Optimal and Secure Protocols in the IETF 6TiSCH communication stack

Nicola Accettura, *Member, IEEE* and Giuseppe Piro, *Member, IEEE*
Department of Electrical and Information Engineering (DEI)
Politecnico di Bari, Italy
Email: {nicola.accettura,giuseppe.piro}@poliba.it

Abstract*—In order to cope with large multi-hop resource-constrained and IPv6-compliant Low-power and Lossy Networks (LLNs), based on IEEE802.15.4 radios, novel protocols have been standardized within the IETF. More recently, the IEEE802.15.4e Timeslotted Channel Hopping (TSCH) MAC amendment has been designed to meet the requirements of industrial applications, by reducing idle-listening and improving reliability in the presence of narrow-band interference and multi-path fading. To integrate this new powerful MAC within the framework of IPv6-based LLN protocols, a new IETF working group has been defined, namely "IPv6 over the TSCH mode of IEEE 802.15.4e" (6TiSCH). In a timely way, this paper presents our contribution to the early standardization efforts required to define (i) an optimal distributed scheduling technique able to allocate resources between any couple of neighbors, while seconding the minimal bandwidth requirements and avoiding collisions, and (ii) a scalable framework supporting setting-up and maintenance of secured domains. Supported by the scientific interest to this reasearch topic, we strongly believe that the 6TiSCH stack will be a viable solution for a wide gamut of optimal and secured IoT applications in industrial environments.

I. Introduction

The notion of "Internet of Things" (IoT) was early conceived in 1999 by Kevin Ashton [1] to mean the binding of Radio Frequency Identifiers information to the Internet. Soon, this notion became a technological paradigm enabling advanced and desired services, including monitoring and control in industrial plants. In a more recent form, the IoT is supposed to be capable of managing a potentially very large number of smart wireless devices forming a capillary networking infrastructure that can be connected to the Internet [2]. Although this opportunity has been recognized as a key factor for future economic growth and sustainability of governments and markets [3], there are still some technological issues hindering a pervasive IoT deployment.

First of all, IoT devices are usually energy-constrained, since they are powered by batteries or through energy-harvesting, while energy consumption is mainly due to radio communications. As a counterpart, energy is wasted by transmission of unneeded data, protocol overhead, and non-optimized communication patterns. In this sense, the scientific community identified the development of energy-saving communication protocols for an industrial IoT as one of the hottest research topics [4], since the main challenge is to provide the highest level of reliability to industrial applications working over inherently unreliable wireless technologies.

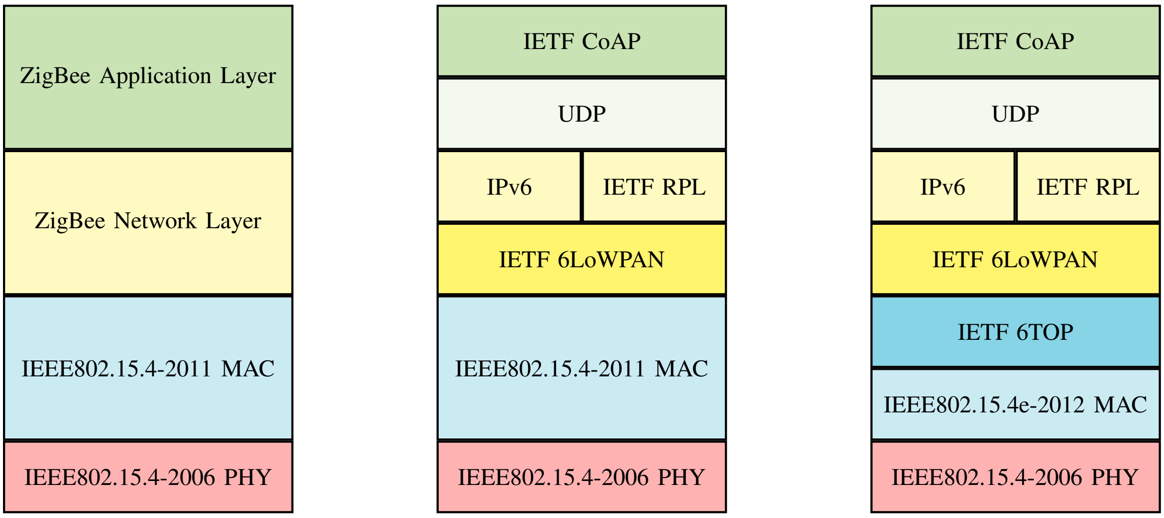
At the same time, the verbosity of meta-data and headers and the requirement for reliability through packet acknowledgements make HTTP and TCP not optimized for very low-power communication. However, the need of bidirectional and facilitated communications between objects would be satisfied by an IP-enabled communication stack [5], which in turn calls for standardized communication approaches [6].

