Standardized Protocol Stack for the Internet of (Important) Things

Maria Rita Palattella, *Member, IEEE,* Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, *Member, IEEE,* Luigi Alfredo Grieco, *Senior Member, IEEE,* Gennaro Boggia, *Senior Member, IEEE,* and Mischa Dohler, *Senior Member, IEEE*

***Abstract*—We have witnessed the Fixed Internet emerging with virtually every computer being connected today; we are currently witnessing the emergence of the Mobile Internet with the exponential explosion of smart phones, tablets and net-books. However, both will be dwarfed by the anticipated emergence of the Internet of Things (IoT), in which everyday objects are able to connect to the Internet, tweet or be queried. Whilst the impact onto economies and societies around the world is undisputed, the technologies facilitating such a ubiquitous connectivity have struggled so far and only recently commenced to take shape.**

To this end, this paper introduces in a timely manner and for the first time the wireless communications stack the industry believes to meet the important criteria of power-efficiency, reliability and Internet connectivity. Industrial applications have been the early adopters of this stack, which has become the de-facto standard, thereby bootstrapping early IoT developments with already thousands of wireless nodes deployed.

Corroborated throughout this paper and by emerging industry alliances, we believe that a standardized approach, using latest developments in the IEEE 802.15.4 and IETF working groups, is the only way forward. We introduce and relate key embodiments of the power-efficient IEEE 802.15.4-2006 PHY layer, the power-saving and reliable IEEE 802.15.4e MAC layer, the IETF 6LoWPAN adaptation layer enabling universal Internet connectivity, the IETF ROLL routing protocol enabling availability, and finally the IETF CoAP enabling seamless transport and support of Internet applications.

The protocol stack proposed in the present work converges towards the standardized notations of the ISO/OSI and TCP/IP stacks. What thus seemed impossible some years back, i.e., building a clearly defined, standards-compliant and Internet-compliant stack given the extreme restrictions of IoT networks, is commencing to become reality.

***Index Terms*—Internet of Things, 802.15.4, 802.15.4e, CoAP, RPL, Standards, IPv6, Protocol Stack.**

I. Introduction

IN EARLY 2000's, Kevin Ashton from the MIT Auto-ID Center [1] proposed the term "Internet of Things", making reference to the binding of Radio Frequency Identifiers (RFID) information to the Internet. Soon, the interest for an Internet of connected objects raised the attention of governments and leading IT companies that recognized the concept as one of their key axes for future economic growth and sustainability. The concept of Internet of Things was adopted by the European Union in the Commission Communication on RFID, published in March 2007 [2].

The Council's conclusions of November 2008 on Future Networks and the Internet, recognized that *"the Internet of Things is poised to develop and to give rise to important possibilities for developing new services but that it also represents risks in terms of the protection of individual privacy"* [3]. In 2008, the U.S. National Intelligence Council (NIC) reported that *"By 2025 Internet nodes may reside in everyday things, food packages, furniture, paper documents, and more. Today's developments point to future opportunities and risks that will arise when people can remotely control, locate, and monitor even the most mundane devices and articles. Popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development and military capability"* [4].

Although the IoT is a widely used term, its definition is still fuzzy due to the large amount of concepts it includes, and the ambiguity and opposed meanings of the two terms that compose the name "Internet of Things" [5]. Several definitions overlap in the literature, for example, in [6] the IoT stands for a *"world-wide network of interconnected objects uniquely addressable, based on standard communication protocols"*. Whilst Atzori et al. [7] consider IoT as much more than uniquely addressable objects, it envisages the existence of services that may interface Things having identities and virtual personalities operating in smart spaces and using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Further conceptual designs, visions and application spaces of the IoT are exposed in [8]–[14], all of which converge to the view that simple embedded sensor networking is now evolving to the much needed standards and Internet enabled communication infrastructure between objects.

Structurally, the IoT requires software architectures that are able to deal with a large amounts of information, queries, and computation, making use of new data processing paradigms, stream processing, filtering, aggregation and data mining, all of this sustained by communication standards such as HyperText Transfer Protocol (HTTP) [15] and Internet Protocol

Manuscript received 12 October 2011; revised 2 April 2012 and 8 October 2012.

M. R. Palattella is with the SnT, University of Luxembourg, Luxembourg (e-mail: maria-rita.palattella@uni.lu).

X. Vilajosana is with the Universitat Oberta de Catalunya, Barcelona, Spain and the BSAC, University of California, Berkeley (e-mail: xvilajosana@uoc.edu; xvilajosana@eecs.berkeley.edu).

T. Watteyne is with the BSAC, University of California, Berkeley, and the Dust Networks/Linear Technology (e-mail: watteyne@eecs.berkeley.edu; twatteyne@linear.com).

N. Accettura, L. A. Grieco, and G. Boggia are with the "Dip. di Elettrotecnica ed Elettronica", Politecnico di Bari, v. Orabona 4, 7015, Bari, Italy (e-mail: n.accettura@poliba.it; a.grieco@poliba.it; g.boggia@poliba.it).

M. Dohler is with the Centre Tecnologic de Telecomunicacions de Catalunya (CTTC), Spain (e-mail: mischa.dohler@cttc.es).

Digital Object Identifier 10.1109/SURV.2012.111412.00158

(IP) [16]. In contrast, due to the nature of IoT objects, very low power consumptions are required so any object can plug into the Internet while being powered by batteries or through energy-harvesting. Energy is wasted by transmission of unneeded data, protocol overhead, and non-optimized communication patterns; these need to be taken into account when plugging objects into the Internet. Existing Internet protocols such as HTTP and Transmission Control Protocol (TCP) [17] are not optimized for very low-power communication, due to both verbose meta-data and headers, and the requirements for reliability through packet acknowledgement at higher layers, which hinders the adaptation of existing protocols to run over that type of networks.

The objects conforming to the IoT have a wide range of connotations and understandings, including RFID [5], Wireless Sensor Networks (WSNs), Machine-to-Machine (M2M) [18], [19], among others. However, in the actual sense of its name, the IoT pertains to the ability to interconnect as well as Internet-connect objects, things, machines, etc. There are three core requirements related to this ability:

- **A Low Power Communication Stack.** The majority of objects are not able to draw power from the mains, and have batteries at best. This means that finding enough energy to power processing and communication is a major challenge. Whilst we are ready to recharge our mobile phones on a daily basis, changing batteries in millions of objects is impractical, at best. Any stack must therefore exhibit a low average power consumption. Indeed, the stack discussed in this paper obeys precisely this requirement.
- **A Highly Reliable Communication Stack.** Although the Internet is a best-effort transport medium, protocols incorporate error detection, retransmissions and flow control. These techniques are applied at various protocol layers concurrently, which leads to a reliable end-to-end experience, albeit in a rather inefficient way. For the IoT to merge seamlessly into the Internet, it needs to offer the same reliability we are used to on the Internet – with the additional requirement that said reliability is achieved at highest possible efficiency.
- **An Internet-Enabled Communication Stack.** Enabling another dialect of the Internet has profound implications on the protocol design. The Internet is exhibiting emergent behavior today because communication is bi-directional; it is hence of utmost importance to ensure that communication from objects but also towards objects is facilitated. Furthermore, the explosion of the Internet can arguably be attributed to the ability of any machine around the world to talk to any other machine, all this facilitated by one universal language, IP; it is hence of paramount importance that the IoT is IP enabled [13]. **This in turn calls for standardized communication approaches, which is core to the exposition in this paper.**

Identifying the requirement above has taken some time, as shown in Table I. Early conceptual designs can be traced back to the emergence of the Distributed Sensor Networks program [21] at the MIT Lincoln Labs [22]. It aimed at developing and extending target surveillance and tracking technology in systems that employ multiple spatially distributed sensors and processing resources. The WSN field really took off with the concept of "Smart Dust" and the eponymous DARPA project [23], [24], lead by Prof. Kristofer S.J.Pister from the University of California, Berkeley. In the following years, the concept of a ubiquitous WSN has not only been demonstrated but also awaken commercial interest. A variety of pioneering companies emerged, including Dust Networks, Ember, Millennial, Sensicast, Moteiv and Arch Rock. All of these companies had in one form or another their proprietary hardware and communication stack. It was quickly recognized, however, that having a multitude of proprietary systems connected to the Internet does impede the much hoped-for scalability and explosion of the IoT.

TABLE I
EVENTS WHICH HAVE HELPED SHAPING THE WORLD OF THE IOT.

Year	Event
1967	REMBASS Remotely Monitored Battlefield Sensor System
1978	Distributed Sensor Networks for Aircraft Detection Lincoln Labs - Lacoss
1992	RAND Workshop - Future Technology Driven Revolutions in Military Conflict. Concepts behind Smart Dust emerge.
1993- 1996	DARPA ISAT studies - many WSN ideas and applications discussed. Deborah Estrin leads one of the studies.
1994	LWIM - Low Power Wireless Integrated Microsensors - Bill Kaiser (UCLA)
1997	Smart Dust proposal written, Kris Pister (Berkeley)
1998	Seth Hollar makes wireless mouse collars
1999	Endeavour project proposed by Randy Katz, David Culler (Berkeley) PicoRadio project started by Jan Rabaey (Berkeley)
2000	Crossbow begins selling 'Berkeley motes'
2001	Multiple demos proving viability
2002	Dust, Ember, Millennial, Sensicast founded
2003	IEEE802.15.4-2003 standard Moteiv (now Sentilla) founded
2004	ZigBee 1.0 standard ratified TSMP 1.1 shipping
2005	Arch Rock founded
2006	ZigBee 2006 standard ratified IEEE802.15.4-2006 standard
2007	WirelessHART standard ratified IETF 6LoWPAN's RFC4944 published WirelessHART shown to achieve 99.999% reliability [20]
2008- 2009	IETF workgroup Routing Over Low-power Lossy links (ROLL) created. IEEE802.15.4e work group created
2010- 2011	IEEE802.15.4e's MAC protocol ratified IEFT 6LoWPAN's RFC4944 updated IETF ROLL's RPL routing protocol ratified

Starting in 2003, various IEEE and IETF standardization bodies started putting together a framework to the communication protocols of the emerging systems.

The standard with the longest-standing impact is IEEE802.15.4 [25], which defines a low-power Physical (PHY) layer, and upon which most IoT technologies have built. It also defines a Medium Access Control (MAC), which has been the foundation of ZigBee 1.0 and ZigBee 2006 [26]. It became soon clear that the single-channel nature of this MAC protocol caused its reliability to be unpredictable, especially in multi-hop settings. An alternative which uses channel-hopping to combat multipath fading and external interference was developed and commercialize by Dust Networks [27]. This protocol, called Time Synchronized

Mesh Protocol (TSMP) [28], became the de-facto standard for reliable low-power wireless in industrial application. Time synchronized channel hopping, the foundation of TSMP, became the foundation of the WirelessHART standard [29]. In 2011, time synchronized channel hopping was integrated into the IEEE802.15.4 standard through the IEEE802.15.4e working group, and will thus become a MAC protocol in the next revision of the IEEE802.15.4 standard. Various IETF WGs, notably 6LoWPAN [30] as a convergence layer, ROLL RPL [31] as a routing protocol, and CoAP [32] facilitate the integration of low-power wireless networks into the Internet. These layers and their tight interaction are hence seen as instrumental in making the IoT happen from a technology point of view, and are thus surveyed and described in great details in subsequent sections.

Low-power, reliable, wireless multihop networks have been a reality for years. For example, Emerson, a process management giant[1], indicates to have deployed over 9200 networks on all continents, clocking over 987 million hours of operating hours. These network run time synchronized channel hopping. Different technology providers target different application spaces, ranging from the steel industry [33], to refineries [34], [35], chemical plants [36], maritime ports [37], industrial applications [38] and remote monitoring [39]. Time synchronized channel hopping is an existing and proven technology; this paper discusses how it is being applied to the Internet of Things.

