IETF97 – Seoul

Chairs:
Pascal Thubert
Thomas Watteyne
Mailing list:
6tisch@ietf.org
Jabber:
6tisch@jabber.ietf.org

Etherpad for minutes:
http://etherpad.tools.ietf.org:9000/p/notes-ietf-97-6tisch

IPv6 over the TSCH mode of IEEE 802.15.4e

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 3979 (updated by RFC 4879).

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 3979 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.

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-96-6tisch
** Recordings and Minutes are public and may be subject to discovery in the event of litigation.
*** Please make sure you sign the blue sheets

Administrivia

- Blue Sheets
- Scribes
- Jabber

Agenda

Intro and Status (Chairs) [5min]

Note-Well, Blue Sheets, Scribes, Agenda Bashing

New Charter and status docs (Chairs) [10min]

Status tatus minimal, 6LoRH, 802.15 IE

Milestones

Dynamic Scheduling

<draft-ietf-6tisch-6top-protocol> (Xavier Vilajosana) [20min]

<draft-ietf-6tisch-6top-sf0> (Diego Dujovne on meetecho) [15min]

Security

<draft-vucinic-6tisch-minimal-security (Malisa Vucinic) [15min]

<draft-richardson-6tisch-dtsecurity-secure-join> (Michael Richardson) [20min]

Any Other Business [2min]

Intro and Status

Status Documents

- draft-ietf-6tisch-minimal [WG doc]
  - Thanks Charlie for reviews!
  - -16 published on 28 June
  - Current status: AD Followup
- draft-ietf-6tisch-6top-protocol [WG doc]
  - -01 published 27 June
  - Tested at ETSI plugtests
- draft-ietf-6tisch-6top-sf0 [WG doc]
  - -01 published 8 July
  - Tested at ETSI plugtests
- draft-ietf-6tisch-architecture [WG doc]
  - -10 published 10 June
- draft-satish-6tisch-6top-sf1
  - -01 published 17 July

News from ROLL and 6lo

Paging Dispatch at 6lo and Routing Dispatch at ROLL, passed IESG, passed IANA, RFC Editor queue

Backbone router WG doc being split -> RFC6775 update, asked for adoption

draft-sarikaya-6lo-ap-nd adopted at 6lo

Milestones

Apr 2016 - Second submission of draft-ietf-6tisch-minimal to the IESG

Apr 2016 - WG call to adopt draft-ietf-6tisch-6top-sf0

Apr 2016 - WG call to adopt draft-ietf-6tisch-6top-sublayer

Jul 2016 - 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

Action Plan

- Agile I-Draft->code->test then plugtest
- Security Convergence (2 stages approach)

