Lessons Learned from the 6TiSCH Plugtests

Maria Rita Palattella[1(✉)], Xavier Vilajosana[2], Tengfei Chang[3], Miguel Angel Reina Ortega[4], and Thomas Watteyne[5]

[1] SnT, University of Luxembourg, Luxembourg, Luxembourg
maria-rita.palattella@uni.lu
[2] Universitat Oberta de Catalunya, Barcelona, Spain
xvilajosana@uoc.edu
[3] University of Science and Technology, Beijing, China
tengfei.chang@gmail.com
[4] ETSI, Sophia Antipolis, France
miguelangel.reinaortega@etsi.org
[5] Inria, EVA Team, Paris, France
thomas.watteyne@inria.fr

Abstract. The principal barrier to massive IoT technology adoption is the lack of interoperability and the resulting segmented nature of the IoT market. To cope with that the European Research Cluster on the Internet of Things (IERC), the International Telecommunication Union (ITU) and the European Telecommunication Standards Institute (ETSI) promote the development of interoperability events to enforce real standard compliance and interoperability between vendors. In this paper, we summarize the lessons learned during the first ETSI Plugtests event on the technology developed by the IETF 6TiSCH working group. 6TiSCH technology is cornerstone to the Industrial Internet of Things, enabling operational technologies to converge to the Internet by providing seamless IP connectivity and standardized management. The event clearly demonstrated the importance of such interoperability testing early on in the standards development. Interoperability was tested between implementations of 6TiSCH technology from multiple vendors. A total of 221 tests were performed, with a 93.7 % success rate.

Keywords: Interoperability · 6TiSCH · Plugtests · OpenWSN

1 Introduction

The Internet of Things (IoT) allows a large number of heterogeneous devices to interconnect, bringing new market opportunities and opening new technical challenges. The Internet is expected to grow to up to 50 billion "things" by 2020, according to a 2011 Cisco-IBSG prediction. The amount of data traffic they will be injecting into the network will increase, up to an annual rate of 84 % for machine-to-machine (M2M) communication, by 2018 [1]. Technology is developing on how to deal with huge numbers of smart things, how to make sense out

B. Mandler et al. (Eds.): IoT 360° 2015, Part II, LNICST 170, pp. 415–426, 2016.
DOI: 10.1007/978-3-319-47075-7_46

of the amount of data they generate ("big data"), and how to efficiently use network resources to avoid the collapse of the network, and to allow the coexistence of flows with different Quality of Service (QoS) requirements. The first barrier to adoption is the lack of interoperability and the resulting segmented nature of the market. According to the European Research Cluster on the Internet of Things (IERC) and the International Telecommunication Union (ITU), lack of interoperability is one of the biggest obstacles to IoT market development [2].

The term "interoperability" was initially defined for Information Technology (IT) as "the ability of exchange data" [3]. A broader definition was proposed by the Network Centric Operations Industry Consortium (NCOIC), to take into account social, political and organizational factors that affect systems and system performance, when integrating them all together [4]. Interoperability issues arise when devices from different manufacturers interconnect.

Early IoT adoption was delayed because of the development of incompatible proprietary solutions that maintain the cost of goods and operations high. As is often the case, standardization bodies and industry consortia agreed on the need to develop standards that would guarantee inter-operation between devices from different vendors [5]. The Internet Engineering Task Force (IETF) is the body behind most standards used in today Internet. Various IETF Working Groups, such as 6lo[1], ROLL[2] and 6TiSCH[3] develop standards to allow seamless integration of low-power wireless networks into the Internet.

Standardization is only the first step to allow widespread adoption of a new technology. Once the standard is written, one has to make sure the different products that claim to implement it really work together. This is done by defining a set of "interop tests". Well-established test methodologies such as ETSI EG 202 237 [6] and ETSI EG 202 568 [7] distinguish two classes of tests: *Conformance* and *Interoperability*.

Conformance testing aims at checking whether a product correctly implements a particular standardized protocol. It determines whether or not the Implementation Under Test (IUT) meets the requirements specified for the protocol itself. This includes message format and message sequence. Conformance testing is done on a single device.