In the recent past, the ZigBee Alliance [7] introduced a communication stack able to form wireless sensor networks meeting the typical requirements of low data-rate lossy links interconnecting low-power devices. In details, the IEEE802.15.4 standard [8] for low-rate communications in star topologies was adopted to define the physical and Medium Access Control (MAC) layers. Instead, the upper layers were conceived by the Alliance itself, with the aim of enlarging the network in a multi-hop fashion and guaranteeing the device reachability (see Fig. 1a).

Nonetheless, ZigBee was not able to easily plug that kind of networks into the IP-based Internet, thus impeding a concrete IoT. As a matter of fact, the IETF standardization body recently proposed new protocols supporting IPv6 communications in IoT-compliant multi-hop Low-power and Lossy Networks (LLNs). Specifically, three different IETF working groups (WGs) [9], [10], [11] have been involved for defining three layers of such stack.These protocols, together with IPv6 and UDP, are supposed to work in all IEEE802.15.4 based networks, and have been included in the so-called ZigBeeIP stack [12], as pictured in Fig. 1b.

Furthermore, it was quickly recognized that the single-channel nature of the IEEE802.15.4 MAC causes its reliability to be unpredictable and that the CSMA/CA access technique introduces radio overhearing and idle-listening in multi-hop settings [4]. The first milestone in the definition of a MAC protocol able to mitigate multipath fading and external interference was put by the Time Synchronized Mesh Protocol (TSMP) [13], which became the de-facto standard for reliable low-power wireless in industrial application. In 2011, the IEEE standardization body integrated the foundation of TSMP, i.e., Timeslotted Channel Hopping (TSCH), into the IEEE802.15.4e MAC amendment [14].

Although, the joint standardization efforts put in place by IETF and IEEE have led to an emergent IoT communication



(a) ZigBee stack.

(b) ZigBeeIP stack.

(c) 6TiSCH stack.

Fig. 1: Communication stacks for the Internet of Things.

stack for industrial applications [4], there are still some pendant issues to be faced for a viable IoT. Indeed, the IEEE802.15.4e standard is based on both Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) and allows devices to communicate by following a common schedule. However, it does not define the policies to build and maintain such communication schedule. In addition, mechanisms for protecting such networks by security threats are also required. With the aim of facing these issues, we are currently contributing to the standardization efforts of the IETF "IPv6 over the TSCH mode of IEEE 802.15.4e" Working Group (6TiSCH WG) [15]. In details, the 6TiSCH WG has been recently setup to introduce a new intermediate layer, namely the 6TiSCH Operation Sublayer (6TOP) [16] (see Fig. 1c).

From these premises, the present paper aims to shed some light on the main features of this new communication stack. Indeed, Sec. II summarizes the recently standardized IETF protocols for an IoT-compliant communication stack, pointing out the main features preparatory for the discussion that follows. Then, by introducing the IEEE802.15.4e TSCH MAC protocol, Sec. III explains what the 6TiSCH WG is achieving for a correct operation of the upper layers over TSCH, with a major focus on our contribution to the definition of signalling strategies for resource scheduling and of a security framework for lightly exchanging keying material. Finally, Sec. IV draws conclusions and envisages future works.

