Internet of Things Standards: Who Stands Out from the Crowd?

While time-to-market constraints are accelerating the deployment of a variety of fragmented and proprietary IoT products, there is still a lack of understanding of what an IoT service is meant to be, what its consequences are, and how to promote standard IoT services. The author gives a concise but comprehensive survey of IoT service definition, regulation, and standardization activities. The author discuss mainstream standards as well as emerging, independent, and state-funded projects.

Aref Meddeb

The author is with the National School of Engineering, University of Sousse.

Abstract

While time-to-market constraints are accelerating the deployment of a variety of fragmented and proprietary IoT products, there is still a lack of understanding of what an IoT service is meant to be, what its consequences are, and how to promote standard IoT services. This article gives a concise but comprehensive survey of IoT service definition, regulation, and standardization activities. We discuss mainstream standards as well as emerging, independent, and state-funded projects.

Introduction

So far, the implications and impact of IoT are not fully understood and should be explored by standards organizations and industry consortia so that strategic roadmaps can be developed [1]. In particular, there are significant gaps between legislative mechanisms concerning privacy between many countries such as Europe, Canada, and the US. Fragmented IoT implementations exacerbate this issue and could potentially drive users away from IoT.

Since its inception, there were several movements and actions opposing IoT. In particular, RFID deployment in schools is raising a lot of opposition (rfidinschools.com). Also, some seem to be frightened by IoT. There are fears that a sort of "global government" will become able to control the world population to the extent where individuals may be remotely governed, tracked, and even "alienated."

Perhaps the most challenging obstacles on the way toward IoT are trust, security and privacy (TSP). Questions include: Will customers feel comfortable having their bank account, insurance, location, and health information available on the net and accessible by or via objects? How can we protect ourselves, and our homes, computers, cars, etc. from illegal monitoring and/or remote control? How to authenticate sensed data and tag reading? With IoT devices deployed everywhere, successful attacks can be very embarrassing.

On the other hand, IoT applications in industrial environments bring a plethora of concerns [2]. Industries may be skeptical when it comes to introducing communicating devices in their premises such as offices, plants, and supply chains. For example, businesses may be worried about fraudulent access to their inventories, work orders, and strategic business plans. Remote monitoring and/or control can have drastic consequences.

Another challenging issue is regulation. A recent consultation that drew over 600 responses from industry, government, academia, citizens, and consumer groups shows that opinions differ on what policymaking is needed for IoT. Industry stakeholders argue that unnecessary regulation could cripple innovation and compromise IoT business models. Consumers, on the other hand, are worried about the potential impact of IoT with regard to data protection and privacy. Innovation cannot be achieved at the expense of fundamental human rights. However, it may not be fair to place the emphasis solely on the potential problems of IoT. In fact, IoT is expected to grow mainly through users' trust.

Further, while there are claims about the need for common IoT standards, there are actually an overwhelming number of standards for IoT, emanating from mainstream standards development organizations (SDOs), mainly IETF, ITU-T, IEEE, ETSI, ISO/IEC, and the International Society of Automation (ISA), as well as other state-funded and international projects [3]. Therefore, without unified effort, instead of converging toward common standards, this overwhelming number of proposals might contribute to further exacerbating the confusion about services and regulation. In fact, IoT standardization is a very crowded area, to the extent that it is often compared to a war [4]. As such, we believe it is necessary to synthesize all ongoing activities to help researchers and stakeholders get a clear view of what is going on in terms of IoT standardization actions worldwide.

We first give a comprehensive overview of some of the main challenges IoT needs to overcome in terms of service definitions and regulation. These are discussed later. We illustrate that there is no general consensus on, nor common understanding about, IoT services. We provide a survey of IoT standards. State-funded and independent IoT projects, as well as initiatives, clusters, forums, etc., are described. We finally conclude the article by summarizing the most important findings and by "connecting the dots" between the standardization activities.

IoT Service Definitions

The term *Internet of Things* was first introduced back in 1999 by the Auto-ID Labs (autoidlabs.org) (formerly the Auto-ID Center of MIT), primarily for networked radio frequency identification (RFID) devices. Since then the concept has evolved, and nowadays IoT encompasses many other technologies including wireless sensor networks (WSN), near field communications (NFC), biotechnology and body area networks (BAN), machine-to-machine (M2M) communications, and other "legacy" personal area networks (PAN) such as WiFi, Bluetooth, etc. [5].

0163-6804/16/$25.00 © 2016 IEEE

Inexpensive, highly personalized, ubiquitous, and instantaneous services constitute key success factors for IoT. Unfortunately, so far there is no general consensus on what IoT is exactly meant to be. There is seemingly a "race" between IoT stakeholders to the extent that driven by time-to-market constraints and business requirements, most proposals made so far are fragmented and fail to consider all facets required to deliver a globally accepted IoT service. These proposals often lead to ambiguous and even contradictory definitions. For example, some proposals assimilate IoT to Web 3.0; others claim it is primarily based on RFID and similar systems; others associate IoT with machine-to-machine (M2M) communications; while others focus on WSN. Perhaps IoT is all of this. However, between web semantics, radio frequency identification, and sensor networks, there is a huge vacuum that needs to be filled by adequate standards and definitions to pave the way toward an IoT *ecosystem*.