Interoperability testing is done between multiple devices from different vendors. Interoperability testing aims at verifying end-to-end functionality between at least two devices from different vendors. Conformance testing in conjunction with interoperability testing provide both the proof of conformance and the guarantee of inter-operation. ETSI EG 202 237 [6] and ETSI EG 202 568 [7] describe several approaches on how to combine these two methods. The most common approach consists in Interoperability Testing with Conformance Checks, where reference points between the devices under test are monitored to verify the appropriate sequence and contents of protocol messages, such as API calls and

[1] http://tools.ietf.org/wg/6lo/charters.

[2] http://tools.ietf.org/wg/roll/charters.

[3] http://tools.ietf.org/wg/6tisch/charters.

interface operations. Interoperability events are branded as "Plugtests^{TM}" when organized by the European Telecommunications Standards Institute (ETSI)[4].

The first ETSI "Plugtests" event took place in 1999. Since then, ETSI organizes an average of 12 Plugtests per year, covering diverse technologies. Such events provide essential feedback to technical committees, and help them improve standards and accelerate the standards-making process. They also enable engineers to get together and test the interoperability of their implementations, which reduces a product's time-to-market. ETSI organized the first Plugtests on the technology developed by the IETF 6TiSCH working group. 6TiSCH is emerging as a key enabler of industrial IoT (iIoT) [8].

6TiSCH aims at "gluing" together an IP-enabled upper stack developed by IETF (6LoWPAN, RPL, CoAP) with the IEEE802.15.4e Timeslotted Channel Hopping (TSCH) MAC protocol [9]. TSCH inherits from well-established industrial standards such as WirelessHART. The 6TiSCH protocol stack results in an IP-enabled and low-power protocol stack for Industrial applications, able to fulfill their stringent requirements in terms of reliability, latency, and power consumption [10,11]. Because 6TiSCH federates different IoT standards developed by the IETF and the IEEE, testing interoperability between 6TiSCH implementations is challenging.

The first 6TiSCH Interop Plugtests event was organized by ETSI in Prague, Czech Republic on 17–19 July 2015. It was co-located with the IETF93 standardization meeting. The event was supported by OpenMote[5] and sponsored by the European Commission and Inria. 15 organizations – companies, open-source projects and academic partners – took part in the event. During the Plugtests, different vendors assessed the level of interoperability of their own implementation against others. They also checked whether their understanding of the implemented IEEE and IETF protocol specifications was correct. The scope of the event was on the "Minimal 6TiSCH Configuration" [12]. Interoperability tests included fundamental protocol operations such as synchronization and link-layer security.

The remainder of this paper is organized as follows. Section 2 summarizes the 6TiSCH minimal implementation, together with the configuration of parameters which were used during the Plugtests. Section 3 describes the golden device and the Wireshark dissector, two supporting tools developed for the event. Section 4 presents the detailed list of tests which were performed. Section 5 summarizes the lessons learned from the event. Section 6 concludes the paper.

2 Minimal 6TiSCH Configuration

The 6TiSCH "minimal" configuration [12] defines the basic set of rules for a 6TiSCH network to operate. Due to the wide and extensive configuration set enabled by the IEEE802.15.4e specification [9], it becomes mandatory to define a set of rules and requirements for vendors to inter-operate. The purpose of

[4] http://www.etsi.org/about/what-we-do/plugtests.

[5] http://www.openmote.com/.

the "minimal" document is twofold. First, include a fallback mode of operation, enabling all minimal-compliant networks to run using a common and basic configuration set and enabling it in case of network failure or lost of configuration. Second, support early interoperability events and guide early technology adopters to the integration of IETF standards on top of the TSCH MAC layer.

During the preparation of the Plugtests, and especially the writing of the Test Description, the minimal draft represented the main reference document, providing guidelines on how to make implementations compliant to the standard, from basic functionality, such as IEEE802.15.4e TSCH header configuration, use of Information Elements, to most advanced security settings (e.g. generation of the nonce, authentication and authorization keys).