The core contributions of this paper can thus be summarized as follows:

- For the first time, a detailed survey on the new IEEE802.15.4e MAC and IETF ROLL RPL routing standards is provided; indeed, these standards have been discussed in various sources at different technical depths but such a detailed exposure with explanations is unprecedented.
- The introduction of a clear vision on a workable communication stack for the IoT using proven standards and the accumulated expertise of the authors, is also unprecedented.
- Finally, this paper shun away from using high-level approaches to defining the IoT but rather introduced concrete protocols as well as the reasoning why they will succeed and last.

To this end, Section II introduces the IEEE802.15.4-2006 PHY, along with the main features of low-power radio hardware suitable for the IoT protocol stack. Section III then details the IEEE802.15.4e Time Synchronized Channel Hopping (TSCH) MAC protocol, showing how it is able to provide both high reliability and energy-efficiency. IETF 6LoWPAN (IPv6 addressing) and IETF ROLL RPL (routing) are covered in Section IV and Section V, respectively. We then discuss the novelty introduced by the CoAP protocol at the application layer in Section VI. Section VII finally concludes this article and presents possible paths for future research.

[1]http://www.emerson.com/

II. Low-Power PHY Layer – IEEE 802.15.4-2006

This section underlines the importance of a low-power physical (PHY) layer which, together with an energy-efficient MAC layer, enables lower power connectivity among smart objects in the future IoT.

A. Low-Power Radio Hardware

A radio translates bytes of digital information into an electromagnetic signal for transmission over the air. When transmitting, the radio uses a modulation scheme to encode bytes of data into an analog signal. This signal is then amplified by a Power Amplifier (PA) before being sent over the antenna. A low-power radio typically outputs $0\ dBm$, or $1\ mW$. Fading and shadowing causes the amplitude of that signal to weaken as it travels through the air. When it is picked up by the receiver antenna, the signal is too weak to be demodulated directly, and the radio uses a Low-Noise Amplifier (LNA) to bring it to a level the demodulator can handle. The power of the weakest signal that the radio can successfully receive is called its sensitivity. A radio with a $-90\ dBm$ sensitivity (a typical number for low-power radios) can successfully demodulate signals as weak as $1\ pW$.

When on, the modulator, demodulator, PA and LNA all draw substantial amounts of current, making the radio the most power-hungry component in most designs. The radio, however, does not consume any energy when off. The challenge of a good communication stack is to enable reliable transmission of data, while keeping the radio off most of the time. Radio duty cycle is the portion of time the radio is on, either transmitting or receiving. It is a good indicator of the power consumption of the mote. An energy-efficient communication stack has a duty cycle (far) lower than $1\ \%$.

Table II-A lists data sheet numbers for commercially-available low-power radios from different vendors. Radios can change the power they transmit at, usually over a range going from -50 dBm to +5 dBm. Since 0 dBm (i.e, 1 mW) is the default transmit power for most radios, we choose to show the transmit current at that power. The receive current is the current drawn by the radio when in receive mode; a radio draws the same current when idle listening (without receiving a packet), or actively receiving bytes. A common misconception is to consider a system is energy-efficient when the motes transmit few packets. Table II-A shows that radios draw about the same current in transmit and receive mode. Optimizing the power consumption of a system therefore consists in lowering the duty cycle of the radio as a whole, i.e. having the radio off most of the time.

In most designs, motes are battery-powered, and it is impractical to change batteries. The goal of an energy-efficient solution is to increase the lifetime of a mote by decreasing its average current consumption. This can be done by choosing a radio which draws little current, and by using a protocol which runs the radio at a low duty cycle. Let's take some examples by assuming the mote is powered by a pair of AA batteries, holding $3000\ mAh$ of charge. If we use the AT86RF231 (which draws $\approx 13\ mA$ when on) and a protocol which left the radio on all the time (i.e. radio duty cycle is $100\ \%$), the batteries will be depleted in $3000\ mAh/13\ mA = 230\ h$, or

TABLE II
COMPARISON OF DIFFERENT 802.15.4-COMPLIANT DEVICES.

Vendor	Product	Sensitivity [dBm]	Transmit current [mA] @ 0 dBm	Receive current [mA]
Atmel	AT86RF231 [a]	-101	14.0	12.3
Dust Networks/ Linear Tech.	LTC5800 [b]	-91	5.4	4.5
Ember	EM357 [b]	-100	27.5	25.0
Freescale	MC13233 [b]	-94	26.6	34.2
Microchip	MRF24J40 [a]	-95	23.0	19.0
NXP/Jennic	JN5148 [b]	-95	15.0 (1.8 dBm)	17.5
Texas Instr.	CC2520 [a]	-98	25.8	18.8

[a] Radio only.
[b] System-on-Chip (radio and micro-controller).

10 days. If, on the same hardware, we use a protocol with a 1 % radio duty, the lifetime increases by a factor of 100, to 32 months. If, on top of that, we replace the radio by the lower-power LTC5800 (which draws $\approx 5\ mA$ when on), the lifetime increases to $3000\ mAh/(5\ mA \times 1\%) = 60000\ h$, or 7 years.

B. PHY of IEEE 802.15.4-2006

The most prominent standard in low-power radio technology is IEEE802.15.4 [25]. It defines both the PHY layer (e.g., the modulation scheme used) and the MAC layer (e.g., in a network, which mote talks when, on which channel). The first revision of the standard was published in 2003, with a revision in 2006. Several working groups are currently working on improving the standard in preparation for its next revision. These groups are identified by a letter, e.g. IEEE802.15.4e to be discussed below.

The IEEE802.15.4 PHY is a healthy trade-off between energy-efficiency, range, and data rate targeted at building-sized networks. While the current standard defines multiple PHY layers, the most widely used is the one operating in the $2.4-2.485\ GHz$ frequency band, a worldwide and unlicensed band.

In this band, the IEEE802.15.4 PHY layer uses Offset-Quadrature Phase-Shift Keying (O-QPSK) modulation with a 2 $Mbps$ physical data rate. Internally to the radio, every group of 4 bits of data sent for transmission are encoded as 32 chips ("physical bits") using a simple lookup table. From a user's perspective, the bitrate appears to be 250 $kbps$, although internally 8 more chips are sent over a 2 $Mcps$ link. This technique is referred to as Direct Sequence Spread Spectrum (DSSS) and known to yield extra robustness.

IEEE802.15.4 defines 16 frequency channels, located every 5 MHz between 2.405 GHz and 2.480 GHz. The channels themselves are only 2 MHz wide, so channel i does not interfere with channel $i-1$ or $i+1$; channels are said to be orthogonal. The radio can arbitrarily send and receive on any of those channels, and every compliant radio is able to switch channels in no more than 192 μs.

When a radio sends a packet, it starts by transmitting a physical preamble for 128 μs to allow for the receiver to lock to its signal. It then sends a well-known Start of Frame Delimiter (SFD) to indicate the start of the physical payload. The first byte of the physical payload indicates the length (in bytes) of the payload itself. Its maximum value is 127, which limits the length of a packet to 128 bytes when including the length byte. A radio listening continuously demodulates what it hears. When no other mote is transmitting, it hears white noise and the stream of bits coming out of the demodulator is random. The circuitry in the receiver looks for a physical preamble to "lock onto". Once locked on, the receiver waits for the SFD, then for the length byte. It then fills a receive buffer with the number of bytes indicated in the length byte, after which it can switch off. After successfully receiving a packet, the radio indicates reception to the micro-controller. From a implementer's point of view, the only requirements are to send packets of at most 128 bytes, and to have the first byte indicate how many bytes follow. Although in a protocol stack the bytes following the length byte comply to different header formats (e.g. MAC, routing, transport), they can be arbitrary as far as the radio is concerned.

III. POWER-SAVING LINK LAYER – IEEE 802.15.4E

IEEE802.15.4 also defines a MAC protocol, i.e. the layer interacting directly with the radio. It defines the format of the MAC header (with fields such as source and destination address) and how motes can communicate with each other. This MAC layer is geared toward star networks, in which all motes communicate directly with a special coordinator mote. It is ill-suited for low-power multi-hop networking mainly because of the following reasons:

- **Powered routers.** While it is possible to use the existing IEEE802.15.4 MAC protocol for multi-hop routing, the motes which are relaying the data need to keep their radio on all the time (100 % duty cycle). In a mesh network, each mote also acts as a router. Using the existing IEEE802.15.4 MAC protocol leads to a power hungry solution.
- **Single channel operation.** The wireless medium is unreliable in nature and propagation effects, such as shadowing and multi-path fading, as well as temporarily varying interference can cause wireless links to break. If the network operates on a single channel, this causes network instabilities which can lead to network collapse.

The IEEE802.15.4e working group was created in 2008 to redesign the IEEE802.15.4 MAC protocol. Through time synchronization and channel hopping, it enables high reliability while maintaining very low duty cycles, both highly recommended requirements for the emerging IoT. IEEE802.15.4e [40] is only a MAC protocol change, which does not require any changes to the hardware.

Time Synchronized Channel Hopping (TSCH), part of IEEE802.15.4e standard since 2010, is the latest generation of highly reliable and low-power MAC protocol, and thus very suitable for a protocol stack for IoT. The initial concept emerged in the proprietary Time Synchronized Mesh Protocol (TSMP) [28] in 2006. Following its successful adoption by the industrial automation community, TSMP was adapted into the WirelessHART standard [29]. While those different standards might have adopted different packet formats and higher-layer commands, the underlying technology is the

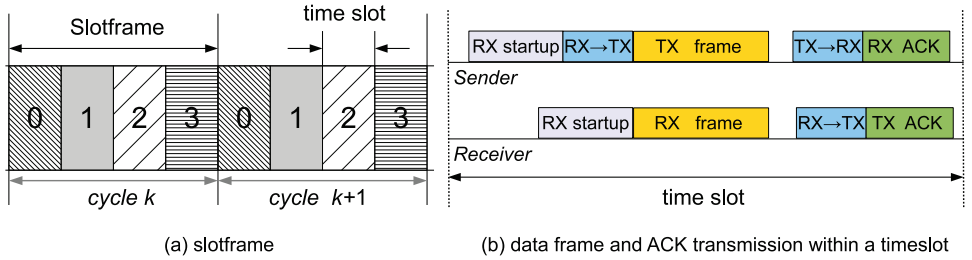

Fig. 1. A 4-slot slotframe and timeslot diagram of an acknowledged transmission.

same: synchronize the motes for energy efficiency, channel hop for reliability.

A. Slotframe Structure

In TSCH, motes synchronize on a slotframe structure. A slotframe is a group of slots which repeat over time. Each mote follows a schedule which tells it what to do in each slot. In a given slot, a mote can either transmit, receive, or sleep. In a sleeping slot, the mote does not turn on its radio. For each active slot, the schedule indicates with which neighbor to transmit or receive, and on which channel offset (see Sec. III-C).

As shown in Fig. 1, a single slot is long enough for the transmitter to send a maximum length packet, and for the receiver to send back an acknowledgment indicating good reception. While the duration of a slot is implement-specific, 10 ms is a possible value suggested in [40].

When an upper layer generates a packet, it sends it to the MAC layer which stores the packet in a transmit queue. At each transmission slot, the MAC layer checks whether it has a packet in its queue destined to the neighbor associated with that slot. If not, it goes back to sleep without turning its radio on. If yes, it transmits the packet and waits for the ACK. If an ACK is received, it removes the packet from the queue. Otherwise, it keeps the packet in the queue for future retransmission. A number of retransmissions is kept for every packet to avoid staleness.