Figure 1 depicts a high-level IoT stand-alone or "silo" architecture with most commonly used verticals including IPv6 over low-power wireless personal area networks (6LoWPAN), Zigbee (www.zigbee.org), Z-Wave (www.z-wave.com), wireless highway addressable remote transducer (WirelessHART http://en.hartcomm.org), ISA100.11a, Bluetooth Low Energy (BLE), RFID, Developers Alliance for Standards Harmonization of ISO/IEC 18000-7 (DASH7), Building Automation and Control Network (BACNet, http://bacnet.org), Local Operating Network (LonWorks, www.onmark.org), KNX (http://knx.org), and INSTEON (www.insteon.com). These are interconnected via an IPv6 backbone to familiar or legacy technologies such as 3G/4G/5G, WiFi, LiFi, Home Plug, vehicular networks (VANETs), as well as PSTN and IPv4 enterprise networks.

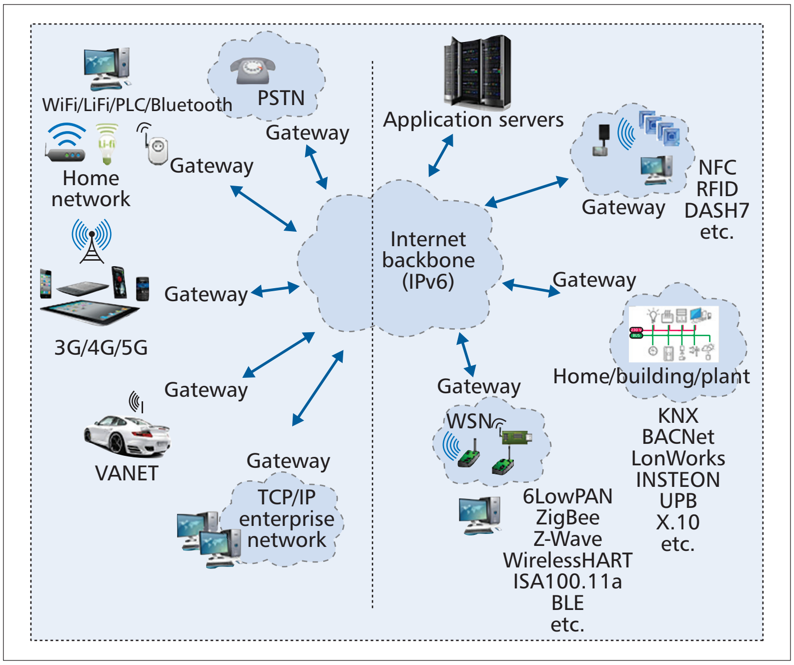

Figure 1. IoT services in Silo architecture.

Although most of these technologies are streamlined and widely deployed, in an IoT ecosystem where secure end-to-end interoperability will be needed, global standards and regulatory rules will be required [6]. For instance, there is a myriad of home automation "industry standards." Popular wired technologies include X-10 (X-10.com), universal powerline bus (UPB), KNX, LonWorks, and BACnet. On the other hand, Z-Wave and ZigBee are some of the most popular wireless solutions, while INSTEON is a combined wireless/wired solution. Each of these solutions has its own advantages and drawbacks, but the most important concern is that often they do not interoperate.

Similarly, WirelessHART and ISA100.11a are two of the most popular technologies used for smart plant, field process, and automation systems, yet they do not interoperate at all, although they both rely on the IEEE 802.15.4 MAC layer.

Beyond technical and syntactic interoperability, semantic interoperability constitutes another challenge to IoT systems. In a fully heterogeneous environment, semantic interoperability uses a common ontology for describing resources across fragmented IoT systems [7]. For instance, the ontology of the World Wide Web Consortium (W3C) semantic sensor networks (SSN) incubator group aims to overcome the limitations of XML formats and the fragmentation of sensor ontologies. However, this ontology describes sensors, observations, and related concepts, but not domains. Thus, it was further extended to specific IoT domains and applications such as smart cities and smart homes [8].

Further, the open source cloud solution for the Internet of Things (www.openiot.eu) project provides a common semantic layer enabling the annotation of sensors and devices as W3C SSN compliant sensors. In fact, OpenIoT is an open source cloud-based platform supporting components such as sensor middleware and cloud data storage.

Furthermore, as a result of the proliferation of big data, cloud computing, and sensor networks, "sensing as a service" is emerging as a promising IoT paradigm aiming at leveraging the sensed "big" data [9]. In fact, if all gathered big data is not processed, it may be useless to sense it. For example, in the smart city domain, the huge amount of video streams, environmental monitoring, surveillance, and traffic control may be vey difficult to track. If this sensed information is made available on the net, then there is almost surely someone who might exploit at least part of this information.

IoT Service Regulation

While regulation of the traditional Internet is primarily driven by service, regulation of IoT is primarily driven by trust, security, and privacy. However, there are some fears that regulation might cripple the development of IoT.