draft-ietf-6tisch-6top-protocol

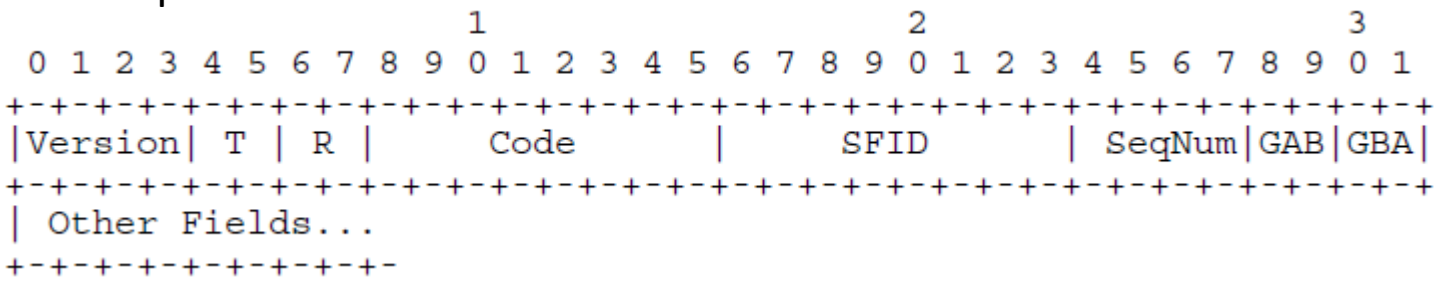
Qin Wang (Ed.)
Xavier Vilajosana

Status

- Status
  - draft-ietf-6tisch-6top-protocol-03
  - Published 31 Oct 2016
- New
  - Added type field in the 6top IE header
  - Added cellOptions to request (ADD,DELETE,STATUS, LIST)
  - Added cell suggestion in ADD response
  - Best effort number of cells in LIST response
- Next
  - Stable and ready?

Type Field

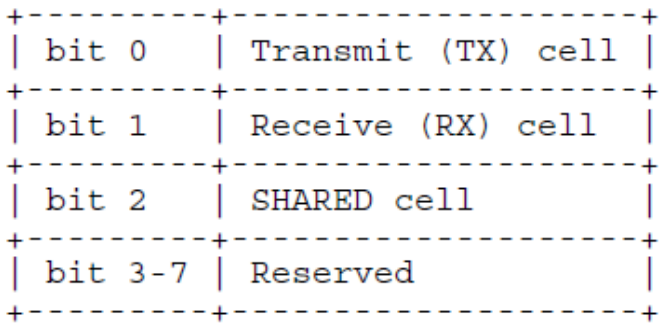
- 6top IE field



Value of the "Type" field	Meaning
b00	6P Request
b01	6P Response
b10	6P Confirmation (3-step 6top Transaction only)
b11	Reserved

Added Type field to differentiate a Request from a Response and from a Confirmation

CellOptions bitmap

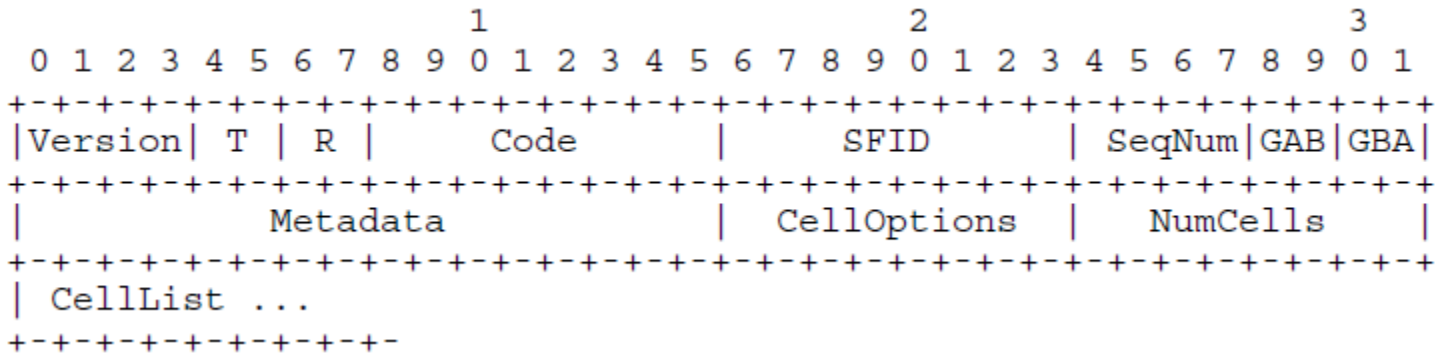


bit 0	Transmit (TX) cell
bit 1	Receive (RX) cell
bit 2	SHARED cell
bit 3-7	Reserved