At each reception slot, a mote turns on its radio right before the time it expects to receive the packet. If it receives a packet destined for it, it sends an acknowledgment, turns off its radio, and forwards the packet to the upper layer for processing. If it does not receive anything after some timeout, it returns to sleep. This means that either the transmitter had nothing to say, or that the packet got lost due to interference or fading.

Fig. 2 shows an example topology and the associated schedule. Here, the slotframe is 5 slots long, and there are 6 channel offsets (the concept of channel offset is presented in Sec. III-D). Each mote in the network only cares about the cells it participates in. For example, when G has a packet to send to D, it waits for slot 3, and sends it on channel offset 0. It will stay off for the other cells. If a packet needs to go from G to A, it will first be sent from G to D, be buffered at D, then sent from D to A in the next frame. Note that, as depicted in Fig. 2, while most cells are dedicated, some can be shared between different links (e.g. $D \rightarrow A$ and $C \rightarrow A$). IEEE802.15.4e defines a simple backoff scheme for shared cells in case a collision occurs.

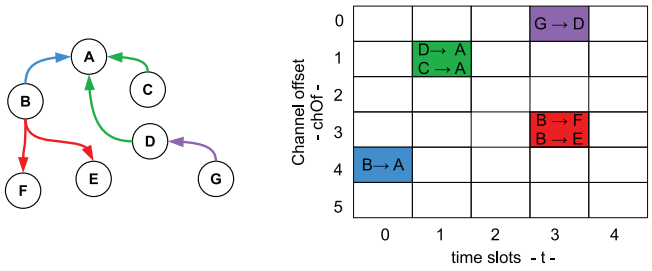

Fig. 2. Dedicated and shared links.

B. Scheduling

IEEE802.15.4e defines how the MAC layer *executes* a schedule (as described in Sec. III-A). It does not specify how such as schedule is *built*. A schedule needs to be built carefully so that, when mote A has a transmit slot to mote B, B is actually listening for packets from A. Similarly, if A is no longer a neighbor of B (e.g. it moved or switched off), B should not be listening anymore for packets from A. While all these rules are intuitive, they also illustrate that the network's schedule needs to be both carefully built, and constantly refreshed as links come and go in the network. Scheduling can either happen in a centralized or a distributed way:

- In a **centralized** approach, a specific "manager" mote is responsible for building and maintaining the network schedule. Every mote in the network regularly updates the manager with the list of other motes it can hear, and the amount of data it is generating. From that neighbor information, the manager draws the connectivity graph. From the data generation demands, it assigns slots to the different links in the connectivity graph. Once this schedule is built, the manager informs each mote about the links in the schedule it is participating in. The motes then simply follow these instructions. When there is a change in the connectivity (i.e., a mote lost a neighbor), the manager updates its schedule and informs the affected motes.
  In practice, networks often have a gateway mote which connects it to the Internet (see Section IV). In a centralized approach, that mote often also manages the IEEE802.15.4e schedule. This type of approach has been commercially available since TSMP, and tens of thousand such networks have been deployed.
  A centralized approach builds very efficient schedules. Since the manager knows exactly what the network looks like, it can apply centralized scheduling techniques. In

the case the topology is constantly changing, with motes moving, requiring the network to re-form continuously, a distributed approach might be used.

- In a **distributed** approach, motes decide locally on which links to schedule with which neighbors. One can imagine opting for this approach in mobile networks, or when the network has many gateway motes. The simplest solution is for each node to schedule a link to each neighbor. This is the approach adopted by Tinka *et al.* [41], which evaluates this approach by simulation and experimentally. A more complex problem is when multiple motes generate data at a constant rate, which requires links to be scheduled along the multi-hop route this data travels over. Internet-like reservation protocols such as the Resource Reservation Protocol (RSVP) [42] and the Multi Protocol Label Switching (MPLS) protocol [43] could be applied, although this is remains a very open issue.

C. Synchronization

Device-to-device synchronization is necessary to maintain connectivity with neighbors in a slotframe-based network. As shown in Fig. 1, no beacon is transmitted in a IEEE802.15.4e network for TSCH applications.

Two methods are defined for allowing a device to synchronize to the network: (I) *Acknowledgment-Based* synchronization and (II) *Frame-Based* synchronization. The former involves the receiver calculating the delta between the expected time of frame arrival and its actual arrival, and providing that information to the sender mote in its acknowledgment. This allows a sender mote to synchronize to the clock of the receiver. The latter involves the receiver calculating the delta between the expected time of frame arrival and its actual arrival, and adjusting its own clock by the difference. This allows a receiver mote to synchronize to the clock of the sender.

When there is traffic in the network, motes which are communicating implicitly re-synchronize using the data frames they exchange. If they have not been communicating for some time (typically 30 s), motes exchange an empty data frame (called keep-alive messages) to re-synchronize.

In a typical IEEE802.15.4e TSCH network, time propagates outwards from the coordinator. It is very important to maintain unidirectional time propagation and avoid timing loops. Each device periodically synchronizes its network clock to at least one other device, and it also provides its network time to its neighbor motes. Each mote determines whether to follow a neighbor's clock based on the presence of a *ClockSource* flag in the corresponding neighbors record (configured by the network manager in a centralized system). It has to be specified that the direction of time propagation is independent of data flow in the network.

D. Channel Hopping

The IEEE802.15.4e TSCH MAC adds channel hopping to time slotted access. Channel hopping implies frequency diversity that mitigates the effects of interference and multipath fading. Moreover, the use of several frequencies increases the network capacity, because more motes can transmit their frames at the same time, using different channel offsets. Channel hopping combined with slot access improves also reliability. The advantages derived from the channel hopping have been already tested and analyzed [44], [45].

Let (t, $chOf$) be the slot and the channel offset, respectively, assigned to a given link. The channel offset, *chOf*, is translated to a frequency f (i.e., a real channel) using (1).

$$f = F\{(ASN + chOf) \bmod n_{ch}\} \tag{1}$$

where *ASN* is the *Absolute Slot Number*, i.e. the total number of slots that elapsed since the network was deployed. The ASN is incremented at each slot and shared by all devices in the network. In detail, $ASN = (k \cdot S + t)$, where k is the slotframe cycle, as shown in Fig. 1. The function F is realized with a look-up-table, containing the set of available channels. The value n_{ch} (i.e., the number of available physical frequencies) is the size of such a look-up-table. Moreover, the following constraints on t and $chOf$ hold: $0 \leq t \leq S-1$, and $0 \leq chOf \leq n_{ch} - 1$. In an IEEE802.15.4e network, 16 channels are available. Furthermore, a blacklist can be used to restrict the set of allowed channels for coexistence purposes. If the slotframe size, S, and the number of channels, n_{ch}, are relatively prime, the translation function assures that each link rotates through k available channels over k slotframe cycles. In other words, successive frames over a same link are sent over different physical frequencies in successive slotframe cycles k.

E. Network Formation

Network formation in TSCH networks includes two components: *advertising* and *joining*. A new device trying to join the network listens for *Advertisement* command frames. When at least one of these frames is received, the new mote joins the network by sending a *Join Request* command frame to an advertising device.

In a centralized management system, *Join Request* frames are routed to the network manager. In a distributed management system, they can be processed locally. When a new mote is accepted into the network, the advertiser activates the mote by setting up slotframes and links between the new mote and other existing ones. These slotframes and links can also be deleted and/or modified after a mote has joined the network.

1) Network Ramp-Up: Fig. 3 shows the messages exchanged during the network build up phase in a simple scenario with a network manager (mote A) and two motes B and C, using a slotframe of 7 slots. For each exchanged message, we specify the slot ASN used for that transmission. Moreover, we mark the beginning of each new slotframe occurrence, specifying the value of the slotframe cycle, k. As it can be seen in Fig. 3, several messages are sent in consecutive slotframe cycles.

We suppose that the TSCH network is based on a centralized management system. In other words, mote A is the network manager which defines the links for allowing broadcast and dedicated communications in the network. Being the first mote in the network, the mote A starts one slotframe, to which other motes may later synchronize. It reserves the first two slots within the slotframe to itself for broadcasting

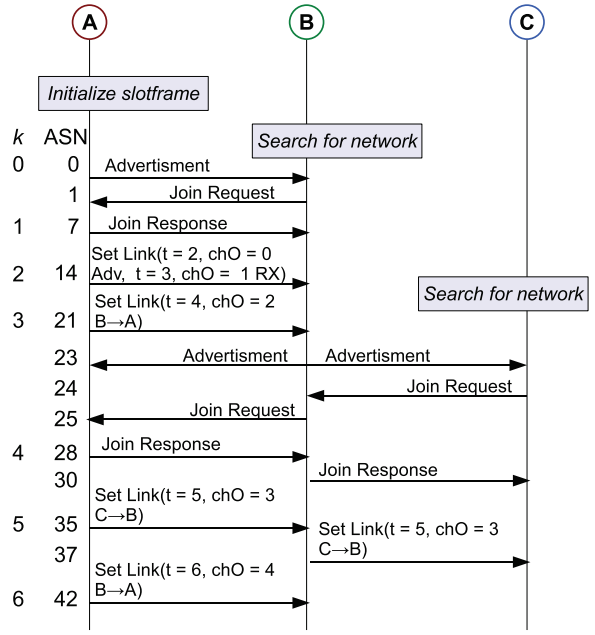

Fig. 3. Messages exchanged during the network build up phase.

the *Advertisement* command frames and receiving the *Join Request* frames, respectively. As soon as other devices join the network, mote A assigns slots and channel offsets to each of them.

Fig. 4 shows the links scheduled within the slotframe, during the network build up phase. Mote A assigns the same channel offset value, $chOf = 0$, to all the broadcast links, and $chOf = 1$ to all the dedicated links used for receiving Join Request frames.

As already specified, the use of the same *chOf* does not imply the use of the same channel. In fact, in the frequency translation function, given by Eq. (1), the value of *chOf* is the same, but the value of t is different, and therefore it results in a different channel to be used.

In order to allow frames generated by mote C to reach mote A, a slot is reserved for each dedicated link along the path $C \rightarrow B$, $B \rightarrow A$.

Once all the motes have joined the network, i.e., the network manager has not received any *Join Request* frames during a timeout period, the Advertising procedure can be disabled. Afterwards, the procedure could be activated again, with a given frequency, in order to check if there are new devices that wait to join the network.

IV. Connecting to the Internet – IETF 6LoWPAN

As well known, in the Internet a packet passes through many different interconnected networks on its way from source to destination. Thus, considering the link layer technology of each traversed network, there needs to be an "IP-over-X" specification to define how to transport IP packets. In many cases, to map the services required by the IP layer on the services provided by the lower layer (i.e, the link layer), the "IP-over-X" specification can introduce a (sub)layer of its own, often called *adaptation layer* [46]. Following the same strategy, in the process of shaping the IoT world, the IETF IPv6 over Low power WPAN (6LoWPAN) working group has

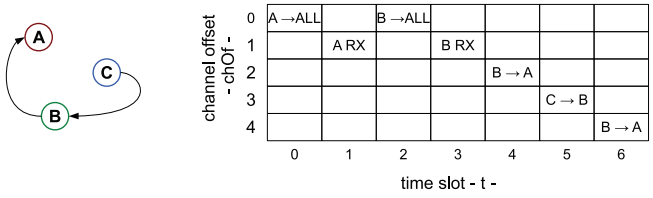

Fig. 4. Time pattern within the 7 slots slotframe defined during the network build up phase in Fig. 3.

started in 2007 to work on specifications for transmitting IPv6 over IEEE 802.15.4 networks.

Typically, Low power WPANs are characterized by: small packet sizes[2], support for addresses with different lengths, low bandwidth, star and mesh topologies, battery supplied devices, low cost, large number of devices, unknown node positions, high unreliability, and long idle periods during when communications interfaces are turned off to save energy [30], [47] – [50].

