The Internet of Things (IoT): An Overview

Article · December 2015

CITATIONS
91

READS
34,823

3 authors, including:

Antar Abdul-Qawy
SUMAIT University
28 PUBLICATIONS **341** CITATIONS
SEE PROFILE

Srinivasulu Tadisetty
39 PUBLICATIONS **285** CITATIONS
SEE PROFILE

RESEARCH ARTICLE OPEN ACCESS

The Internet of Things (IoT): An Overview

Antar Shaddad Abdul-Qawy*, Pramod P. J**, E. Magesh**, T. Srinivasulu*
*(KU College of Engineering and Technology, Kakatiya University, Warangal, India
Email: {eng.antar2007, drstadisetty}@gmail.com)
** (Centre for Development of Advanced Computing (C-DAC), Hyderabad, India
Email: {pramodpj, magesh}@cdac.in)

ABSTRACT
Information and Communications Technology (ICT) controls our daily behaviors. It becomes a main part of our life critical infrastructure bringing interconnection of heterogeneous devices in different aspects. Personal computing, sensing, surveillance, smart homes, entertainment, transportation and video streaming are examples, to name a few. As a critical living entity, Internet is contentiously changing and evolving leading to emerging new technologies, applications, protocols and algorithms. Acceleration of wireless communication trends brings an ever growing innovation in Internet connectivity and mobile broadband. Infrastructureless communication devices become ubiquitous, smart, powerful, connectible, smaller, cheaper, and easier to deploy and install. This opens a new future direction in the society of ICT: the Internet of Things (IoT). Nowadays, the IoT, early defined as Machine-to-Machine (M2M) communications, becomes a key concern of ICT world and research communities. In this paper, we provide an overview study of the IoT paradigm, its concepts, principles and potential benefits. Specifically, we focus on the IoT major technologies, emerging protocols, and widespread applications. This overview can help those who start approaching the IoT world aiming to understand and participate to its development.
Keywords: ICT, IOT, M2M, Smart Objects, Heterogeneous Devices.

I. INTRODUCTION

How would be the world without Internet? It is difficult to imagine such scenario we have never seen. Today, the Internet becomes more and more important for everybody in both personal life and professional life. Different devices such as smart phones, sensors, mobile computers, and more other smart objects are examples of things everyday we are dealing with. These and other IoT related technologies significantly affect new ICT and enterprise systems technologies [1]. In the early evolution, it is known as "Internet of Computers"; then changed to "Internet of People"; and recently, with the rapid development in the ICT, it is recognized as the "Internet of Things". In the IoT, different devices and smart objects are included to expand the Internet and become accessible and uniquely identified. The connectivity is enhanced from "any-time, any-place" for "any-one" into "any-time, any-place" for "any-thing" [2]. In the ICT innovations and economy developments, a significant focus has shifted to the IoT related technologies where it is widely considered as one of the most important infrastructures of their promotion and one of the future promise strategies. The main aim is to enable interaction and integration of the physical world and the cyber space [3].

The IoT is considered as a pillar of future Internet and expected to enable intelligent operations and advanced communications of devices, smart objects, systems, and services. Indeed, it is a new revolution in communication technology which means that everything, from tires to hairbrush, will be assigned a unique identifier so can be addressed, connected to other things and exchange information. There is no exact or standard definition of the IoT yet. In [3], it is defined as "based on the traditional information carriers including the Internet, telecommunication network and so on, Internet of Things (IoT) is a network that interconnects ordinary physical objects with the identifiable addresses so that provides intelligent services". In [4], the author suggested a definition of IoT as "a worldwide network of interconnected objects uniquely addressable, based on standard communication protocols", semantically as its origin expression is composed of two words: "Internet" and "Things". However, the true value of IoT is in its ability to connect a variety of heterogeneous devices including everyday existing objects, embedded intelligent sensors, context-aware computations, traditional computing networks and smart objects that differ in their design, systems, protocols, intelligence, applications, vendors, and sizes. These entities are able to communicate and integrate with each others to collect, generate, process, and exchange data through applications and management systems residing on data centers or network clouds. This helps to carryout complex operations and intelligent tasks cooperatively and to make decisions independently