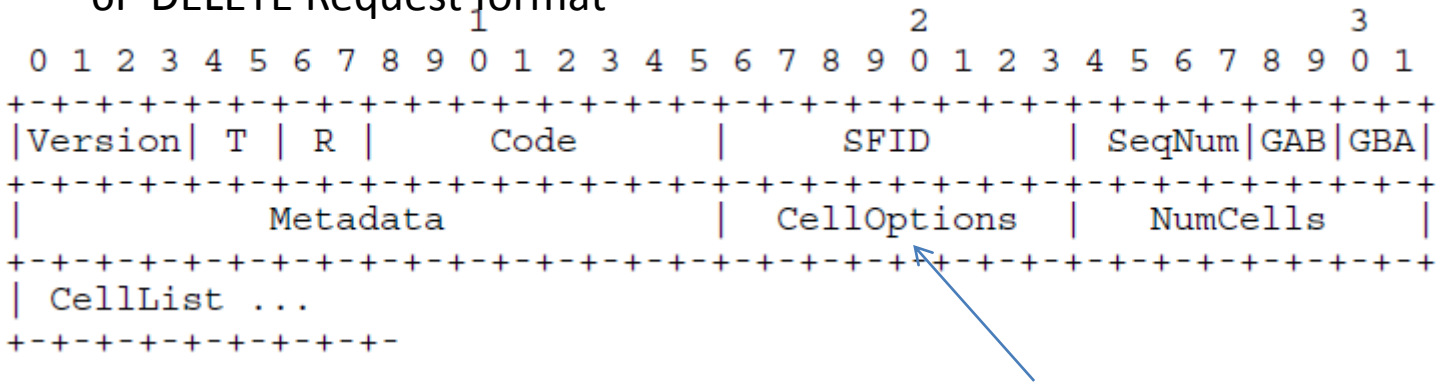
Figure 10: Format of the CellOptions field

Added a bitmap of flags to a 6P command so that a node can schedule/request/or delete TX, RX, SHARED cells
CellOptions field is used in 6P ADD, 6P DELETE, 6P STATUS, and 6P LIST Request.