II. IETF standards for IoT-compliant networks

The Internet Engineering Task Force (IETF) has been dedicating many efforts to the definition of standard protocols for IoT networks. Specifically, as shown in Fig. 1b, different layers of the TCP/IP stack have been interested from this standardization approach. To the aim of supporting IP-based communications and easily plugging wireless sensor networks into the Internet, it was early recognized that: (i) an adaptation layer was required to fit IPv6 packets in IEEE802.15.4 frames, through header compression mechanisms; (ii) a routing protocol able to preserve the battery lifetime while satisfying the typical requirements of multihop LLNs was needed, since the same tradeoff cannot be reached by well-known protocols for ad-hoc wireless networks (e.g., OLSR and AODV) [17]; (iii) a simplified version of HTTP for constrained environment was highly desired. As a consequence, three working group were created to address these issues, namely 6LOWPAN [11], ROLL [10] and CORE [9]. The remaining part of these section is dedicated to briefly describe the main outcomes of these working groups.

A. *IETF 6LoWPAN*

The IETF IPv6 over LOw power Wireless Personal Area Networks WG (6LOWPAN WG) [11] has recently standardized 6LoWPAN [18][19] as an adaptation layer able to "Internet-connect" multi-hop wireless networks based on low-power link-layer communication technologies.

Among others, the IEEE802.15.4 physical layer allows a maximum frame length equal to 127 bytes. Being the IPv6 default minimum MTU size equal to 1280 bytes, a no-fragmented IPv6 packet could be too large to fit in an IEEE802.15.4 frame. Moreover, the overhead due to the 40 bytes long IPv6 header would waste the scarce bandwidth available at the PHY layer. As we can see, 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. In this sense, 6LoWPAN provides some interesting features that allows IEEE802.15.4 smart devices to be equipped with IPv6 connectivity, thus solving a number of issues, i.e., handling network auto-configuration, supporting applications with a high number of devices (and of addresses), easing the internet-working with other IP-based infrastructures as in the IoT vision.

In details, 6LoWPAN is an intermediate layer between IPv6 and IEEE 802.15.4 MAC levels [20], which enables link-layer forwarding and fragmentation; it is also able to compress IPv6 header and *Next Headers*, by suppressing redundant information that can be inferred from other layers in the communication stack [19]. Further issues envisaged by 6LoWPAN encompass the auto-configuration of IPv6 addresses, the reduction of routing and management overhead, the adoption of lightweight application protocols (or novel data encoding techniques), and the support for security mechanisms [21].

B. IETF RPL

The need for a routing protocol able to manage IoT-compliant multi-hop LLNs has triggered the interest and the work of the IETF Routing Over Low power and Lossy networks WG (ROLL WG) [10]. The ROLL main outcome is the IPv6 Routing Protocol for LLNs (RPL), recently standardized in RFC 6550 [22]. RPL is a gradient-based distance-vector routing protocol that can ease the formation and the management of networks based on short-range low-power links. RPL can support a wide variety of link layers, including ones that are constrained, potentially lossy, or typically utilized in conjunction with host or router devices with very limited resources [22]. More specifically, RPL has been designed to fulfill typical requirements of a LLN in building/home automation, industrial environments, and urban applications [4]. Furthermore, RPL strictly adheres to the IPv6 architecture: a gradient is set up and maintained using signaling messages carried as options of IPv6 Router Advertisements.

In the most typical RPL scenarios, few LLN sinks coordinate a large set of smart wireless devices through multi-hop paths. In details, RPL organizes a network topology as a Directed Acyclic Graph (DAG) that is partitioned into one or more Destination Oriented DAGs (DODAGs), each one rooted at an LLN sink. A DAG is built according to path costs, which in turn represent a combination of link and node metrics/constraints (e.g., available energy resources, workload, throughput, latency, reliability). More specifically, RPL minimizes the costs to reach any LLN sink (from any device) by means of an Objective Function, which can be defined in many ways to grant for a very high flexibility with respect to the operating scenario. To be useful in a wide range of LLN application domains, the RPL protocol specification has been explicitly decoupled from the definition of objective functions [23], [24] and routing metrics [25].