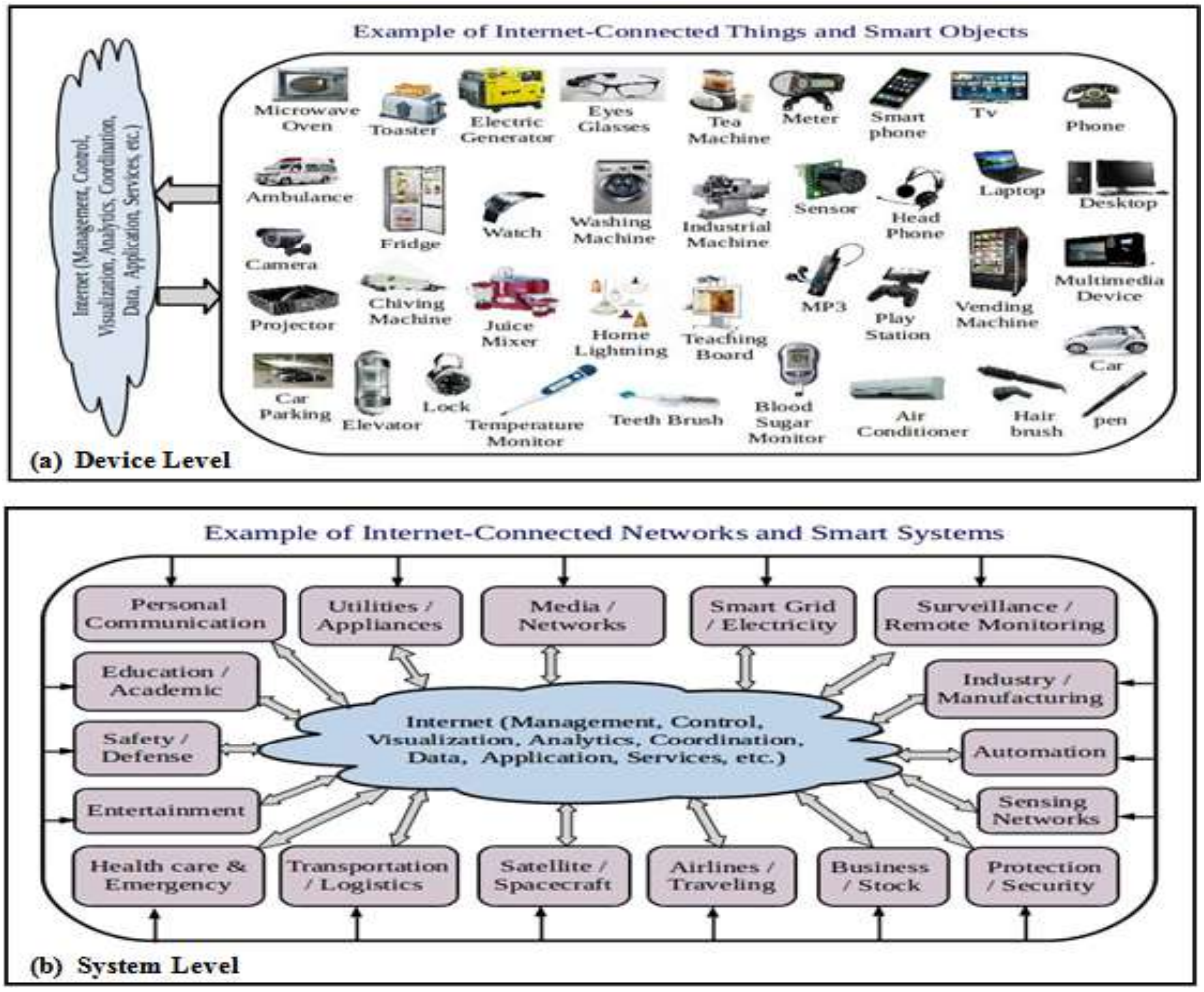

Fig. 1: Internet of Things: Devices and Systems Level Interconnection.

without human interventions. Fig. 1.a and Fig. 1.b depict the offered interconnection of different ubiquitous objects in the IoT in terms of individual devices and connected systems.

This paper provides the reader with a comprehensive view of the key aspects of the IoT and enabling factors in one integrated article; systematically organized and briefly illustrated. The rest of the paper is organized as follows: Section II presents vision and concepts of the IoT, more specifically M2M, key features, and LLNs (Low Power and Lossy Networks). Section III provides a discussion of the IoT elements and major technologies. In Section IV, we give briefs about protocols and standards considered for the IoT. Section V introduces the most relevant applications; while the research directions/future challenges, as discussed in literature, are listed in Section VI. We conclude the paper in Section VII.

II. VISION AND CONCEPTS

In the near future, the number of Internet-connected things would be highly larger than the number of people. The objects surround our environments will be linked to the Internet in one form or another. The physical and ICT worlds would be integrated together giving a vision beyond the realm of the traditional networks. The communication is not going to be people to people; it's not going to be people accessing information. It's going to be about machines talking to other machines on behalf of people [5]. Different communication technologies and products such as cellular phone, from GSM to HSDPA, satellite, Ethernet, WiFi, WiMAX, Bluetooth, ZigBee, etc. would became parts of the IoT realm and be embedded with M2M capabilities [6]. The most paramount side of the IoT vision is the inclusion of smart things. These objects are seamlessly connected to the Internet and fitted with intelligence, computing, sensing, remote monitoring, and control capabilities.

A. From M2M to IoT

Machine to Machine (M2M) communications is a broad term refers to technologies that allow mechanical or electronic devices to connect with other devices and freely automate data transmission and measurement using the wireless networks. The

key component of M2M is a small hardware module embedded in the main and larger device such as sensor, monitoring system, automobile, air conditioner, surveillance camera, or alarm system, which usually needs to communicate with other devices in the network. In fact, there is not big difference between this small module and the type of communication radio or transceiver circuits embedded in the cell phone and smart objects. The difference is that M2M device does not require some functionality of these objects such as display, camera, MP3 drivers, audio codecs, sound control, or keyboard for example [6]. It does not need any manual assistance or human intervention to perform the process of communication and data exchange. Generally, M2M and IoT are analogous. IoT is more adopted in the consumer space while M2M has a stronger industrial connotation [7]. In the broader sense of ICT, the two acronyms are equivalent and refer to the same paradigm. Indeed, IoT is the new name of the M2M concept that relies on IP-based networks. The concept of M2M was first used during World War II for identifying friend or foe to prevent pilots from hitting friendly targets. An early discussion of the M2M communications emergence is introduced in [6] by Juan Conti. He stated that even a lot of the M2M systems were deployed but they were not called as that. Instead, such systems were called based on their abstract function such as "building automation", "patient monitoring", "automated meter reading", "automated asset tracking", "fleet management", or "stolen vehicle recovery system."

However, the M2M technology has been growing significantly and affects every aspect of our life. Different industrial and business domains such as computer, food, agricultural, electrical, mining, oil and gas, extremely make use of the M2M communications in several applications. Machine maintenance, measuring, security, remote monitoring & controlling, chain supplying, and asset tracking are examples. End-user also benefits from this technology in many applications such as wearable objects, home automation and smart cars. In [6], the author has listed three technological factors that are together bringing the importance of the M2M: (i) the proliferation of industrial machines and home appliances embedded with powerful and low-cost processing units, (ii) the integration of the Internet as a standardized distribution network, and (iii) the declining of wireless technology prices. Nowadays, the IoT, which relies on IP-based networks, would be able to accommodate a wider variety of heterogeneous devices and smart objects, manage and analyze large amount of data exchanged while maintaining a scalable and seamless connectivity. According to Gartner forecasts, the Internet-connected things would reach to 4.9 billion in 2015 and will be 25 billion by 2020 [8] (see Table 1). Even though this is extremely large, Cisco says it will be 50 billion [9]; Morgan Stanley says 75 billion [10]. The IoT would support total services spending of $69.5 billion in 2015 and $263 billion by 2020 [8].

Table 1: IoT Units Installed Base by Category. Source: Gartner Inc [8].