So far, a large part of the Internet community is opposing internet regulation. As a matter of fact, the *Internet Society* (internetsociety.org) works to ensure that three key aspects of the Internet are retained: *permissionless innovation*, *open access*, and *collaboration*. One of the most important arguments is that regulators may not be able to anticipate how IoT will evolve and that regulatory rules could have unintended consequences. As a matter of fact, according to Vinton Cerf, "Regulation is tricky…we're going to have to experience the problems before we understand the nature of the problems."

Besides, IoT regulation might be more beneficial for consumers than for governments. For instance, in the USA, state and federal regulators are working to restrict government and private-sector control of IoT.

On the other hand, several technology companies are promoting the virtues of self-regulation when it comes to managing consumer data [10]. They further stress the benefits of leveraging large amounts or big data to simplify daily tasks and give consumers the option to make conscious decisions. According to the Consumer Technology Association (CTA, cesweb.org) (former Consumer Electronics Association), "Big data innovation would be stifled by governmental regulation." AT&T also prefers "proactive, industry-led initiatives and best-practices guidelines" to ensure appropriate handling of sensitive consumer data.

However, without regulation, security features provided by vendors can be very poor. According to a recent technical risk assessment performed on 43 healthcare mobile applications (privacyrights.org), only 15 percent of the apps encrypted all of the transmitted data. Further, none of the apps encrypted data stored on the users' mobile device. Furthermore, most apps connect to third-party sites without the user's knowledge. Another important finding was that 72 percent of the apps were considered to be presenting medium (32 percent) to high (40 percent) risk with respect to privacy. Further, the apps that presented the lowest privacy risk were paid apps.

In fact, according to some views, specific IoT regulations may not be needed. Only issues specific to IoT and which cannot be adequately addressed by existing rules may require specific policies. For instance, the European *General Data Protection Regulation* provides a regulatory framework that may address IoT-specific privacy concerns.

According to some views, specific IoT regulations may not be needed. Only issues specific to IoT and that cannot be adequately addressed by existing rules may require specific policies. For instance, the European General Data Protection Regulation provides a regulatory framework that may address IoT-specific privacy concerns.

IoT Mainstream Standardization Activities

SDOs such as IETF, ITU-T, ETSI, ISO/IEC, and IEEE are actively working on service definitions, architectures, and security aspects. While each of these SDOs may have a particular perspective regarding IoT, a significant effort is currently being carried out to bring these perspectives closer.

IETF Standardization Activities

Back in 2006, the IETF started working on a set of IoT standards. The work originally focused on running IP over IEEE 802.15.4 devices and has since then evolved into a much larger project. The IETF draft "The Internet of Things–Concept and Problem Statement" provides an overview of IoT and its related issues.

Most of the IETF efforts focus on the network layer. Some of the most popular standards include IPv6 over Low-Power Wireless Personal Area Networks, i.e. 6LoWPAN (RFC 4919), Transmission of IPv6 Packets over IEEE 802.15.4 Networks (RFC 4944), Neighbor Discovery Optimization for 6LoWPANs (RFC 6775), Routing over Low-Power and Lossy Networks (ROLL), which primarily developed the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) (RFC 6550).

Furthermore, the IETF's "IPv6 over Networks of Resource-Constrained Nodes" (6lo) WG is currently working on how to transport IPv6 packets over various resource-constrained networks. In particular, a series of drafts are being considered to investigate the transmission of IPv6 packets over NFC, Bluetooth Low Energy (BLE), multi slave twisted pair (MS/TP), i.e. BACnet networks, and ITU-T G.9959 networks.

In addition, since the World Wide Web is a key component in the success of the current Internet, an embedded counterpart is needed, yielding the Web of Things (WoT). The IETF Constrained RESTful Environments (CoRE, RFC 6690) WG is currently working on how to allow the integration of constrained devices with the Internet at the service level. In particular, the Constrained Application Protocol (CoAP, RFC 7252) is a Web transfer protocol intended for constrained and lossy networks.

With regard to TSP, the IETF has recently created two new WGs: DTLS in Constrained Environments (DICE), and Authentication and Authorization for Constrained Environments (ACE). A large number of other IETF RFCs and drafts dealing with IoT can be found at www.ietf.org.

ITU-T Standardization Activities

While the ITU-T has been primarily working on switched, connection oriented networks, its involvement in the Internet, primarily through the Next Generation Network (NGN) framework, assures a converged approach in developing IoT architectures. Note that collaboration between ITU-T and IETF is not new; back in 1998, RFC 2436 set the scope of this collaboration.

In 2005, the ITU-T published a report on IoT as one of the ITU-T Internet report series. It covers topics including "enabling technologies, business opportunities, public policy challenges, and implications for the developing world." The ITU-T's IoT Global Standards Initiative (IoT-GSI) is intended to promote a unified approach and develop recommendations "enabling IoT on a global scale" and to "act as an umbrella for IoT standards activities worldwide" (www.itu.int/en/ITU-T/gsi). This will in turn give service providers the means to offer a large variety IoT services. ITU-T also created the Joint Coordination Activity on Internet of Things (JCA-IoT) to coordinate ITU-T's work on IoT, including network aspects of Identification of Things and ubiquitous sensor networks (USN).