RPL topologies are constructed by means of an information dissemination mechanism, enabling minimal configuration in the devices and allowing them to operate mostly autonomously. In this sense, to establish paths towards the roots, each RPL node periodically and link-locally multicasts DAG Information Option (DIO) messages, containing information about its position with respect to the LLN sink (i.e., the *rank*), the objective function, IDs, and so forth. To avoid redundancies and to control the signaling overhead, the *trickle* algorithm 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. In addition, RPL allows information to be propagated downwards along the DODAGs, using the Destination Advertisement Object for handling downward routes.

Finally, RPL manages security at the networking layer. Indeed, a RPL device may operate in three security modes: (i) *unsecured*, employing no security mechanism; (ii) *pre-installed*, assuming that a node has pre-installed keys used to protect RPL messages; and (iii) *authenticated*, with nodes retrieving keys from an authentication authority. Generally speaking, for both *pre-installed* and *authenticated* configurations data confidentiality and message integrity are offered through the AES-128 encryption scheme. In this context, the ROLL WG is further investigating additional countermeasures against threats and attacks that could compromise security at the networking layer [26].

C. IETF CoAP

In the IoT vision, LLN devices are supposed to communicate and to be queried through application layer protocols, e.g., HTTP. However, a straightforward implementation of RESTful architectures such as the client/server model defined by HTTP is not possible and an adaptation is required [4].

In this context, the IETF Constrained RESTful Environments Working Group (CORE WG) [9] has defined the Constrained Application Protocol (CoAP) [27], 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. It has to be noted that the CORE WG has been defining a subset of the RESTful specification, which will be interoperable with HTTP but also adapted to constrained environments. Unlike HTTP, CoAP is an asynchronous request/response protocol adopting UDP at the transport layer, with endpoints acting as both clients and servers. Structurally, CoAP is divided in two sublayers, a *message layer* guaranteeing reliability and sequencing and a *request/response layer* able to map requests to responses and their semantics.

With the aim of securing the application layer through protection of CoAP messages, the CORE WG has proposed also a framework based on the DTLS protocol [28]. In particular, four security modes are defined: *NoSec Mode*, which does not provide any security feature, *PreSharedKey Mode* and *RawPublicKey Mode*, which impose the initialization of a DTLS session by using a pre-loaded key-list already set into devices, and *Certificate Mode*, which exploits X.509 certificates validated by an Authority to perform both authentication and key negotiation mechanisms.

III. IPv6 over the TSCH mode of IEEE 802.15.4e

When integrated with some routing strategies for extending wireless sensor networks in a multi-hop fashion, the existing IEEE802.15.4 MAC [8] standard results inefficient in terms of energy consumption, due to radio overhearing and, in general, to the lack of some technique able to duty-cycle the radio activity. In addition, the IEEE802.15.4 single-channel CSMA/CA access technique performs worse in multi-hop topologies, because of the hidden and exposed terminal problems, thus further jeopardizing the applications in terms of reliability and delays.

To face these issues, the IEEE802.15.4e amendment [14] has been released on April 2012 with the aim of redesigning the existing IEEE802.15.4 MAC standard toward a low-power multi-hop MAC, better suitable for the emerging needs of IoT and embedded industrial applications [5], [29]. In detail, the Timeslotted Channel Hopping (TSCH) protocol has been proposed to address process automation facilities for oil and gas industry, chemical products, water/waste water treatments, green energy production, climate control. The smart devices in a IEEE802.15.4e TSCH network communicate by following a TDMA schedule. However, the portion of the ZigBeeIP stack defined by the IETF, as surveyed in the previous section, cannot be integrated "as is" with TSCH. After introducing the main features of the IEEE802.15.4e TSCH MAC protocol and pointing out some implementation details left open in the standard, we present the standardization activities started by the recently formed IETF "IPv6 over the TSCH mode of IEEE 802.15.4e" working group (6TiSCH WG) [15] and our contribution in the definition of scheduling and security techniques for TSCH enabled LLNs.