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2,874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	3,032.0	3,750.0	4,880.6	25,006.6

B. Key Features and Characteristics

The IoT refers to networks of heterogeneous devices rather than traditional networks of homogeneous devices. Things, in the IoT, involve a variety of embedded devices and smart objects whose interconnection is expected to enable advanced & intelligent applications and to make the communications and automation, mostly in all areas, easier and achievable. In [11], the authors defined three categories which the IoT refers to: (i) the network interconnecting heterogeneous and smart devices which is an expansion of traditional Internet, (ii) the required technologies to support and realize this interconnection (such as RFIDs, sensor/actuators, etc) and (iii) the services and applications exploiting this vision in different areas. An ambient intelligence is early proposed using Wireless Sensor Networks (WSN). A large number of smart sensors are deployed to monitor environmental conditions and send an alert signal, for any change, to a control system which responds with appropriate action. Such a mechanism can be adopted in different areas with different purposes like surveillance systems, health care, home automation, etc. The IoT is the paradigm which aims to achieve functionality of such forest like networks intelligently and interactively. Three main pillars are identified in [11] for building the IoT: a thing should be (i) identifiable, (ii) able to communicate, and (iii) able to interact. In [3], three objectives of the IoT are proposed: (i) "more extensive interconnection which refers to extensiveness in the number of devices, type of devices technologies, and the mode of interconnection, (ii) "more intensive information perception" which refers to the collaboration to integrate the data from different objects that is subjected to non-uniformity, inconsistency, inaccuracy, etc., and (iii) "more comprehensive intelligent service" where the smart objects provide

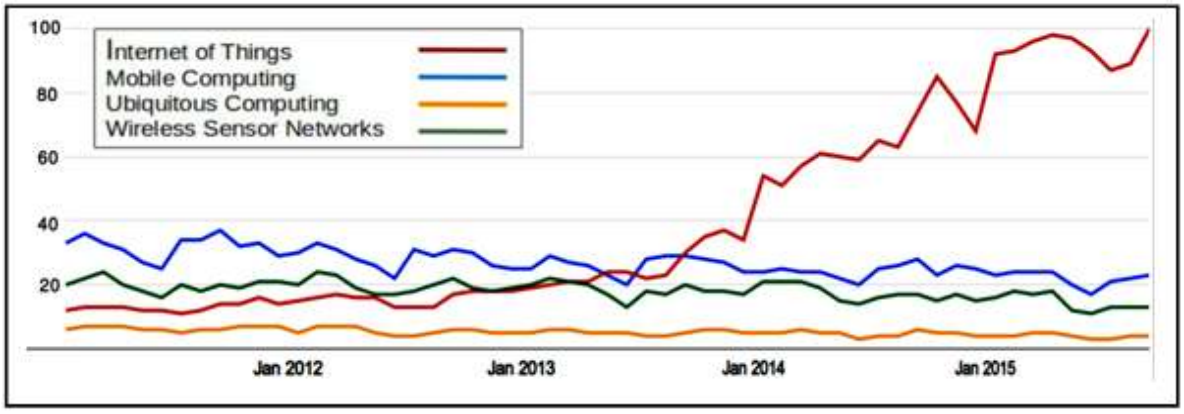

Fig. 2: Research popularity since 2011 of the Internet of Things, Mobile Computing, Ubiquitous Computing, and Wireless Sensor Networks (source: Google search trends [12]).

intelligent services and efficiently control the environment.

However, the complexity of the IoT lies on how to achieve such aims by expanding and evolving the traditional Internet. This would be realized by integrating a number of key technologies (Section III) with the IP-based networks. Three steps are identified in development trends: (i) embedding intelligence to things so they can act automatically and alone, (ii) making things able to be connected to other things, and (iii) enabling interaction and information exchange between these things [5]. The intelligence embedded to smart objects, which is independent of network and not related to the Internet, is a key feature of the IoT and already have been seen in several devices & applications. The air conditioner can keep the temperature at the desired level; A sliding door opens, waits and closes; the food information can remotely be read using RFID technology, to name a few. Ubiquitous computing, mobile computing, and wireless sensor networks are integral parts of the IoT, in the broader sense. The web search popularity for these paradigms and the IoT during the last five years, as obtained by Google search trends [12], is shown in Fig. 2 indicating the superiority of the IoT. We can see how it significantly increased in the last two years. It is likely to continue as more attention would be paid and advance IoT technologies would emerge enabling a promise future Internet.

C. LLNs

As discussed above, billions of things and smart objects are integrated together in a network making up the IoT. The types of these things at most are battery-powered entities, deployed in mesh topology and wirelessly connected. Therefore, these devices typically are embedded with limited power, memory, and processing resources. The IoT network generally is optimized for energy saving and operates under a variety of such working constraints [13], [14]. Such formed networks also referred as so celled Low power and Lossy Networks (LLNs) or IP smart objects networks [13].

LLNs have some characteristics that make them distinguished from other traditional networks and open promised opportunities in the near future research. These features, in some cases, my limit their construction, architecture and communication capabilities; and affect, in general, the main attributes such as power efficiency, link reliability, and maximum achievable throughput [14]–[16]. As most of the network devices are autonomous and battery-powered, the LLNs work with a very small bound "on" state to reduce energy consumption; a majority of nodes are asleep most of time and wake up periodically [14], [17]. Both the network nodes and links are put to the work under predefined constraints. For nodes, the constraints may be on processing power, memory, or energy (battery power); while constraints on links may include high loss rates, low data rates, and instability [14], [16]. LLNs are optimized to minimize the time a packet is en-route; therefore, it is proposed to work with restricted frame-size links. The links are unidirectional and have asymmetric property to support uplink and downlink directions separately with substantially different bandwidth in most cases [16]. Moreover, LLNs support different types of traffic patterns, not only simple unicast point-to-point, but also Multipoint-to-Point (MP2P) and Point-to-Multipoint (P2MP) [14]–[17]. For such characterized networks, to successfully interact with the surrounding world and efficiently utilize these resource-limited devices, a number of IETF working groups and industry alliances have addressed LLNs. Several protocols are developed (see Section IV).