- 6P ADD Request format



- 6P DELETE Request format



effective only when CellList empty

Suggestion in 6P Response

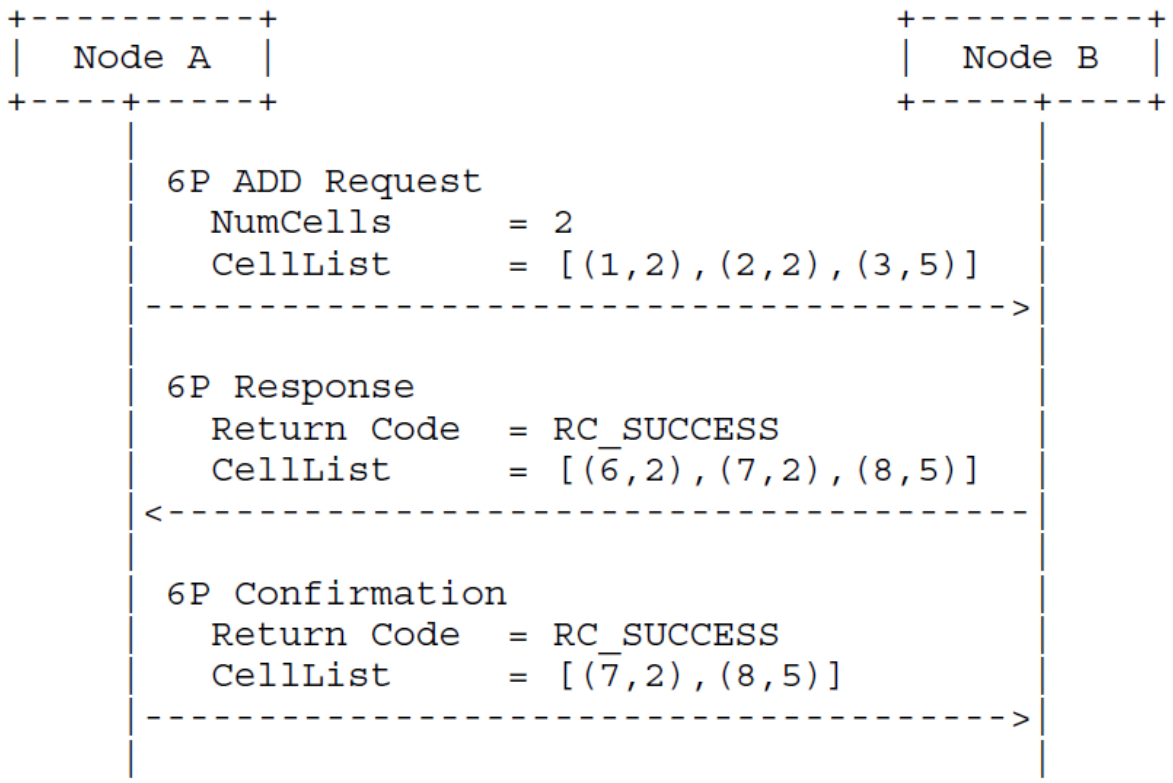
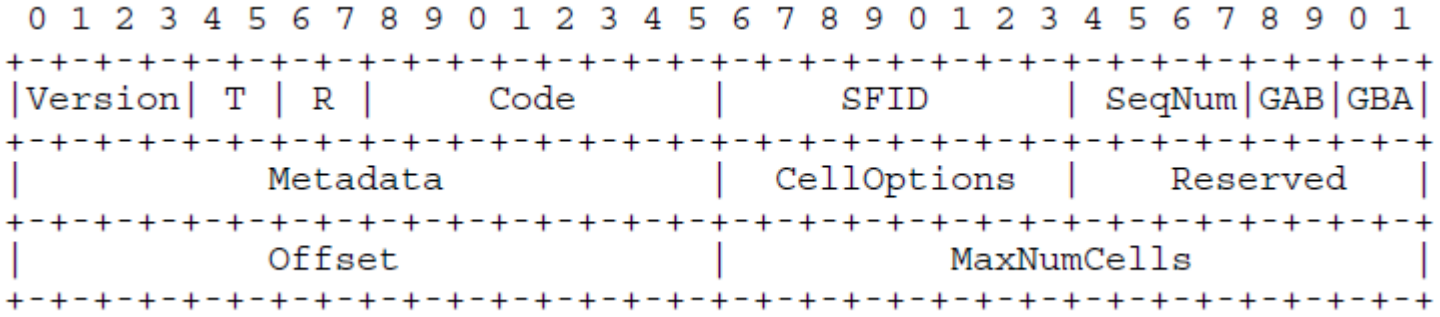


Figure 6: A 3-step 6P Transaction with cell suggestion.

On a failed 6P ADD, receiver side uses the 6P response to suggest a number of cells that are accepted

Best effort number of cells in response

- LIST Request format



Section 4.3.10

When node B receives a LIST request, the returned CellList in the 6P Response contains between 1 and MaxNumCells cells, starting from the specified Offset, as many as fit in the frame. Node B MUST return at least one cell, unless the specified Offset is beyond the end of B's cell list in its schedule. If node B has less than Offset cells of CellOptions type, the CellList it returns is empty.

Other considerations

Are we missing something?

draft-ietf-6tisch-6top-sf0

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

Cell Estimation Algorithm

Evolution:

- In the beginning, SF0 (On-The-Fly Scheduling) assumed that the application on each node would request for bandwidth (2013)

- This generated the initial Bandwidth Estimation Algorithm, which considered the incoming traffic, and the local (application-generated) traffic for the estimation.

- Since the inception of 6P and SF0, the original assumption is no longer valid.