In 2012, ITU-T Study Group 13 (SG 13) approved a set of recommendations that define IoT, characterize its emerging environment, and outline the "functional requirements of machine-oriented communication applications in an NGN context." Among these recommendations, Y.2060 defines IoT as "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies." An overview and a detailed description of an IoT *Reference Model* are also provided in rec. Y.2060.

On the other hand, ITU-T SG 15 is actively working on communication aspects related to smart grids. Recommendations of particular importance include G.9903 and G.9905, which normatively reference 6loWPAN and its header compression mechanisms. In fact, Rec. G.9903 adopted the IEEE 802.15.4 and the IETF 6LoWPAN MAC and adaptation layers, respectively.

Finally, the ITU-T SG17 is working on cyber security and identity management for IoT and related environments, including cloud computing, smart grids, web services, etc. Among the recommendations approved by SG17, Rec. X.1205 provides an overview of cyber security. A list of selected IoT-related ITU-T recommendations is given in Table 1.

ISO/IEC Standardization Activities

The ISO/IEC (www.iec.ch) Special Working Group 5 (SWG 5) of the ISO/IEC Joint Technical Committee 1 (JTC 1) was established in 2012 as a result of a growing interest in the field of IoT by other SDOs. JTC 1 has tight relationships with ITU-T SG-17 on various security aspects. The relationship is at various levels including *joint work* (level 1), *technical collaboration by liaison mechanism* (level 2), and *information liaison* (level 3).

ISO/IEC JTC 1/SWG 5 does not actually develop standards, but rather consolidates standardization activities and identifies current and future IoT trends and needs. A number of documents were issued by the SWG, including a collection of definitions and a mind map describing technologies related to IoT, as well as application domains, requirements, and stakeholders. A list of definitions collected from various standards organizations is divided into four categories: IoT, M2M, machine type communications (MTC), and cyber-physical systems (CPS).

The ISO/IEC NP 19654 standard introduces a reference architecture (RA) as a "generalized system-level architecture of IoT systems that share common domains." The IoT RA also provides rules, guidance, and policies for building a specific IoT system architecture. IoT RA also aims to help develop interoperable IoT systems that interact seamlessly. The IoT RA includes three key enabling technology areas:

1) IoT system of interest.
2) Communications technology.
3) Information technology.

An IoT system of interest includes smart health care, agriculture, environment, grid, building, transportation, city, etc. The IoT RA standard also describes a conceptual model where seven IoT domains are defined:

1) *IoT System:* System that is to be developed, implemented, and operated. This domain includes descriptions of target applications and services of the IoT system. These include health care, grid, home, etc.

Reference	Title	Status (year)
Y.2060	Overview of the Internet of Things	In force (2012)
Y.2061	Requirements for support of machine-oriented communication applications in the NGN environment	In force (2012)
Y.2062	Framework of object-to-object communication for ubiquitous networking in next generation networks	In force (2012)
Y.2063	Framework of the web of things	In force (2012)
Y.2064	Energy saving using smart objects in home networks	In force (2014)
Y.2065	Service and capability requirements for e-health monitoring services	In force (2014)
Y.2066	Common requirements of the Internet of Things	In force (2014)
Y.2067	Common requirements and capabilities of a gateway for Internet of Things applications	In force (2014)
Y.2068	Functional framework and capabilities of the Internet of Things	In force (2015)
Y.2069	Terms and definitions of the Internet of Things	In force (2012)
Y.2070	Requirements and architecture of home energy management systems and home network services	In force (2015)
Y.2074	Requirements for Internet of Things devices and operation of Internet of Things applications during disaster	In force (2015)
Y.2213	NGN service requirements and capabilities for network aspects of applications and services using tag-based identification	In force (2008)
F.771	Service description and requirements for multimedia information access triggered by tag-based identification	In force (2008)
G.9903	Narrow-band OFDM power line communication transceivers for G3-PLC networks	In force (2014)
G.9905	Centralized metric based source routing	In force (2013)
H.621	Architecture of a system for multimedia information access triggered by tag-based identification	In force (2008)
X.1601	Security framework for cloud computing	In force (2014)
X.1205	Overview of cyber security	In force (2008)
X.1311 (Common with ISO/IEC 29180:2012)	Information technology – security framework for ubiquitous sensor networks	In force (2014)
X.1312	Ubiquitous sensor network middleware security guidelines	In force (2011)
X.1313	Security requirements for wireless sensor network routing	In force (2012)
X.1314	Security requirements and framework of ubiquitous networking	In force (2014)
X.1171	Threats and requirements for protection of personally identifiable information in applications using tag-based identification	In force (2009)
X.672	Object identifier resolution system (ORS)	In force (2010)
X.660	General procedures and top arcs of the international object identifier tree	In force (2011)

Table 1. ITU-T recommendations related to IoT.