Given the aforementioned features, it is clear that the adoption of IPv6 on top of a Low power WPAN is not straightforward, but poses strong requirements for the optimization of this adaptation layer. For instance, due to the IPv6 default minimum MTU size (i.e., 1280 bytes), a no-fragmented IPv6 packet would be too large to fit in an IEEE 802.15.4 frame. Moreover, the overhead due to the 40 bytes long IPv6 header would waste the scarce bandwidth available at the PHY layer.

For these reasons, the 6LoWPAN working group has devoted huge efforts for defining an effective adaptation layer in [51], [52]. Further issues encompass the auto-configuration of IPv6 addresses [53], the compliance with the recommendation on supporting link-layer subnet broadcast in shared networks [54], the reduction of routing and management overhead, the adoption of lightweight application protocols (or novel data encoding techniques), and the support for security mechanisms (i.e., confidentiality and integrity protection, device bootstrapping, key establishment and management).

A. 6LoWPAN Frame Format

To manage IPv6 packet, allowing link-layer forwarding and fragmentation, 6LoWPAN uses an intermediate adaptation layer between IPv6 and IEEE 802.15.4 MAC levels [51]. IPv6 header and *Next Headers* may be compressed, by suppressing redundant information that can be inferred from other layers in the communication stack [52].

Specifically, all 6LoWPAN encapsulated datagrams (that should be transported over IEEE 802.15.4 MAC) are prefixed by a stack of headers, each one identified by a type field. In particular, the header types can be logically grouped in four categories, depending on the function they play in the 6LoWPAN adaptation strategy, as shown in Table III and summarized below:

- a *NO 6LoWPAN Header* is used for specifying that the received packet is not compliant to 6LoWPAN specifications and therefore it has to be discarded (this allows the

[2]In an IEEE 802.15.4 WPAN, the maximum packet length to be transmitted on physical layer is 127 bytes.

TABLE III
6LOWPAN HEADER TYPES.

First 2 bits		Following bit combinations	
NO 6LoWPAN	00	xxxxxx	Any combination
Dispatch	01	000000	Additional Dispatch byte follows
		000001	Uncompressed IPv6 Addresses
		000010	LOWPAN_HC1 compressed IPv6
		010000	LOWPAN_BC0 broadcast
		1xxxxx	LOWPAN_IPHC compressed IPv6
Mesh Addressing	10	xxxxxx	Any combination
Fragmentation	11	000xxx	First Fragmentation Header
		100xxx	Subsequent Fragmentation Header

coexistence with other no-6LoWPAN nodes in the same network).

- A *Dispatch Header* is used to compress an IPv6 header or to manage link-layer multicast/broadcast.
- A *Mesh Addressing Header* allows IEEE 802.15.4 frames to be forwarded at link-layer, turning single-hop WSNs in multi-hop ones.
- A *Fragmentation Header* is used when a datagram does not fit within a single IEEE 802.15.4 frame.

It is worth to note that each header may be present or not, depending on the needs. Moreover, headers should appear in a precise order, as described in the sequel.

The IEEE 802.15.4 standard does not define any routing capability and relies on functions of upper layers to do this task. At this aim, a routing protocol that can be used for populating the routing table will be described in Sec. V. Anyway, two devices do not require direct reachability in order to communicate because an *Originator* device may use other intermediate devices as forwarders toward the *Final Destination* device. To realize the frame delivery using a unicast communication, a *Mesh Addressing Header* is used prior to any other headers of the 6LoWPAN encapsulation. For each forwarder node, it includes the link-layer addresses of the considered forwarding node and of the next-hop node, in addition to the link-layer addresses of the *Originator* and of the *Final Destination*.

When some form of multicast/broadcast communication at link layer is needed for controlled flooding mechanisms (e.g., the one described in Sec.V) or for topology discovery, a *Broadcast Header* immediately follows the *Mesh Addressing Header* (if present). It is a kind of *Dispatch Header* (see below) and it includes a 1-byte long *Sequence Number* for detecting and, thus, suppressing duplicate packets.

The *Fragmentation Header* can be used for fragmentation purposes and it must follow *Mesh Addressing* and *Broadcast* headers, if present. Such a header includes: the *Datagram Size*, that is the dimension of the entire IP packet before link layer fragmentation (it shall be the same for all link layer fragments of an IP packet); the *Datagram Tag*, which identifies univocally the original fragmented IP packet; and the *Datagram Offset* that specifies the offset of the fragment from the beginning of the payload (obviously it is present only in the second and subsequent fragments).

Finally, the *Dispatch Header* category includes several kinds of headers, used for encapsulating and, optionally, compressing an IPv6 packet. Therefore, a *Dispatch Header*, except the *Broadcast* one, must follow all the other ones described till now. The 6LoWPAN specifications consider the *LOWPAN_IPHC* encoding scheme for compressing IPv6 header, as defined in IETF RFC 6282 [52]. It substitutes the original scheme suggested in the IETF RFC 4944 [51]. However, new implementations of 6LoWPAN should support *LOWPAN_HC1* decompression for backward compatibility issues. Therefore, both compression schemes are identified by different *Dispatch Types* (see Table III).

B. Header Compression

Within the same WPAN, many IPv6 header fields are expected to be common and/or easy to derive without requiring their explicit indication by the sender. As an example, the *Payload Length* can be inferred either from the *MAC Frame Length* or from the *Datagram Size* field in the fragmentation header (if present); *Hop Limit* will be set to a well-known value by the source; addresses assigned to 6LoWPAN interfaces are formed with an *Interface Identificator* derived directly from MAC addresses.

The *LOWPAN_IPHC* encoding scheme performs effective compression of unique local, global, and multicast IPv6 addresses, based on shared states. To this end, a 13-bit *LOWPAN_IPHC* encoding field is appended to the first 3 bits of the *Dispatch Type*. If some of the IPv6 header fields have to be carried in clear, they follow the *LOWPAN_IPHC* encoding. In the best case, the *LOWPAN_IPHC* can compress the IPv6 header down to 2 bytes in an IPv6 link-local communication (i.e., a direct single-hop communication). When a packet is routed through multiple hops, *LOWPAN_IPHC* can compress the IPv6 header down to 7 bytes.

6LoWPAN provides also a technique to compress IPv6 next-headers, namely the *LOWPAN_NHC* encoding. Compression formats for different next-headers are identified by a variable-length bit-pattern which immediately follows the *LOWPAN_IPHC* compressed header. Each next-header in the original IPv6 packet will be present in the compressed one in the same order and it will encoded with the appropriate *LOWPAN_NHC* format.

Finally, the RFC 6282 allows a compression format for UDP headers using *LOWPAN_NHC*. The UDP Length field is always elided, as it can be inferred from lower layers using the 6LoWPAN *Fragmentation Header* or the IEEE 802.15.4 header. The Checksum field can be also elided if authorized by upper layers. Source and destination ports can be compressed if they match some common cases and, hence, the compression result is carried in-line after the *LOWPAN_NHC* encoding field; the length of the compression result can range from a minimum of 8 bits (i.e., 4 bits for each port) to 32 bits (i.e., both ports are not compressed). Not compressed or partially compressed fields are carried in-line, appearing in the same order as they do in the original UDP header. In the best case, an UDP header can be compressed to only 2 bytes, i.e., one byte for the *LOWPAN_NHC* encoding field and the other one for the compressed ports.

V. ROUTING – IETF ROLL

Routing issues are very challenging for 6LoWPAN, given the low-power and lossy radio-links, the battery supplied nodes, the multi-hop mesh topologies, and the frequent topology changes due to mobility. Successful solutions should take into account the specific application requirements, along with IPv6 behavior and 6LoWPAN mechanisms [46]. An effective solution is being developed by the IETF "Routing Over Low power and Lossy (ROLL) networks" working group. Recently, it has proposed the leading IPv6 Routing Protocol for Low-power and Lossy Networks (LLNs), RPL, based on a gradient-based approach [31], [49], [50], [55].

RPL can support a wide variety of different link layers, including ones that are constrained, potentially lossy, or typically utilized in conjunction with host or router devices with very limited resources, as in building/home automation, industrial environments, and urban applications [56] – [59]. It is able to quickly build up network routes, to distribute routing knowledge among nodes, and to adapt the topology in a very efficient way. For these characteristics, it is suitable also for smart grid communications [60].

In the most typical setting entailed by RPL, the nodes of the network are connected through multi-hop paths to a small set of root devices, which are usually responsible for data collection and coordination duties. For each of them, a Destination Oriented Directed Acyclic Graph (DODAG) is created by accounting for link costs, node attributes/status information, and an Objective Function, which maps the optimization requirements of the target scenario. It is identified with a *DODAGID*. The topology is set-up based on a *Rank* metric, which encodes the distance of each node with respect to its reference root, as specified by the Objective Function. Regardless the way it is computed (see Sec. V-C for more details), the *Rank* should monotonically decrease along the DODAG and towards the destination, in accordance to the gradient-based approach.

RPL can encompass different kinds of traffic and signaling information exchanged among nodes (as well ancillary data structures) depends on the requirements of the considered data flows.

The *Multipoint-to-Point* (*MP2P*) is the dominant traffic in many LLN applications. It is usually routed towards nodes with some application relevance, such as the LLN gateway to the larger Internet or to the core of private IP networks. In general, these destinations are the DODAG roots and they act mainly as data collection points for distributed monitoring applications. Contrariwise, *Point-to-Multipoint* (*P2MP*) data streams can be used for actuation purposes, by means of messages sent from DODAG roots to destination nodes. Finally, *Point-to-Point* (*P2P*) traffic is necessary to allow communications between two devices belonging to the same LLN, e.g., a sensor and an actuator. In this case, a packet will flow from the source towards the common ancestor of those two communicating devices; then, downward towards the destination.

As an obvious consequence, RPL has to discover both upward routes (i.e., from nodes to DODAG roots) in order to enable MP2P and P2P flows, and downward routes (i.e., from DODAG roots to nodes) to support P2MP and P2P traffic.

A. RPL Topology Formation

The simplest RPL topology is made by a single DODAG with just one root, e.g., a WSN monitoring a small size area.

A more complex scenario encompassed by RPL is composed of multiple uncoordinated DODAGs with independent roots, that is, the LLN is split in several partitions depending on the needs of the application context.

A more sophisticated and flexible configuration could contain a single DODAG with a virtual root that coordinates several LLN root nodes. The main advantage in this case, with respect to the previous one, is the absence of limitations on the parent set selection, given that all nodes belong to the same virtual DODAG, although a stronger coordination is needed among the root nodes.

Depending on the application requirements, it is also possible to combine the three examples presented so far in more complex topologies.

Moreover, multiple instances of RPL may run concurrently on the network devices and each instance has specific routing optimization objectives, such as the minimization of delay and energy consumption. To this aim, a *RPLInstanceID* is employed to identify one of the possible RPL instances running on the same network.

The formation of all these possible kinds of topologies relies on the RPL information dissemination mechanism, which enables a minimal configuration in the nodes and allows them to operate mostly autonomously. In this sense, a key role is played by DODAG Information Option (DIO) messages, containing information about the *Rank*, the Objective Function, the IDs, and so on. They are multicasted (periodically and link-locally) by each node to create the DODAG, thus establishing paths towards the roots.

In detail, according to RPL specifications, in order to implement network formation and management operations, all nodes execute several operations: they send and receive DIOs; they compute their own *Rank*, based on the information included in the received DIOs; they join a DODAG and select a set of possible parents in that DODAG among all nodes in the neighborhood; they select the preferred parent among the possible ones.

A node receiving a DIO message uses its information to join a new DODAG, or to maintain an existing one, according to the Objective Functions and the *Ranks* of their neighbors. It can also detect possible routing loops. To reach these goals, the following function is used:

$$DAG_{Rank(N)} = \lfloor Rank(N)/MinHopRankIncrease \rfloor \quad (2)$$

where N is the node identifier, $Rank(N)$ is the *Rank* of node N, $\lfloor x \rfloor$ is the greatest integer less than or equal to x; and *MinHopRankIncrease* is the implementation-dependent minimum hop rank increase value, representing the minimum difference between the *Rank* of a node and the *Ranks* of its possible parents.