III. ELEMENTS AND MAJOR TECHNOLOGIES

To be realized as a fully integrated future Internet, the IoT requires essential technology

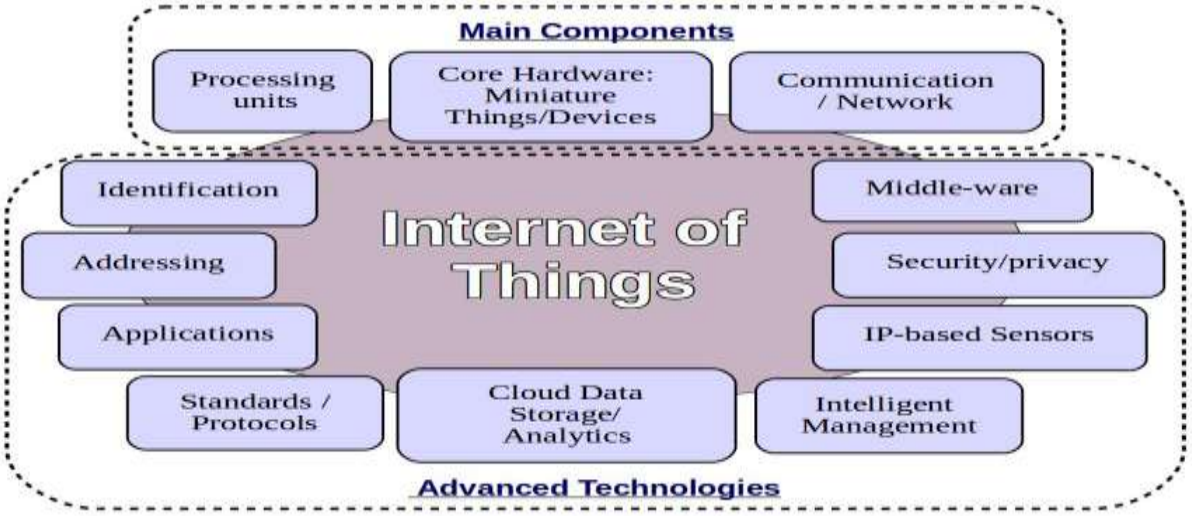

Fig. 3: Key Elements and Technologies for the IoT.

components that are incorporated together to form the IoT world (see Fig. 3). In this section we discuss the key enabling technologies. The aim is to present a brief about each element indicating its role in the IoT paradigm.

A. Identification & Addressing

The IoT contains extremely large number of scattered devices and hence the identification, discovery, and addressing schemes are essential technologies for the IoT. Every object included into the IoT networks must be uniquely identified. This is not only to distinguish IoT elements, their locations and functionalities, but also to automatically and remotely control these elements through the Internet [18]. Thus, to achieve such objectives, different schemes/technologies have been used including uID [19], URN [20], RFID [21], [22], and IPv6 addressing [23], [24]. RFID (Radio frequency identification) is a wireless communication technology used for remotely object identification. A tiny electronic microchip called RFID tag is attached to the object (even an animal or a person) acting as a barcode to store the object unique identifier and other more information in form of Electronic Product Code (EPC). The ID and information can be obtained in a seamless and automatic way using a remote RFID reader. The reader can initiate an appropriate communication signal using radio frequency triggering the tag. RFID tag respond by sending the ID and/or the other stored information based on the query signal sent. There are three types of RFID tags: passive, active, and semi-passive tags. The active RFID tags are battery-powered and have transmitters for communication. The passive RFID tags, which are the majority, usually harvest the power from the reader's transmitted signal. Semi-passive tags have batteries to power the microchip only while they harvest the power from the reader for radio communication.

RFID technology can be used for items monitoring and tracking in timely manner even if they are not in line-of-sight [25]. Thus, it has been widely used in several applications of the IoT such as supply chains, cargo tracking, electronic tolls, remote-sensing, asset management, pharmaceutical production, and hospital laboratories [1], [26]. The IPv6 has been adopted for the IoT to overcome the IPv4 inability to meet the rapid growth of addressing space requirements [23], [24]. It guarantees an adequate capacity of addressing pool for the future sharp increase. The IPv6 have been utilized to support scalable addressing schemes and a secure access to the resources uniquely and remotely. Moreover, it have introduced advanced mechanisms to support Internet mobility and devices handover. A lightweight IPv6 also is an important development scheme which is used for home appliances and smart objects addressing [18], [27].

B. Embedded Sensors

With the recent advances in the sensing technologies, WSN has been improved more and more, gaining the ability of working in harsh and hazardous environments. WSN typically utilizes a large number of spatially distributed sensors or sensor-embedded devices which can be efficiently cooperate with RFID technology. These elements have different functionalities such as monitoring physical/environmental conditions and tracking the status of things like their locations, temperature, and movements [25]. Optimizations such as the reduction of device size, weight, energy consumption and cost as well as the enhancements in wireless communications have enabled the IoT to employ intelligent sensors as an essential technology in a major part of its networks. Such Intelligent sensors,

which use real-time remote sensing, enable the ability to gather, analysis, process, share, and distribute, to centralized systems, a variety of environmental information [18]. As such, they can augment the awareness of a certain environment and, thus, act as a further bridge between physical and digital world [25]. Moreover, RFID sensor networks (RSN) can be built by integrating of sensing and RFID technologies to support the sensing, computing, and communication capabilities in a passive system [25].

C. Protocols & Middleware

In the IoT, billions of devices and smart objects, having different capabilities, require a means for exchanging and transmitting the information collected or generated at the device level. However, the IoT devices are expected to be connected together and able to talk in a way or another. An IoT object must be able to communicate with other devices: identify the proper path to the destination, understand the received messages, and consequently respond with an appropriate manner. Thus, standard protocols become key requirements for the IoT world. This makes it straightforward to achieve the full functionality of such constrained devices while maintaining the desired level of network performance. The mobility in the IoT is one of the major issues. A mobile device frequently moves from one place to another. It requires, in most cases, to be handed-over from the current attachment point to another. The communication protocols must be aware of such nature in the majority of the IoT devices [25]. Intelligent mechanisms are required in order to provide a seamless handover and reduce the delay imposed at different layers. In Section IV, we discuss some of the protocols considered for the IoT devices [25]. Intelligent mechanisms are required in order to provide a seamless handover and reduce the delay imposed at different layers. In Section IV, we discuss some of the protocols considered for the IoT.

