6TiSCH

IPv6 over the TSCH mode of IEEE 802.15.4

IETF 99 Prague
Monday 17 July 2017

Chairs:
Pascal Thubert
Thomas Watteyne

Etherpad for minutes:
http://etherpad.tools.ietf.org:9000/p/notes-ietf-99-6tisch?useMonospaceFont=true

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

I E T F

Reminder:

Minutes are taken *
This meeting is recorded **
Presence is logged ***

* Scribe; please contribute online to the minutes at:
  http://etherpad.tools.ietf.org:9000/p/notes-ietf-99-6tisch?useMonospaceFont=true

** Recordings and Minutes are public and may be subject to discovery in the event of litigation.

*** From the Webex login

Agenda

13:30	**Intro and Status (Chairs)**	[35min]
	• Note-Well, Blue Sheets, Scribes, Agenda Bashing	[5min]
	• Status of the work; progress vs. charter	[5min]
	• Summary 1st F-Interop 6TiSCH Interoperability Event (Maria Rita Palattella)	[10min]
	• Summary OpenWSN hackathon (Tengfei Chang)	[5min]
13:55	**Dynamic Scheduling**	[25min]
	• 6top protocol draft-ietf-6tisch-6top-protocol-07 (Xavi Vilajosana)	[15min]
	• Service Function 0 draft-ietf-6tisch-6top-sf0-05 (Diego Dujovne)	[10min]
14:20	**Security**	[30min]
	• draft-ietf-6tisch-minimal-security-03 (Mališa Vučinić)	[15min]
	• update security DT and other derived work (Michael)	[15min]
	• draft-ietf-6tisch-dtsecurity-secure-join-01	
	• draft-richardson-6tisch-join-enhanced-beacon-01	
	• draft-richardson-6tisch-minimal-rekey-01	

Agenda

14:50 Unchartered items, time permitting [QS]

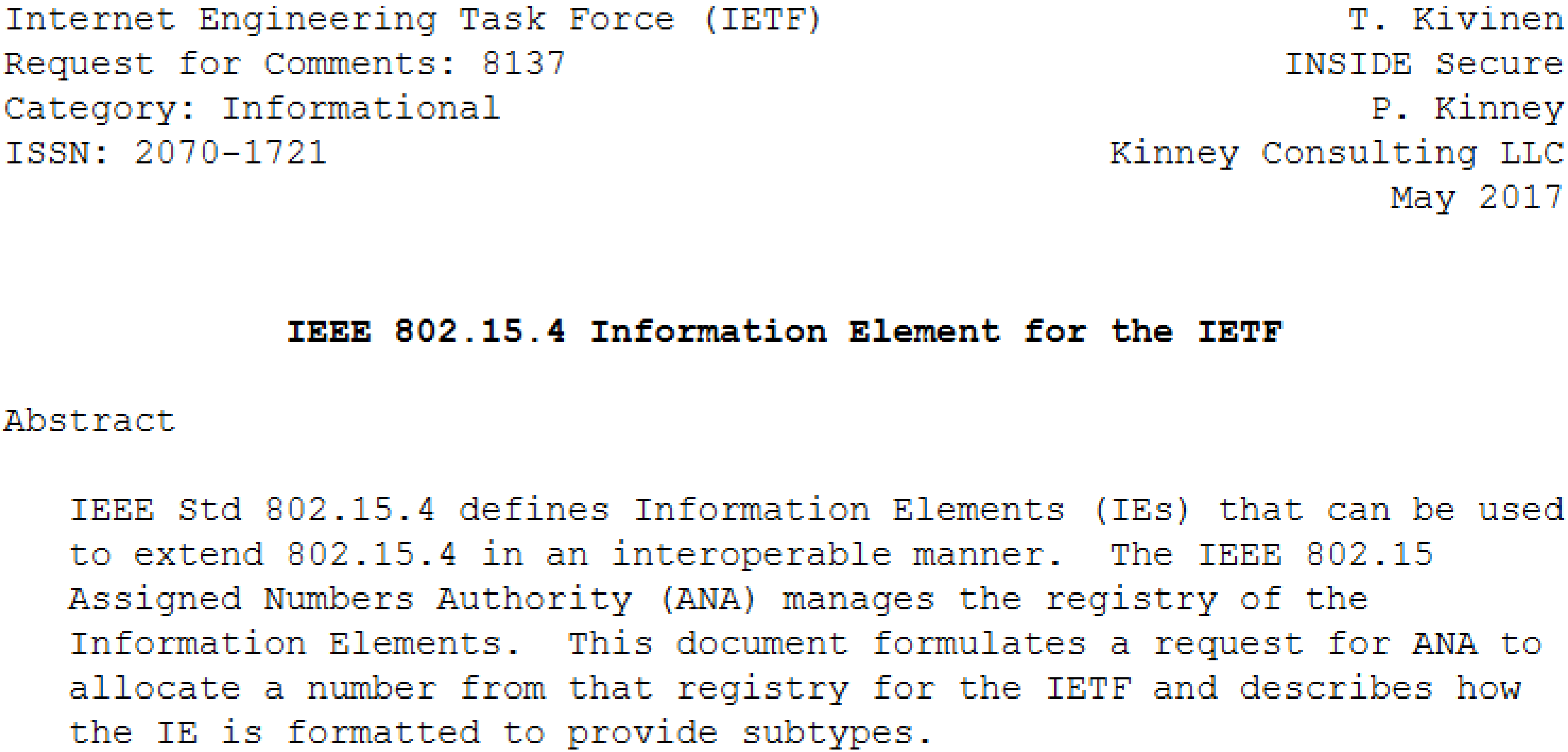
- draft-duquennoy-6tisch-asf (Simon Duquennoy) [10min]
- draft-munoz-6tisch-examples-02 (Jonathan Muñoz) [5min]
- draft-papadopoulos-6tisch-pre-reqs-00 (Georgios Papadopoulos) [5min]
- draft-lijo-6lo-expiration-time-04 (Lijo Thomas) [5min]

15:25 AOB […]

Volunteers

- notetaker 1: Dominique Barthel
- notetaker 2: Francesca Palombini
- Jabber scribe: Ines Robles
- Jabber: Michael Richardson

RFC 8137



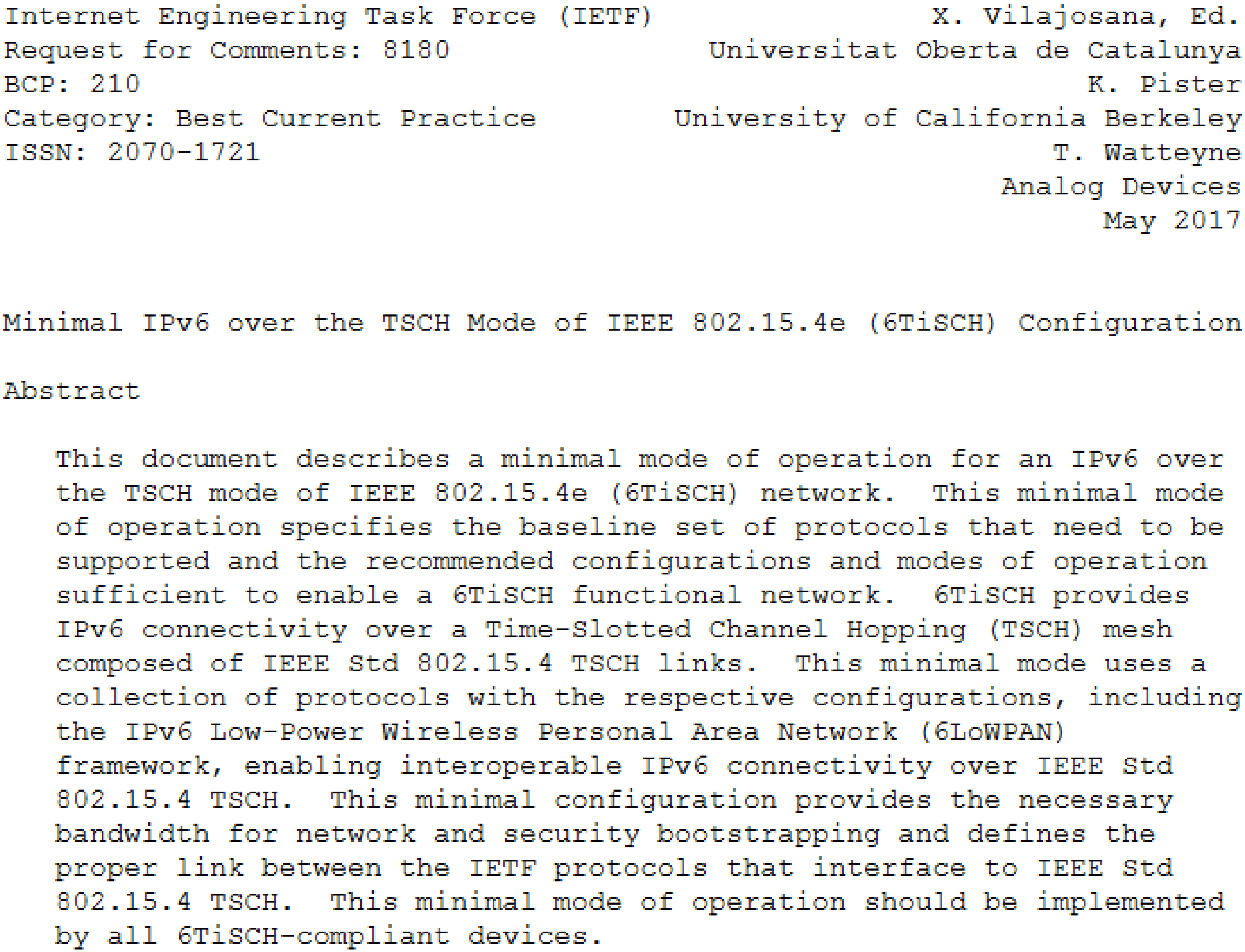
```
Internet Engineering Task Force (IETF)                        T. Kivinen
Request for Comments: 8137                                 INSIDE Secure
Category: Informational                                        P. Kinney
ISSN: 2070-1721                                   Kinney Consulting LLC
                                                                May 2017
```

IEEE 802.15.4 Information Element for the IETF

Abstract

IEEE Std 802.15.4 defines Information Elements (IEs) that can be used to extend 802.15.4 in an interoperable manner. The IEEE 802.15 Assigned Numbers Authority (ANA) manages the registry of the Information Elements. This document formulates a request for ANA to allocate a number from that registry for the IETF and describes how the IE is formatted to provide subtypes.

RFC 8180



```
Internet Engineering Task Force (IETF)               X. Vilajosana, Ed.
Request for Comments: 8180                 Universitat Oberta de Catalunya
BCP: 210                                                        K. Pister
Category: Best Current Practice          University of California Berkeley
ISSN: 2070-1721                                              T. Watteyne
                                                           Analog Devices
                                                                 May 2017
```

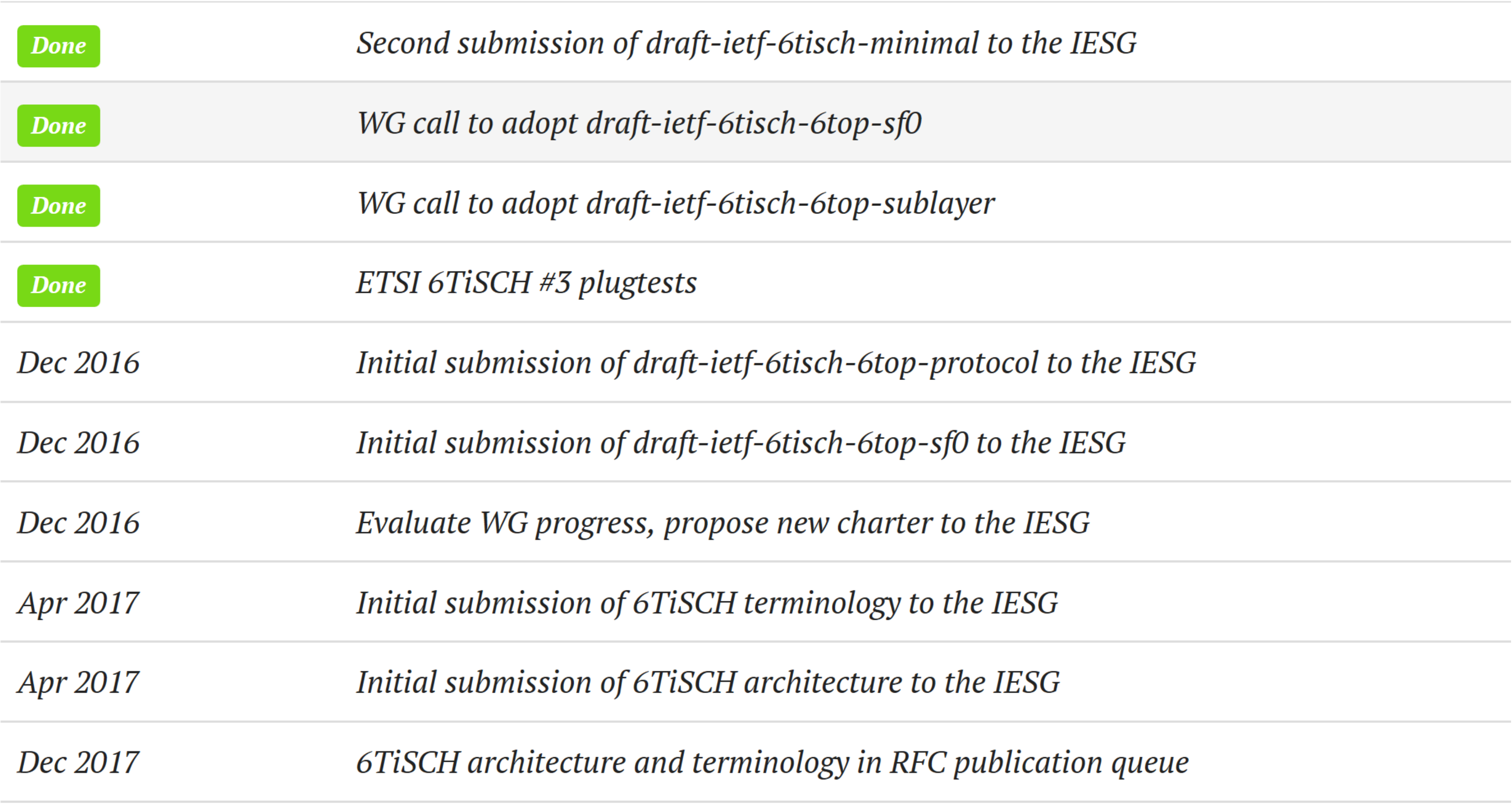
Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration

Abstract

This document describes a minimal mode of operation for an IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) network. This minimal mode of operation specifies the baseline set of protocols that need to be supported and the recommended configurations and modes of operation sufficient to enable a 6TiSCH functional network. 6TiSCH provides IPv6 connectivity over a Time-Slotted Channel Hopping (TSCH) mesh composed of IEEE Std 802.15.4 TSCH links. This minimal mode uses a collection of protocols with the respective configurations, including the IPv6 Low-Power Wireless Personal Area Network (6LoWPAN) framework, enabling interoperable IPv6 connectivity over IEEE Std 802.15.4 TSCH. This minimal configuration provides the necessary bandwidth for network and security bootstrapping and defines the proper link between the IETF protocols that interface to IEEE Std 802.15.4 TSCH. This minimal mode of operation should be implemented by all 6TiSCH-compliant devices.