A. IEEE802.15.4e TSCH

The TSCH protocol combines TDMA with an FDMA scheme. In details, all nodes in the network are synchronized using a slotframe structure, which is a group of timeslots repeating over time (i.e., TDMA). The timeslot length is enough for allowing a dedicated and acknowledged (hence reliable) transmission between a sender device and a receiver one. Furthermore, the availability of multiple channel offsets permits to increase the network capacity, since many couples of devices can exchange their frames in the same timeslot, using different channel offsets (i.e., FDMA). The slotframe structure can be thought as a matrix, with each element, i.e., a *cell*, being identified by the timeslot position in the slotframe itself and by a channel offset. Actually, a cell can be shared among many devices (communicating with contention-based schemes).

Although a cell in the slotframe structure is strictly identified by a channel offset, the mapped physical frequency changes slotframe by slotframe according to a translation function. In this sense, channel hopping implies frequency diversity that mitigates the effects of narrow-band interference and multi-path fading. Besides, some physical channels can be blacklisted for coexistence purposes.

Each device in a TSCH network follows a *schedule* which specifies how to act in each timeslot (i.e., transmit, receive, or turn the radio off). Furthermore, for each active slots, the schedule indicates the couple of communicating neighbors and the channel offset to use as well. The allocation can be programmed such that the predictable transmission pattern matches the traffic. This avoids idle listening, and extends battery lifetime for constrained devices.

While IEEE802.15.4e defines the mechanisms for a TSCH mote to communicate, it does not define the policies to build and maintain the communication schedule, match that schedule to the multi-hop paths maintained by RPL, adapt the resources allocated between neighbor nodes to the data traffic flows. Moreover, there is no specification on how to enforce a differentiated treatment for data generated at the application layer and signaling messages needed by 6LoWPAN and RPL to discover neighbors, to react to topology changes, or to self-configure IP addresses [30].

Finally, although the IEEE802.15.4 standard and its IEEE802.15.4e amendment describe procedures and parameters to be adopted for handling secured MAC frames with a high level of accuracy, they do not specify how to manage the initialization of a secure IEEE 802.15.4 domain, as well as to negotiate and/or exchange encryption keys [31].

B. 6TiSCH objectives

To solve the pendant issues inherent to IEEE802.15.4e, thus permitting a viable integration in multi-hop IPv6-enabled networks organized by RPL, the IETF 6TiSCH working group has been recently built and it started producing several Internet Drafts, each one addressing specific purposes. In general, a new set of primitives has been being defined for a minimal implementation of TSCH-compliant networks [32] and more complex architectures as well [33]. The main outcome of the standardization efforts of the 6TiSCH WG will be the 6top layer [16], which exploits the IEEE802.15.4 frame header to include further information to be exchanged in the network.

Specifically, the sloframe structure will provision some signalling timeslots, used as shared cells for exchanging minimal information for the network set up. In this sense, Enhanced Beacons will be transmitted in this portion of the slotframe by devices that already joined the network, in order to allow new devices to hear them and possibly join the network. The same timeslotted space in the slotframe will be used for signalling messages related to upper layer protocols.

Given the availability of some field extensions in the IEEE802.15.4 frame header format, the 6TiSCH WG is defining new Information Elements that can be exchanged between one-hop neighbors or forwarded for communication between far devices, thus allowing several optimizations. In this sense, 6TOP will be the main instrument for translating signalling commands coming from all the layers in the stack in link-layer exchanged messages.