The middleware software layer also is an essential in such massive networks having different application systems, different functionalities, and variable data types. Middleware enables the interaction between the ‘’Internet” and “things”. It acts as an interface enabling the various applications on heterogeneous systems to easily and seamlessly communicate with each others. Middleware software layer has a major role in hiding the underlying details. This facilitates developing of new applications and software services for distributed environment independently of the underlying technologies [25].

D. Cloud-based Storage & Analytics

The IoT dense networks result in unprecedented amount of data. This data needs to be intelligently gathered, analyzed, processed, and stored for more efficient and smart monitoring, actuation and real-time decision making [18]. Some of applications in the IoT also require big data storage, large processing rate to realize real-time control, and high speed broadband networks to flow data, audio, or video [26]. However, intelligent algorithms need to be developed for making sense of such big data and efficiently manage the IoT applications requirements. Cloud computing, cloud-based storage, and cloud-based analytics provide an ideal solution paradigms for handling, storing and real time processing such massive data from unpredictable number of devices [18], [26]. The data is collected from different IoT devices into the cloud. Then, it can be aggregated/consolidated with other data from Internet resources, analyzed, and processed using cloud-based services. Thus, provide useful information for the end users. Moreover, it may be used by intelligent systems for better automatic actuation and remote control.

E. Applications

Without applications, the IoT makes no sense. IoT applications provide a real-time message delivery and reliable communications. They introduce all the system functionalities to the end-user through myriad of connected devices. The physical connectivity is achieved by networks and devices, whereas the robust interactions of device-to-device and human-to-device are provided by the IoT applications [26]. In the human-device applications, visualization is considered as one of the key features that allows user to easily interact with the environment and efficiently present and understand the collected information [18], [26]. In device-to-device applications, intelligence is usually implemented for enabling dynamic interactions. This allows devices to automatically monitor the environment, identify the problems, collaborate, and independently make the proper decisions without human intervention [26]. In Section V, we discuss more about the IoT applications.

F. Core Hardware

In addition to what are mentioned above, IoT devices/smart objects, whatever they are (consumer electronics devices, home appliances, intelligent cars, wireless sensors, or industrial machineries), typically consist of main entity components (IoT core hardware). This includes memory, processing units, power supply, transceiver capabilities, etc. Here, the things almost comprise a variety of communication technologies and terminals integrated to support M2M connectivity between various objects and making them more versatile. Moreover, they usually contain several A/D for sensor interfacing with the main intelligent system [18]. However, these things, integrated with other technologies, are able to capture

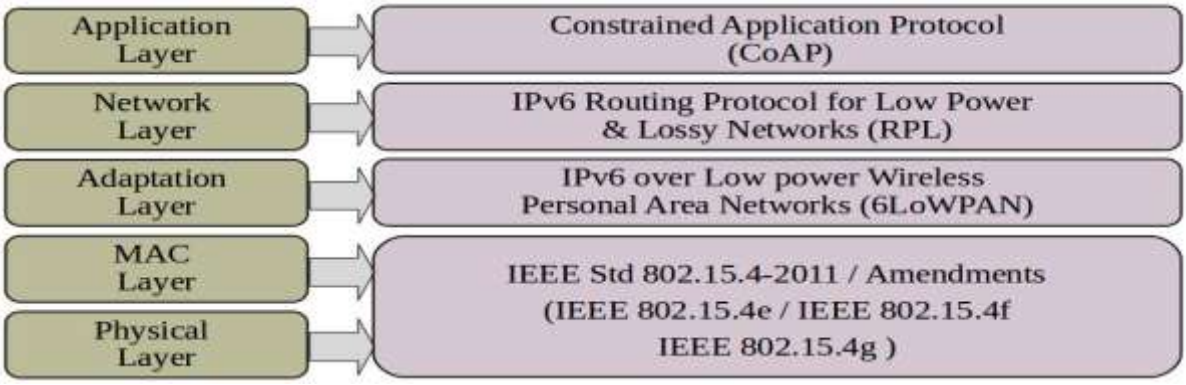

Fig. 4: Emerging Protocols for the IoT.

an internal change or environmental event and pass to the applications which are able to interpret this event into meaningful information. This information then can be used to automatically control the situation in self-managed autonomous systems, shared with the other objects in proximity to make some decisions of their own, or sent through communication hardware to the intelligent system in cloud.

IV. PROTOCOLS

The IoT typically is a very large scale network consisting of heterogeneous constrained devices and smart objects. Such constrained network imposes a significant impact on designing of different protocols. However, taking this into account, generally, enables for designing a broad set of standards and protocols. These protocols are supposed to offer efficient and scalable communications and allow developing and deploying applications/services adopted for a variety of environments. In the next subsections, we discuss some developed protocols that are considered for the IoT/LLNs as shown in Fig. 4.

A. IEEE 802.15.4

The IEEE 802.15.4 is a standard designed by IEEE 802.15 working group in IETF which defines the physical (PHY) and media access control (MAC) layers for low data rate, low-power, and short-range wireless personal area network (LR-WPANs) [17], [29]. The original version is provided in 2003 supporting data rates of 20, 40, and 250 kb/s with a 10-meter communications range of ubiquitous communication between devices. Afterward, EEE 802.15.4a/c/d are provided as improvements expanding the PHY layer with several additional frequency bands and transmission techniques. IEEE Std 802.15.4-2011, a revision for the previous amendments, is provided to roll them in a single standard supporting a maximum data rate of 850 kb/s with a focus on the interoperability technical requirements [29]. Later, a number of amendments are introduced such as IEEE 802.15.4e, IEEE 802.15.4f, and IEEE 802.15.4g [30]–[32]. The IEEE 802.15.4e [30] is released in order to improve and add functionality to the MAC sub-layer. A channel hopping strategy is adopted to enhance the support for industrial markets, and improve the robustness to overcome the multi-path fading and external interference. In IEEE 802.15.4f [31], the PHY is improved to support flexibility and better performance in the high dense deployments of autonomous devices, and active RFID systems wherever in the world. This amendment supports a wide range of applications that characterized with several constraints such as low cost, low power consumption, multiyear battery life, reliable communications, precision location, and reader options [17], [31]. The IEEE 802.15.4g supports out-door low data rate, wireless, smart-grid networks requirement and offers a higher transmission range equal to 1km and a large packet size of 2047 byte [17], [32].