Milestones

New milestones for secure join work?



Done	*Second submission of draft-ietf-6tisch-minimal to the IESG*
Done	*WG call to adopt draft-ietf-6tisch-6top-sf0*
Done	*WG call to adopt draft-ietf-6tisch-6top-sublayer*
Done	*ETSI 6TiSCH #3 plugtests*
Dec 2016	*Initial submission of draft-ietf-6tisch-6top-protocol to the IESG*
Dec 2016	*Initial submission of draft-ietf-6tisch-6top-sf0 to the IESG*
Dec 2016	*Evaluate WG progress, propose new charter to the IESG*
Apr 2017	*Initial submission of 6TiSCH terminology to the IESG*
Apr 2017	*Initial submission of 6TiSCH architecture to the IESG*
Dec 2017	*6TiSCH architecture and terminology in RFC publication queue*

ETSI

World Class Standards

1st F-Interop 6TiSCH Interoperability Event *REPORT*

Maria Rita Palattella

Miguel Angel Reina Ortega

14-15 July 2017

Prague, Czech Republic

Overview of the Event

- Event organized by:
  - ETSI (European Telecommunications Standards Institute)
  - LIST (Luxembourg Institute of Science and Technology)
- Supporting Companies/Projects:
  - OpenMote (hardware, www.openmote.com)
  - OpenWSN (firmware www.openwsn.org)
- Event sponsored and funded by:
  - European Commission
  - through the H2020 F-Interop project
- 16 participating companies
- independent implementations
  - 5x 6TiSCH
  - 6x OSCOAP

Participating People

Participating Things ☺

Summary of Event Planning

- 1 preparation call
  - ETSI/LIST/Experts group led and organized
  - Collaborating Web conf (GotoMeeting) on 3.7.2017
  - Included Vendor Participants
- Test Plan Development
  - 6TiSCH -> Led by Maria Rita Palattella, Tengfei Chang, Malisa Vucinic
  - F-Interop Online Testing Tools -> Remy Leone
  - OSCoAP -> Led by Francesca Palombini

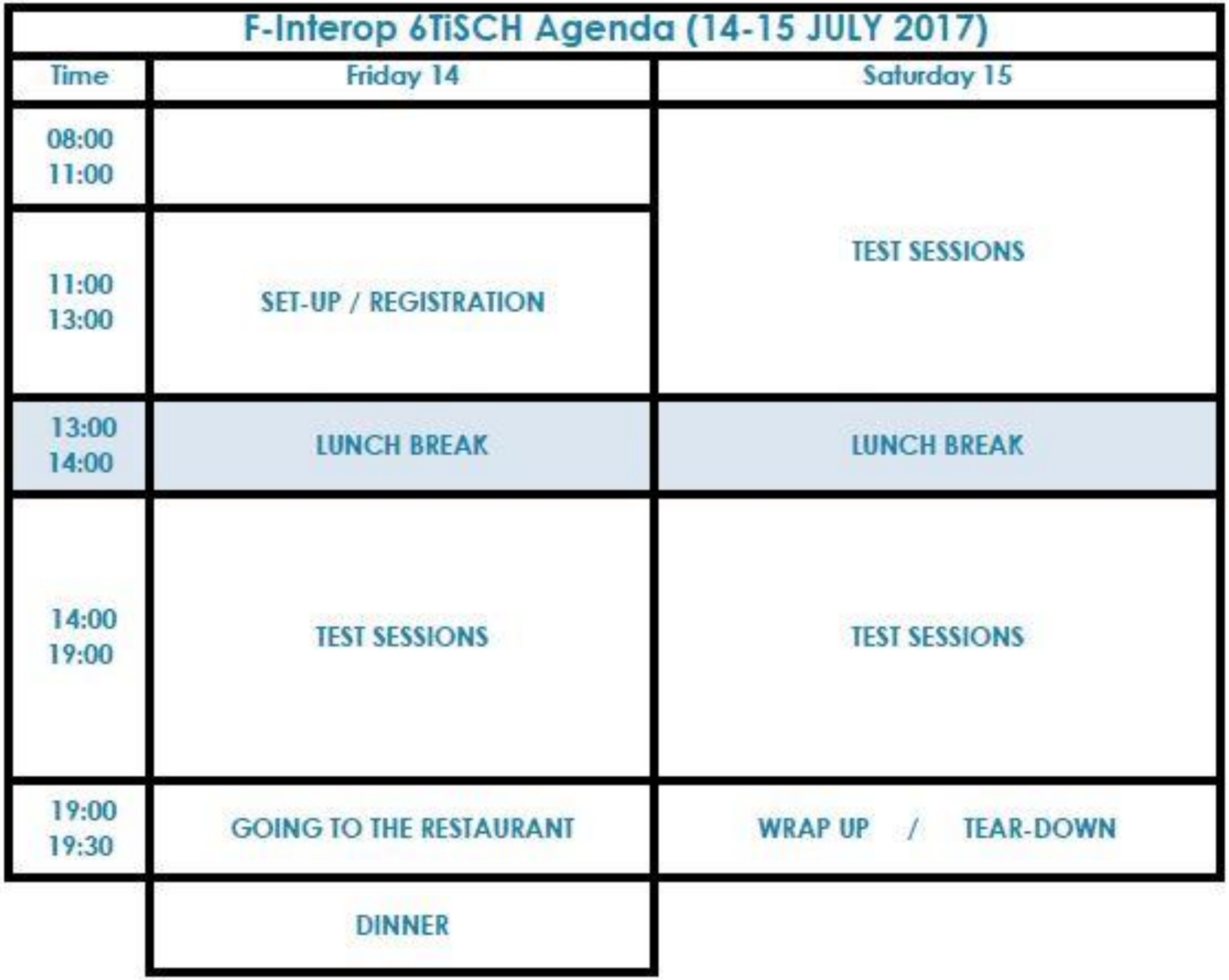
Test descriptions

6TiSCH Tests description (publicly available)

Testing: Synch, Minimal, 6top, L2 security, Secure joining

1	TD_6TiSCH_SYN_01
2	TD_6TiSCH_MINIMAL_01
3	TD_6TiSCH_MINIMAL_02
4	TD_6TiSCH_MINIMAL_03
5	TD_6TiSCH_MINIMAL_04
6	TD_6TiSCH_MINIMAL_05
7	TD_6TiSCH_MINIMAL_06
8	TD_6TiSCH_L2SEC_01
9	TD_6TiSCH_SECJOIN_01
10	TD_6TiSCH_SECJOIN_02
11	TD_6TiSCH_SECJOIN_03
12	TD_6TiSCH_SECJOIN_04
13	TD_6TiSCH_6P_01
14	TD_6TiSCH_6P_02
15	TD_6TiSCH_6P_03
16	TD_6TISCH_6P_04

Agenda



F-Interop 6TiSCH Agenda (14-15 JULY 2017)

Time	Friday 14	Saturday 15
08:00 11:00		TEST SESSIONS
11:00 13:00	SET-UP / REGISTRATION	
13:00 14:00	LUNCH BREAK	LUNCH BREAK
14:00 19:00	TEST SESSIONS	TEST SESSIONS
19:00 19:30	GOING TO THE RESTAURANT	WRAP UP / TEAR-DOWN
	DINNER	

ETSI
Meeting
1st F-Interop 6TiSCH Interoperability Event
6TiSCH
F-Interop
Testing platform for network interop

```
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
No.      Time        Source                      Destination  Protocol      Length  Info
2724 1141.99...  00:15:8d:00:00:35:ca:c7     Broadcast    IEEE 802.15.4  141 Enhanced Beacon, Dst: Broadcast, Src: Jennic_00:00:3
2725 1141.99...  fe80::215:8d00:35:cac7      fe80::21...  ICMPv6         128 Echo (ping) request id=0x00f0, seq=11136, hop limit=
2726 1141.99...  00:17:0d:00:00:00:00:02     00:15:8d...  IEEE 802.15.4  121 Ack, Dst: Jennic_00:00:35:ca:c7, Src: DustNetw_00:00:
2727 1142.00...  fe80::215:8d00:35:cac7      fe80::21...  ICMPv6         128 Echo (ping) request id=0x00f0, seq=11136, hop limit=
2728 1142.00...  ::17:d00:0:2                ::15:8d0...  ICMPv6         149 Echo (ping) reply id=0x00f0, seq=11136, hop limit=64
2729 1142.00...  ::17:d00:0:2                ::15:8d0...  ICMPv6         149 Echo (ping) reply id=0x00f0, seq=11136, hop limit=64
2730 1142.00...  00:15:8d:00:00:35:ca:c7     00:17:0d...  IEEE 802.15.4  121 Ack, Dst: DustNetw_00:00:00:00:02, Src: Jennic_00:0
2732 1142.99...  00:15:8d:00:00:35:ca:c7     00:17:0d...  IEEE 802.15.4  121 Ack, Dst: DustNetw_00:00:00:00:02, Src: Jennic_00:0
2733 1142.99...  fe80::215:8d00:35:cac7      fe80::21...  ICMPv6         128 Echo (ping) request id=0x00f0, seq=11136, hop limit=
2734 1142.99...  00:17:6d:00:00:00:00:02     00:85:8d...  IEEE 802.15.4  121 Ack, Dst: 00:85:8d:00:00:35:ca:c7, Src: Core_0d:00:00:

    Sequence Number: 184
    Destination PAN: 0xc0ca
    Destination: Jennic_00:00:35:ca:c7 (00:15:8d:00:00:35:ca:c7)
    Extended Source: DustNetw_00:00:00:00:02 (00:17:0d:00:00:00:00:02)
    FCS: 0x0060 (Correct)
  6LoWPAN
    .... 0001 = Page Number: 1
    6LoRH: Routing Protocol Information
    IPHC Header
    Next header: ICMPv6 (0x3a)
    Source: ::17:d00:0:2
    Destination: ::15:8d00:35:cac7

0060  b8 ca c0 c7 ca 35 00 00  8d 15 00 02 00 00 00 00   ......5.. ........
0070  0d 17 00 f1 82 05 2b 80  7a 55 3a 00 17 8d 00 00   ......+. zU:.....
0080  00 00 02 00 15 8d 00 00  35 ca c7 81 00 f3 1f 00   ........ 5.......
0090  f0 2b 80 60 00                                     .+.`.
```

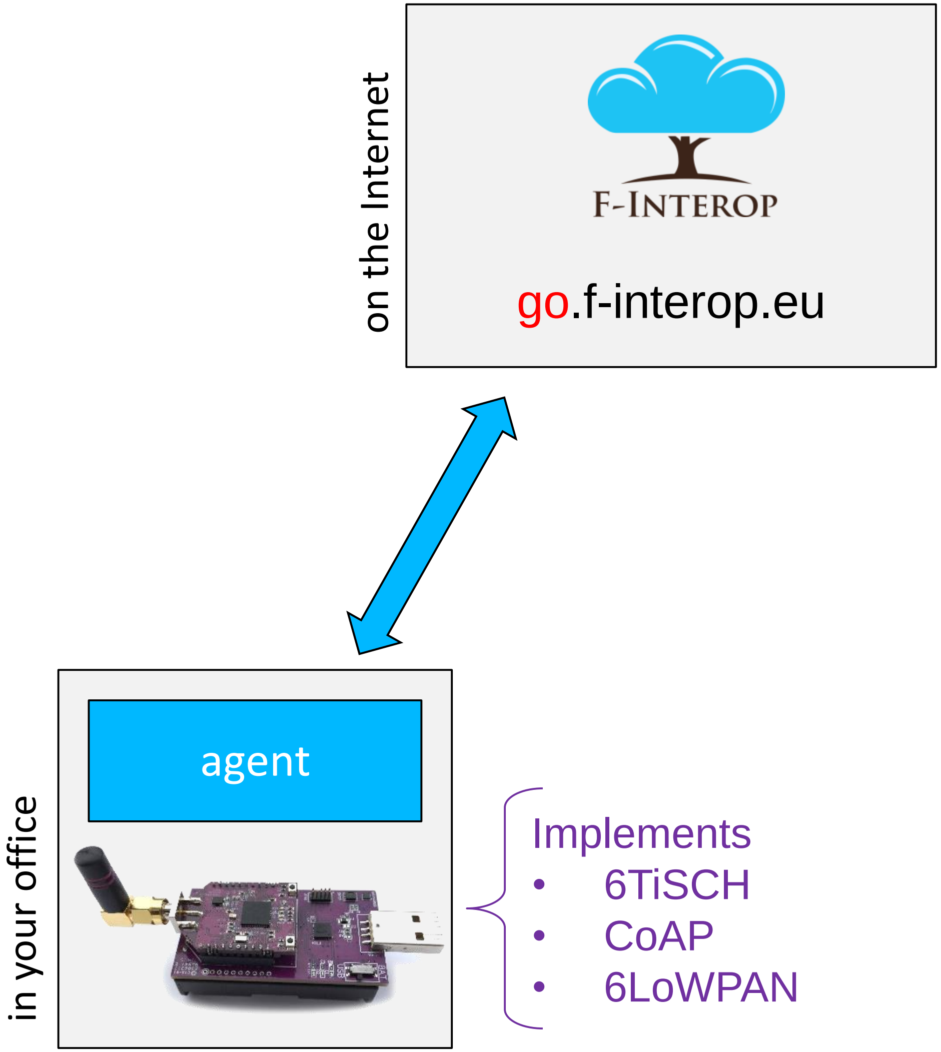
Results Reporting

- The results of each interoperability test session have been recorded in a dedicated web application software: the ETSI Test Report Tool (TRT)
  - After each test execution the interoperability result is agreed among all participants and then recorded
  - After each test session the report is submitted to ETSI