1) Optimal resource scheduling techniques: As written before, the lack of a scheduling technique in the IEEE802.15.4e TSCH MAC is one of the hottest topics in the 6TiSCH WG. As matter of fact, resource scheduling algorithms can be conceived according to different requirements. Generally speaking, these algorithms can be grouped according to the presence/lack of a central *manager* device. In a *centralized* approach, a specific manager is responsible for building and maintaining the network schedule: after having gathered information about the neighborhood and, possibly, the bandwidth requirements of each device, the manager figures out how the network topology is built and assigns cells to communicating neighbors; once this schedule is built, the manager informs each node about the assigned specific schedule. Actually, a topology change can imply a partial or total recomputation of the schedule (with a consequent additional signaling overhead). Instead, a *decentralized* approach bounds the signalling overhead through aggregation of the information propagated towards the manager and by allowing devices to locally adapt the minimal scheduling information injected by the manager in the network to the requirements of their own neighbors. Finally, in a *distributed* approach, devices decide locally how to schedule cells in agreement with neighbor requirements. This approach is more fitting to mobile networks or to networks with many gateways, although it is prone to packet collisions.

Several techniques are available in the scientific literature, ranging from centralized techniques [34] to decentralized/distributed ones [35], [36]. In the 6TiSCH architecture, a centralized scheduling algorithm could work at the application layer in conjunction with the Path Computation Element (PCE) Communication Protocol (PCEP) [37], designed specifically for communications between a Path Computation Client (PCC) and a PCE. Being a PCEP session established only over a TCP connection, the 6TiSCH WG is working on defining how a PCE can manage the network schedule through CoAP communications [33].

To permit also decentralized and distributed scheduling approaches in 6TiSCH environment, we are currently involved in designing an optimal distributed scheduling technique, namely On-The-Fly (OTF) scheduling [38]. OTF will be able to dynamically allocate TSCH cells between any couple of neighbours, while seconding the minimal bandwidth requirements and avoiding collisions as much as possible. Given that the instantaneous routing pattern organized by RPL is a tree rooted at an LLN sink, an intermediate device in the underlying routing graph, i.e., having a selected parent device and some children nodes, should receive and forward the traffic delivered by its children toward the sink and send its own traffic to the parent. In other words, the links involved (i.e., that between the considered device and its parent, and those between the device and each of its children) have different bandwidth requirements, hence a different number of cells to be allocated in the slotframe structure. This approach has been recognized to be valid, according to previous works [34], [35], and it is being employed in the definition of OTF policies. In addition, OTF will provision mechanisms to adapt the number of cells allocated, depending on the changes in the bandwidth requirements. Finally, it has to be noted that OTF will interact directly with the 6TOP layer: it will manage the bandwidth requirements according to the traffic generated by the application layer and to the needs related to neighbors claiming bandwidth through 6TOP messages.

2) Securing the MAC layer: In order to address the security issues left open in the IEEE802.15.4 standard, the 6TiSCH WG is further defining: (i) keying material and authentication mechanisms needed by new devices for joining an existing network; (ii) a method permitting secure delivery of application data between neighbors; and (iii) a scheme able to grant a secure transfer of signaling data between devices and 6TiSCH [30].

In this regard, some efforts have been spent designing a complete security architecture (addressing node authentication and data confidentiality at both link and transport layer of the communication stack) [39], and defining the related implementation requirements [40].

We are also contributing in conceiving a complete, simple, and standard compliant framework supporting a number of security features for the MAC layer [41]. First of all, five different security levels can be configured allowing a wide range of heterogeneous IoT networks: (i) in a *Fully Secured* network confidentiality and data integrity are provided for all packets; (ii) in *Unsecured* network no security service is supported; (iii) only message integrity is guaranteed in a *Partial Secured* network; (iv) an *Hybrid Secured* network protect unicast communications between devices supporting security capabilities, and (v) the *Flexible Secured* option identifies a network as *Fully Secured* configuration, unless at least one node is not supporting security capabilities, causing the network to be *Hybrid Secured*.

In such framework, three different keys are employed: a *MasterKey*, i.e., the initial secret shared among all the devices, the *DefaultKey*, which is used to encrypt broadcast messages, and the the *LinkKey*, negotiated between a couple of devices to protect their unicast communications.