The IEEE 802.15.4 provides real-time appropriateness with provision of guaranteed time slots, secure communications, transfer reliability, CSMA/CA, link quality indication (LQI) and energy detection. Moreover, it offers a technological simplicity and very low manufacturing and operation costs [29]. The IEEE 802.15.4 is the foundation for several protocol stacks such as ZigBee, WirelessHART, MiWi, and RPL and 6LoWPAN [17].

B. 6LoWPAN

The IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) is a standard for adaptation layer allowing IPv6 packets to be sent and received over IEEE 802.15.4 based links [33]. It realizes the idea of applying Internet protocol to the small autonomous devices, as the only available solution for smart object networks or LLNs. Thus, enabling such constrained devices to be connected in a very large number, to the Internet [17], [33], [34]. Moreover, 6LoWPAN supports mobility where the devices, at most, are deployed in an ad-hoc fashion without predefined locations and move continuously. For mapping from IPv6 network to that of IEEE 802.15.4, 6LoWPAN performs three key functions:

(i) IPv6 header compression, (ii) IPv6 packet fragmentation, and (iii) layer-2 forwarding [17].Foreach,aseparate6LoWPANheader is included when necessary. In the first, the IPv6 header is compressed down where the fields that can be obtained from the context are omitted and the remaining are send unmodified. In the second, the packets larger than IEEE 802.15.4 MTU are fragmented at the sender and re-assemble at the destination. In the third function, which is called mesh-under and suitable for small & local networks, the IP routing is not performed. The packets are forwarded to the destination over multiple radio hops by adaptation layer. This routing is made at link layer level depending of 6LoWPAN header and IEEE 802.15.4 frame [17], [34].

C. RPL

The IPv6 Routing Protocol for LLNs (RPL) is a network layer protocol designed for low power and lossy networks [14], [35]. RPL has been developed with the objective of meeting application-specific requirements for LLNs (Section II-C) identified by ROLL (Routing Over LLNs) working group in IETF. These requirements are define for, but not limited to, a set of application areas: industrial, building automation, home automation, and urban sensor networks. As per the evaluation, ROLL have found that the existing protocols such as OSPF, IS-IS, AODV, and OLSR do not satisfy all the specified requirements. These protocols which use only static link metrics, do not take devices statues such as processing resources, memory, residual energy or hardware failures into account when creating best/shortest path [14], [17].

The RPL is an extensible proactive IPv6 distance vector protocol which supports for mesh routing environments, shortest-path constraint-based routing (on both links and nodes) and different traffic patterns including MP2P, P2MP and P2P. It considers routing optimization objectives independently of packet processing & forwarding and can be run over various different link layers. That includes constrained link layers or those utilized in conjunction with highly constrained devices such as, but not limited to, low power WPAN (802.15.4) or PLC (Power Line Communication) technologies [35]. In addition, the RPL includes measures for power conservation such as adapting the sending rate of control messages and updating the topology only when data packets have to be sent [16]. On a network, more than one instance of RPL can be run simultaneously. Each such instance may consider a set of different and potentially antagonistic constraints or optimization objectives [35]. The RPL builds a loop free Destination Oriented Directed Acyclic Graph (DODAG) based on such criteria. Objective Function (OF) defines such constraints and objectives and identify how to use them for building such graph (DODAG & OF are out of scope here. For more about the RPL, see [14], [16], [17], [35]).

D. CoAP

The Constrained Application Protocol (CoAP) is a web based application layer protocol designed by the Constrained RESTful Environments (CoRE) working group in IETF [36]. It offers interactive M2M communications for autonomous devices and smart objects through the standard Internet. It is intended to be used in the low power and constrained networks such as LLNs/IoT and 6LoWPAN that require remote monitoring & manipulating. CoAP is a lightweight version of HTTP that supports simplicity, low message overhead, reduced parsing complexity, and limited need for packet fragmentation in such constrained environments and devices. Moreover, it is a platform that provides a request/response interaction model between applications and easily facilitates the integration of the embedded networks with existing web [36], [37]. Plus, it has more features for M2M such as built-in discovery, proxy-mode support, multicast support, reliable delivery, and asynchronous message exchanges [17], [36]. The packets in the CoAP are much smaller, simpler to generate and easier to parse with less memory used. CoAP is datagram based which runs over UDP, not TCP. However, it may be used on top of SMS and other packet based communication protocols [38].

V. APPLICATIONS

Advancements in the IoT motivate for adoption more and more applications of such innovative technology. IoT applications have increasingly overspread industries and public/private sector organizations saving our time, resources and efforts. Applications of the IoT have been categorized in literature based on different classification criteria and factors putting them into several distinguished domains such as presented in [2], [11], [18], [39], [40] and [28]. In [28], three major domains of IoT applications are identified: industry, environment, and society (see Table 2). These fields are cohesively linked and interrelated with each others and can not be isolated. Within each broad domain, more and more applications can be further identified. The base requirements of these applications in such domains are often the same with a marginal difference depending on the main functionality of the application. In this section we briefly investigate some of the common and widely used applications of the IoT.

Monitoring and controlling systems are common applications of the IoT. Data about environment or networked objects is collected (sensed or calculated), sent to an intelligent system (centralized or

Table 2: IoT Application Domains - Description and Examples. (Source: CERP-IOT [28]).