The minimal specification also defines the network formation process, by indicating what is the period of the Enhanced Beacons and the specific Information Elements sent during the joining process. The layer 2 synchronization structure is defined as being the same as the routing topology, which is created by the RPL routing protocol [13].

All communication in a TSCH networks is orchestrated by a schedule. Time is sliced in timeslots, and timeslots are grouped in a slotframe which continuously repeats over time. The communication schedule indicates the use of each slot. In a minimal network, this schedule is the same for all nodes, and does not change over time. The schedule to use is announced by nodes already part of the network through Enhanced Beacons (EBs), a type of link-layer frames (see Fig. 1). In a minimal network, one active time slot is used in an "slotted Aloha" fashion, i.e. it is shared by all nodes. The IEEE802.15.4e TSCH default channel hopping template and timeslot timings are announced in the EBs, and time source neighbor selection is determined by the smallest join priority received by the node.

The minimal 6TiSCH configuration also defines how the Routing Protocol for Low Power and Lossy networks (RPL) [13] is configured to operate on top of a TSCH MAC Layer, and what the operation modes are. The Objective Function

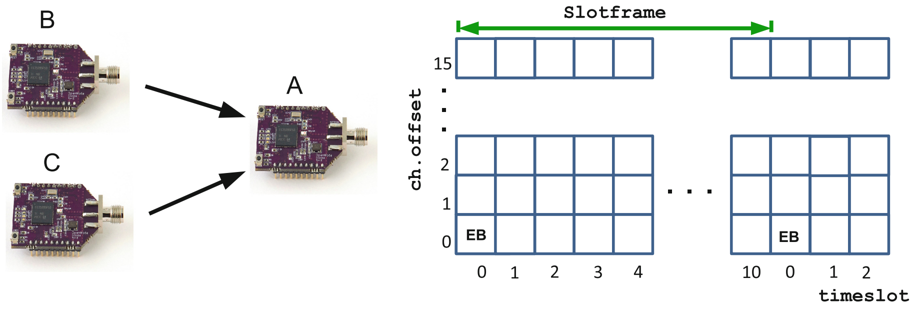


Fig. 1. The minimal schedule used during the interop event. We use a single 11-slot slotframe. The first slot in the slotframe is configured as an slotted Aloha slot, shared by all nodes in the network. Enhanced Beacons are also sent in that slot.

Zero (OF0) [14] is used to ensure the optimization of RPL routes within a RPL instance. According to the minimal draft, any compliant implementation must implement RPL and use the non-storing mode of operation when possible, and be able to use the storing mode of RPL when device characteristics permit. A policy to avoid parent selection hysteresis is used to avoid frequent parent changes due to slight rank differences.

Table 1 summarizes the configuration parameters as defined by the 6TiSCH minimal configuration, which were used during the plugtest event.

Table 1. 6TiSCH Plugtest minimal configuration.

Field	Value	Description
Slotframe length	11	11 slots per slotframe
Slotframe and link	1 active slot	Marked as shared, timekeeping, TX and RX
Timeslot template	Default	IEEE802.15.4e TSCH default slot template
Channel hopping template	Default	IEEE802.15.4e TSCH default channel hopping template
Security key K1	Well-known, as per [12]	Set to `6TiSCH minimal15`
Security key K2	Randomly generated	Set to `deadbeeffacecafe`
RPL objective function	OF0 [14]	With Rf = 1, Sr = 0 and Sp = 2 * ETX [15]

3 Golden Device

To allow participants to do pre-testing, and get ready for the 6TiSCH Plugtests event, a *Golden Device* (GD) was developed. The *Golden Device* is pre-programmed with firmware that passed conformance tests, and is known to implement the 6TiSCH protocol stack correctly. Each vendor received a GD before the event, allowing them to test their implementation against it, and verify inter-operability by going through the test description (see Sect. 4).