Upon a DIO message is received from a neighbor, a node setups its own *Rank* to a value that is a function of both

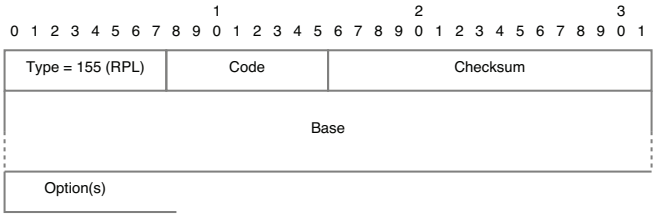

Fig. 5. RPL encapsulation in an ICMPv6 packet.

the neighbor *Rank* and the cost to reach the DODAG root through it. The considered node lets that its set of possible parents contain only that neighbor, if one of the following conditions is true: (i) the node *Rank* was not already setup; (ii) the old value, A, of the node *Rank* and the computed one, B, verify the relation $DAG_{Rank(A)} > DAG_{Rank(B)}$. Instead, if $DAG_{Rank(A)} = DAG_{Rank(B)}$, the neighbor is added to the set of possible parents. In other cases, the DIO is not further considered. Finally, each node can select its preferred parent within its set of candidate parents based on several possible rules, such as Objective Function, path cost, *Rank*, and so on.

On the other hand, a node advertises its presence, the affiliation with a DODAG, the routing cost, and the related metrics by sending DIO messages to nodes in its neighborhood, only if it has already computed its own *Rank*. An exception is allowed to the DODAG root, which is configured to get its own *Rank* equal to the value *MinHopRankIncrease*, and to send it with the *DODAGID*, the routing cost, and the related metrics into DIO messages. In this way, a DODAG is constructed in a widening-wave fashion, starting from the DODAG root.

It is worth to remark that these procedures are useful to establish upward routes only. Therefore, in presence of P2MP and P2P traffics, an additional mechanism is required to create downward paths. To this end, RPL uses Destination Advertisement Object (DAO) messages to back-propagate routing information from leaf nodes to the roots. They are triggered by the reception of a DIO message, or in global and local repair operations. After receiving a DAO message, each node forwards it to its parent at the expiration of a timer, which is implementation-dependent [31].

To avoid redundancies and to control the signaling overhead, the *trickle* algorithm [61] triggers, for each node, a new DIO message only when the overall amount of control packets already sent in the neighborhood of that node is small enough.

B. RPL Control Messages and Metrics

RPL control messages are encapsulated into ICMPv6 packets, according to [62]. The structure of a message is reported in Fig. 5.

The Code field indicates which kind of control message is present after the Checksum. The Base field is the RPL message header and it contains only the basic information related to the functions of the carried object. Instead, the Options field is the body of such messages and, depending of the needs, it may be composed of any combination of optional functions (padding, metric containers, route information, DODAG configuration, RPL target, and so on).

Each RPL message has a secure variant providing integrity and protection as well as optional confidentiality and delay features.

Regarding the possible metrics (which can be fruitfully exploited for timely adapting the topology to changing network conditions) RPL can use [63]: node energy, hop count, link throughput, latency, link reliability, and link color. In particular, with the term "colors" RPL refers to specific properties of links, so that the link color is used to include or exclude such links from the paths.

This richness of information, from on side, makes RPL highly adaptable to different operating conditions. On the other hand, it is necessary to keep under control the adaptation rate of routing metrics in order to avoid path instabilities, which would severely impair LLN performance and scalability.

All the available metrics can be advertised in control messages.

C. The Objective Function

In RPL, the Objective Function translates key metrics and constraints into a *Rank*, which models the node distance from a DODAG root, in order to optimize the network topology in a very flexible way. Furthermore, the Objective Function allows the selection of a DODAG to join and the identification of a number of peers in that DODAG as parents. Generally speaking, the parent selection at a node could be triggered in response to several events, such as the reception of a DIO message, a timer elapse, all DODAG parents become unavailable, or a trigger indicating that the state of a candidate neighbor has changed. After the Objective Function has scanned all the interfaces at a node to check whether they can be eligible for establishing a link in the topology, all candidate neighbors are examined to evaluate if they can act as RPL router. These preliminary operations are useful to exclude all those links and candidate nodes that do not match basic Objective Function compatibility rules, e.g., related to security issues, performance, an so on. Then, the node scans the list of the candidate parents that passed the preliminary tests. The *Rank* that would result from having each of them as parent is evaluated. The preferred parent is elected as the one that can grant the smallest *Rank*, provided that this *Rank* is smaller than the one currently held by the node itself. Obviously, these operations can be iterated when more than one parent has to be selected.

The Objective Functions proposed by IETF are described below.

1) Objective Function 0: It requires only the information in the RPL DIO header. A node *Rank* is obtained by adding a normalized scalar, *RankIncrease*, to the *Rank* of a selected preferred parent. The *RankIncrease* value is a multiple of 0x100, so that *Rank* values can be stored in one octet. Given that in the RPL main specification [31] there is neither default Objective Function, nor default metric container, it might happen that two implementations, following different guidelines for a specific problem or environment, will not support a common Objective Function which they could interoperate with. Therefore, Objective Function 0 is designed as a common denominator among all the generic implementations.

It ignores metric containers and it leaves to implementation the responsibility to compute how link properties are transformed into a *RankIncrease*.

2) Minimum Rank Objective Function with Hysteresis: It is designed to find the paths with the smallest path cost while preventing excessive churn in the network [64]. A node switches to the minimum cost path, *NewPathCost*, only if the following inequality is verified:

$$NewPathCost < CurrentPathCost - \gamma \qquad (3)$$

where *CurrentPathCost* is the path cost of the current path, and γ is the *PARENT_SWITCH_THRESHOLD*, implementing hysteresis.

This Objective Function may be used with any additive metric listed in [63] as long the routing objective is to minimize the given routing metric. Besides, it employs a DODAG parent set with only one node. This node is automatically chosen as the preferred parent. As a consequence, any candidate neighbor may become the preferred parent.

VI. Transport Layer and Above – IETF CoAP

A LLN using IPv6 provides world-wide Internet integration given that nodes can be addressed and information can be routed through the network without requiring specialized NAT techniques at the gateways. However, for complete Internet compatibility, some features which are not addressed by the network layer are required. On one hand, it would be desirable that a node manage multiple non-interfering requests. This issue can be dealt by specialized application code running at each node or by multiplexing network layer through the use of the concept of port. Besides, end to end reliability cannot be guaranteed by network layer as its task needs to be performed over the network routing structure. Usually both functionalities are addressed by upper-network layers such as transport and application in the TCP/IP network stack.

On the other hand, application layer protocols provide application independent semantics that facilitate content representation and inter-operability between different applications. Protocols, such as HTTP [15], enable applications to interoperate in a client/server content/resource centric fashion. Internet of Things aims to enable LLNs to interoperate with existing applications without the need of specialized application oriented code, thus requiring LLNs to talk application layer protocols. As classical networks do not need to operate with energy restrictions, content tagging and metadata are not optimized for minimum packet overhead; this limits their integration in LLN applications. Thus, a set of techniques to compress application layer protocol metadata have been proposed without compromising application inter-operability.

A. Transport over LLNs

The Transport layer is responsible of providing end-to-end reliability over IP based networks. TCP [17] provides traffic control and congestion control through Automatic Repeat-Request (ARQ) techniques [65]. It sustains the traffic on the Internet and provides reliability thanks to the control overhead introduced for each transmitted packet. Reliable transport protocols over LLNs are being studied but the amount of information for traffic control and reliability are expensive in terms of number of transmitted packets and end to end packet confirmation which directly maps to energy consumption. Dunkels et al [66] presented a lightweight TCP implementation based on the use of caching that reduces the amount of control packets. Other approaches focus on the use of Selective Repeat variant [67] which selectively acknowledge received packets with the caveat that acknowledgments are end-to-end. So that, they are required to cross the entire network and this is not energy efficient. Due to the expensive energy requirements imposed by end to end reliability and the lack of a clear proposal for reliable transport in LLNs, the use of User Datagram Protocol (UDP) [68] and retransmission control mechanisms at application layer are demonstrating a good trade-off between energy cost and reliability.

UDP is a datagram oriented protocol that provides a procedure for application to send messages to other applications with a minimum of protocol mechanism and overhead. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed (i.e. UDP neither provides guarantees to the upper layer protocols for message delivery nor retains state of UDP messages once sent). Like TCP, UDP provides application multiplexing through the concept of port.

As stated in previous sections, 6LoWPAN removes a number of fields in the IPv6 and UDP headers because they take well-known values, or because they can be inferred from fields in the IEEE 802.15.4 header.

B. Application Layer

In the application scenarios addressed by LLNs, we will find a range of devices involved with very different capabilities, from full servers to constrained devices consisting of 8-bit or 16-bit microcontrollers with wireless network interfaces such as IEEE 802.15.4 compliant radios. In that kind of scenarios, there is the need to restrict the use of different protocols to a certain subset that can interoperate across device types, inclusively at application layer. Experience with protocol gateways translating between protocols providing similar services, tells us that such gateways can cause nasty operational problems since protocol semantics are often not 100% translatable in some corner cases. In addition, the use of web services on the Internet applications has become the de-facto standard which draws that application layer interoperability have to be in conformance with a representational state transfer architecture of the web [15].

Due to the restrictions imposed by LLNs, a straightforward implementation of RESTful architectures such as the client/server model defined by HTTP is not possible and an adaptation is required. While REST architectures make assumptions on efficient reliable transport and are not strictly constrained by payload size as expensive fragmentation is dealt at lower layers, a LLN has to carefully take into account several of these features as the services offered by lower layers are considerably more restrictive. 6LoWPAN for example supports the expensive IPv6 packet fragmentation into 127 bytes long packets, but an abuse of that makes the network inoperable. Thus a requirement for application layer is to limit the packet extension.

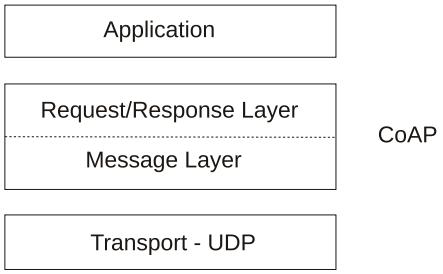

Fig. 6. CoAP architecture.

The IETF Constrained RESTful Environments (CORE) working group [69] has defined the Constrained Application Protocol (CoAP) [32] which easily translates to HTTP for integration with the web, while meeting specialized requirements such as: multicast support, very low overhead, and simplicity for constrained environments. CoAP has been designed as a generic protocol for LLNs taking into account the features of the underlying architecture [70]. The CORE working group, instead of blindly making a compression of HTTP [15], defined a subset of the RESTful specification, making it interoperable with HTTP but also specializing it for so constrained environments. The summary of the main features addressed by CoAP are [32]:

- Constrained web protocol specialized to M2M requirements.
- Stateless HTTP mapping through the use of proxies or direct mapping of HTTP interfaces to CoAP.
- UDP transport with application layer reliable unicast and best-effort multicast support.
- Asynchronous message exchanges.
- Low header overhead and parsing complexity.
- URI and Content-type support.
- Simple proxy and caching capabilities.
- Optional resource discovery.

Unlike HTTP, CoAP is an asynchronous request/response protocol over a datagram oriented transport such as UDP. The client/server architecture of HTTP is slightly different in CoAP as end-points do not assume a so clear role. This is motivated by the nature of the underlying transport, which is asynchronous (i.e., datagram oriented), and both endpoints acting as clients and servers. The architecture of CoAP is divided in two layers, a *message layer* in charge of reliability and sequencing and a *request/response layer* in charge of mapping requests to responses and their semantics (see Fig. 6).