2) *Sensing Devices:* Domain representing all physical entities such as sensors, tag readers, etc.
3) *Things/Objects:* Physical (things) and virtual (objects) domain that includes entities that are part of the IoT system domain that do not have sensors. These include displays, alarms, smartphones, etc.
4) *Control/Operations:* Domain representing organizations that manage the system activities of an IoT system.
5) *Service Providers:* Domain representing organizations providing IoT services.
6) *Customers:* Domain representing the end user of goods (both tangible and intangible) and services provided by the organizations in the *service providers* domain or by the IoT system in IoT *systems of interest*.
7) *Markets:* Domain representing operators and participants in the IoT system and service provider markets.

Various ISO/IEC standards related to IoT have been published or are under development. The ISO/IEC 30101 standard addresses sensor networks supporting smart grid systems, while ISO/IEC NP 19637 and ISO/IEC NP 18765 deal with testing and identification aspects, respectively.

Further, through an industry led association, KNX emerged as a standard based on ISO/IEC 14543. KNX combines three previous industry standards: the European Home Systems (EHS) Protocol, BatiBUS, and the European Installation Bus (EIB). KNX supports various physical media including twisted pair (TP), power line communications (PLC), radio, infrared, and Ethernet. This latter is referred to as KNXnet/IP and provides different mechanisms to encapsulate KNX messages into IP packets. There are also options to use IP directly as a native KNX medium.

Furthermore, the LonMark control system utilizes the ISO/IEC14908-1 and related standards. The ISO/IEC 14908-1 describes protocol stacks and services provided by layers 2 to 7. LonMark specifies a communication protocol for local area control networks providing peer-to-peer communication, and is suitable for implementing both peer-to-peer and master-slave control.

Also, DASH7 is an emerging active-RFID technology allowing tag to tag communications based on ISO/IEC 18000-7. This technology is gaining wide acceptance as it provides an open source platform, a bit rate of 200 Kbit/s, up to 2 Km of transmission range (at low bit rates), location accuracy of about one meter, low energy consumption, and a powerful security suite. In particular, DASH7 was adopted by the US Department of Defense and NATO. Table 2 gives a list of selected ISO/IEC IoT standards.

Reference	Title	Status (Year)
ISO/IEC NP 19654	Internet of Things reference architecture (IoT RA)	Under development (2014)
ISO/IEC NP 19637	Sensor network testing framework	Under development (2014)
ISO/IEC NP 18765	Uniform identification scheme for sensor network managed object	Under development (2014)
ISO/IEC 30101	Sensor network and its interfaces for smart grid system	Published (2014)
ISO/IEC 14543	Information technology – home electronic systems (HES) – Part 3-10: wireless short-packet (WSP) protocol optimized for energy harvesting – architecture and lower layer protocols	Published (2012)
ISO/IEC 14908-1	Information technology – control network protocol — part 1: protocol stack	Published (2012)
ISO/IEC 24767	Information technology – home network security	Published (2008)
ISO/IEC 29180	Information technology – telecommunications and information exchange between systems – security framework for ubiquitous sensor networks	Published (2012)
ISO/IEC 15961-1	Information technology – radio frequency identification (RFID) for item management: data protocol – part 1: application interface	Published (2013)
ISO/IEC 15962	Information technology – radio frequency identification (RFID) for item management — data protocol: data encoding rules and logical memory functions	Published (2013)
ISO/IEC 15963	Information technology – radio frequency identification for item management – unique identification for RF tag	Published (2009)
ISO/IEC 18000-x	Information technology – radio frequency identification for item management – part x	Published
ISO/IEC 24791-x	Information technology – radio frequency identification (RFID) for item management – software system infrastructure – part x	Published

Table 2. ISO/IEC specifications related to IoT.

IEEE Standardization Activities

The IEEE created an IoT Web portal (iot.ieee.org) that provides news, events, and publications regarding IoT. Further, the IEEE P2413 standard defines an architectural framework for IoT, including "descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains." As of December 2015, the P2413 WG includes 25 member companies.

For a unified IoT architectural framework, IEEE intends to interact with ongoing standardization activities in order to cover the various applications, their requirements, and specific IoT functionalities in the framework in order to ensure that the framework can be referenced by these standardization activities. IEEE also intends to establish liaison with other standards groups and organizations. An initial liaison group will include IEEE 802.24, IEC SG 8, and oneM2M (see below).

To accelerate the development process, IEEE P2413 has put in place a number of *working* and *ad hoc* groups. These include the "Scope and Applicability," the "Standardization Landscape," and the "Networking" working groups; and the "oneM2M review" ad hoc group. The work is expected to be completed in 2016.

One of the main goals of the IEEE standards is to reduce fragmentation in the various IoT verticals. For instance, the flagship 802.15.4 standard has become a de facto MAC and PHY layer protocol for various IoT technologies.

The IEEE 802.15 WG is also actively working on other IoT standards: Part 15.5 dealing with *Mesh Topology Capability in WPAN*; Part 15.6 dealing with MAC and Physical Layer Specifications for WPANs used in or around a body; and Part 15.7 dealing with *Short-Range Wireless Optical Communication Using Visible Light*.