Cell Estimation Algorithm

Evolution:

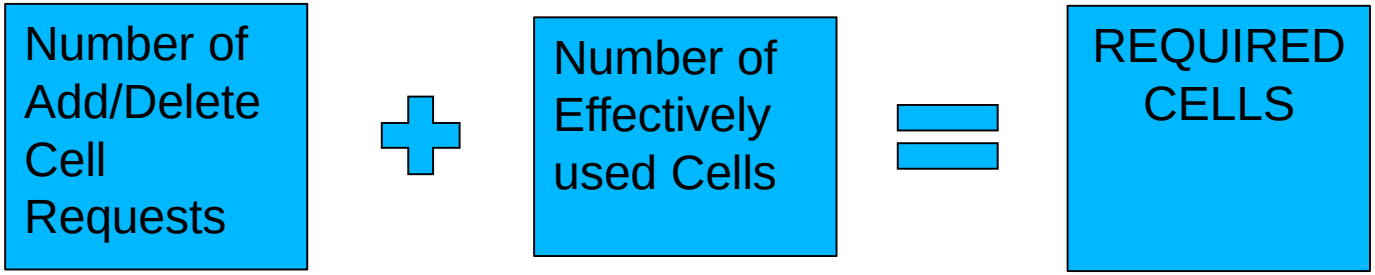
- In SF0 -02 we still include incoming traffic and we replaced application traffic with the outgoing traffic to estimate the new traffic requirement.

- However, this is still an overestimation.

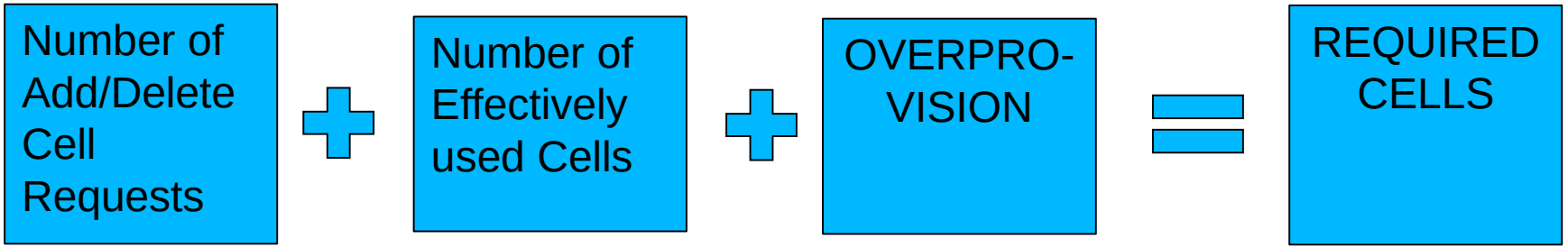
- After recent discussions on the ML, the proposal is to use only the outgoing traffic growth to estimate the new traffic requirement

Cell Estimation Algorithm

- Alternative 1

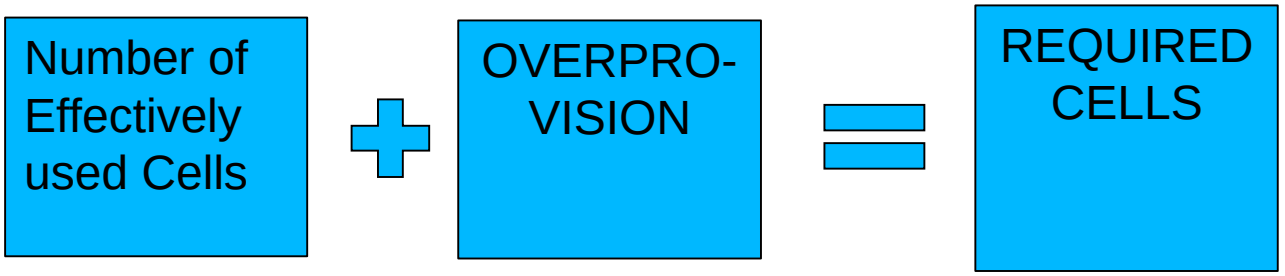


- Alternative 2 (to guarantee a fixed overprovisioning to detect changes on effectively used Cells)



Cell Estimation Algorithm

- Alternative 3 (Recent discussion, still not included on -02)



- SF0 is based on a neighbor-to-neighbor negotiation:
- We do not know if the incoming requested add/delete cell destination is the local node or if it will be routed to another neighbor
- Including it would add unnecessary uncertainty, resulting in possible under- or over-provisioning.