1) Message layer: The function of the CoAP message layer is to control message exchanges over UDP between two endpoints. Requests and Responses share a common message format. Messages are identified by an ID used to detect duplicates and for reliability. There are four types of messages which are specified in the header.

- *Confirmable:* messages that require a response, which can be piggybacked in an acknowledgement or sent asynchronously in another message if the response takes too time to be computed. Confirmable messages that cannot be processed are replied with a Reset message. Responses to confirmable messages are also confirmable messages that need to be acknowledged.
- *Non-Confirmable:* Messages that do not need to be neither acknowledged nor replyed.
- *Acknowledgement:* Messages that confirm the reception of a confirmable message. They can contain the piggybacked response to the confirmable message.
- *Reset:* In case a confirmable message cannot be processed.

In addition, multicast messages are supported being only possible for Non-Confirmable messages.

2) Request/Response layer: CoAP request and response semantics are carried in CoAP messages, which include either a method code or response code, respectively. Optional (or default) request and response information, such as the URI and payload content-type are carried as CoAP options. A Token Option is used to match responses to requests independently from the underlying messages. As CoAP is implemented over non-reliable transport, CoAP messages may arrive out of order, appear duplicated or be lost without notice. Thus, CoAP needs to implement a reliability mechanism with the following features:

- Simple stop-and-wait retransmission reliability with exponential back-off for confirmable messages.
- Duplicate detection for both confirmable and non-confirmable messages.
- Multicast support.

Reliability works over *Confirmable* messages. Upon reception of such message, receiver must acknowledge it or reject it by sending a *Reset* message. The sender retransmits the *Confirmable* message at exponentially increasing intervals, until it receives an *acknowledgment* (or *Reset* message), or runs out of attempts (controlled by a retransmission counter). *Non-confirmable* messages are never acknowledged nor rejected. In case they cannot be processed, they are ignored.

Request and Responses are mapped to each other thanks to the token embedded into the header. A Request consists of the method that should be applied to the resource, of the identifier of the resource, of a payload and an Internet media type (if any), and of an optional meta-data about the request. A Response is identified by the Code field in the CoAP header. Similar to the HTTP Status Code, the CoAP Response Code indicates the result of the attempt to understand and satisfy the request.

3) CoAP frame: CoAP messages are encoded in a simple binary format. As shown in Fig. 7, a message consists of a fixed-sized CoAP Header followed by options in Type-Length-Value (TLV) format and a payload. The number of options is determined by the header. The payload is made up of the bytes after the options, if any; its length is calculated from the datagram length. The main fields on the frame are the following:

- Version: 2 bits that show the CoAP version number. Set to 1 in the current version.
- Type: 2 bits that indicate the type of message. In particular, we can have the messages: (0) Confirmable, (1) Non-Confirmable, (2) Ack, (3) Reset.
- Option Count: 4 bits, indicate the number of options in the option header.

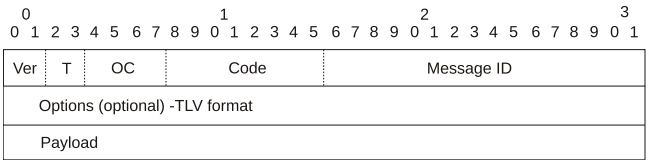

Fig. 7. CoAP frame format.

- Code: 8 bits that indicate if the message is a request or a response. In case of request, indicates the request method (GET, PUT, and so on). In case of a response, the Response code (2.01, 4.03, and so on).
- Message ID: 16 bits field with a unique ID to match *Confirmable* and *Acknowledgments* or *Reset* messages and to detect duplicates.
- Options: Option list in TLV format.
- Payload: The content of the message, usually a resource representation. Its type is defined by the Content-Type Option. Error responses include a human-readable description of the error such as "Bad Gateway".

4) CoAP basic methods: CoAP offers the methods for a RESTful architecture.

- **GET**: Idempotent and safe operation that retrieves a representation for the information corresponding to the resource identified by the request URI.
- **POST**: Requests the processing of the representation enclosed in the resource identified by the request URI. Normally it results in a new resource or the target resource being updated. The method is neither safe nor idempotent.
- **PUT**: Requests that the resource identified by the request URI be updated or created with the enclosed representation. The representation format is specified by the media type given in the Content-Type Option. PUT is not safe but idempotent.
- **DELETE**: The method requests that the resource identified by the request URI be deleted.

Responses are identified by Response codes analogous to HTTP Status codes. Due to space limitations only some of them are commented in this section. The full list of codes can be found at [32].

- **Success**: Codes 2.XX represent that the request has been received, understood and accepted. For example, code 2.01 is analogous to HTTP code 201 "Created" but only in response to POST and PUT requests.
- **Client Error**: Codes 4.XX are returned when a client incurred in some error. For example, code 4.04 is the same as HTTP code 404 "Not Found".
- **Internal Server Error**: Code 5.xx returned when a server is not able to carry out the request. For example 5.02 analogous as HTTP 502 code "Bad Gateway".

5) Caching and Proxying: The goal of caching in application layer protocols is to reduce the required network bandwidth thanks to the reuse of prior response messages to satisfy a specific current request. In some cases, a cached response can be used without requiring a network request, considering the constraints of LLNs, this extremely benefits the lifetime, latency and network round-trips. Contrarily to HTTP, CoAP responses are defined to be cacheable according to the Response Code in the header definition. For this purpose, a freshness mechanism based on a Max-Age option is used. Responses are tagged by the server (i.e., the end-point answering) with an explicit age that will maintain the response cached until its expiration. By default the Max-Age option is 60 s.

CoAP distinguishes between requests to an origin server and a request made through a proxy. A proxy is a CoAP end-point that can be tasked by CoAP clients to perform requests on their behalf. This may be useful, for example, when the request could otherwise not be made, or to serve the response using a cache in order to reduce response time and network bandwidth or energy consumption. CoAP requests to a proxies are made as *Confirmable* or *Non-Confirmable* requests to the proxy end-point, but setting the Proxy-Uri Option and splitting the request URI to the Uri-Host, Uri-Port, Uri-Path and Uri-Query Options. As in the architecture of Internet caching and proxying are fundamental to alleviate the traffic in LLNs.

6) CoAP URIs: CoAP URIs are very similar to HTTP URIs. The "coap" URI scheme has been identified for CoAP resources and for providing the means to locate the resources. As in RESTful architectures, resources are organized hierarchically and governed by a potential origin server listening for requests on a given port. The structure of the URI follows the model defined in [71]:

coap-URI = "coap:" "//" host [":" port] path-abempty ["?" query] .

The host can be provided either as an IP address, or a name which should be resolved using a resolution service such as DNS. The port is the UDP port where the end-point is listening and the path defines the resource in that host. Finally, as in RESTful resources, the query in the form of "key=value" pairs enables the parametrization of the resource.

As indicated in [32] application designers are encouraged to make use of short, but descriptive URIs. Since the environments addressed by CoAP are usually constrained for bandwidth and energy, the trade-off between these two qualities should lean towards the shortness, without ignoring descriptiveness.

Resource discovery is related to how CoAP end-points are addressed and it is defined in [72]. Basically, the function of the discovery mechanism is to provide URIs ("links") for the resources offered, complemented by information describing the relationship between the resource description and each resource as well as other attributes.

7) Application layer protocols mapping: As CoAP implements a subset of the HTTP functionalities, there is a direct mapping between them. Besides CoAP can be easily mapped to the Session Initiation Protocol (SIP) [73] and the Extensible Messaging and Presence Protocol (XMPP) [74] as they have some similarity with HTTP.

- CoAP-HTTP Mapping enables CoAP clients to access resources on HTTP servers through an intermediary. This is initiated by including the Proxy-Uri Option with an "http" URI in a CoAP request to a CoAP-HTTP proxy, or by sending a CoAP request to a reverse proxy that maps CoAP to HTTP. The mapping is straightforward,

requiring the translation of the HTTP Status codes to the Response Codes in CoAP.

- HTTP-CoAP Mapping enables HTTP clients to access resources on CoAP servers through an intermediary. This is initiated by specifying a "coap" URI in the Request-Line of an HTTP request to an HTTPCoAP proxy, or by sending an HTTP request to a reverse proxy that maps HTTP to CoAP. The mapping requires a filtering of those codes, options, and methods that are not supported by CoAP.

VII. Concluding Remarks

A. Lessons Learned

In this paper, for a first time, a very promising wireless communication stack for the IoT has been deeply analyzed along with the underlying implications entailed with its adoption. The main properties of all the layers of this protocol architecture have been outlined in order to help readers gain fundamental lessons on the principles of such a technological solution, which really enables the IoT on a broader scale with respect to first generation ZigBee-like equipments. The key lessons this survey has intended to provide are not only limited to the accurate outline of new generation protocols deriving from the hard work of two specific standards bodies with 100+ contributors. The motivations behind the choice of focusing on this protocol stack are an integral part of this survey, since they shed some light on the limitations of communication stacks conceived so far for the IoT. Moreover, the paper helps the reader catch the reasons why this new proposal is quickly gaining consensus in *Important Industrial* applications. In fact, among the lessons we wish to leave to readers, there is the knowledge of authors about real industrial plants equipped with protocol stacks based on time synchronized channel hopping, which would never be possible to deploy using past generation communication technologies (including ZigBee) [33]- [39]. As a matter of fact, there are oil rigs off the Californian cost which use much of precisely this stack today, and tens of thousand networks have been deployed. In addition, there are smart city deployments worldwide with enormous amounts of nodes and mimicking the discussed stack in large parts. All these pragmatical lessons are also corroborated by academic studies (e.g., [75]–[77]) and open source developments [78] that fully confirm the effectiveness of the wireless communication stack taken as a subject of this survey.

B. Conclusions

Frost & Sullivan confirm that the industrial segment is the fastest growing market for sensors, corroborating the notion of an Internet of Important Things. The world market over all industry segments is estimated at some 36 billion Euros, showing the importance of that market but also underlying the need of getting its design right. It has to be noticed that *Important* stands for not only economical terms, but also for the implications of enriching Internet with the information of millions (or even billion in the coming future) of real world critical, unattended sensing and actuating objects. The latter are omnipresent and important *per se* as they inter-actuate physically not only with other smart objects, but also with human beings.

The aim of this paper has hence been to outline a technically viable communication architecture able to support the stringent energy and connectivity needs of the emerging IoT. To this end, we have seconded the community's view in the need of a standardized architecture which replaces proprietary approaches by means of a transparent end-to-end architecture.

From a PHY perspective, we found that the current IEEE 802.15.4-2006 PHY layer(s) suffice in terms of energy efficiency. In the end, it is the actual hardware implementation which dictates the exact current draws and thus the energy needed to transmit a given information bit. Current hardware implementations by e.g., Dust Networks are already very close to the limit of possibilities when it comes to short-range and medium-rate communication. Given that a large amount of IoT applications however will require only a few bits to be send, it may be advisable to commence looking into a standardized PHY layer which allows ultra low rate transmissions over very narrow frequency bands, with the obvious advantage of enormous link budgets and thus significantly enhanced ranges.

From a MAC perspective, we found that the current IEEE 802.15.4-2006 MAC layer(s) do not suffice which essentially triggered the existence of the IEEE 802.15.4e working group. We have presented in great details the MAC protocol of this new family which is tailored to industrial multihop/mesh applications under extreme fading and interference conditions. Channel hopping, albeit not novel in the wireless communications community, has been successfully applied to this embedded MAC; in addition to a rigid slot structure allowing for enormous energy savings since transmitter and receiver only wake up when truly needed. Some open issues pertain also to this family in that no optimal centralized or decentralized scheduling protocols have been put forward; nor is it entirely clear which approach is to be preferred.