The golden device uses an OpenMote-CC2538 [16], which features a Texas Instruments CC2538 micro-controller and radio. The CC2538xFnn is a wireless micro-controller System-on-Chip (SoC) for high-performance IoT applications. It combines an ARM Cortex-M3 micro-controller with an IEEE802.15.4 radio [17]. The OpenMote-CC2538 also features a serial port, which is used for outputting help information and verify interoperability.

Two different images were implemented on the GD, one acting as DAGroot (GD/root), and the other as packet sniffer (GD/sniffer).The source code of both golden images is based on the OpenWSN project[6]. In detail, the images contain the 6TiSCH configuration defined in the minimal draft [12]. On the GD/root, security can be enabled/disabled, through switches activated during compilation of the source code. In addition, both images have several configurable interfaces serving for the interoperability test during the Plugtests.

By interacting with a Python script over the serial interface, the vendor can configure the device, set the value of different parameters (e.g. frequency, slotframe size), or trigger the transmission of a given type of packet. Table 2 summarizes the different configuration which can be enabled on a device using that script.

Table 2. Golden device commands [18]

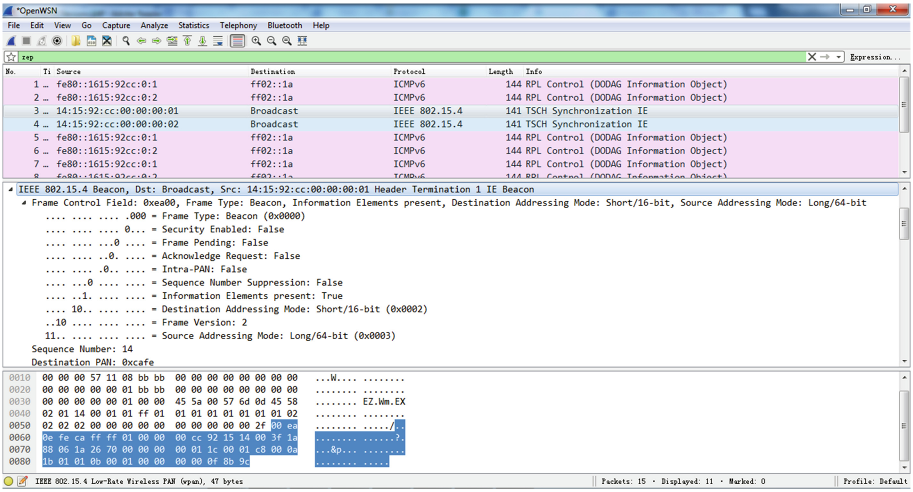
Command scope	Command ID	Length	Parameter	Range	Unit
Configure frequency	0	1 byte	Frequency number	0, 11 ~ 26	
Send EB	1	2 bytes	Sending period	0 ~ 65535	s
Send KA	2	2 bytes	Sending period	0 ~ 65535	ms
Send DIO	3	2 bytes	Sending period	0 ~ 65535	ms
Send DAO	4	2 bytes	Sending period	0 ~ 65535	ms
Set slotframe size	5	2 bytes	Slotframe length	0 ~ 65535	
Set rank value	6	2 bytes	Rank	0 ~ 65535	
Enable/disable ACK reply	6	1 byte	Option	True (enable) False (disable)	

The configuring commands, listed in Table 2, can be applied to GD/root. The *configure frequency* command is the only one which applies to the GD/sniffer, for activating it on a specific channel. By setting the frequency value to 0, channel hopping is enabled, and all the 16 available channels defined in [17] are used. Otherwise, the device can be forced to operate on a single channel (through 11 to 26).

The script also responds to output to assist in the tests. For example, by interacting with GD/root, the script shows the Absolutely Slot Number (ASN) and the time correction every time the golden device receives a packet from a different device. This is useful for tracking the clock drift between devices.

To help verify the format of packets during the interoperability test, the GD/sniffer listens on a specific frequency and injects the received packets into Wireshark. Wireshark is the de-facto tool for network protocol analysis. During the Plugtests, a Wireshark version with the dissector of IEEE802.15.4e/6TiSCH (Fig. 2), developed by Orange Labs, was used [19].