Tests Outcomes

Total	Passed	Failed	Not Applicable
156	85	14	57
	85,9 %	14,1 %	36,5%

F-Interop Online testing tool



Tests for:

- 6TiSCH
- CoAP
- 6LoWPAN
- LWM2M
- OSCOAP
- 6TiSCH-join
- EDHOC
- LoRaWAN
- *your tests here!*

Implements

- 6TiSCH
- CoAP
- 6LoWPAN

RPL test shown

Feedback for the WG

- It works!
- RFC8180: works on all implementations ☺
- Minor suggestions for draft-ietf-6tisch-6top-protocol:
  - In ADD command, if no cell can be reserved:
    - return error code NORES with empty CellList
    - rather than error code SUCCESS with empty CellList
  - remove the text that recommends sending a CLEAR on a generation mismatch
    - rather, discuss ”roll-back” policy

Conclusions – 1st 6TiSCH F-Interop Plugtests

- Conclusion
  - Great success! Enabled to verify interoperability of RFC8180, and maturity of other drafts
  - Progress through implementation and real testing.

- Next plugtests
  - Fully remote F-Interop based plugtests in the fall
  - Date TBA

ETSI

World Class Standards

THANKS!

Maria Rita Palattella
Luxembourg Institute of Science and Technology
maria.rita.palattella@list.lu

Summary Hackathon

Tengfei Chang

Admin

- On Sunday 16 July (14-15 was plugtests)
- ~same participants as during the plugtests
- Goals/scope (https://www.ietf.org/registration/MeetingWiki/wiki/99hackathon)
  - Champion(s)
    - Tengfei Chang
    - Peter Kietzmann
    - Remy Leone
    - Jonathan Munoz
    - Malisa Vucinic
    - Xavi Vilajosana
    - Thomas Watteyne
  - Project(s)
    - RIOT support
    - F-Interop
    - 6TiSCH Wireshark Dissector
    - ARMOUR Secure Join
    - 6LoWPAN fragmentation

Outcome

- Integration of OpenWSN stack in RIOT
  - Adaptation of RIOT hardware driver code
  - Creating OpenWSN stack package used for integrating with RIOT
  - **→ 6TiSCH is now supported in all major open-source implementations!**
- F-interop platform progress
  - updating the bootstrap of test session: flashing hardware, control remotely testing devices.
- Join Security
  - refactoring JRC code
  - generate network keys at random each time OpenVisualizer is initialized
  - **→ full 6TiSCH solution, including secure bootstrap, in OpenWSN!**
- OpenWSN
  - housekeeping: fixing and cleanup of all OpenMote and TelosB projects
  - design of commissioning (“1-touch security”) through nvparam module
  - added PIO and Configuration Option in RPL DIO (RFC6550)
  - **→ full OpenWSN/Contiki interop!**

draft-ietf-6tisch-6top-protocol

Qin Wang (Ed.)
Xavier Vilajosana
Thomas Watteyne

Status

- Last Update: 27 June 2017
- Version: 07
- Status: Very stable draft.
- Implementations exist
- Interoperability tests at the ETSI Plugtest
- Next
  - WGLC ?

Minor Changes

- Reviewed return codes;
  - Inverting NORES and BUSY error codes for concurrent transactions.
  - Changing error code from RESET to CELLLIST_ERR when deleting unscheduled cells.
  - Adding missing implementations.
- Received and addressed WG reviewers comments:
  - Jonathan Munoz
  - Charlie Perkins
- Since last IETF meeting:
  - Reordered sections. Merged protocol behavior and command description
  - Renamed STATUS to COUNT
  - Written-out IANA section

Plugtest Outcome

- 6P ADD
  - Always returns SUCCESS.
  - Cell List Size tells if success, partial success or failure to add
  - Proposed Change:
    - Use return code SUCCESS when fully or partially allocated
      - List will tell if total or partial
    - Use NO_RES code as a return code if none of the cells could be allocated.

Plugtest Outcome

- Correcting GEN errors without CLEAR.
  - Problem: CLEAR is costly and GEN error comes from previous transaction.
  - Before CLEAR we can do some things which require some small change:
  - Proposal:
    - In LIST and COUNT operations.
      - Do GEN checking
      - BUT also return the results of the operation.
    - Add text in 4.4.7.3 (see next slide)

Plugtest Outcome

When a schedule generation inconsistency is detected:

o If the code of the 6P Request is different from CLEAR, the node MUST reply with error code GEN_ERR.

o If the code of the 6P Request is COUNT or LIST, the node MUST execute the operations and return the requested values. This can be used by the SF to correct the inconsistency.

o If the code of the 6P Request is CLEAR, the schedule generation inconsistency MUST be ignored.

Next Steps

- Clarify use of IETF IE together with 6top Information Element
- Resolve Plugtest outcome
- WGLC?

draft-ietf-6tisch-6top-sf0-05

Diego Dujovne (Ed.)
Luigi Alfredo Grieco
Maria Rita Palattella
Nicola Accettura

Status

- Goal: Dynamic and Distributed Scheduling Function Zero for 6tisch
- News: Revision from comments
- Next: ?

Tickets

#Ticket 66, 67, 70, 71, 72, 74, 76, 78, 79, 80, 81, 84, 86, 87, 93, 94, 95: Typos, expressions, deleted text.

#Ticket 67: Transferred to sections from Intro:

- Cell Estimation Algorithm
- Allocation Policy

Tickets

#Ticket 68: Difference between allocated and used cells

- Allocated cell **reserves a resource**
- Used cell is when the **resource is filled with a packet**.

- We count those used **during the last slotframe**.
- SF0 **only allocates TX** cells to the neighbor.
- There are **no shared cells** allocated by SF0.

Tickets

#Ticket 69: Definition of overprovision

Overprovisioning:

- Is the action and effect of **increasing a value representing an amount of resources**.

- In the case of SF0, overprovisioning is done as **a provision to reduce traffic variability effects on packet loss**, to the expense of **artificially allocating a number of cells.**

Tickets

#Ticket 75: Relocation

- It is defined on section **4.3.3 of the 6P draft**
- SF0 **only decides when** the relocation mechanism is activated.
- The replacement cells are **selected randomly** among the available ones.
- There are **no retransmissions** on SF0. If the allocation fails and the bad PDR condition prevails, retriggered on the next slotframe.

Tickets

#Ticket 77: Triggering events

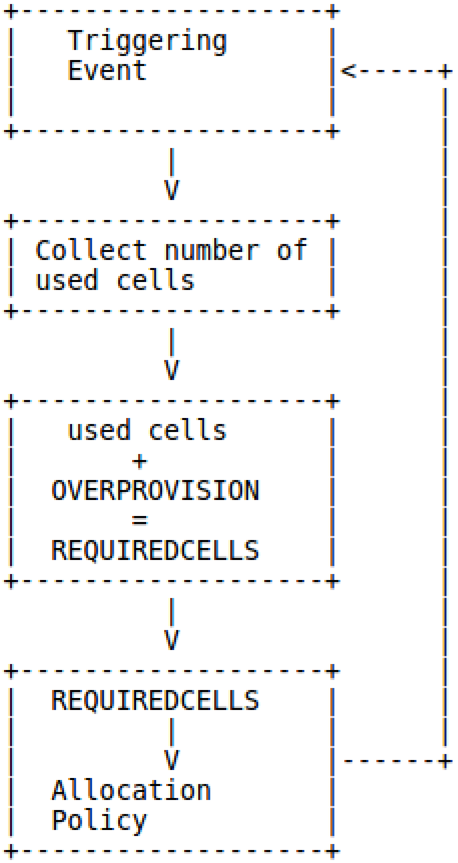
- There is only one triggering event left: When there is a **change in the number of used cells** towards any of the neighbours

#Ticket 82, 83: Cell Estimation Algorithm

- Collect the number of used cells **towards a particular neighbor during the last slotframe**

Tickets

#Ticket 85: Flow diagram for Cell Estimation Algorithm



```
+-------------------+
|   Triggering      |
|   Event           |<-----+
|                   |      |
+-------------------+      |
          |                |
          V                |
+-------------------+      |
| Collect number of |      |
| used cells        |      |
+-------------------+      |
          |                |
          V                |
+-------------------+      |
|   used cells      |      |
|       +           |      |
|  OVERPROVISION    |      |
|       =           |      |
|  REQUIREDCELLS    |      |
+-------------------+      |
          |                |
          V                |
+-------------------+      |
|  REQUIREDCELLS    |      |
|         |         |      |
|         V         |------+
|  Allocation       |
|  Policy           |
+-------------------+
```

Tickets

#Ticket 88: OVERPROVISION value

- It is implementation-specific
- A value of 0 (Zero):
  - **Case 1:** The number of scheduled cells is equal to the number of used cells: the algorithm cannot detect an increase in cell usage. Since there is no space for new packets to the neighbour, they are dropped at the queue.
  - **Case 2:** The number of scheduled cells is higher than the number of used cells: the algorithm detects an increase in cell usage. However, the number of used cells will tend to fill the scheduled cells and it will fall into Case 1.
- Conclusion: Zero means that the number of scheduled cells towards a neighbor **will not grow on top of the initial value**.

Tickets

#Ticket 89: OVERPROVISION relationship with SF0THRESH

- There is **no intended relationship**.
- They are independent on purpose to keep modularity.
- The Cell Estimation Algorithm decides **how many** cells to schedule
- The Allocation Policy decides **when** to schedule
- Along the history of SF0, we have changed the Cell Estimation Algorithm without changing the Allocation Policy. This results in complete separation between the two blocks

Tickets

#Ticket 90: CellList error handling

- SF0 **does not handle errors**. If a transaction does not succeed, it will be triggered on the next slotframe if the change in resources is still not satisfied.
- The cells on the CellList will be **randomly chosen**. Although we can add an advantage from the CellList response, we try to keep SF0 simple.

Tickets

#Ticket 91: 6P Timeout value

- SF0 has now a **per-transaction timeout value** which is implementation-specific.

#Ticket 92: PDR Definition

- Packet Delivery Rate (PDR) **is calculated per cell**, as the **percentage** of acknowledged packets, for the **last 10 packet transmission attempts**. There is no retransmission policy on SF0.

Tickets

#Ticket 96: Allocation Policy mechanism

- Initial Value of SCHEDULEDCELLS:

  Node Behavior at Boot

  - “In order to define a known state after the node is restarted, a CLEAR command is issued to each of the neighbor nodes to enable a new allocation process and **at least a SF0THRESH number of cells MUST be allocated to each of the neighbours.”**
  - SFOTHRESH value is implementation-specific

- There is **no formula** to determine the number of cells to ADD or DELETE. The number of cells to ADD or DELETE is implementation-specific
- SF0THRESH is supposed to be a **fixed value**. A variable SF0THRESH has not been considered for the draft to keep it simple.

SF0 / Questions

Questions?