Cell Estimation Algorithm

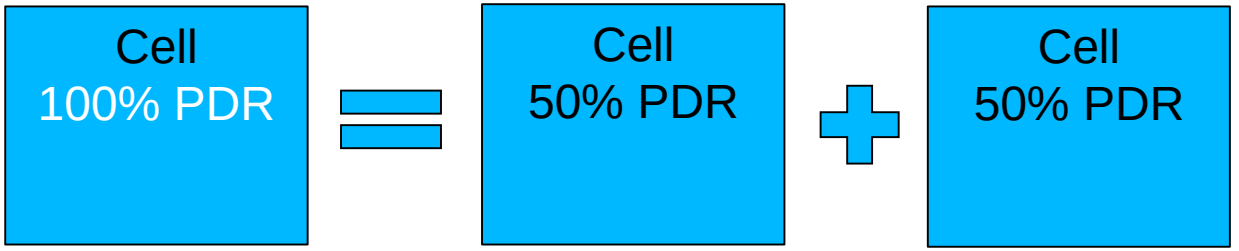
Question:

- Do you agree in using Alternative 3?

Cell Estimation Algorithm

Bandwidth to Cell transition:

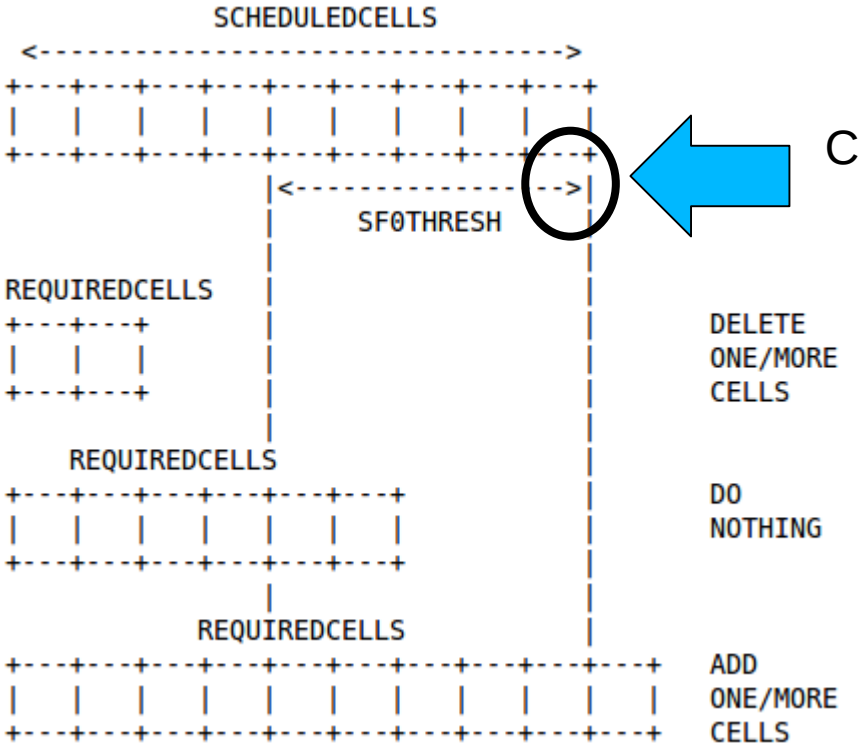
- SF0 originally kept the difference between Bandwidth and Cells to take into account the individual PDR of each cell.
- Example:



- Now, we directly estimate required cells without taking into account the PDR.
- The Cell Relocation Algorithm is aimed to keep an average PDR on all allocated cells

Cell Allocation Policy

Went back to the original (On-The-Fly) Diagram.



Change this to

---|

We have only one SF0THRESH value.