[6] http://www.openwsn.org/.


*OpenWSN
File Edit View Go Capture Analyze Statistics Telephony Bluetooth Help
zep
Expression...

```
No.     Ti Source                   Destination    Protocol       Length Info
     1 … fe80::1615:92cc:0:1        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
     2 … fe80::1615:92cc:0:2        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
     3 … 14:15:92:cc:00:00:00:01    Broadcast      IEEE 802.15.4    141 TSCH Synchronization IE
     4 … 14:15:92:cc:00:00:00:02    Broadcast      IEEE 802.15.4    141 TSCH Synchronization IE
     5 … fe80::1615:92cc:0:1        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
     6 … fe80::1615:92cc:0:2        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
     7 … fe80::1615:92cc:0:1        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
     8 … fe80::1615:92cc:0:2        ff02::1a       ICMPv6           144 RPL Control (DODAG Information Object)
```

```
IEEE 802.15.4 Beacon, Dst: Broadcast, Src: 14:15:92:cc:00:00:00:01 Header Termination 1 IE Beacon
  Frame Control Field: 0xea00, Frame Type: Beacon, Information Elements present, Destination Addressing Mode: Short/16-bit, Source Addressing Mode: Long/64-bit
    .... .... .... .000 = Frame Type: Beacon (0x0000)
    .... .... .... 0... = Security Enabled: False
    .... .... ...0 .... = Frame Pending: False
    .... .... ..0. .... = Acknowledge Request: False
    .... .... .0.. .... = Intra-PAN: False
    .... ...0 .... .... = Sequence Number Suppression: False
    .... ..1. .... .... = Information Elements present: True
    .... 10.. .... .... = Destination Addressing Mode: Short/16-bit (0x0002)
    ..10 .... .... .... = Frame Version: 2
    11.. .... .... .... = Source Addressing Mode: Long/64-bit (0x0003)
  Sequence Number: 14
  Destination PAN: 0xcafe
```

```
0010  00 00 00 57 11 08 bb bb  00 00 00 00 00 00 00 00   ...W.... ........
0020  00 00 00 00 00 01 bb bb  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 01 00 00  45 5a 00 57 6d 0d 45 58   ........ EZ.Wm.EX
0040  02 01 14 00 01 01 ff 01  01 01 01 01 01 01 01 02   ........ ........
0050  02 02 02 00 00 00 00 00  00 00 00 00 00 2f 00 ea   ........ ...../..
0060  0e fe ca ff ff 01 00 00  00 cc 92 15 14 00 3f 1a   ........ ......?.
0070  88 06 1a 26 70 00 00 00  00 01 1c 00 01 c8 00 0a   ...&p... ........
0080  1b 01 01 0b 00 01 00 00  00 00 0f 8b 9c            ........ .....
```

```
IEEE 802.15.4 Low-Rate Wireless PAN (wpan), 47 bytes    Packets: 15 · Displayed: 11 · Marked: 0    Profile: Default
```

Fig. 2. Wireshark running the IEEE802.15.4e TSCH/6TiSCH dissector.

4 Tests Description

Prior to the Plugtests event, a group of four experts, together with ETSI support, prepared the 6TiSCH Plugtests Test Description (TD) [18]. The latter contains a set of test scenarios to be executed by vendors. The TD was distributed to participants some weeks before the event, allowing for comments and fine-tuning of the document itself. The TD document will be published in the future as an ETSI ISG IP6 group specification so maintenance and revisions can easily be performed for further 6TiSCH Plugtests.

The TD includes 18 tests, performed in two different configuration: *Single Hop*, with 1 DAGroot (DG) and 1 mote (6N), and *Multi Hop* with 1 DAGroot, and two motes, connected in a linear topology.

The tests are classified in four different groups, based on the type of features they aim to verify: Synchronization (`SYNCH`), Packet Format (`FORMAT`), RPL features (`RPL`), and Security (`SEC`). Each group contains several tests, summarized in Table 3.