Diego Dujovne
Diego.dujovne@mail.udp.cl
Universidad Diego Portales
Faculty of Engineering
School of Informatics and Telecommunications
Santiago, Chile

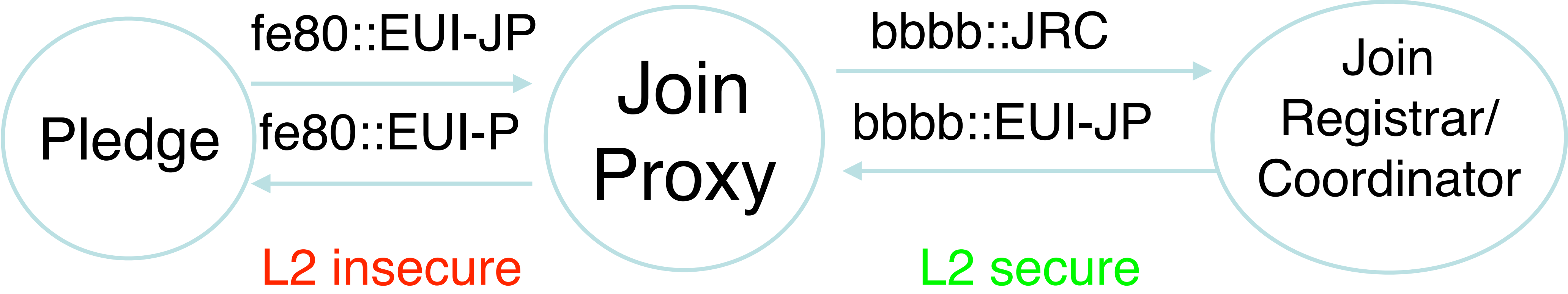
draft-ietf-6tisch-minimal-security

Mališa Vučinić, Inria
Jonathan Simon, Analog Devices
Kris Pister, UC Berkeley
Michael Richardson, Sandelman Software Works

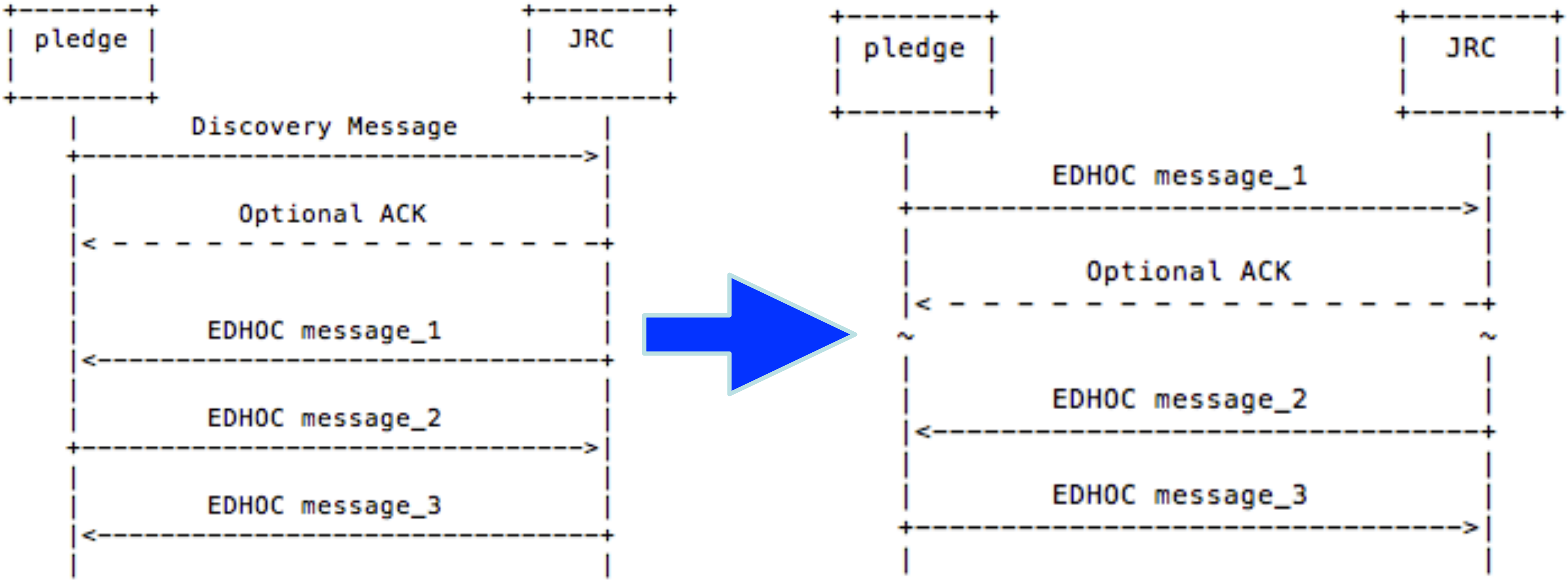
Status

- News
  - draft-ietf-6tisch-minimal-security-03
  - Published on June 15th 2017
- Implementation with PSKs in OpenWSN completed, Contiki ongoing
- Summary of updates in -03

Communication Overview



Update #1: Security Handshake



```
+----------+                 +----------+
| pledge   |                 |   JRC    |
|          |                 |          |
+----------+                 +----------+
    |      Discovery Message      |
    +---------------------------->|
    |                             |
    |        Optional ACK         |
    |<- - - - - - - - - - - - - - +
    |                             |
    |                             |
    |       EDHOC message_1       |
    |<----------------------------+
    |                             |
    |       EDHOC message_2       |
    +---------------------------->|
    |                             |
    |       EDHOC message_3       |
    |<----------------------------+
    |                             |
```

```
+----------+                   +----------+
| pledge   |                   |   JRC    |
|          |                   |          |
+----------+                   +----------+
    |                               |
    |        EDHOC message_1        |
    +------------------------------>|
    |                               |
    |          Optional ACK         |
    |<- - - - - - - - - - - - - - - +
    ~                               ~
    |                               |
    |        EDHOC message_2        |
    |<------------------------------+
    |                               |
    |        EDHOC message_3        |
    +------------------------------>|
    |                               |
```

- Optional with PSKs
- Mandatory with asymmetric keys

Update #2: How pledge learns JRC address

- Join Proxy (JP) statelessly forwards to JRC
- How JP knows the address of JRC?
    - Learns at join time when it acted as a pledge
    - Join Response now contains the address
    - Omitted if JRC is co-located with DAG root, implied from DODAG ID
    - Assumption: DAG root pre-configured with the address

Update #3: Mandatory to Implement Algorithms

- AEAD algorithm:
  - AES_CCM_16_64_128 from COSE
  - 8 byte authentication tag
  - Corresponds to 802.15.4 CCM* in nonce length
- Hash:
  - SHA-256
- Asymmetric:
  - P-256 Elliptic Curve (secp256r1)
  - ECDSA with SHA-256 signature algorithm

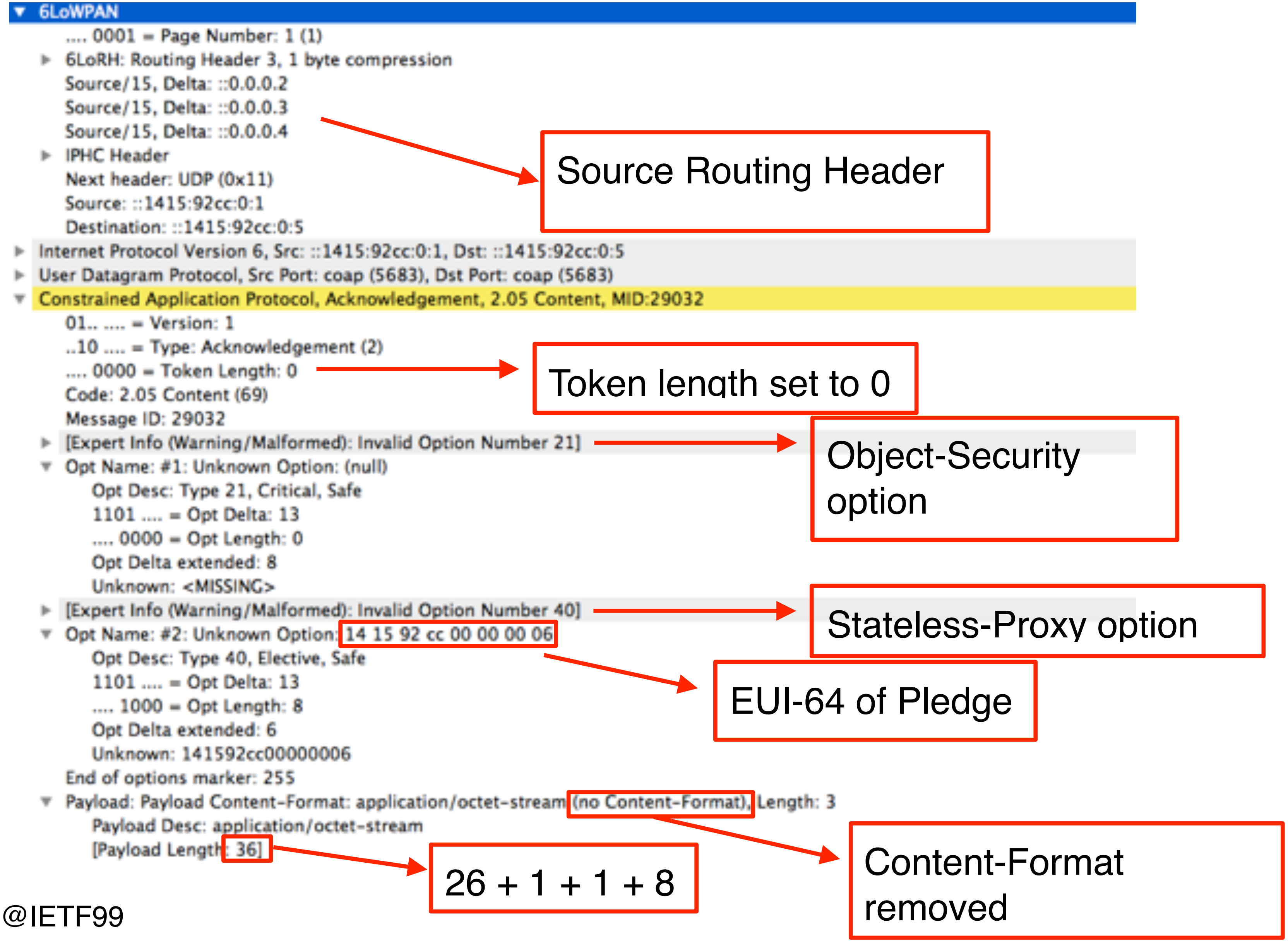
Implementation Status

- In OpenWSN ecosystem with Pre-Shared Keys:
  - draft-ietf-core-object-security-03 in Python
  - draft-ietf-6tisch-minimal-security-03 in Python (JRC)
  - draft-ietf-core-object-security-03 in C
  - draft-ietf-6tisch-minimal-security-03 in C (Pledge and Join Proxy)
- In Contiki:
  - draft-ietf-core-object-security-03
  - draft-ietf-6tisch-minimal-security-03 (ongoing)
  - draft-selander-ace-cose-ecdhe-07 (ongoing)

Implementation Experience

- Issue #1: Problems to fit Join Response in 127 bytes with multiple hops
  - Bottleneck is the link from DAG root to first hop
  - Due to the source routing header, there is a limit on max depth of the network without fragmentation
- Issue #2: Policy by which JP should accept insecure L2 frames from pledges
- Additional clarifications in the document needed on hooks to lower layers

Issue #1: Packet size



```
▼ 6LoWPAN
      .... 0001 = Page Number: 1 (1)
    ▶ 6LoRH: Routing Header 3, 1 byte compression
      Source/15, Delta: ::0.0.0.2
      Source/15, Delta: ::0.0.0.3
      Source/15, Delta: ::0.0.0.4
    ▶ IPHC Header
      Next header: UDP (0x11)
      Source: ::1415:92cc:0:1
      Destination: ::1415:92cc:0:5
▶ Internet Protocol Version 6, Src: ::1415:92cc:0:1, Dst: ::1415:92cc:0:5
▶ User Datagram Protocol, Src Port: coap (5683), Dst Port: coap (5683)
▼ Constrained Application Protocol, Acknowledgement, 2.05 Content, MID:29032
      01.. .... = Version: 1
      ..10 .... = Type: Acknowledgement (2)
      .... 0000 = Token Length: 0
      Code: 2.05 Content (69)
      Message ID: 29032
    ▶ [Expert Info (Warning/Malformed): Invalid Option Number 21]
    ▼ Opt Name: #1: Unknown Option: (null)
         Opt Desc: Type 21, Critical, Safe
         1101 .... = Opt Delta: 13
         .... 0000 = Opt Length: 0
         Opt Delta extended: 8
         Unknown: <MISSING>
    ▶ [Expert Info (Warning/Malformed): Invalid Option Number 40]
    ▼ Opt Name: #2: Unknown Option: 14 15 92 cc 00 00 00 06
         Opt Desc: Type 40, Elective, Safe
         1101 .... = Opt Delta: 13
         .... 1000 = Opt Length: 8
         Opt Delta extended: 6
         Unknown: 141592cc00000006
      End of options marker: 255
    ▼ Payload: Payload Content-Format: application/octet-stream (no Content-Format), Length: 3
         Payload Desc: application/octet-stream
         [Payload Length: 36]
```

Source Routing Header

Token length set to 0

Object-Security option

Stateless-Proxy option

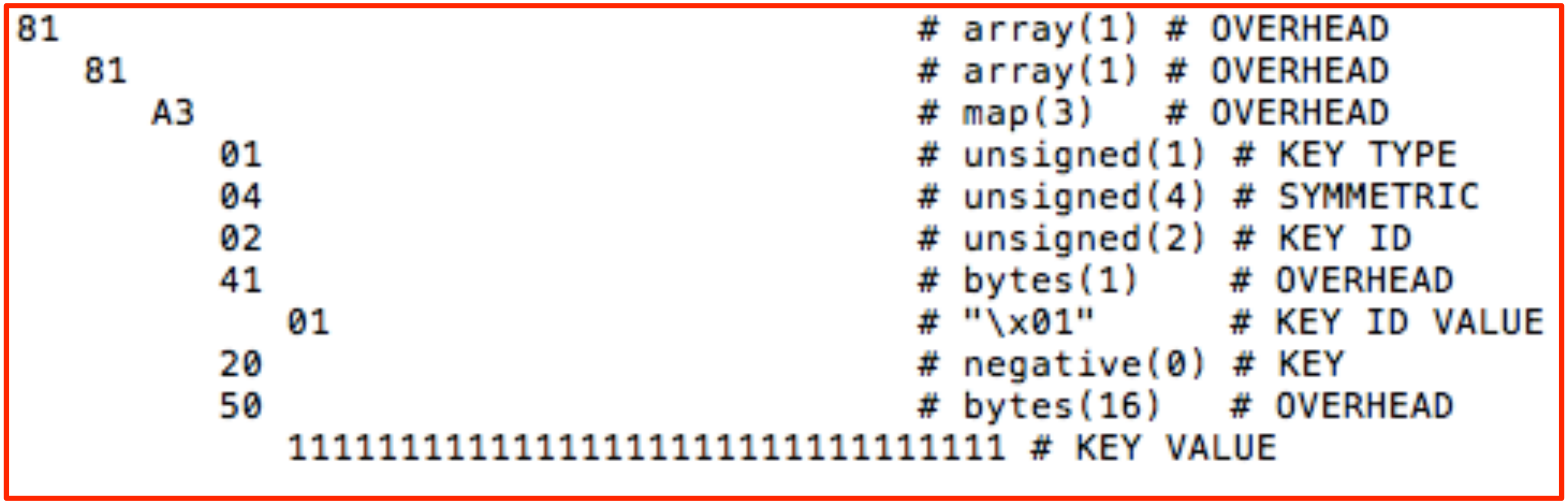
EUI-64 of Pledge

Content-Format removed

26 + 1 + 1 + 8

Issue #1: Packet size

- Join Response without short and JRC's address



```
81                                      # array(1) # OVERHEAD
   81                                   # array(1) # OVERHEAD
      A3                                # map(3)   # OVERHEAD
         01                             # unsigned(1) # KEY TYPE
         04                             # unsigned(4) # SYMMETRIC
         02                             # unsigned(2) # KEY ID
         41                             # bytes(1)    # OVERHEAD
            01                          # "\x01"      # KEY ID VALUE
         20                             # negative(0) # KEY
         50                             # bytes(16)   # OVERHEAD
            11111111111111111111111111111111 # KEY VALUE
```