Domain	Description	Indicative examples
Industry	Activities involving financial or commercial transactions between companies, organizations and other entities	Manufacturing, logistics, service sector, banking, financial governmental authorities, intermediaries, etc.
Environment	Activities regarding the protection, monitoring and development of all natural resources	Agriculture & breeding, recycling, Environmental management services, energy management, etc.
Society	Activities/initiatives regarding the development and inclusion of societies, cities, and people	Governmental services towards citizens and other society structures (eparticipation), einclusion (e.g. aging, disabled people), etc

distributed) and then a right decision is made. This allows continuously tracking the working behavior, reconfiguring operating parameters, and thus automatically adjusting the resulting performance of the system. WSN is early adopted in such scenarios and have constantly been a main technology in the security and climate control systems. Nowadays, IP-based WSN identified as a subnet of the IoT networks providing enhanced flexibility, interaction, and dynamics to the environmental monitoring applications [18]. This includes measuring the natural phenomena such as wind, storm, rainfall, temperature, pollution, river height, etc. and keeping track of the mobile objects in real time anywhere and anytime [26]. Surveillance and security in different scenarios such as in homes, markets, malls, enterprises etc., are also noticeably adopted using IoT-based WSN technologies.

In a smart city, an integrated digital infrastructure is adopted. The key services are managed in an intelligent automated manner to enable higher efficiency, and lower operational costs. For example, in the smart grid, a smart metering is employed to constantly monitor the electricity points in the city scale. Based on data collected, such system enables to improve the way energy is consumed and helps to maintain the load balancing and high QoS [18]. Moreover, the smart traffic system provides advanced traffic control in which the care traffic is monitored at the big cities scale and highways. This system offers services to the car drivers by providing alternative traffic routes to avoid congestion [11]. In a smart home/building, the equipments and appliances such as washing machine, oven, fridge, air conditioner, ventilation, hating, sliding door, etc., are controlled automatically via an intelligent management system. For example a computer receives data on the building's environment and issue commands to devices, or the device itself is equipped with an intelligence capability of doing such task. Such systems offer a cohesive living environment with better tasks scheduling, notifications, security and resource management such as energy conservation. Health care systems also benefit from the IoT technology to provide more efficient care services. Body Area Network (BAN) is an example of data analytics in which the patient behavior/condition is constantly monitored. For instance, networked in-body nanosensors are envisioned in [40]. Such nonosensors collaborate with on-body sensors that are worn or put on the body of human, to measure various physiological parameters. These parameters are uploaded through several IP-based interfaces to the centralized servers or monitoring system. The specialists and physicians can access this data and respond in real-time and effectively intervention and treatment [18].

In the business domain, intelligent systems are utilized to discover and resolve business issues in order to make proper response and achieve customer's satisfaction [26]. In supply/delivery chain and distribution logistics, for instance, items and perishable goods tracking is one of the common applications making use of RFID technology. Using collected information, the remote buyer/supplier is able to continuously monitor the status and movement of the goods, for example, the current locations, quantity, environmental conditions, and the expected time of availability in the market [11]. Thus, making this information automatically accessible to the customers. In the manufacturing, smart factories have become prominent helping to improve the production process. In such systems, the intelligence is embedded in the machineries and equipments. Thus, making them able to improve their performance through self-management capabilities. Moreover, these components are connected together via robust coordination and controlling system. Human intervention is largely reduced resulting in a number of key benefits such as faster production/delivery time, less cost, improved quality, and safer working environments [1], [28].

However, information exchange & sharing, enterprises collaboration, smart banking, crowd monitoring, infrastructure monitoring, smart transportation, water measurement and more others

are just examples of the IoT applications. Extremely increase in the smart applications is expected to invade our life in the near future.

VI. DISCUSSION

As a fast-emerging fast-growing technology, the IoT open unprecedented opportunities for more developments and investments in the ICT. However, open issues and challenges emerge highlighting research trends and requiring more attentions. Recent research papers, reports and surveys provide several discussions for such challenges that face IoT developers. As the IoT is still in its infancy, the challenges span over different levels including big data management, analytics & mining, architecture standardization, scalability, privacy & security, clock synchronization, energy management, protocols, visualization, and QoS, [1], [11], [18], [26], [41]–[44]. Moreover, social IoT, and nano-IoT are new emerging dimensions as introduced in [40], [45] respectively. Such issues are expected to be further addressed in the near future and more cooperation efforts are needed. In particular, we assert the importance of paying special attentions to the following two issues: (i) energy-efficiency which is considered as a main objective of designing the IoT solutions. As the number of connected objects rapidly grow-up, the power consumption extremely increase; therefore, energy-efficient techniques are needed for developing green IoT systems [1], [11], [41]. (ii) clock-synchronization which becomes a critical technology for coherent distributed systems. A scalable time synchronization is required for enabling data consistency, better coordination, and task scheduling [11], [42]. Moreover, with a dynamic timing synchronization, an IoT device can time its sleep pattern making it possible to conserve higher energy [40]. We expect further participations in order to reduce the impact of such technical hurdles. Thus, building a coherent and consistent IoT world in which a thing or a smart object becomes survivable, interoperable and adaptable to be attached and work in any environment.

VII. CONCLUSION

The IoT is a cyber-physical system that integrates billions of heterogeneous devices and smart objects. These things are enabled by various technologies such as identification, embedded sensors, intelligent management, protocols, data storage/processing/analytics, etc. A wide range of IoT applications have been adopted and deployed in the last few years. In this paper, an overview study of the Internet of Things is presented introducing the vision, concepts, features and the promise future. Brief discussions of the main technologies, the newly developed protocols, and the most common applications of the IoT are provided. The research directions/future challenges are listed for more efforts in the near future. We emphasize the importance of the power-efficiency and time-synchronization as future trends that, we believe, need a significant focus and more investigations. The major contribution of this paper is that it brings the main aspects of the IoT and its relevance together in one paper, presented in a straightforward and unverbose manner.