Moreover, IEEE 802.15.4e Time Slotted Channel Hopping (TSCH) recently amended the MAC layer of the IEEE 802.15.4 standard for industrial automation and process control networks. TSCH evolved directly from WirelessHART and ISA100.11a. To further consolidate standardization efforts, the IETF's 6TiSCH WG is currently working on IPv6 over TSCH in order to facilitate the adoption of IPv6 in industrial environments.

ETSI Standardization Activities

ETSI (www.etsi.org) has just introduced the low throughput network (LTN) as a WAN, bidirectional wireless networking technology. Key different features compared to common WSNs include long-range transmission (up to 40 km in line of site) and communication with buried underground equipment.

There are three new ETSI group specifications (GS) related to LTN: GS LTN 001, GS LTN 002, and GS LTN 003, dealing with, respectively, use cases, LTN functional architecture, and definitions of protocols and interfaces. The functional architecture makes use of an IP-based transport network such as 3rd Generation Partnership Project (3GPP), Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN), and 3GPP2.

ETSI also published a set of technical specifications (TS) covering service requirements, the *M2M functional architecture*, and CoAP interoperability. Table 3 gives a list of selected ETSI group and technical specifications, as well as technical reports (TR) related to IoT. Note that current ETSI M2M standardization activities are primarily done under the oneM2M umbrella (see below).

Reference	Title	Status (Year)
GS LTN 001	Low throughput networks (LTN); use cases for low throughput networks	Published (2014)
GS LTN 002	Low throughput networks (LTN); functional architecture	Published (2014)
GS LTN 003	Low throughput networks (LTN); protocols and interfaces	Published (2014)
TS 102 689	Machine-to-machine communications (M2M); M2M service requirements	Published (2013)
TS 103 104	Machine-to-machine communications (M2M); interoperability test specification for CoAP binding of ETSI M2M primitives	Published (2013)
TS 102 690	Machine-to-machine communications (M2M); functional architecture	Final draft for proposal (2014)
TR 102 966	Machine-to-machine communications (M2M); interworking between the M2M architecture and M2M area network technologies	Published (2014)
TR 102 935	Machine-to-machine communications (M2M); applicability of M2M architecture to smart grid networks; impact of smart grids on M2M platform	Published (2012)
TR 102 898	Machine to machine communications (M2M); use cases of automotive applications in M2M capable networks	Published (2013)
TR 102 857	Machine-to-machine communications (M2M); use cases of M2M applications for connected consumer	Published (2013)
TR 102 732	Machine-to-machine communications (M2M); use cases of M2M applications for eHealth	Published (2013)
TR 102 725	Definitions	Published (2013)
TR 101 584	Machine-to-machine communications (M2M); study on semantic support for M2M data	Published (2013)
TR 102 449	Telecommunications and internet converged services and protocols for advanced networking (TISPAN); overview of radio frequency identification (RFID) tags in the telecommunications industry	Published (2006)
TR 102 644	Electromagnetic compatibility and radio spectrum matters (ERM); RFID plugtests to investigate the interoperability of tags manufactured by different vendors;	Published (2009)

Table 3. ETSI specifications related to IoT.

oneM2M Standardization Activities

In 2012, the oneM2M standardization body emerged as a unified effort of SDOs: ETSI from Europe, ATIS (Alliance for Telecommunications Industry Solutions) and TIA (Telecommunications Industry Association) from the US, CCSA (China Communications Standards Association), TTA (Telecommunications Technology Association of Korea), and ARIB (Association of Radio Industries and Businesses) and TTC (Telecommunication Technology Committee) from Japan. TSDSI (Telecommunications Standards Development Society, India) also joined oneM2M in May 2015.

As of December 2015, 224 companies and six universities had joined oneM2M. The goal is to develop common specifications for "M2M services that have been vertically integrated" so far and to propose a "common M2M service layer that can be embedded in various hardware and software." Table 4 gives a list of oneM2M technical reports and technical specifications (TS) related to IoT. Note that oneM2M TS are common with ETSI, ATIS, TTA, and TTC.

3GPP Standardization Activities

Cellular technologies are being adapted to meet IoT requirements. In particular, LTE Release-12 (Rel-12) of the 3GPP (www.3gpp.org) introduces a power save mode and simplified signalling procedures to provide additional battery savings. Rel-12 also allows LTE modems to be significantly less complex and cheaper than current modems. Further, 3GPP has identified ways to increase the coverage of LTE, making it possible to communicate with objects in difficult to reach locations.

LTE Rel. 12 is paving the way toward 5G, and may constitute a major step toward ubiquitous access to IoT and M2M services. The advent of LTE enabled IoT devices may constitute a key milestone in the development of IoT *mobility* and *long reach* features.