Three consecutive phases have been identified in order to configure a secured domain: in the *Setting-up* phase devices store all the secrets required for initializing a secured domain; the *Bootstrap* phase is that related to the initialization process and to the computation of the key that will protect broadcast messages at the MAC layer; in the end, the *Key Negotiation* phase exploits the Key Management Protocol to negotiate keys between couple of devices. Finally, it is worth noting that the specification [41] includes also the interaction between 6TOP and the MAC layer during all the introduced phases.

IV. Conclusion and future works

In this paper, we have presented the evolution and the future trend of a standardized energy-efficient and IPv6-enabled communication stack compliant with the Internet of Things vision. In details, the historical background of the 6TiSCH stack has been described in some details, starting from the pioneering and very first commercially viable ZigBee stack and passing from its descendant ZigBeeIP. As matter of fact, the latter gave a strong impulse to an actual deployment of standardized IoT network solutions. However, some additional standardization issues were raised as the IEEE802.15.4 MAC layer was not conceived for multi-hop networks. With the introduction of the IEEE802.15.4e amendament and, among other, the most powerful and reliable TSCH MAC, researchers and practitioners began focusing on the implementation details left open, while envisaging the integration of IEEE802.15.4e TSCH as MAC layer with the IETF protocols standardized for Low-power and Lossy Networks. It was the birth of the IETF 6TiSCH working group, which is currently architecturing a further evolution of an IoT power-efficient communication stack, while accounting for security issues at the MAC layer. In this context, we have introduced the expected 6TiSCH outcomes and highlighted our contribution. Future works will investigate the behavior of such communication stack by simulations and with experiments, in order to assess its performance for a wide gamut of optimal and secured industrial applications.

Acknowledgments

This publication was supported by the PON project RES NOVAE, ERMES-01-03113, DSS-01-02499 and EURO6-01-02238, funded by the Italian MIUR and by the European Union (European Social Fund).

Moreover, the authors would like to acknowledge the other Internet Draft co-authors, Diego Dujovne, Gennaro Boggia, Luigi Alfredo Grieco and Maria Rita Palattella, and the IETF 6TiSCH Chairs Pascal Thubert and Thomas Watteyne for the guidance and input provided.

References

[1] K. Ashton, “That ”internet of things thing,” *RFiD Journal*, vol. 22, pp. 97–114, 2009.

[2] O. Hersent, D. Boswarthick, and O. Elloumi, *The Internet of Things: Key Applications and Protocols*, 2nd ed. Wiley, 2012.

[3] *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

[4] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, “Standardized Protocol Stack for the Internet of (Important) Things,” *Communications Surveys & Tutorials, IEEE*, 2012.

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

[6] Hong, Sungmin and Kim, Daeyoung and Ha, Minkeun and Bae, Sungho and Park, Sang Jun and Jung, Wooyoung and Kim, Jae-Eon, “SNAIL: an IP-based wireless sensor network approach to the Internet of Things,” *Wireless Communications, IEEE*, vol. 17, no. 6, December 2010.

[7] ZigBee Alliance. [Online]. Available: www.zigbee.org

[8] IEEE std. 802.15.4, *Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, Standard for Information Technology, 16 June 2011.

[9] IETF Working Group, “Constrained RESTful Environments (CORE).” [Online]. Available: http://tools.ietf.org/wg/core/

[10] ——, “Routing Over Low Power and Lossy networks (ROLL).” [Online]. Available: http://tools.ietf.org/wg/roll/

[11] ——, “IPv6 over Low power WPAN (6LOWPAN).” [Online]. Available: http://tools.ietf.org/wg/6lowpan/

[12] D. Sturek, “Zigbee ip stack overview,” *ZigBee Alliance*, 2009.

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

[14] *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*, IEEE, 16 April 2012.

[15] IETF Working Group, “IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH).” [Online]. Available: http://tools.ietf.org/wg/6tisch/

[16] Q. Wang, X. Vilajosana, and T. Watteyne, *6TiSCH Operation Sublayer (6top) draft-wang-6tisch-6top-sublayer-00 (work in progress)*, IETF 6TiSCH WG, February 2014.