- 26 bytes to encode key (16 bytes) and key ID (1 byte)
- Uses CBOR + COSE structures
- Can be optimized with compressed COSE approach like used in OSCOAP

Issue #2: Join Proxy Policy

- Proposal: Provide a mechanism to accept insecure L2 packets at JP only upon a trigger (i.e. DAG root button press)

- Needed signal that join is allowed in EB
  - One option to use draft-richardson-6tisch-join-enhanced-beacon
  - Another option to reserve 0xFF of Join Metric in EBs to signal that node will NOT accept insecure L2 frames
    - Upon a trigger, fill Join Metric with the value according to RFC8180 (calculated from the DAG rank)

Conclusion

- PSK variant stable and implementation ready
- Settled down for EDHOC roles in the asymmetric variant, yet to implement
- Implementations of PSK variant available
- Will publish -04 with implementation experience before WGLC
- Reviews welcome

draft-…-6tisch-dtsecurity-secure-join-01.txt

Michael Richardson
Benjamin Damm

Status

- Goal: Zero-touch join protocol, inspired from ANIMA BRSKI work.
- News:
  - ANIMA voucher document (“ownership claim token”) is almost in WGLC. (GRASP is in RFC-editor queue)
  - ANIMA BRSKI document was rewritten in April/May, and is much more readable.
  - Area Directors will find a home for EDHOC this week.
-

Status – Next Steps

- Rewrite dtsecurity-secure-join to parallel BRSKI document with:
  - TLS → EDHOC,
  - HTTP → CoAP
  - minimal-security Join Request bootstrapped
- There should be a virtual 1:1 between sections in BRSKI and dtsecurity-secure-join.
  - This could result in some empty sections: tell me this makes sense.
  - The title should change to include the words “zero-touch”

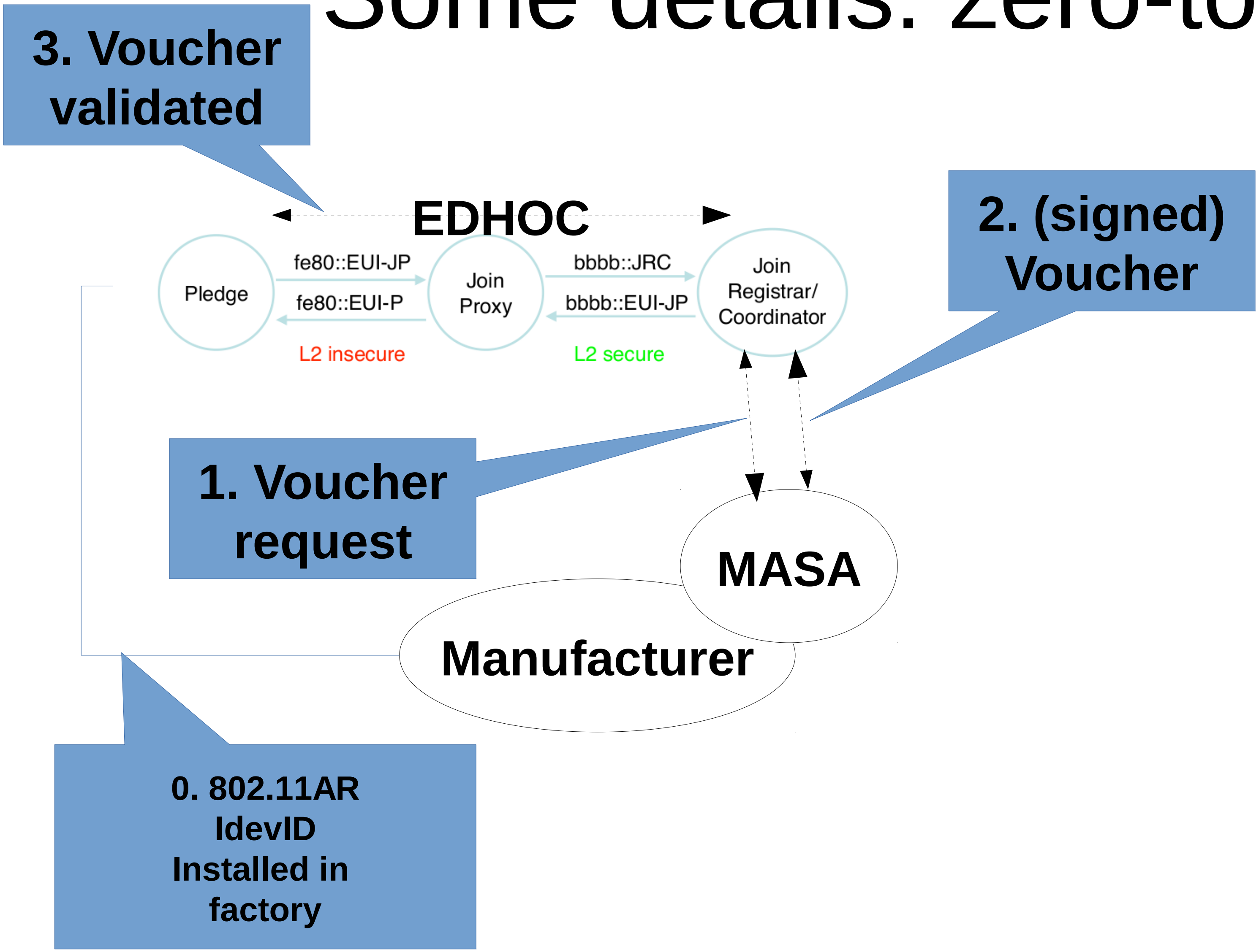
Related documents: Enhanced Beacon

- IEEE802.15.4 Informational Element encapsulation of 6tisch Join Information
- draft-richardson-6tisch-join-enhanced-beacon-01
- Authors: Michael Richardson and Diego Dujovne.
  - Awaiting WG adoption.
  - Enhancements suggested by 6tisch minimal to permit 0xff join preference to indicate “turn off join” (proxy).

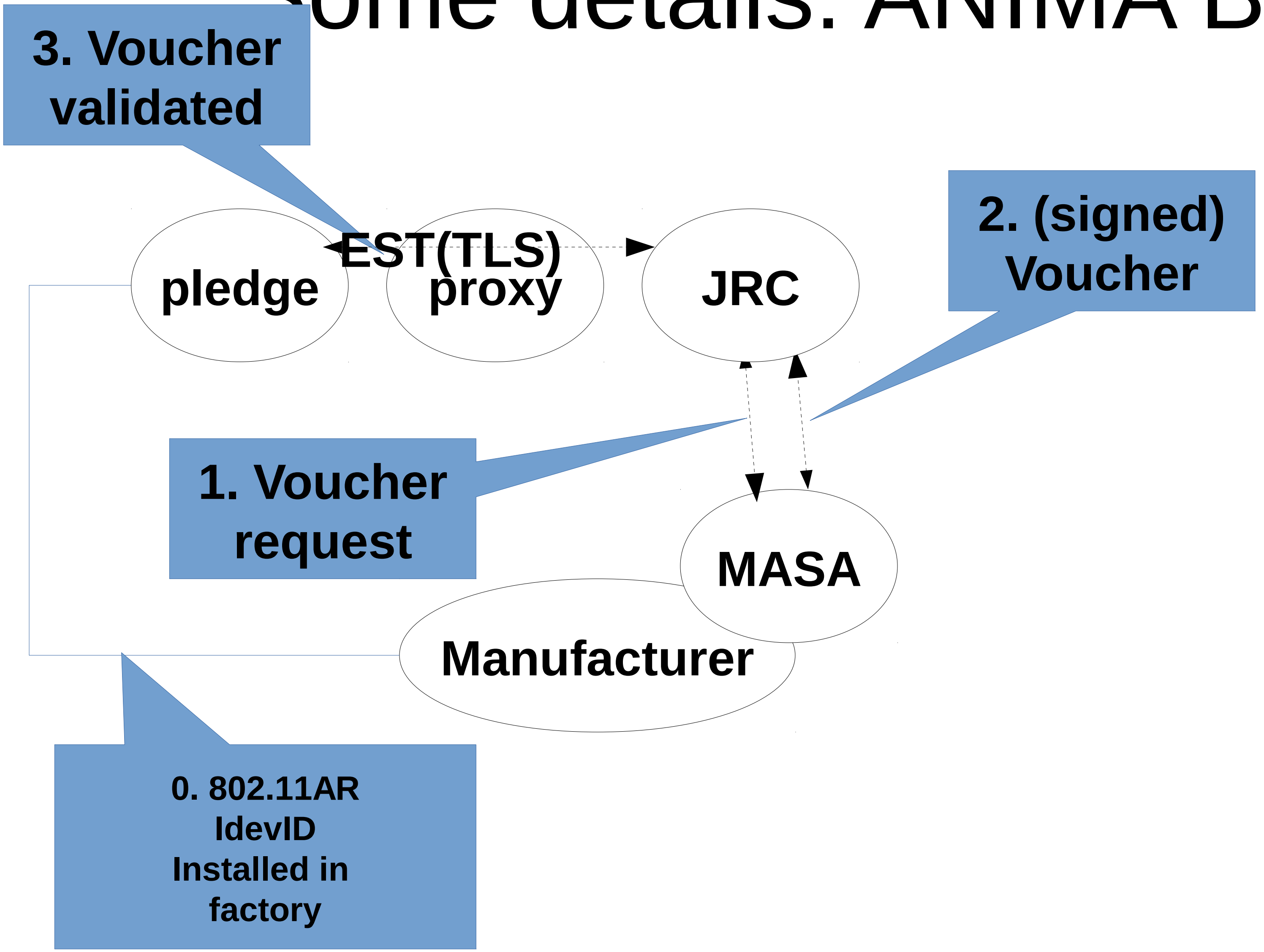
Related documents:

- Minimal Security rekeying mechanism for 6TiSCH
  - draft-richardson-6tisch-minimal-rekey-02
- Authors: Michael Richardson, Peter van der Stok.
  - Needs revision and work.
  - Intended to be COMI based, using keys setup from minimal-security and/or EDHOC. Details of keying are not yet stable.
- Covers case of network that either lives long enough to need a rekey, or any network that might need to remove a malicious/p0wned node from it’s network.

Some details: zero-touch



Some details: ANIMA BRSKI



Some other contrasts

6tisch

- Pledge discovers Proxy vis Enhanced Beacon
- Proxy provisioned with Pledge address via JoinRequest
- CoAP/EDHOC/ OSCOAP

ANIMA/BRSKI

- Pledge discovers Proxy vis GRASP M_FLOOD
- Proxy discovers JRC via GRASP
- TLS/EST
  - Leading to LDevID, and creation of ACP.

BRSKI diagram from TXT

```
                                          .
                                          .+------------------------+
   +--------------Drop Ship-------------->.| Vendor Service         |
   |                                      .+------------------------+
   |                                      .| M anufacturer|         |
   |                                      .| A uthorized  |Ownership|
   |                                      .| S igning     |Tracker  |
   |                                      .| A uthority   |         |
   |                                      .+--------------+---------+
   |                                      ..............   ^
   V                                                       |
+-------+     ............................................|...
|       |     .                                           |  .
|       |     .  +------------+       +-----------+       |  .
|       |     .  |            |       |           |       |  .
|Pledge |     .  |   Circuit  |       | Domain    <-------+  .
|       |     .  |   Proxy    |       | Registrar |          .
|      <-------->            <------->            |          .
|       |     .  |            |       |           |          .
|X.509  |     .  +------------+       +-----+-----+          .
|IDevID |     .                             |                .
|       |     .           +-----------------+----------+     .
|       |     .           | Key Infrastructure         |     .
|       |     .           | (e.g. PKI Certificate      |     .
+-------+     .           |       Authority)           |     .
              .           +----------------------------+     .
              .                                              .
              ................................................
                            "Domain" components
```

Innovation Liaison Officer

Xavi Vilajosana

draft-duquennoy-6tisch-asf

Simon Duquennoy, Inria
Xavi Vilajosana, UOC
Thomas Watteyne, Inria

Overview

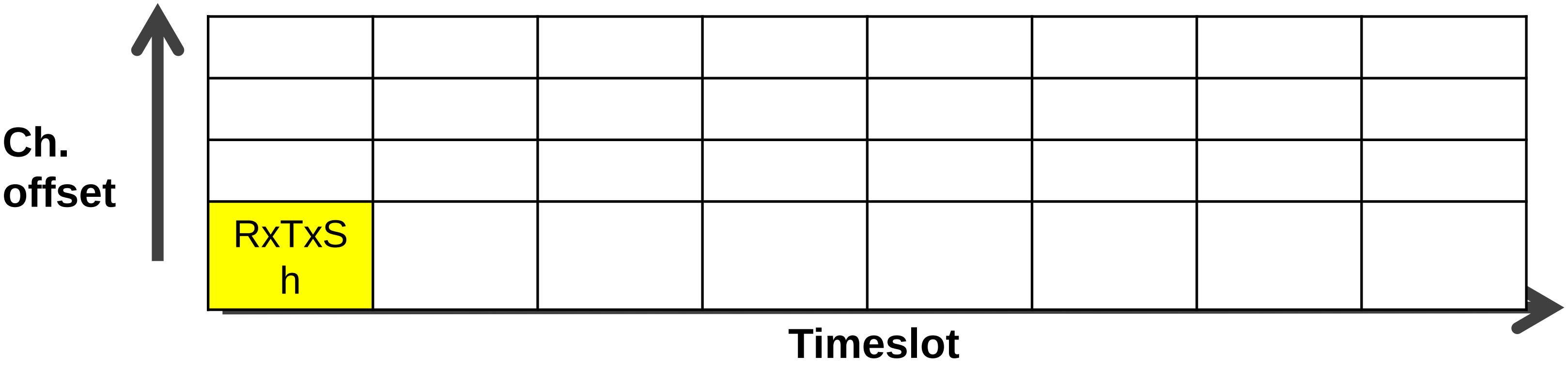
- ASF: Autonomous Scheduling Function
- 1) Autonomous slotframes
  - – Slots based on a hash of neighbor’s MAC address
  - – Slots added/removed locally, no extra signaling
- 2) Slotframe per traffic plane
  - – E.g. one for TSCH sync, one for RPL control, one for application
  - – The length of each slotframe dictates per-plane capacity

Application and Limitations

- High reliability over distributed routing
  - Schedule adapts instantly to what e.g. RPL decides
  - 5 nines demonstrated in 100+ node testbeds
- No stringent energy/latency requirements
  - Cells are not cascaded along the path
  - Only shared slots
  - Schedule is provisioned for worst case

1/3: Rendez-vous slotframe

- Equivalent to 6tisch-minimal RFC 8180
- Used for rendez-vous
- E.g. RPL control, 6LoWPAN-ND, etc.