Reference	Title	Status (Year)
TR0001	oneM2M use cases collection	Published (2013)
TR0002	Architecture analysis – part 1: analysis of architectures proposed for consideration by oneM2M	Published (2013)
TR0003	Architecture analysis – part 2: study for the merging of architectures proposed for consideration by oneM2M	Published (2013)
TR0006	Study of management capability enablement technologies for consideration by oneM2M	Published (2013)
TR0008 (ETSI TR118508)	Analysis of security solutions for the oneM2M system	Published (2014)
TR0009	Protocol analysis	Published (2014)
TS 0001 (ETSI TS 118 101)	Functional architecture	Published (2015)
TS 0002 (ETSI TS 118 102)	Requirements	Published (2015)
TS 0003 (ETSI TS 118 103)	Security solutions	Published (2015)
TS 0004 (ETSI TS 118 104)	Service layer core protocol specification	Published (2015)
TS 0005 (ETSI TS 118 105)	Management enablement (OMA)	Published (2015)
TS 0006 (ETSI TS 118106)	Management enablement (BBF)	Published (2015)
TS 0008 (ETSI TS 118 108)	CoAP protocol binding	Published (2015)
TS 0009 (ETSI TS 118 109)	HTTP protocol binding	Published (2015)
TS 0010 (ETSI TS 118110)	MQTT protocol binding	Published (2015)
TS 0011 (ETSI TS 118 111)	Common terminology	Published (2015)

Table 4. oneM2M technical reports and specifications related to IoT.

Independent and State-Funded Projects

While the mainstream SDOs are actively working on IoT service definitions and architectures, many independent and state-funded projects are being carried out to support and promote IoT worldwide, ranging from alliances (ipso-alliance.org, allseenalliance.org), architectures (iot-a.eu), consortiums (iofthings.org, industrialinternetconsortium.org, openinterconnect.org), forums (iot-forum.eu, wireless-iot.org), groups (threadgroup.org), initiatives (iot-i.eu, homegatewayinitiative.org), projects (iot6.eu, probe-it.eu, openiot.eu, ict-iotest.eu, iot-at- work.eu, iot-icore.eu), research clusters (internet-of-things-research.eu), and the list goes on! Despite the crowd, “newcomers” keep stepping in, such as the Wireless IoT Forum recently.

Among the state-funded projects, the European Internet of Things Architecture (IoT-A) seems to be standing out from the crowd and gaining reasonable acceptance. On the other hand, with more than 100 stakeholders, the Industrial Internet Consortium (IIC) and the AllSeen Alliance may stand out from the crowd as industry-led activities. IIC works on an architectural framework for the Industrial Internet and plays a key role in the development of IoT. The other IoT “activities” are summarized in Table 5.

Conclusion: Connecting the Dots

The goal of a standard is typically to unify interfaces, protocols, and services so that various systems can be interconnected. After this overview of IoT standards, a legitimate question is: Do we have a common and clear understanding of a standard IoT service? The answer is quite mitigated. In fact, to some extent, the overwhelming number of standards might have contributed in further exacerbating the ambiguity about service and may deepen the interoperability issues. In fact, most of these standards limit their scope to specific domains (M2M, WSN, RFID, etc.) and stakeholders yielding isolated and/or redundant solutions.

We believe that SDOs should further unify their efforts around IETF’s streamlined protocols, namely IP and its variants, i.e. primarily 6LoWPAN in the network layer and CoAP in the application layer; and on the IEEE 802.x.y standard (primarily 802.15.4) in the MAC and PHY layers, be it for M2M, WSN/USN, or tag communications. All smart home/grid/city/transportation services may use these streamlined standard protocols. As further emphasized in an IETF liaison statement “lessons learned about cooperation between SDOs” (http://datatracker.ietf.org/liaison/549/), “SDOs should minimize potential duplicate work, and minimize this via collaboration, not competition.”

As a matter of fact, ETSI and the Internet Protocol for Smart Objects (IPSO) alliance organized a successful CoAP “Plugtest” interoperability in March 2012. Also, in July 2013, a 6LoWPAN Plugtests event gave vendors the opportunity to assess the level of interoperability of their products and verify the correct interpretation of IETF based specifications. The tests were carried out using the 2006-2.4 GHz release of the IEEE 802.15.4 PHY/MAC standard. While almost all implementations have exhibited a great level of basic compatibility, i.e. data was sent and interpreted correctly, compliance with RFC 6775 (6LoWPAN-ND) was very low.

The IETF is also actively working on consolidating standardization efforts of various bodies. The 6Lo WG is currently working on how to transport IPv6 packets over NFC, BLE, MS/TP, and ITU-T G.9959 networks. On the other hand, the 6TiSCH WG is working on IPv6 over IEEE 802.15.4e TSCH in order to accelerate the adoption of IPv6 in industrial environments.

As another collaboration initiative, the Global Standards Collaboration (GSC) encompasses 11 SDOs including ARIB, ATIS, CCSA, ETSI, IEEE-SA, ITU-T/-R, TIA, TSDSI TTA, and TTC. So far, the IETF, a key player in IoT development, is not a GSC member, while ISO and IEC are expected to join during the 20th meeting in India, in 2016. One of the main goals of GSC is to harmonize standards to guarantee compatibility of communication equipment. In July 2014, the 18th meeting of the GSC was hosted by ETSI where IoT, critical communications (CC), big data, M2M, and software defined networking (SDN) and their applications in various domains, primarily in emergency communication systems, were discussed. Note that ISO/IEC JTC 1 was among the guests during that meeting. In July

2015, the 19th meeting of the GSC was hosted by ITU and also focused on IoT, CC, and 5G. The various SDOs agreed to further increase collaboration and leverage existing efforts such as oneM2M.