Cell Allocation Policy

Number of cells to Add/Delete

- The OTF draft specified: "***The number of soft cells to be scheduled/deleted for bundle resizing is out of the scope of this document and it is implementation-dependent***".
- We would like to reinstate this phrase (eliminating the bundle term).
- **Do you think we can suggest a value here?**

Timeout Calculation

- After a long discussion with Nicola and Qin on the ML, it can be said that:
  - The worst-case timeout can achieve one minute with typical values.
  - Proposal:
    - Add a 6P ACK to override MAC-level timeouts and include only 6P-related processing and response times
  - Refer to the ML for further details on the timeout calculation.

Timeout Calculation

- There is a contradiction on the 6P draft, first saying that the SF MAY define the timeout on section 4.1.1 and then that the SF MUST define the timeout on section 5.2

Cell Types on SF0

- Although 6P enables the use of Shared, TX or RX cells on the SFs,
- We only allocate TX Cells on SF0:
  - There is always one direction (from a node towards a neighbor)
  - We do not assume symmetric links in terms of cells between neighbors
  - There is still no signaling available to decide if the new allocated cells could be Shared or TX.

6P SF Compliance

- Added a compliance section taken from the requirements list on the 6P draft
  - Only missing two MUST items:
    - Timeout
    - Statistics (PDR) definition

Performance Evaluation

- Current Performance evaluation is based on the 6tisch simulator:

Palattella, M. R., Watteyne, T., Wang, Q., Muraoka, K., Accettura, N., Dujovne, D., ... & Engel, T. (2016). On-the-Fly Bandwidth Reservation for 6TiSCH Wireless Industrial Networks. *IEEE Sensors Journal*, *16*(2), 550-560.

- We need further experimental evaluation. I ask for volunteers to help on this issue.

Cell Relocation

- SF0 proposes a simple algorithm to trigger a cell relocation: When a cell achieves “PDR 20% less than the average of the rest of the allocated cells”

- However, we need **performance evaluation work** on the current algorithm to adjust the values or propose a new calculation method.

draft-vucinic-6tisch-minimal-security-00

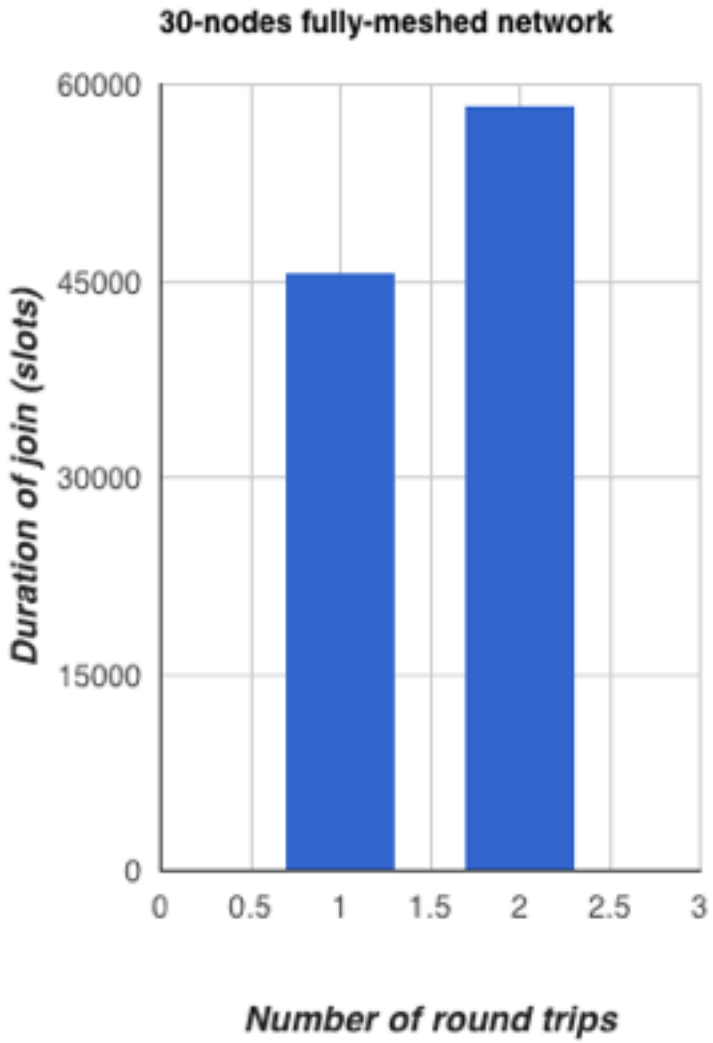
Mališa Vučinić, Inria
Jonathan Simon, Linear Technology
Kris Pister, UC Berkeley