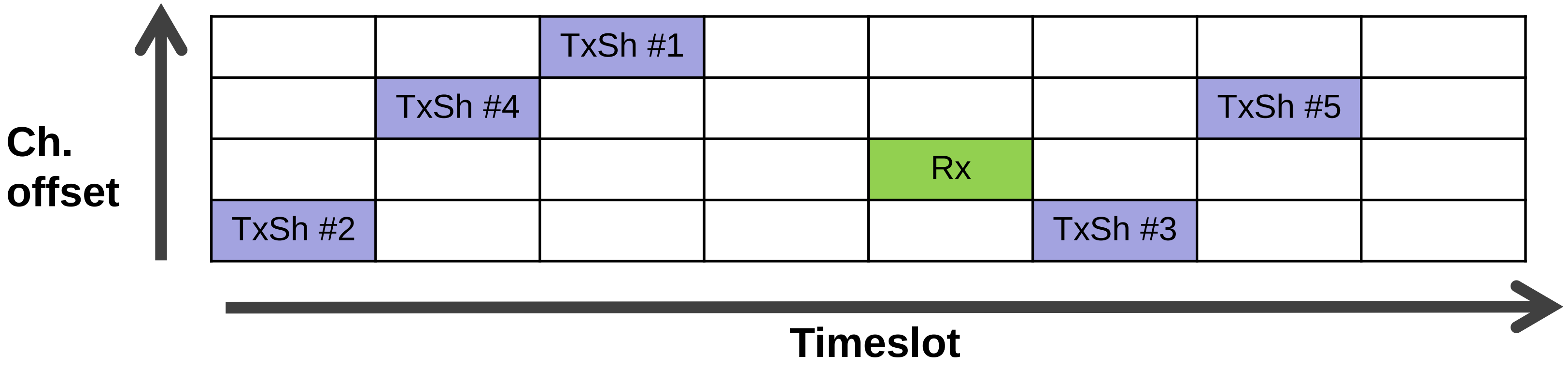
Ch. offset

RxTxSh

Timeslot

2/3 Receiver-based slotframe

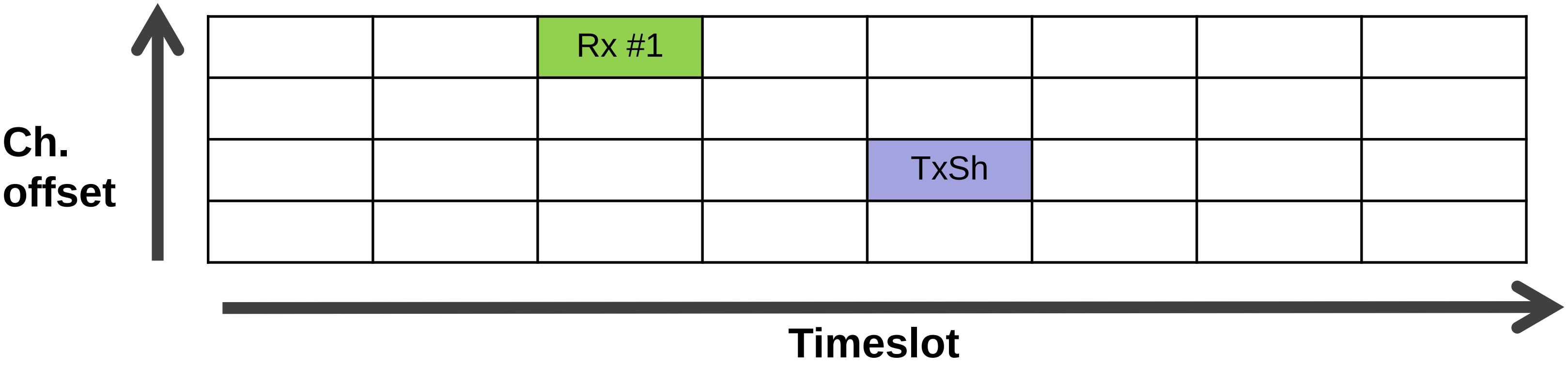
- Nodes have one fixed Rx cell
- Nodes have one Tx (Shared) cell for each neighbor (IPv6 nbr cache)
- E.g. use for unicast to any neighbor



		TxSh #1					
	TxSh #4					TxSh #5	
				Rx			
TxSh #2					TxSh #3		

3/3 Sender-based slotframe

- Nodes have one fixed Tx (Shared) cell
- Nodes have one Rx cell for each neighbor (IPv6 nbr cache)
- E.g. use for received from a privileged neighbor, e.g. TSCH time source



Putting it all together

- Each slotframe takes care of a traffic plane (traffic filter)
- Each slotframe uses a different subset of ch. offset
- As slotframes repeat, cells will overlap
  - – Apply standard IEEE slot precedence
  - – Slotframe len that are co-prime are preferred

Draft Status

- Description of the slotframe types
- Definition of cell coordinates (hash of MAC)
- Example schedule with 4 slotframes
- Definition of configuration parameters
- Open issue: configuration discovery
  - Proposal: new EB IEs
  - Other option: 6P commands (not preferred because adds a transition state between minimal and ASF)

Feedback?

- On the nature of ASF and its slotframes?
- On what the draft should cover and not?
- On configuration parameters?
- On configuration discovery?
- Anything else?

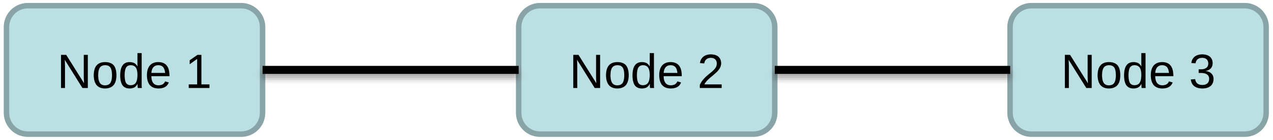
draft-munoz-6tisch-examples-02

Jonathan Munoz
Emmanuel Riou
Dominique Barthel

What? Why?

- Goal
  - informational
  - examples of different 6TiSCH frames

- Tools and setup
  - 3 nodes running OpenWSN in simulation mode
  - captured using latest official Wireshark build



TOC

- Table of Contents
- 1. TEMPORARY EDITORIAL NOTES
- 2. Tools Used
- 3. Network Topology
- 4. Examples Frames
  - 4.1. Enhanced Beacon
  - 4.2. RPL DIO
  - 4.3. RPL DAO
    - 4.3.1. RPL DAO from 2
    - 4.3.2. RPL DAO from 3
  - 4.4. ACK Frame
  - 4.5. ICMPv6 echo request/reply
    - 4.5.1. ping 2
    - 4.5.2. ping 3
  - 4.6. 6P Commands and Response
    - 4.6.1. 6P ADD
    - 4.6.2. 6P COUNT
    - 4.6.3. 6P DELETE
    - 4.6.4. 6P RELOCATE
    - 4.6.5. 6P LIST
    - 4.6.6. 6P CLEAR

5. IANA Considerations
6. Security Considerations
7. Acknowledgments
8. External Informative References
Authors' Addresses

[ping 3] ICMPv6 echo request 1->2

```
IEEE 802.15.4 Data, Dst: 14:15:92:cc:00:00:00:02,
                    Src: 14:15:92:cc:00:00:00:01
Frame Control Field: 0xec21, Frame Type: Data
    .... .... .... .001 = Frame Type: Data (0x0001)
    .... .... .... 0... = Security Enabled: False
    .... .... ...0 .... = Frame Pending: False
    .... .... ..1. .... = Acknowledge Request: True
    .... .... .0.. .... = Intra-PAN: False
    .... ...0 .... .... = Sequence Number Suppression: False
    .... ..0. .... .... = Information Elements present: False
    .... 11.. .... .... = Destination Addressing Mode:
                          Long/64-bit (0x03)
    ..10 .... .... .... = Frame Version: 2
    11.. .... .... .... = Source Addressing Mode:
                          Long/64-bit (0x03)

Sequence Number: 34
Destination PAN: 0xcafe
Destination: 14:15:92:cc:00:00:00:02 (14:15:92:cc:00:00:00:02)
Extended Source: 14:15:92:cc:00:00:00:01
(14:15:92:cc:00:00:00:01)
FCS: 0x0366 (Correct)
6LoWPAN
.... 0001 = Page Number: 1
6LoRH: Routing Header 3, 8 byte compression
    100. .... = Routing Header 6lo: Critical Routing Header
(0x04)
    ...0 0000 .... .... = 6loRH Hop Number - 1: 0x0000
    .... .... 0000 0011 = 6loRH Type: Routing Header 3,
                          8 byte compression (0x0003)
Source/8, Delta: ::1415:92cc:0:2
```

```
IPHC Header
    011. .... = Pattern: IP header compression (0x03)
    ...1 1... .... .... = Traffic class and flow label:
Version, traffic class, and flow label compressed (0x0003)
    .... .0.. .... .... = Next header: Inline
    .... ..00 .... .... = Hop limit: Inline (0x0000)
    .... .... 0... .... = Context identifier extension: False
    .... .... .0.. .... = Source address compression:
Stateless
    .... .... ..00 .... = Source address mode: Inline (0x0000)
    .... .... .... 0... = Multicast address compression: False
    .... .... .... .0.. = Dest address compression: Stateless
    .... .... .... ..00 = Dest address mode: Inline (0x00)
Next header: ICMPv6 (0x3a)
Hop limit: 64
Source: bbbb::1
Destination: bbbb::1415:92cc:0:3
Internet Protocol Version 6, Src: bbbb::1, Dst:
bbbb::1415:92cc:0:3
0110 .... = Version: 6
.... 0000 0000 .... .... .... .... .... = Traffic class:
                                0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... .... = Differentiated
                               Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... .... = Explicit
Congestion Notification: Not ECN-Capable Transport (0)
.... .... .... 0000 0000 0000 0000 0000 = Flowlabel:
0x00000000
Payload length: 18
Next header: ICMPv6 (58)
Hop limit: 64
Source: bbbb::1
Destination: bbbb::1415:92cc:0:3
Internet Control Message Protocol v6
Type: Echo (ping) request (128)
Code: 0
Checksum: 0x13f9 [correct]
Identifier: 0x3943
Sequence: 1
```

[ping 3] ICMPv6 echo request 2->3

```
IEEE 802.15.4 Data, Dst: 14:15:92:cc:00:00:00:03,
                    Src: 14:15:92:cc:00:00:00:02
Frame Control Field: 0xec21, Frame Type: Data
    .... .... .... .001 = Frame Type: Data (0x0001)
    .... .... .... 0... = Security Enabled: False
    .... .... ...0 .... = Frame Pending: False
    .... .... ..1. .... = Acknowledge Request: True
    .... .... .0.. .... = Intra-PAN: False
    .... ...0 .... .... = Sequence Number Suppression: False
    .... ..0. .... .... = Information Elements present: False
    .... 11.. .... .... = Destination Addressing Mode:
                          Long/64-bit (0x03)
    ..10 .... .... .... = Frame Version: 2
    11.. .... .... .... = Source Addressing Mode:
                          Long/64-bit (0x03)
Sequence Number: 35
Destination PAN: 0xcafe
Destination: 14:15:92:cc:00:00:00:03 (14:15:92:cc:00:00:00:03)
Extended Source: 14:15:92:cc:00:00:00:02
(14:15:92:cc:00:00:00:02)
FCS: 0x793f (Correct)
6LoWPAN
IPHC Header
    011. .... = Pattern: IP header compression (0x03)
    ...1 1... .... .... = Traffic class and flow label:
Version, traffic class, and flow label compressed (0x0003)
    .... .0.. .... .... = Next header: Inline
    .... ..00 .... .... = Hop limit: Inline (0x0000)
    .... .... 0... .... = Context identifier extension: False
    .... .... .0.. .... = Source address compression:
Stateless
```

```
 .... .... ..00 .... = Source address mode: Inline (0x0000)
    .... .... .... 0... = Multicast address compression: False
    .... .... .... .0.. = Dest address compression: Stateless
    .... .... .... ..00 = Dest address mode: Inline (0x0000)
Next header: ICMPv6 (0x3a)
Hop limit: 64
Source: bbbb::1
Destination: bbbb::1415:92cc:0:3
Internet Protocol Version 6, Src: bbbb::1, Dst:
bbbb::1415:92cc:0:3
0110 .... = Version: 6
.... 0000 0000 .... .... .... .... .... = Traffic class:
                               0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... .... = Differentiated
                               Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... .... = Explicit
Congestion Notification: Not ECN-Capable Transport (0)
.... .... .... 0000 0000 0000 0000 0000 = Flowlabel:
0x00000000
Payload length: 18
Next header: ICMPv6 (58)
Hop limit: 64
Source: bbbb::1
Destination: bbbb::1415:92cc:0:3
Internet Control Message Protocol v6
Type: Echo (ping) request (128)
Code: 0
Checksum: 0x13f9 [correct]
Identifier: 0x3943
Sequence: 1
```