From a networking perspective, the introduction of the IETF 6LoWPAN protocol family has been instrumental in connecting the low power radios to the Internet and the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity. Indeed, both WGs enabled IPv6 connectivity which is a great asset in guaranteeing global reachability, true scalability, reliable security and, since IP-enabled networks have been successfully engineered and deployed for decades now, the same engineering skills maintaining and troubleshooting these type of emerging networks; this is an enormous advantage over proprietary solutions. Various open issues pertain to the networking layer, however; examples are a suitable choice of the embodiment of the objective function, inclusion of trust, ability to run over any link layer protocol and not only those which have regular beacons, etc.

From an application perspective, the introduction of the IETF CoAP protocol family has been instrumental in ensuring that application layers and applications themselves do not need to be re-engineered to run over low-power embedded networks. Indeed, the current approach allows for the same design principles as currently used in general Internet application designs, thus acting as a true enabler for the IoT.

The introduced stack, in one form or another, is currently being evangelized by various industrial alliances. Of impor-

tance to the development of an IoT are arguably the Zigbee and IPSO alliances. Whilst the Zigbee alliance has traditionally been proponent of the IEEE 802.15.4-2006 PHY/MAC embodiments and an alliance-proprietary protocol stack (referred to as profile) on top, it is lately adopting above IETF recommendations at networking layers. The IPSO alliances, on the other hand, is very actively pushing for IPv6 enabled solutions to be adopted across the industry with the ultimate aim to facilitate true connectivity.

This paper has shed light onto some of the most recent and emergent design paradigms related to the communications stack of a viable Internet of Things. A lot of tweaking and optimizing is still ahead of us but we believe that the major bulk of design work is accomplished and that the current stack will have a significant impact in the take-off of the IoT.

ACKNOWLEDGEMENTS

This publication is based in parts on work performed in the framework of the projects VITRO-257245, EXALTED-258512, CALIPSO-288879, OUTSMART-285038 and SWAP-251557, which are partially funded by the European Community. The Authors would like to acknowledge the contributions by the various colleagues from these projects. This work was supported in part also by the project ERMES PON 01_03113/3, funded by the Italian MIUR, the funding of which is gratefully acknowledged. Xavier Vilajosana is funded by the Spanish Ministry of Education under Fullbright-BE grant (INF-2010-0319).

REFERENCES

[1] Auto-ID Labs, Available online: http://www.autoidlabs.org.

[2] *European Commission Communication on RFID*, European Union. COM(2007) 96., March 2007. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pd

[3] Council ot The European Union, *Transport, Telecommunications and Energy*, Available online: http://www.internet-of-things-research.eu/documents.htm, 27 November 2008.

[4] U.S. National Intelligence Council (NIC), *Global Trends 2025: A Transformed World*, NIC, Available online: www.dni.gov/nic/NI-2025-project.html, November 2008.

[5] Y. Huang and G. Li, "Descriptive Models for Internet of Things," in *International Conference on Intelligent Control anf Information Processing, ICICIP*, August 2010.

[6] INFSO D.4 Networked Enterprise RFID INFSO G.2 Micro Nanosystems in Co-operation with the Working Group RFID of the ETP EPOSS, "Internet of Things in 2020, Roadmap for the Future, Version 1.1," European Commission, Information Society and Media, Tech. Rep., May 2008.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, October 2010.

[8] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From Todays's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View," *IEEE Wirelesss Commun.*, vol. 17, no. 6, pp. 44 – 51, December 2010.

[9] L. Coetzee and J. Eksteen, "The Internet of Things - Promise for the Future? An Introduction," in *IST-Africa Conference Proceedings*, May 2011.

[10] E. Fleisch, "What is the Internet of Things? - An Economic Perspective," Auto-ID Labs, Tech. Rep., 2010.

[11] European Research Cluster on Internet of Things (IERC), *Internet of Things - Pan European Research and Innovation Vision*, IERC, Available online: http://www.internet-of-things-research.eu/documents.htm, October 2011.

[12] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of Wireless Sensor Networks towards the Internet of Things: A Survey," in *19th International Conference on Software, Telecommunications and Computer Networks, SoftCOM*, September 2011.

[13] J. P. Vasseur and A. Dunkels, *Interconnecting Smart Objects with IP: The Next Internet*. Morgan Kaufmann, 2010.

[14] O. Hersent, D. Boswarthick, and O. Elloumi, *The Internet of Things: Key Applications and Protocols*. Wiley, 2012.

[15] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, *HyperText Transfer Protocol – HTTP/1.1*, RFC 2616, Internet Engineering Task Force RFC 2616, June 1999. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2616.txt

[16] J. Postel, *Internet Protocol*, RFC 791, Internet Engineering Task Force RFC 791, September 1981.

[17] ——, *Transmission Control Protocol*, RFC 793, Internet Engineering Task Force RFC 793, September 1981. [Online]. Available: http://www.rfc-editor.org/rfc/rfc793.txt

[18] G. Lawton, "Machine-to-Machine Technology Gears up for Growth," *Computer*, vol. 37, no. 9, pp. 12 – 15, 2004.

[19] ETSI TS 102 689 v1.1.1, "Machine-to-Machine communications (M2M): M2M service requirements," August 2010.

[20] D. Lance, L. William, and S. Jonathan, "Channel-Specific Wireless Sensor Network Path Data," in *16th IEEE International Conference on Computer Communications and Networks (ICCCN)*, August 2007.

[21] R. Lacoss, *Distributed Sensor Networks*. MIT/LL (Massachusetts Institute of Technology/Lincoln Laboratory) , 1983.

[22] "MIT Lincoln Laboratory," Available online: http://www.ll.mit.edu/.

[23] J. M. Kahn, H. Katz, and K. S. J. Pister, "Next century challenges: Mobile Networking for Smart Dust," in *ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom*, August 1999.

[24] K. S. J. Pister, J. M. Kahn, and B. E. Boser, "Smart Dust: Wireless Networks of Millimeter-Scale Sensor Nodes," *Highlight Article in Electronics Research Laboratory - Research Summary*, 1999.

[25] IEEE std. 802.15.4, *Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks(LR-WPANs)*, Standard for Information Technology Std., September 2006.

[26] ZigBee Alliance, Available online: www.zigbee.org.

[27] D. Networks, Available online: www.dustnetworks.com.

[28] K. S. J. Pister and L. Doherty, "TSMP: Time Synchronized Mesh Protocol," in *International Symposium on Distributed Sensor Networks, DSN*, November 2008.

[29] HART Communication Protocol and Fundation , Available online: http://www.hartcomm2.org.

[30] N. Kushalnagar, G. Montenegro, and C. Schumacher, *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, RFC 4919, Internet Engineering Task Force RFC 4919, August 2007.

[31] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. P. Vasseur, and R. Alexander, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, RFC 6550, Internet Engineering Task Force RFC 6550, March 2012.

[32] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, *Constrained Application Protocol (CoAP)*, IETF CoRE Working Group, February 2011.

[33] Endress+Hauser, "First Applications of WirelessHART Networks in the Steel Industry," Endress+Hauser, Tech. Rep., August 2010.

[34] ——, "Monitoring System of the Farm Storage Tank at Grupo Petroqumico Beta (GPB), Coatzacoalcos, Mexico," Endress+Hauser, Tech. Rep., July 2012.

[35] Control Global, "How Wireless Speeds Innovation at BP - The Strategic Role of Wireless in Refining Automation Technology," Control Global, Tech. Rep., November 2008.

[36] Endress+Hauser, "WirelessHART at BASF - Challenging Applications in the Production of High-Quality Catalysts in De Meern, the Netherlands," Endress+Hauser, Tech. Rep., April 2011.

[37] I. Vilajosana, J. Llosa, M. Martinez, and J. C. Pacho, "Wireless Sensors Helps Monitoring one of World Most Advanced Load and Unload Harbor Terminals," Worldsensing. Loadsensing product website. White Paper. Available at http://www.loadsensing.com/index.php/projects, April 2012.

[38] Control Global, "Far From Quiet on the Wireless Front - From PowerGen to Petrochem, Fiber Production to Gas Distribution, Wireless Field Networks Continue to Prove their Process Automation Mettle," Control Global, Tech. Rep., March 2009.

[39] Linear Technology, "Wireless Sensor Networks Make It Possible to Predict Precious Water Supplies," Linear Technology, Tech. Rep., 2012.

[40] *802.15.4e-2012: IEEE Standard for Local and Metropolitan Area Networks – Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer*, Institute of Electrical and Electronics Engineers Std., 16 April 2012.

[41] A. Tinka, T. Watteyne, and K. S. J. Pister, "A Decentralized Scheduling Algorithm for Time Synchronized Channel Hopping," *Ad Hoc Networks*, vol. 49, no. 4, pp. 201–216, 2010.

[42] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*, RFC 2205, Internet Engineering Task Force RFC 2205, September 1997.

[43] IETF, "MPLS-TP Internet Drafts and RFCs."

[44] T. Watteyne, A. Mehta, and K. S. J. Pister, "Reliability Through Frequency Diversity: Why Channel Hopping Makes Sense," in *Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, PE-WASUN*, October 2009.

[45] B. Kerkez, T. Watteyne, and M. Magliocco, "Fleasibility Analysis of Controller Design for Adaptive Channel Hopping," in *ICST International Workshop on Performance Methodologies and Tools for Wireless Sensor Networks, WSNPERF*, October 2009.

[46] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, ser. Wiley Series on Communications Networking & Distributed Systems. John Wiley & Sons, 2010.

[47] J. W. Hui and D. E. Culler, "Extending IP to Low-Power, Wireless Personal Area Networks," *IEEE Internet Computing*, vol. 12, no. 4, pp. 37 – 45, July-August 2008.

[48] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture," Internet Protocol for Smart Object (IPSO) Alliance, White Paper, April 2009.

[49] J. W. Hui and D. E. Culler, "IPv6 in Low-Power Wireless Networks," *Proc. IEEE*, vol. 98, no. 11, pp. 1865 – 1878, November 2010.

[50] K. Jeonggil, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, and P. Levis, "Connecting Low-power and Lossy Networks to the Internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 96 – 101, April 2011.

[51] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, RFC 4944, Internet Engineering Task Force RFC 4944, September 2007.

[52] J. Hui and P. Thubert, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*, RFC 6282, Internet Engineering Task Force RFC 6282, September 2011.

[53] M. Crawford, *Transmission of IPv6 Packets over Ethernet Networks*, RFC 2464, Internet Engineering Task Force RFC 2464, December 1998.

[54] P. Karn, C. Bormann, G. Fairhurst, D. Grossman, R. Ludwig, J.Mahdavi, G. Montenegro, J. Touch, and L. Wood, *Advice for Internet Subnetwork Designers*, RFC 3819, Internet Engineering Task Force RFC 3819, July 2004.

[55] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet, "RPL: The IP routing protocol designed for low power and lossy netwroks," Internet Protocol for Smart Object (IPSO) Alliance, White Paper, April 2011.

[56] J. Martocci, *Building Automation Routing Requirements in Low-Power and Lossy Networks*, RFC 5867, Internet Engineering Task Force RFC 5867, June 2010.

[57] A. Brandt, J. Buron, and G. Porcu, *Home Automation Routing Requirements in Low-Power and Lossy Networks*, RFC 5826, Internet Engineering Task Force RFC 5826, April 2010.

[58] K. S. J. Pister and P. Thubert, *Industrial Routing Requirements in Low-Power and Lossy Networks*, RFC 5673, Internet Engineering Task Force RFC 5673, October 2009.

[59] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, *Routing Requirements for Urban Low-Power and Lossy Networks*, RFC 5548, Internet Engineering Task Force RFC 5548, May 2009.