4.1 `SYNCH` Tests

Synchronization is fundamental in TSCH-based networks, given the slotted nature of the communication. Devices *must* keep tight synchronization. Devices are equipped with clocks for keeping track of time. But, clocks in different devices drift with respect to one another. Therefore, they need to periodically resynchronize. The aim of the `SYNCH` tests is to check whether a device can synchronize with the DAGroot parent, by exchanging EB frames; keep synchronization by sending Keep Alive (KA) messages; and recover synchronization, after clocks

Table 3. List of 6TiSCH Tests performed during the Plugtests [18].

#	ID	Description
1	SYNCH-01	Check that a 6N can synchronize to the EB sent by the DR
2	SYNCH-02	Check that a 6N can synchronize to DR using KA messages
3	SYNCH-03	Check that a 6N's clock drifts if there is no re-synchronization
4	SYNCH-04	Check that the 6N can recover synchronization after de-synchronization
5	FORMAT-01	Check the format of the IEEE802.15.4e EB packet
6	FORMAT-02	Check the timing template of TSCH time slot defined in [12] is correctly implemented
7	FORMAT-03	Check channel hopping is correctly implemented according to [12]
8	FORMAT-04	Check the number of retransmissions is implemented following [12]
9	FORMAT-05	Check the minimal schedule is implemented according to [12]
10	FORMAT-06	Check the 6N sets its slotframe size correctly when joining the network
11	SEC-01	Check the 6N is correctly authenticated with K1, when it synchronizes to DR with EB
12	SEC-02	Check the data packet sent by 6N is correctly encrypted with K2
13	RPL-01	Check the value of EB join priority of a child 6N and a parent DR
14	RPL-02	Check the rank of 6N is computed correctly according to [12]
15	RPL-03	Check a 6N child changes its time source neighbor (parent) correctly
16	RPL-04	Check the format of RPL DIO message
17	RPL-05	Check the format of RPL DAO message
18	RPL-06	Check IP extension header in 6LoWPAN

drifts, applying the time correction specified in the ACK, sent after successful reception of the KA message.

4.2 FORMAT Tests

The set of FORMAT tests are mainly interoperability tests with conformance checks, aiming to check appropriate sequence and content of protocol messages. For instance, the format of the EB frame, and a set of Information Elements (IEs) is verified by printing out the different fields of the EB, with the Wireshark dissector. In detail, the format of the following IEs is verified: (i) the *synchronization IE* which contains the ASN and the Join Priority field, used to initially synchronize the nodes and establish the layer 2 topology; (ii) the *timeslot template IE* which announces the timeslot timing for nodes joining the network; (iii) the *channel hopping IE* which announces the channel sequence used to hop in frequencies; and finally (iv) the *frame and link IE* which advertises the initial network schedule used by joining nodes to communicate.

Some of the FORMAT tests checked conformance with IEEE802.15.4e [17] (related to EBs format and slotframe size), while others checked conformance with the minimal draft [12], for the implementation of timeslot template, channel hopping template, number of retransmissions, and minimal schedule. In test FORMAT-03, channel hopping is enabled. For all tests, the use of a packet sniffer and the Wireshark dissector were instrumental for checking the final outcomes of the tests.

4.3 SEC Tests

6TiSCH networks adopt link-layer security mechanisms, as defined by [17]. In the minimal draft, two security mechanisms are considered: authentication and encryption. Authentication applies to all packet content, while encryption applies to header IEs and MAC payload.

The minimal draft assumes the existence of two cryptographic keys, which can be pre-configured. One of the keys, K1, is used to authenticate EBs. For early interoperability tests, as the one performed during the Plugtests event, K1 is set to 36 54 69 53 43 48 20 6D 69 6E 69 6D 61 6C 31 35 ("6TiSCH minimal15"). To facilitate logical segregation of distinct networks, EBs are authenticated, with no payload encryption.