[ping 3] ICMPv6 echo reply 3->2

```
IEEE 802.15.4 Data, Dst: 14:15:92:cc:00:00:00:02,
                    Src: 14:15:92:cc:00:00:00:03
Frame Control Field: 0xec21, Frame Type: Data
    .... .... .... .001 = Frame Type: Data (0x0001)
    .... .... .... 0... = Security Enabled: False
    .... .... ...0 .... = Frame Pending: False
    .... .... ..1. .... = Acknowledge Request: True
    .... .... .0.. .... = Intra-PAN: False
    .... ...0 .... .... = Sequence Number Suppression: False
    .... ..0. .... .... = Information Elements present: False
    .... 11.. .... .... = Destination Addressing Mode:
                          Long/64-bit (0x03)
    ..10 .... .... .... = Frame Version: 2
    11.. .... .... .... = Source Addressing Mode:
                          Long/64-bit (0x03)
Sequence Number: 23
Destination PAN: 0xcafe
Destination: 14:15:92:cc:00:00:00:02 (14:15:92:cc:00:00:00:02)
Extended Source: 14:15:92:cc:00:00:00:03
(14:15:92:cc:00:00:00:03)
FCS: 0x84f7 (Correct)
6LoWPAN
.... 0001 = Page Number: 1
6LoRH: Routing Protocol Information
    100. .... = Routing Header 6lo: Critical Routing Header
(0x04)
    ...0 .... .... .... = Packet direction:
                          UP false, DOWN true: False
    .... 0... .... .... = Error detected: False
    .... .0.. .... .... = No link to destination: False
    .... ..1. .... .... = Context identifier extension: True
    .... ...1 .... .... = Context identifier extension: True
    .... .... 0000 0101 = 6loRH Type: Routing Protocol
Information
```

```
 RPL Instance: 0x00
    Sender Rank: 0x07
IPHC Header
    011. .... = Pattern: IP header compression (0x03)
    ...1 1... .... .... = Traffic class and flow label:
Version, traffic class, and flow label compressed (0x03)
    .... .0.. .... .... = Next header: Inline
    .... ..10 .... .... = Hop limit: 64 (0x0002)
    .... .... 0... .... = Context identifier extension: False
    .... .... .0.. .... = Source address compression:
Stateless
    .... .... ..01 .... = Source address mode: 64-bits inline
(0x01)
    .... .... .... 0... = Multicast address compression: False
    .... .... .... .0.. = Dest address compression: Stateless
    .... .... .... ..01 = Dest address mode: 64-bits inline
(0x01)
    [Source context: fe80::]
    [Destination context: fe80::]
Next header: ICMPv6 (0x3a)
Source: fe80::1415:92cc:0:3
Destination: fe80::1
Internet Protocol Version 6, Src: fe80::1415:92cc:0:3, Dst:
fe80::1
0110 .... = Version: 6
.... 0000 0000 .... .... .... .... .... = Traffic class:
                                0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... .... = Differentiated
                               Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... .... = Explicit
Congestion Notification: Not ECN-Capable Transport (0)
.... .... .... 0000 0000 0000 0000 0000 = Flowlabel:
0x00000000
```

[ping 3] ICMPv6 echo reply 3->2

```
Payload length: 18
Next header: ICMPv6 (58)
Hop limit: 64
Source: fe80::1415:92cc:0:3
Destination: fe80::1
Internet Control Message Protocol v6
Type: Echo (ping) reply (129)
Code: 0
Checksum: 0x12f9 [incorrect, should be 0x8d6e]
    [Expert Info (Warn/Checksum): ICMPv6 Checksum Incorrect
Identifier: 0x3943
Sequence: 1
Data (10 bytes)
0000  00 01 02 03 04 05 06 07 08 09
        Data: 00010203040506070809
        [Length: 10]
```

[ping 3] ICMPv6 echo reply 2->1

```
IEEE 802.15.4 Data, Dst: 14:15:92:cc:00:00:00:01,
                    Src: 14:15:92:cc:00:00:00:02
Frame Control Field: 0xec21, Frame Type: Data
    .... .... .... .001 = Frame Type: Data (0x0001)
    .... .... .... 0... = Security Enabled: False
    .... .... ...0 .... = Frame Pending: False
    .... .... ..1. .... = Acknowledge Request: True
    .... .... .0.. .... = Intra-PAN: False
    .... ...0 .... .... = Sequence Number Suppression: False
    .... ..0. .... .... = Information Elements present: False
    .... 11.. .... .... = Destination Addressing Mode:
                          Long/64-bit (0x03)
    ..10 .... .... .... = Frame Version: 2
    11.. .... .... .... = Source Addressing Mode:
                          Long/64-bit (0x03)
Sequence Number: 36
Destination PAN: 0xcafe
Destination: 14:15:92:cc:00:00:00:01 (14:15:92:cc:00:00:00:01)
Extended Source: 14:15:92:cc:00:00:00:02
(14:15:92:cc:00:00:00:02)
FCS: 0x7dbc (Correct)
6LoWPAN
.... 0001 = Page Number: 1
6LoRH: Routing Protocol Information
    100. .... = Routing Header 6lo: Critical Routing Header
(0x04)
    ...0 .... .... .... = Packet direction:
                          UP false, DOWN true: False
    .... 0... .... .... = Error detected: False
    .... .0.. .... .... = No link to destination: False
    .... ..1. .... .... = Context identifier extension: True
    .... ...1 .... .... = Context identifier extension: True
    .... .... 0000 0101 = 6loRH Type: Routing Protocol
Information
```

```
  RPL Instance: 0x00
    Sender Rank: 0x03
IPHC Header
    011. .... = Pattern: IP header compression (0x03)
    ...1 1... .... .... = Traffic class and flow label:
Version, traffic class, and flow label compressed (0x0003)
    .... .0.. .... .... = Next header: Inline
    .... ..10 .... .... = Hop limit: 64 (0x0002)
    .... .... 0... .... = Context identifier extension: False
    .... .... .0.. .... = Source address compression:
Stateless
    .... .... ..01 .... = Source address mode: 64-bits inline
(0x01)
    .... .... .... 0... = Multicast address compression: False
    .... .... .... .0.. = Dest address compression: Stateless
    .... .... .... ..01 = Dest address mode: 64-bits inline
(0x01)
    [Source context: fe80::]
    [Destination context: fe80::]
Next header: ICMPv6 (0x3a)
Source: fe80::1415:92cc:0:3
Destination: fe80::1
Internet Protocol Version 6, Src: fe80::1415:92cc:0:3, Dst:
fe80::1
0110 .... = Version: 6
.... 0000 0000 .... .... .... .... .... = Traffic class:
                                0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 00.. .... .... .... .... .... = Differentiated
                               Services Codepoint: Default (0)
    .... .... ..00 .... .... .... .... .... = Explicit
Congestion Notification: Not ECN-Capable Transport (0)
```

[ping 3] ICMPv6 echo reply 2->1

```
.... .... .... 0000 0000 0000 0000 0000 = Flowlabel:
0x00000000
Payload length: 18
Next header: ICMPv6 (58)
Hop limit: 64
Source: fe80::1415:92cc:0:3
Destination: fe80::1
Internet Control Message Protocol v6
Type: Echo (ping) reply (129)
Code: 0
Checksum: 0x12f9 [incorrect, should be 0x8d6e]
    [Expert Info (Warn/Checksum): ICMPv6 Checksum Incorrect]
Identifier: 0x3943
Sequence: 1
Data (10 bytes)

0000  00 01 02 03 04 05 06 07 08 09
    Data: 00010203040506070809
    [Length: 10]
```

Next steps

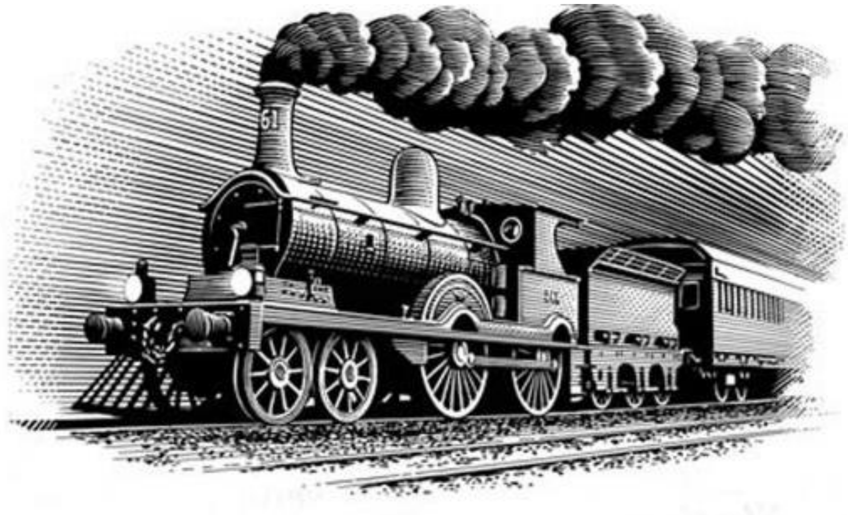
- publish -03 this week:
  - Including 6P LIST commands
  - Editorial changes
- discussion points
  - Is this useful?
  - should this be adopted by the WG?

Exploiting Packet Replication and Elimination in Complex Tracks in 6TiSCH LLNs

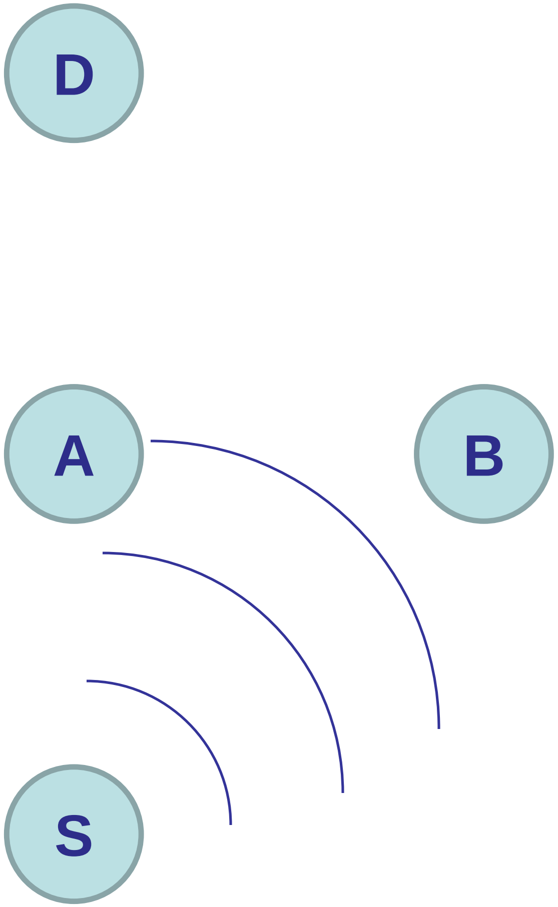
Georgios Z. Papadopoulos
Nicolas Montavont
Pascal Thubert

Toward Determinism

- In addition to reliable communication;
- The information need to be carried out in a pre-defined and constant delay;
- Should exhibit ultra-low jitter performance;

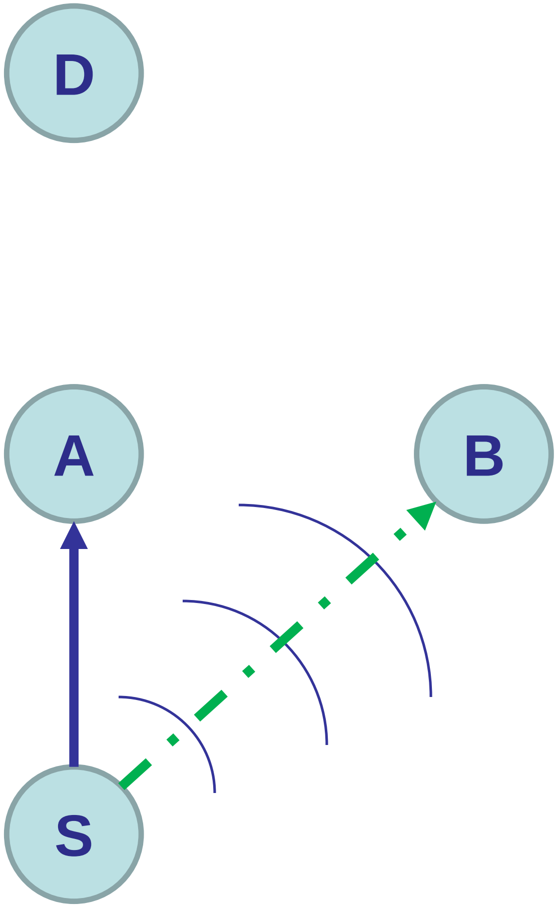


Wireless Topology



Promiscuous Overhearing

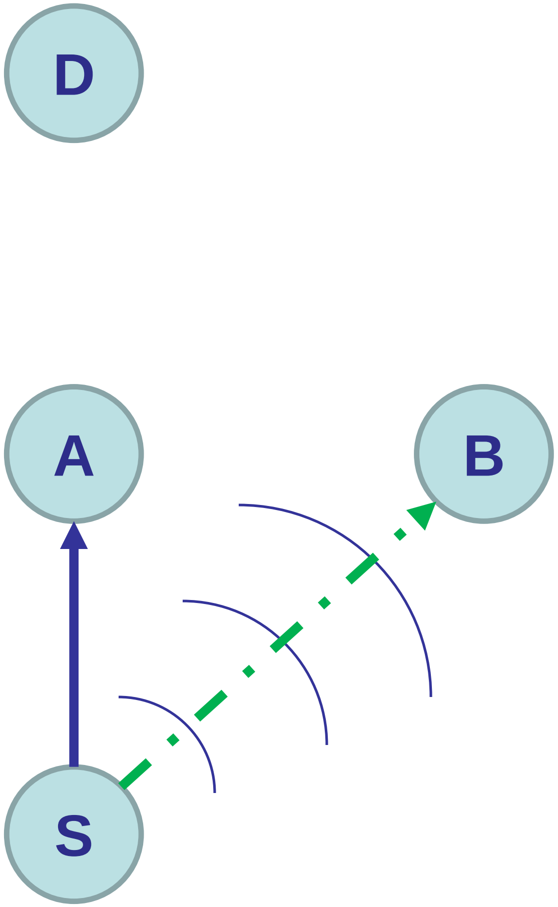
- Overhearing
  - Wireless medium is broadcast
  - any neighbor of a transmitter may overhear a transmission