[60] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi, "The Deployment of a Smart Monitoring System Using Wireless Sensor and Actuator Networks," in *First IEEE International Smart Grid Communications Conference, SmartGridComm*, October 2010.

[61] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, *The Trickle Algorithm*, RFC 6206, Internet Engineering Task Force RFC 6206, March 2011.

[62] A. Conta, S. Deering, and M. Gupta, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version6 (IPv6) Specification*, RFC 4443, Internet Engineering Task Force RFC 4443, March 2006.

[63] J. P. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthe, *Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks*, RFC 6552, Internet Engineering Task Force RFC 6552, March 2012.

[64] O. Gnawali and P. Levis, *The Minimum Rank with Hysteresis Objective Function*, RFC 6719, Internet Engineering Task Force RFC 6719, September 2012.

[65] G. Fairhurst and L. Wood, *Advice to Link Designers on Link Automatic Repeat reQuest (ARQ)*, RFC 3366, Internet Engineering Task Force RFC 3366, August 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3366.txt

[66] A. Dunkels, T. Voigt, and J. Alonso, "Making TCP/IP Viable for Wireless Sensor Networks," in *First European Workshop on Wireless Sensor Networks (EWSN 2004), work-in-progres ssession*, January 2004. [Online]. Available: http://www.sics.se/~adam/ewsn2004.pdf

[67] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, *TCP Selective Acknowledgement Options*, RFC 2018, Internet Engineering Task Force RFC 2018, October 1996. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2018.txt

[68] J. Postel, *User Datagram Protocol*, RFC 768, Internet Engineering Task Force RFC 768, August 1980. [Online]. Available: http://www.rfc-editor.org/rfc/rfc768.txt

[69] Constrained RESTful Environments (core). IETF Working Group, Available online: http://www.ietf.org/dyn/wg/charter/core-charter.html.

[70] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.

[71] T. Berners-Lee, R. Fielding, and L. Masinter, *Uniform Resource Identifier (URI): Generic Syntax*, RFC 3986, Internet Engineering Task Force RFC 3986, January 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3986.txt

[72] Z. Shelby, "CoRE Link Format, draft-ietf-core-link-format," IETF, Internet Draft, June 2011. [Online]. Available: http://tools.ietf.org/id/draft-ietf-core-link-format-06.txt

[73] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, *SIP: Session Initiation Protocol*, RFC 3261, Internet Engineering Task Force RFC 3261, June 2002. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3261.txt

[74] P. Saint-Andre, *Extensible Messaging and Presence Protocol (XMPP): Core*, RFC 3920, Internet Engineering Task Force RFC 3920, October 2004. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3920.txt

[75] N. Accettura, M. R. Palattella, M. Dohler, L. A. Grieco, and G. Boggia, "Standardized Power-Efficient & Internet-Enabled Communication Stack for Capillary M2M Networks," in *IEEE Wirelesss Commun. and Networking Conference, WCNC - Workshop on Internet of Things Enabling Technologies: "Embracing the M2M Communications and Beyond"*, April 2012.

[76] M. R. Palattella, N. Accettura, M. Dohler, L. A. Grieco, and G. Boggia, "Traffic Aware Scheduling Algorithm for Reliable Low-Power Multi-Hop IEEE 802.15.4e Networks," in *23rd IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, September 2012.

[77] ——, "Traffic-Aware Time-Critical Scheduling in Heavily Duty-Cycled IEEE 802.15.4e for an Industrial IoT," in *IEEE Sensors*, October 2012.

[78] T. Watteyne, X. Vilajosana, B. Kerkez, F. Chraim, K. Weekly, Q. Wang, S. D. Glaser, and K. S. J. Pister, "OpenWSN: a Standards-Based Low-Power Wireless Development Environment," *Trans. Emerging Telecommun. Technol.*, vol. 23, no. 5, pp. 480–493, 2012.

Maria Rita Palattella (S'08-M'11) is currently a Research Associate at the Interdisciplinary centre for Security, Reliability and Trust (SnT), part of the Universtity of Luxembourg. From July 2011 to October 2011 she was a Post-Doc fellow at Telecom ParisTech in Paris (France), working on multi-dimensional nested-lattice Wyner-Ziv coding for the FP7 project SmartEN. She obtained her PhD in Electronics Engineering from "Scuola Interpolitecnica di Dottorato" (SIPD) and "Politecnico di Bari," Italy, in February 2011. Between April 2009 and July 2010 she joined the Centre Tecnologic de Telecomunicacions de Catalunya (CTTC) in Barcelona as a visitor Ph.D. student. From June 2009 to January 2010 she also worked in collaboration with the Department of Information and Communication Technologies of Universitat Pompeu Fabra (UPF) in Barcelona. She received her Bachelor Degree in Telecommunication Engineering in 2004 and her Master's Degree in Telecommunication Engineering in 2007, both with honor, from "Politecnico di Bari," Italy. Between May 2007 and December 2007, she was a Research Assistant at the "Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari" (DEE) at Polytechnic of Bari. She received a number of research grants including: a CNIT grant on the project SITEMAT in June 2007 and a SIPD grant in the area "Information and Communication Technologies" (ICT) in 2008. Her main research interests involve the study of wireless sensor networks (WSNs), power-efficient protocols and algorithms for data collection and management in WSNs, MAC protocols and scheduling algorithms for WSNs and embedded systems (i.e., IEEE 802.15.4, IEEE 802.15.4e), Internet of Things standardization.

Nicola Accettura is currently a PhD student in Electronics Engineering at "Politecnico di Bari," Bari, Italy. He has also been enrolled in "Scuola Intepolitecnica di Dottorato" (SIPD) since February 2011. His main research interests are in Wireless Sensor Networks architectures. He has been visiting student at the MAESTRO team of INRIA Sophia-Antipolis (France), focusing on size estimation models for communication networks. He obtained his Bachelor Degree in Computer Systems Engineering in 2004 and his Master's Degree in Telecommunications Engineering in 2007, both from Politecnico di Bari. He received a grant from TELECOM Italia for attending the professional master "Networking for Enterprises & Carriers" at "Scuola Superiore Guglielmo Reiss Romoli"in L'Aquila (Italy) gaining his CCNA, CCNP and CCIP Cisco certifications.

Thomas Watteyne (S'05-M'08) is a Senior Networking Design Engineer at Dust Networks/Linear Technology. Between 2008 and 2010, we worked as a postdoctoral researcher at the Berkeley Sensor & Actuator Center, University of California in Berkeley, in Prof. Kristofer S.J. Pister's team. He is the coordinator of OpenWSN project, an open-source initiative to promote the use of fully standards-based protocol stacks in IoT applications. From October 2005 to September 2008, he was a research engineer at France Telecom R&D/Orange Labs working on energy efficiency and self-organizing for wireless multihop networks, together with the CITI Laboratory, France. At that time, he has also been a member of the Student Activity and Award and Recognitions Committees, while serving as the Electronic Communications Coordinator of IEEE Region 8 (Europe, Africa, Middle-East and Russia). He obtained his PhD in Computer Science (2008) and MSc in Telecommunications (2005) from INSA Lyon, France.

Xavier Vilajosana is an associate professor at the Universitat Oberta de Catalunya (UOC) in the area of computer networks and distributed systems. He is also Chief Innovations Officer and co-founder of Worlsensing. On early 2009 Xavier presented his PhD in Computer Sciences and now he is currently a visiting professor at UC Berkeley in California. During the last years of research he has acquired extensive experiences in Distributed Systems, Wireless Ad Hoc networks, Delay Tolerant networks and Cloud Computing. In addition during 2008, Xavier was visiting researcher of France Telecom, Paris. Amongst others, today, he is actively contributing to the IETF 6LowApp, ROLL and DASH7 working groups, and is a member of the editorial board of various prestigious journals and conferences. At UC Berkeley, Xavier is member of the OpenWSN core team, an open-source protocol stack for embedded devices that implements the main IoT protocols (i.e. IEEE802.15.4e, IETF RPL and IETF CoAP). Xavier's research interests include low power communication protocols, standardization, routing, scheduling and optimization problems in distributed systems.

Luigi Alfredo Grieco (S'02-M'04-SM'12) received the Dr. Eng. degree (with honors) in Electronics Engineering from "Politecnico di Bari," Bari, Italy, in October 1999 and the Ph.D. degree in information engineering from "Universitá di Lecce," Lecce, Italy, on December 2003. During 2004, he worked as research assistant at the Telematics lab. – "Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari". Since January 2005, he has been an Assistant Professor in telecommunications with the "Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari". From March to June 2009, he has been a Visiting Researcher with INRIA (Planete Project, Sophia Antipolis, France), working on the topics of Internet Measurements and Scheduling in WiMax Networks. He has authored more than 100 scientific papers published in international journals and conference proceedings. His main research interests include congestion control in packet-switching networks, quality of service in wireless networks, industrial protocol stacks, Internet multimedia applications, Internet measurements, content centric networking, and real-time video processing using cellular nonlinear networks. He currently serves as Associate Editor for the IEEE Transactions on Vehicular Technology.

Gennaro Boggia (S'99-M'01-SM'09) received, with honors, the Dr. Eng. Degree in Electronics Engineering in July 1997 and the Ph.D. degree in Electronics Engineering in March 2001, both from the "Politecnico di Bari", Italy. Since September 2002, he has been with the department of "Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari", Italy, where he is currently Associate Professor. From May 1999 to December 1999, he was visiting researcher at the "TILab", TelecomItalia Lab (formerly CSELT, Centro Studi e Laboratori Telecomunicazioni), Italy, where he was involved in the study of the Core Network for the evolution of 3G cellular systems. In 2007, he was visiting researcher at FTW (Vienna), where he was involved in activities on passive and active traffic monitoring in 3G networks. He has authored or co-authored more than 90 papers in international journals or conference proceedings. His research interests span the fields of Wireless Networking, Cellular Communication, Protocol stacks for industrial applications and smart grids, Internet measurements, Network Performance Evaluation.

Mischa Dohler (S'01-M'03-SM'07) is now leading the Intelligent Energy [IQe] group at CTTC in Barcelona, with focus on Smart Grids and Green Radios. He is working on machine-to-machine, wireless sensor, femto, cooperative, cognitive and docitive networks. In the framework of the Mobile VCE, he has pioneered research on distributed cooperative space-time encoded communication systems, dating back to December 1999. He has published more than 150 technical journal and conference papers at a citation h-index of 30 and citation g-index of 64, holds a dozen patents, authored, co-edited and contributed to 19 books, has given more than 30 international short-courses, and participated in ETSI, IETF and other standardisation activities. He has been TPC member and co-chair of various conferences, such as technical chair of IEEE PIMRC 2008 held in Cannes, France. He is Editor-in-Chief of ETT and is/has been holding various editorial positions for numerous IEEE and non-IEEE journals. He is Senior Member of the IEEE and Distinguished Lecturer of IEEE ComSoc. He had press coverage by BBC, Wall Street Journal, among others. He is fluent in 6 languages. From June 2005 to February 2008, he has been Senior Research Expert in the R&D division of France Telecom, France. From September 2003 to June 2005, he has been lecturer at King's College London, UK. At that time, he has also been London Technology Network Business Fellow receiving Anglo-Saxon business training, as well as Student Representative of the IEEE UKRI Section and member of the Student Activity Committee of IEEE Region 8 (Europe, Africa, Middle-East and Russia). He obtained his PhD in Telecommunications from King's College London, UK, in 2003, his Diploma in Electrical Engineering from Dresden University of Technology, Germany, in 2000, and his MSc degree in Telecommunications from King's College London, UK, in 1999. Prior to Telecommunications, he studied Physics in Moscow. He has won various competitions in Mathematics and Physics, and participated in the 3rd round of the International Physics Olympics for Germany.