REFERENCES

[1] L. D. Xu et al., "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, Nov 2014.
[2] L. Coetzee and J. Eksteen, "The internet of things - promise for the future? an introduction," in Proceedings of IST-Africa Conference, 2011.
[3] H.-D. Ma, "Internet of things: Objectives and scientific challenges," Computer Science and Technology, Springer, vol. 26, no. 6, Nov 2011.
[4] M. Botterman, Internet of Things: an early reality of the Future Internet. a Workshop Report, European Commission, May 2009.
[5] L. Tan and N. Wang, "Future internet: The internet of things," in Proceedings of 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.
[6] J. Conti, "The internet of things," Communications Engineer, IEEE, vol. 4, no. 6, Dec 2006.
[7] EuroTech Inc., "M2M / IoT software and services," http://www. eurotech.com/en/ products/software+services, Sept 2010.
[8] Gartner Inc., "Gartner says 4.9 billion connected things" will be in use in 2015," http://www.gartner.com/newsroom/id/29057 17, Nov 2014.
[9] N. Earle, "50 billion things, coming to a cloud near you," Cisco, http: //blogs.cisco.com/news/ 50-billion-things-coming-to-a-cloud-near-you, June 2015.
[10] T. Danova, "Morgan stanley: 75 billion devices will be connected to the internet of things by 2020," Business Insider, http://www. businessinsider.in/articleshow/ 23426604.cms, Oct 2013.
[11] D. Miorandi et al., "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, Elsevier, vol. 10, no. 7, Sept 2012.
[12] Google Trends, Google (n.d.), http://www.google.com/trends.
[13] J. Hui and J. Vasseur, "Routing architecture in low-power and lossy networks (LLNs),

draft-routing-architecture-iot-00," https://tools .ietf .org / html/draft-routing-architecture-iot-00, RFC draft, Mar 2011.

[14] IETF ROLL WG., "Routing over low power and lossy networks (ROLL)," https://datatracker.ietf.org/wg/roll/charter/, Apr 2015.

[15] J. Vasseur et al., "RPL: The IP routing protocol designed for low power and lossy networks," IPSO Alliance, Apr 2010.

[16] T. Tsvetkov and A. Klein, "RPL: IPv6 routing protocol for low power and lossy networks," July 2011, http://www.net.in. tum.de/fileadmin /TUM/NET/NET-2011-07-1/NET-2011-07-1 09.pdf.

[17] J. Apcar, "The internet of things: Routing and related protocols," Cisco Live, https://www.ciscolive.com/online/connect/sessionDetail. ww?SESSION ID=77716&back Btn=true, 2014.

[18] J. Gubbi et al., "Internet of things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, Elsevier, vol. 29, no. 7, Sept 2013.

[19] K. Sakamura, "Challenges in the age of ubiquitous computing: A case study of t-engine, an open development platform for embedded systems," in Proceedings of the 28th International Conference on Software Engineering, 2006.

[20] L. Daigle et al., "Uniform resource names (URN) namespace definition mechanisms," https://tools.ietf.org/html/rfc3406, RFC 3406, Oct 2002.

[21] E. Welbourne et al., "Building the internet of things using RFID: The RFID ecosystem experience," Internet Computing, IEEE, vol. 13, no. 3, May 2009.

[22] C. Roberts, "Radio frequency identification (RFID)," Computers & Security, Elsevier, vol. 25, no. 1, Feb 2006.

[23] A. J. Jara et al., "The internet of everything through IPv6: An analysis of challenges, solutions and opportunities," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 4, no. 3, Sept 2013.

[24] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," https://www.ietf.org/rfc/rfc2460.txt, RFC 2460, Mar 1998.

[25] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, Elsevier, vol. 54, no. 15, 2010.

[26] I. Lee and K. Lee, "The internet of things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, Elsevier, vol. 58, no. 4, July 2015.

[27] J. Abeill et al., "Lightweight IPv6 stacks for smart objects: the experience of three independent and interoperable implementations," IPSO Alliance, Nov 2008.

[28] H. o. Sundmaeker, Vision and Challenges for Realising the Internet of Things. a Book, CERP-IOT, European Commission, Mar 2010.

[29] IEEE Inc., "802.15.4-2011-IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (LRWPANs)," IEEE Computer Society, Sept 2011.

[30] IEEE Inc., "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (LR-WPANs) amendment 1: MAC sublayer," IEEE Computer Society, Apr 2012.

[31] IEEE Inc., "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (LR-WPANs) amendment 2: Active radio frequency identification (RFID) system physical layer (PHY)," IEEE Computer Society, Apr 2012.

[32] IEEE Inc., "IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (LR-WPANs) amendment 3: Physical layer (PHY) specifications for low-data-rate, wireless, smart metering utility networks," IEEE Computer Society, Apr 2012.

[33] N. Kushalnagar et al., "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," https://tools.ietf.org/html/rfc4919, RFC 4919, Aug 2007.

[34] E. J. Hui and P. Thubert, "Compression format for IPv6 datagrams over ieee 802.15.4-based networks," https://tools.ietf.org/html/ rfc6282, RFC 6282, Sept 2011.

[35] T. Winter and et al, "RPL: Ipv6 routing protocol for low-power and lossy networks," https://tools.ietf.org/html/rfc6550, RFC 6550, 2012.

[36] Z. Shelby et al., "The constrained application protocol (CoAP)," https: //tools.ietf.org/html/ rfc7252, RFC 7252, June 2014.

[37] B. Villaverde et al., "Constrained application protocol for low power embedded networks: A survey," in Proceedings of 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012.

[38] Eclipse, "MQTT and CoAP, IoT protocols," http://www.eclipse.org/ community/eclipse newsletter/2014/february/article2.php, 2014.
[39] M. Chui et al., "The internet of things," McKinsey Quarterly, vol. 38, no. 2, May 2010.
[40] S. Balasubramaniam and J. Kangasharju, "Realizing the internet of nano things: Challenges, solutions, and applications," Computer, IEEE, vol. 46, no. 2, Feb 2013.
[41] C.-W. Tsaietal., "Future internet of things: open issues and challenges," Wireless Networks, Springer, vol. 20, no. 8, Nov 2014.
[42] J. Stankovic, "Research directions for the internet of things," Internet of Things Journal, IEEE, vol. 1, no. 1, Feb 2014.
[43] R. H. Weber, "Internet of things: Privacy issues revisited," Computer Law & Security Review, Elsevier, vol. 31, no. 5, Oct 2015.
[44] Gartner Inc., "Gartner says the internet of things will transform the data center," http://www.gartner.com/newsroom/id/26846 16, Mar 2014.
[45] L. Atzori et al., "From smart objects" to "social objects": The next evolutionary step of the internet of things," Communications Magazine, IEEE, vol. 52, no. 1, Jan 2014.