- ➢ **A scheduler for multiple receivers;**
- ➢ **ACK collisions?**

Packet Replication

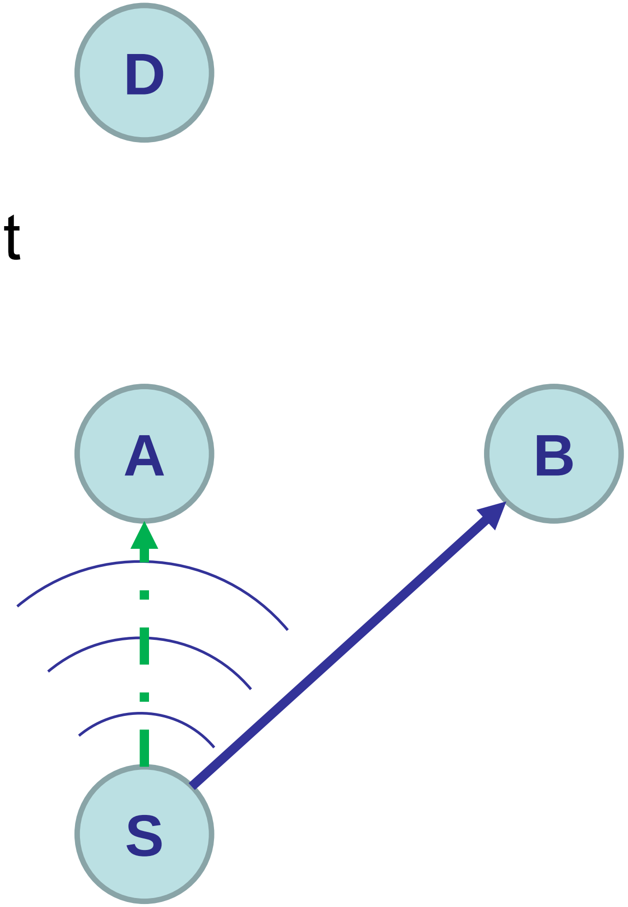
- Replication
  - Data packet is transmitted to both Default & “Alternate” Parent



Packet Replication

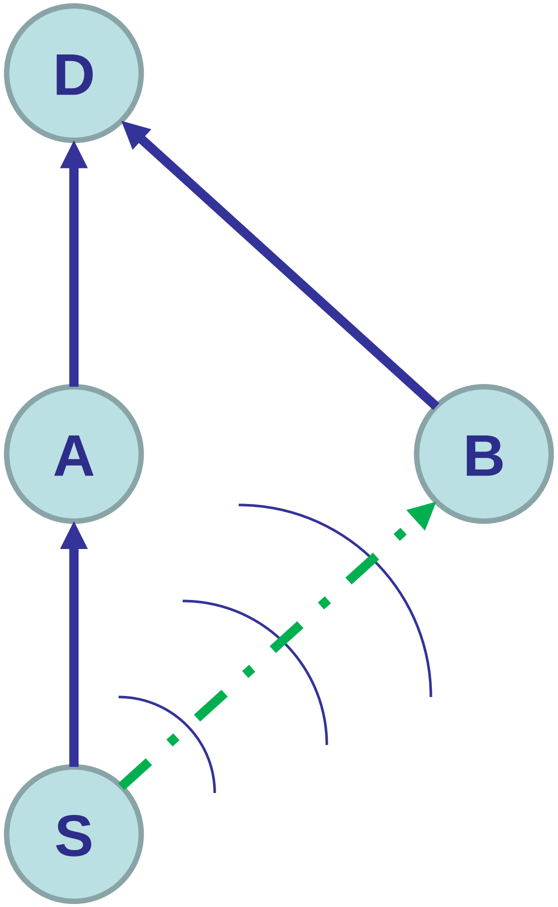
- Replication
  - Data packet is transmitted to both Default & “Alternate” Parent

➢ **`RPL DODAG Information Object (DIO) should be extended`**



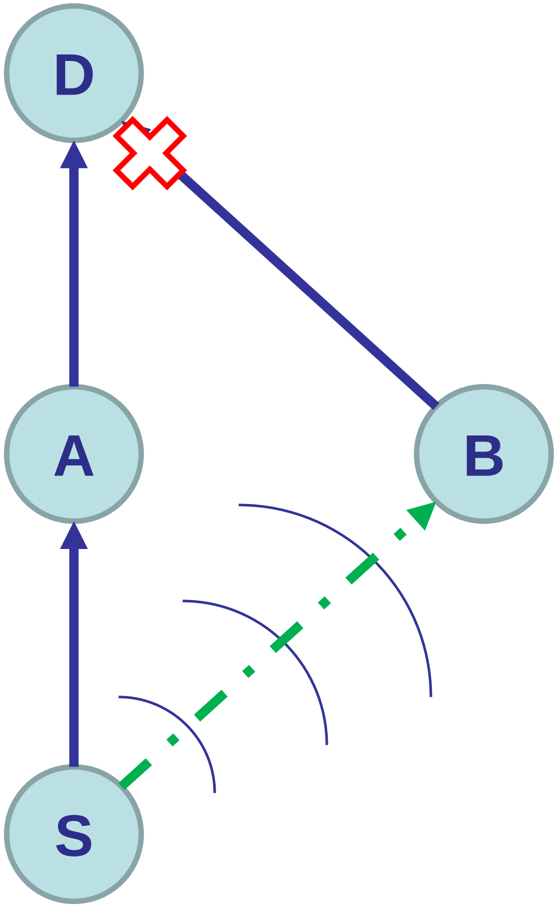
Packet Elimination

- Elimination
  - – Discard the duplicated packet “previously received packet”



Packet Elimination

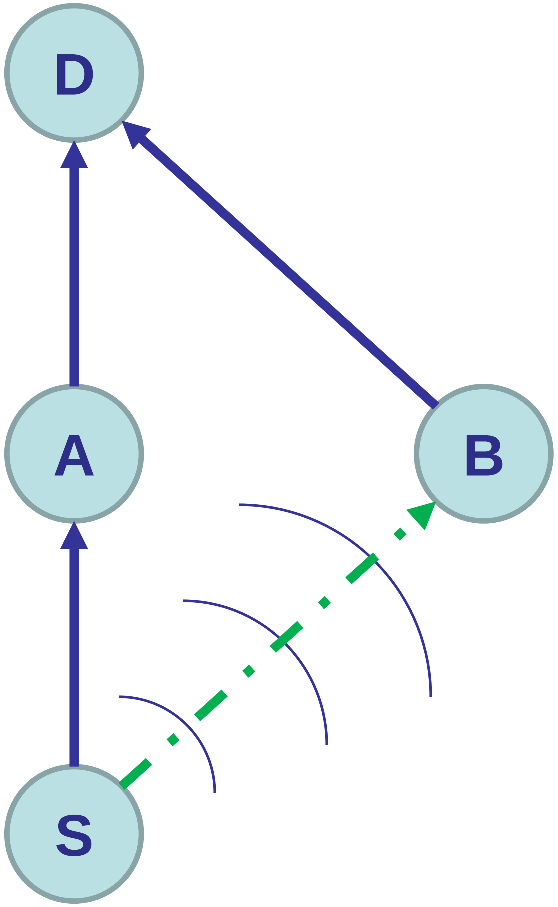
- Elimination
  - – Discard the duplicated packet “previously received packet”



➢ **Tagging Packets for Flow Identification.**

TSCH Schedule: example

Channel offset				
3		S → A S → B		
2				B → D
1				
0	EB		A → D	
	0	1	2	3
	Slotframe			



- ➢ **A scheduler for multiple receivers;**
- ➢ **6P ADD Request Format.**

Requirements

- Alternative Parent Selection;
  - RPL DODAG Information Object (DIO) message format SHOULD be extended
  - routing protocol should be extended to allow for 6TiSCH nodes to select AP(s)
- Promiscuous Overhearing;
  - 6top Protocol should be extended to allow a cell reservation with two receivers
  - 6P ADD Request Format should be transmitted either twice or once in multicast
- Cells without ACKs;
  - only one parent MUST acknowledge the data packet
  - Or an efficient way for double ACKS
- Packet Elimination.
  - Tagging Packets for Flow Identification

Feedback

- Volunteers to REVIEW the draft;
- Feedback for missed Requirements;
- Is PRE relevant in 6TiSCH WG?

Questions?

Georgios PAPADOPOULOS
georgios.papadopoulos@imt-atlantique.fr
georgiospapadopoulos.com

Packet Delivery Deadline Time in 6LoWPAN Routing Header

draft-lijo-6lo-expiration-time-04

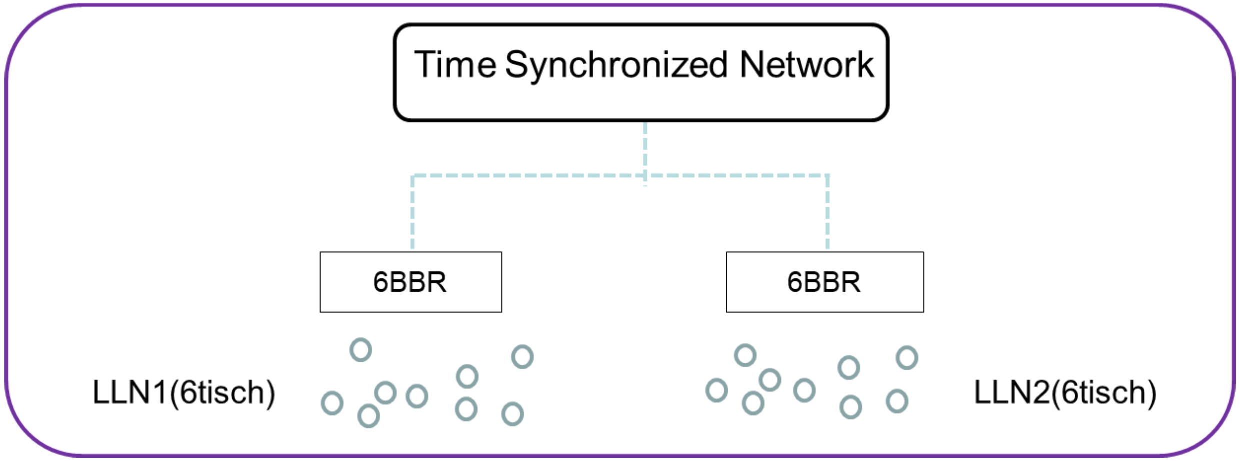
Lijo Thomas <lijo@cdac.in>
Akshay P.M <akshaypm90@gmail.com>
Satish Anamalamudi <satishnaidu80@gmail.com>
S.V.R Anand <anand@ece.iisc.ernet.in>
Malati Hegde <malati@ece.iisc.ernet.in>
Charles E. Perkins <charliep@computer.org>

Motivation and Background

- Delay sensitive industrial M2M IoT applications
- Packet expiration assists in meeting delay constraints in deterministic network
- Positive response from the 6TiSCH ML☺
- Interest from in-band-oam draft authors to include packet expiration time in IPv6 Header
- Applicability *:* 6lo, 6tisch, roll, and detnet

Overview

- Deadline-6LoRHE type for 6LoWPAN dispatch page 1
  - Carries Packet Delivery Deadline Time
  - Optional Packet Origination Time
- Enables delay-aware forwarding and scheduling decisions
- Operates on time-synchronized constrained networks
- Handles different time zones over heterogeneous networks



Deadline – 6LoRHE Format

<table>
<tr><td colspan="10"></td><td colspan="10">1</td><td colspan="10">2</td><td colspan="2">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td><td colspan="5">Length</td><td colspan="8">6LoRH Type = TBD</td><td>O</td><td>D</td><td colspan="3">DTL</td><td colspan="3">OTL</td><td colspan="2">TU</td><td colspan="3">EXP</td><td colspan="3">RSV</td></tr>
<tr><td colspan="16">DT (Variable length)</td><td colspan="16">OT (Optional) (variable length)</td></tr>
</table>

O flag (1 bit)	Origination Time flag 1: Origination Time is present 0 : Origination Time is absent
D flag (1 bit)	Drop flag 1 : SHOULD drop the packet if the deadline time is elapsed 0 : MAY ignore and forward
DTL (3 bits [bbb])	[bbb]+1 = Length of DT field 000 : Length of DTL is "1 octet" : 111 : Length of DTL is "8 octets"
OTL (3 bits [bbb])	[bbb]+1 = Length of OT field 000 : Length of OTL is "1 octet" : 111 : Length of OTL is "8 octets"

TU (2 bits)	Indicates the time units for DT and OT 00 : Time in microseconds 01 : Time in seconds 10 : Network ASN 11 : Reserved
EXP (3 bits)	Multiplication factor (exponent of base 10)
RSV (3 bits)	Reserved

DT (Variable length)	Deadline Time value (8..64-bit)

OT (Variable length)	Origination Time value (Optional) (8..64-bit)

Draft Implementation

- Implemented the draft in OpenWSN platform for a 6tisch network

- The code has been merged with OpenWSN and is available for download !!

  - https://github.com/openwsn-berkeley/openwsn-fw

  - https://github.com/openwsn-berkeley/openwsn-sw

  - Thanks OpenWSN team for your support !!!!

- Recently implemented a basic EDF scheduling policy to demonstrate the draft's applicability

Way Forward

- A scheduling function based on this draft to enable realization of applications with deadlines

Comments and Questions

Thanks !!!