[17] J. Tripathi, J. C. de Oliveira, and J. P. Vasseur, “A Performance Evaluation Study of RPL: Routing Protocol for Low Power and Lossy Networks,” in *44th Annual Conf. Information Sciences and Systems, CISS*, March 2010.

[18] 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, August 2007.

[19] J. Hui and P. Thubert, *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*, RFC 6282, IETF, September 2011.

[20] 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, September 2007.

[21] S. Park, K. Kim, S. Chakrabarti, and J. Laganier, *IPv6 over Low Power WPAN Security Analysis draft-daniel-6lowpan-security-analysis-05 (work in progress)*, March 2011.

[22] 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, IETF, March 2012.

[23] P. Thubert, *Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)*, RFC 6552, Internet Engineering Task Force, March 2012.

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

[25] 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, March 2012.

[26] T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, *A Security Threat Analysis for Routing over Low-Power and Lossy Networks draft-ietf-roll-security-threats-05 (work in progress)*, October 2013.

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

[28] L. Seitz and G. Selander, *Additional Security Modes for CoAP draft-seitz-core-security-modes-00 (work in progress)*, October 2013.

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

[30] T. Watteyne, M. R. Palattella, and L. A. Grieco, *Using IEEE802.15.4e TSCH in an LLN context: Overview, Problem Statement and Goals draft-ietf-6tisch-tsch-00 (work in progress)*, IETF 6TiSCH WG, November 2013.

[31] G. Piro, G. Boggia, and L. A. Grieco, “A Standard Compliant Security Framework for IEEE 802.15.4 Networks,” Seoul, South Korea, Mar. 2014.

[32] X. Vilajosana and K. Pister, *Minimal 6TiSCH Configuration draft-ietf-6tisch-minimal-00 (work in progress)*, IETF 6TiSCH WG, November 2013.

[33] P. Thubert, T. Watteyne, and R. A. Assimiti, *An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4e draft-ietf-6tisch-architecture-01 (work in progress)*, IETF 6TiSCH WG, February 2014.

[34] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel, “On Optimal Scheduling in Duty-Cycled Industrial IoT Applications using IEEE802.15.4e TSCH,” *SENSORS, IEEE*, vol. PP, no. 99, pp. 1–12, June 2013.

[35] N. Accettura, M. R. Palattella, G. Boggia, L. A. Grieco, and M. Dohler, “Decentralized Traffic Aware Scheduling for Multi-hop Low Power Lossy Networks in the Internet of Things,” in *Proc. of IEEE Int. Symp. on a World of Wireless Mobile and Multimedia Networks, WoWMoM*, Madrid, Spain, June 2013.

[36] 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.

[37] J. Vasseur and J. Le Roux, *Path Computation Element (PCE) Communication Protocol (PCEP)*, RFC 5440, IETF, September 2009.

[38] D. Dujovne, L. A. Grieco, M. R. Palattella, and N. Accettura, *6TiSCH On-the-Fly Scheduling draft-dujovne-6tisch-on-the-fly-02 (work in progress)*, IETF 6TiSCH WG, February 2014.

[39] M. Richardson, *Security Architecture for 6top: requirements and structure draft-richardson-6tisch-security-architecture-01 (work in progress)*, IETF 6TiSCH WG, March 2014.

[40] S. Chasko, S. Das, R. Marin-Lopez, Y. Ohba, P. Thubert, and A. Yegin, *Security Framework and Key Management Protocol Requirements for 6TiSCH draft-ohba-6tisch-security-00 (work in progress)*, IETF 6TiSCH WG, October 2013.

[41] G. Piro, G. Boggia, and L. A. Grieco, *A standard compliant security framework for Low-power and Lossy Networks draft-piro-6tisch-security-issues-01 (work in progress)*, IETF 6TiSCH WG, December 2013.