Security Services and Protocol , http://www.ecma-international.org/publications/standards/Ecma-385.htm (2010).
[311] ECMA TC47, Standard ECMA-386 NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES, http://www.ecma-international.org/publications/standards/Ecma-386.htm (2010).
[312] IEEE 802.15 TG 7, IEEE Standard for Local and Metropolitan Area Networks – Part 15.7: Short-Range Wireless Optical Communication Using Visible Light (2011).
[313] IEEE, IEEE 1901: IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications (2010).
[314] IEEE, IEEE 1901.2: IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications (2013).
[315] IEEE, IEEE 1905.1 - IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies (2013).
[316] J. Schneider, T. Kamiya, W3C Recommendation - Efficient XML Interchange (EXI) Format 1.0, http://www.w3.org/TR/exi/ (2011).
[317] ITU-T SG13, ITU-T Y.2060 - Overview of the Internet of things , http://www.itu.int/rec/T-REC-Y.2060/en (2012).
[318] ITU-T SG13, ITU-T Y.2061 - Requirements for the support of machine-oriented communication applications in the next generation network environment, http://www.itu.int/rec/T-REC-Y.2061/en (2012).
[319] ITU-T SG16, ITU-T H.IoT-ID - Requirements and Common Characteristics of IoT Identifier for IoT Service (2013).
[320] ITU-T SG16, ITU-T H.IoT-ID - Common service requirements for Internet of Things (IoT) applications and services (2013).
[321] TIA, TIA -4940 Smart Device Communications Reference Architecture (2011).
[322] L. Atzori, A. Iera, G. Morabito, From ""smart objects" to ""social objects": The next evolutionary step of the internet of things, Communications Magazine, IEEE 52 (1) (2014) 97–105.
[323] T. Schmid, M. B. Srivastava, Exploiting Social Networks for Sensor Data Sharing with SenseShare, in: CENS 5th Annual Research Review, 2007.
[324] D. Guinard, M. Fischer, V. Trifa, Sharing using social networks in a composable Web of Things, in: Proc. of IEEE PERCOM Workshops, 2010, pp. 702–707.
[325] L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl5, H.-W. Gellersen, Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts, in: In Proc. of ACM UbiComp 2001, 2001, pp. 116–122.
[326] L. Atzori, A. Iera, G. Morabito, SIoT: Giving a Social Structure to the Internet of Things, IEEE Communications Letters 15 (11) (2011) 1193–1195.
[327] L. Atzori, A. Iera, G. Morabito, M. Nitti, The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization, Computer Networks 56 (16) (2012) 3594 – 3608.
[328] H. Zargariasl, A. Iera, L. Atzori, G. Morabito, How often social objects meet each other? Analysis of the properties of a social network of IoT devices based on real data, in: Proc. of the 1EEE Globecom, 2013.
[329] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, P. Steggles, Towards a Better Understanding of Context and Context-Awareness, in: Proc. of the 1st ACM International Symposium on Handheld and Ubiquitous Computing (HUC), Springer-Verlag, London, UK, UK, 1999, pp. 304–307.
[330] C. Perera, A. B. Zaslavsky, P. Christen, D. Georgakopoulos, Context Aware Computing for The Internet of Things: A Survey, IEEE Communications Surveys Tutorials 16 (1) (2014) 414–454.
[331] F. Andreini, F. Crisciani, C. Cicconetti, R. Mambrini, Context-aware location in the Internet of Things, in: Proc. of IEEE GLOBECOM Workshops, 2010, pp. 300–304.
[332] F. Andreini, F. Crisciani, C. Cicconetti, R. Mambrini, A scalable architecture for geo-localized service access in Smart Cities, in: Proc. of IEEE Future Network Mobile Summit (FutureNetw), 2011, pp. 1–8.
[333] I. Akyildiz, J. Jornet, The Internet of Nano-Things, IEEE Wireless Communications 17 (6) (2010) 58–63.