A second key, K2, is used to authenticate DATA, ACK, MAC COMMAND frame types and respective header IEs, with payload encryption. For the Plugtests event only, K2 is set to "deadbeeffacecafe".

The SEC tests aimed at checking both authentication of EBs (which are exchanged between the DAGroot and the device, only if they are sharing the same key K1), and encryption/decryption of DATA packets (Echo Request/Reply) with K2. The *Key Index*, advertised in the auxiliary security header of the packets allowed nodes to look up the right key (K1 or K2) before decrypting, during the SEC tests.

4.4 RPL Tests

Devices in a 6TiSCH network use the RPL routing protocol [13] and implement the RPL Objective Function Zero (OF0) [14]. Therefore, beyond checking features which are mainly related to the IEEE802.15.4 TSCH MAC [17], during the Plugtests event, other tests were performed for checking the RPL implementation into vendor devices was correctly done, according to the minimal specification [12]. In detail, tests RPL-01 and RPL-02 checks the value of the EB join priority of child and parent devices, and the value of the rank, which should be computed according to the RPL OF0 function [14]. The rank computation uses a *rank increment* that is added to the parents announced rank upon reception of a DIO. The *rank increment* is computed as a function of a metric: in the interop event $2 * \mathrm{ETX}$ [15] was used.

The RPL tests group also includes conformance tests, to check the format of DIO and DAO messages is according to [13]. Finally, the use of extension headers was verified specially for the cases where IP tunneling (IP-in-IP encapsulation) was required. Mainly, when an IP packet needs to carry hop-by-hop extension headers, these headers are appended to an IP outer header avoiding the modification of the end-to-end scope of the inner header at each hop. The outer header is removed when crossing a border router leaving the inner header untouched. During the tests, IP tunneling was verified using the appropriate Wireshark dissector.

5 Lessons Learned

The overarching goal of the Plugtests event is to create better standards, resulting in better and interoperable products, larger and faster adoption of the technology, and a better end-user experience. This section summarizes the outcomes of the event in term of feedback to the standardization bodies, and lessons learned.

A first and important aspect to note is the importance of a close relationship between the interoperability event participants and the team of experts preparing the test specification. During that phase, the interaction and discussion between experts and participants accelerated the development and correction of standards under test as well as identified open issues in current standard implementations.

During the 6TiSCH Plugtests event, several issues arose from IEEE802.15.4e implementations brought by different participants. Those issues have been notified to the IEEE 802.15.4 task group. The main concern was related to Table 2a from IEEE802.15.4e-2012 [17] which contains inconsistencies. Table 2a specifies how the IEEE802.15.4 header bits in the Frame Control field are compressed (source and destination PANID compression, source and destination address compression). These inconsistencies have been discussed with the IEEE802.15.4 TG, who agreed that a problem exists. But it has been corrected by the IEEE, as indicated by internal IEEE documents. For the Plugtests event, however, only the published text from IEEE802.15.4e-2012 was used for implementations. We foresee that future Plugtests events, which will be based on future revisions of IEEE802.15.4, will hence fix the issue.

Regarding the minimal draft and it latest published version [12], several concerns arose.

One was related to RPL Mode of Operation (MOP). Some vendors implemented the RPL routing protocol in `storing mode`, others in `non-storing mode`. These modes are not interoperable, so these vendors could not build an interoperable multi-hop network during the event. Currently, the minimal draft does not specify the mode to implement. As follow up of the Plugtests, the issue was discussed during the IETF93 6TiSCH WG meeting. The WG agreed that there was a problem, and is discussing internally how to resolve this in a future revision of [12].

Analogously, some implementations were not using an IPv6 prefix information object in the RPL DIO messages to propagate the prefix of the network. Rather, they were using the prefix derived from the DODAGID. Based on this, in future revision of the 6TiSCH TD it would be recommendable to indicate the need of having this option in the DIO packets.