Finally, policymakers may not impose unnecessary regulatory rules on IoT and should identify carefully what information actually requires protection. In order to instill consumer confidence in IoT without slowing its growth, awareness, good practice, and voluntary codes of conduct that stop short of regulation may constitute more viable options.

References

[1] Y.-K. Chen, "Challenges and Opportunities of Internet of Things," 17th ACM/EDAC/IEEE Design Automation Conference, 2012, pp. 383-388.

[2] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Trans. Industrial Informatics*, vol. 10, no. 4, 2014, pp. 2233-2243.

[3] J. Hoebeke *et al.*, "Leveraging Upon Standards to Build the Internet of Things," *19th IEEE Symp. Commun. and Vehicular Tech. in the Benelux*, Nov. 2012, pp. 1–6.

[4] V. Gupta and Jayaraghavendran, "IoT Protocols War and the Way Forward," *28th Int'l. Conf. VLSI Design*, Invited Talk, 2015, pp. 28–28.

[5] A. Al-Fuqaha *et al.*, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2347–76.

[6] D. Uckelmann, M. Harrison, and F. Michahelles, "An Architectural Approach towards the Future Internet of Things," Book Chapter, Springer Berlin Heidelberg, 2011, ISBN 978-3-642-19156-5, pp. 1–24.

[7] M. Presser *et al.*, "The SENSEI Project: Integrating the Physical World with the Digital World of the Network of the Future," *IEEE Commun. Mag.*, vol. 47, no. 4, Apr. 2009, pp. 1–4.

[8] M. Compton *et al.*, "The SSN Ontology of the Semantic Sensor Networks Incubator Group," *J. Web Semantics, Science, Services and Agents on the World Wide Web*, Elsevier, vol. 17, 2012, pp. 25–32.

[9] D. Tracey and C. Sreenan, "A Holistic Architecture for the Internet of Things, Sensing Services and Big Data," *13th IEEE/ACM Int'l. Symp. Cluster, Cloud, and Grid Computing*, 2013, pp. 546–53.

[10] I. Lovrek, A. Caric, and D. Lucic, "Future Network and Future Internet: A Survey of Regulatory Perspective," *22nd Int'l. Conf. Software, Telecommunications, and Computer Networks (SoftCOM)*, 2014, pp. 186–91.

Biography

Aref Meddeb (Aref.Meddeb@infcom.rnu.tn) obtained his engineer's degree from ENIT, Tunisia, in 1992, and both his M.S. and Ph.D. degrees from Ecole Polytechnique, Montreal, Canada, in 1995 and 1998, respectively. From 1993 to 2002 he worked with Alcatel, INRS-Telecom, Teleglobe, and Nortel. He is currently a full professor at the National School of Engineering, University of Sousse. His research interests include Internet of Things, wireless sensor networks, and RFID systems, with a focus on security, QoS, routing, and design.

Name	Number of partners/ members (Jan. 2015)	Year	Link
IOT-A	• 13 companies • 4 universities	2010	http://www.iot-a.eu
IPSO Alliance	• 39 companies • 2 universities	2008	http://www.ipso-alliance.org
AllSeen Alliance	• 106 companies • 3 universities	2014	https://allseenalliance.org
Internet of Things Consortium	• 48 companies	2014	http://iofthings.org
Industrial Internet Consortium	• 127 companies • 7 universities • 3 institutes • 2 foundations • 2 associations	2014	http://www.iiconsortium.org
Open Interconnect Consortium	• 49 companies	2014	http://openinterconnect.org
Internet of Things International Forum (IoTForum)	• 9 companies • 3 universities • 4 institutes • 4 organizations	2013	http://iotforum.org/
Wireless IoT Forum	• 6 companies	2015	http://www.wireless-iot.org/
Thread Group	• 46 companies	2014	http://threadgroup.org/
The Internet of Things Initiative	• 11 companies • 5 universities • 1 institute	2009-2012	http://www.iot-i.eu/
Home Gateway Initiative (HIG)	• 47 companies	2004	http://www.homegatewayinitiative.org/
IoT6 Project	• 3 companies • 6 universities	2011–2014	http://iot6.eu/
Pursuing ROadmaps and BEnchmarks for the Internet of Things (PROBE-IT)	• 1 company • 3 universities • 6 R&D institutions	2012–2014	http://www.probe-it.eu/
Open Source cloud solution for the Internet of Things (OpenIoT)	• 4 universities • 3 companies • 1 research center	2012–2014	http://www.openiot.eu/
Internet of Things Environment for Service Creation and Testing (IoT.est)	• 2 universities • 5 companies	2011–2014	http://ict-iotest.eu
Internet of Things at Work (IoT@Work)	• 5 companies • 1 university	2010–2013	https://www.iot-at-work.eu/
iCore	• 12 companies • 5 research centers • 4 universities	2011–2014	http://www.iot-icore.eu/
European Research Cluster on the Internet of Things	• 38 companies	2009–2015	http://www.internet-of-things-research.eu

Table 5. IoT independent activities.