Finally, multihop tests required to filter packets or force the topology. The use of cables was problematic for MMCX and uFL antenna connectors while for SMA connectors it worked well. Therefore, it might be desirable to avoid forcing multihop topologies with coaxial cables and attenuators. We recommend for the next events one of the following approaches: (1) build/buy shield boxes to put nodes in or (2) ask vendors to add a functionality in their code that filters frames based on their source MAC address.

6 Conclusion

221 tests were performed during the 6TiSCH Pugtests event, and from these, 207 were PASS, resulting in a 93.7 % success rate. This high level of interoperability at the *first* 6TiSCH Plugtests event shows that 6TiSCH industrial IoT deployments will not run into big interoperability issues. The successful outcome can be attributed to the fact that each participant received a Golden Device prior to the event and could test their implementation against it before coming to the Plugtests event. Other 6TiSCH Plugtests will be organized in the future, to allow other vendors to take part, and perform new tests, checking more advanced features of the 6TiSCH technology.

References

1. Cisco-Systems: The Zettabyte Era Trends, Analysis (2014). http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html
2. The Internet of Things: International Telecommunication Union (ITU), Technical report (2005)
3. IEEE: IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. IEEE Std. (1990)
4. Slater, T.: What is Interoperability? Network Centric Operations Industry Consortium - NCOIC, Technical report (2012)
5. Palattella, M.R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L.A., Boggia, G., Dohler, M.: Standardized protocol stack for the Internet of (important) Things. IEEE Commun. Surv. Tutor. **15**(3), 1389–1406 (2013)
6. ETSI: ETSI EG 202 237 V1.1.2 (2007-04). ETSI Guide. Methods for Testing and Specification (MTS), Internet Protocol Testing (IPT), Generic Approach to Interoperability Testing (2007)
7. ETSI: ETSI EG 202 568 V1.1.3 (2007-04). ETSI Guide. Methods for Testing, Specification (MTS). Internet Protocol Testing (IPT). Testing: Methodology and Framework (2007)
8. Dujovne, D., Watteyne, T., Vilajosana, X., Thubert, P.: 6TiSCH: deterministic IP-enabled industrial Internet (of Things). IEEE Commun. Mag. **52**(12), 36–41 (2014)
9. IEEE: IEEE802.15.4. Part. 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer. IEEE Std., April 2012

10. Thubert, P., Watteyne, T., Palattella, M.R., Vilajosana, X., Wang, Q.: IETF 6TSCH: combining IPv6 connectivity with industrial performance. In: International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 541–546. IEEE (2013)
11. Palattella, M.R., Thubert, P., Vilajosana, X., Watteyne, T., Wang, Q., Engel, T.: 6TiSCH Wireless industrial networks: determinism meets IPv6. In: Mukhopadhyay, S.C. (ed.) Internet of Things, pp. 111–141. Springer International Publishing, Switzerland (2014)
12. Vilajosana, X., Pister, K.: Minimal 6TiSCH Configuration. Internet Engineering Task Force Std., Rev. draft-ietf-6tisch-minimal-11 [work-in-progress], 6 July 2015
13. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J., Alexander, R.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. Internet Engineering Task Force Std. RFC6550, March 2012
14. Thubert, P.: Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL). Internet Requests for Comments, Internet Engineering Task Force Std. RFC6552, March 2012
15. De Couto, D.S.J., Aguayo, D., Bicket, J., Morris, R.: A high-throughput path metric for multi-hop wireless routing. Wirel. Netw. **11**(4), 419–434 (2005)
16. Vilajosana, X., Tuset, P., Watteyne, T., Pister, K.: OpenMote: open-source prototyping platform for the industrial IoT. In: 7th EAI International Conference on Ad Hoc Networks (AdHocNets). EAI (2015)
17. IEEE802.15.4. Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Std. (2011)
18. ETSI: ETSI 6TiSCH interoperability test descriptions, 1 26 v1.2 (2015-07) (2015)
19. Munoz, J., Gaillard, G., Barthel, D.: Example Packets for the Minimal 6TiSCH Configuration. Internet Engineering Task Force Std., Rev. draft-munoz-6tisch-minimal-examples-00 [work-in-progress], 6 July 2015