Context

- Terminology
  - **JN**: Joining Node
  - **JCE**: Join coordinating entity
  - **JA**: Join assistant - radio neighbor of JN
- JN provisioned with a “join” credential — **one touch assumption**
  - Pre-Shared Key (PSK)
  - Raw Public Key (RPK)
  - Locally-valid certificate and a trust anchor
- Expects to be configured with
  - K2 from [ietf-6tisch-minimal]
  - short 802.15.4 address

Some preliminary data

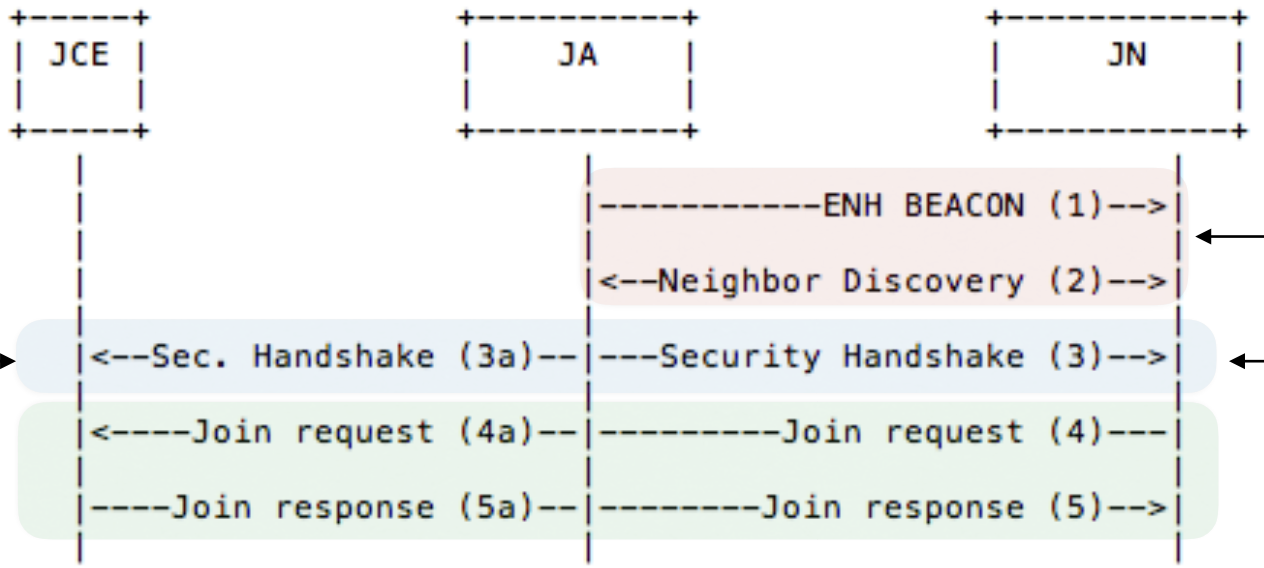
- Emulation of join process using OpenWSN
- Estimate duration of the join process when network is forming
- 30-node fully-meshed network
  - 11 slots in a slotframe



Goals

- Minimize number of exchanges -> single round trip with PSKs
- Minimize join-specific code -> reuse of existing protocols
- Confidentiality + integrity -> end-to-end AES-CCM

Join protocol



optional with PSKs

unprotected

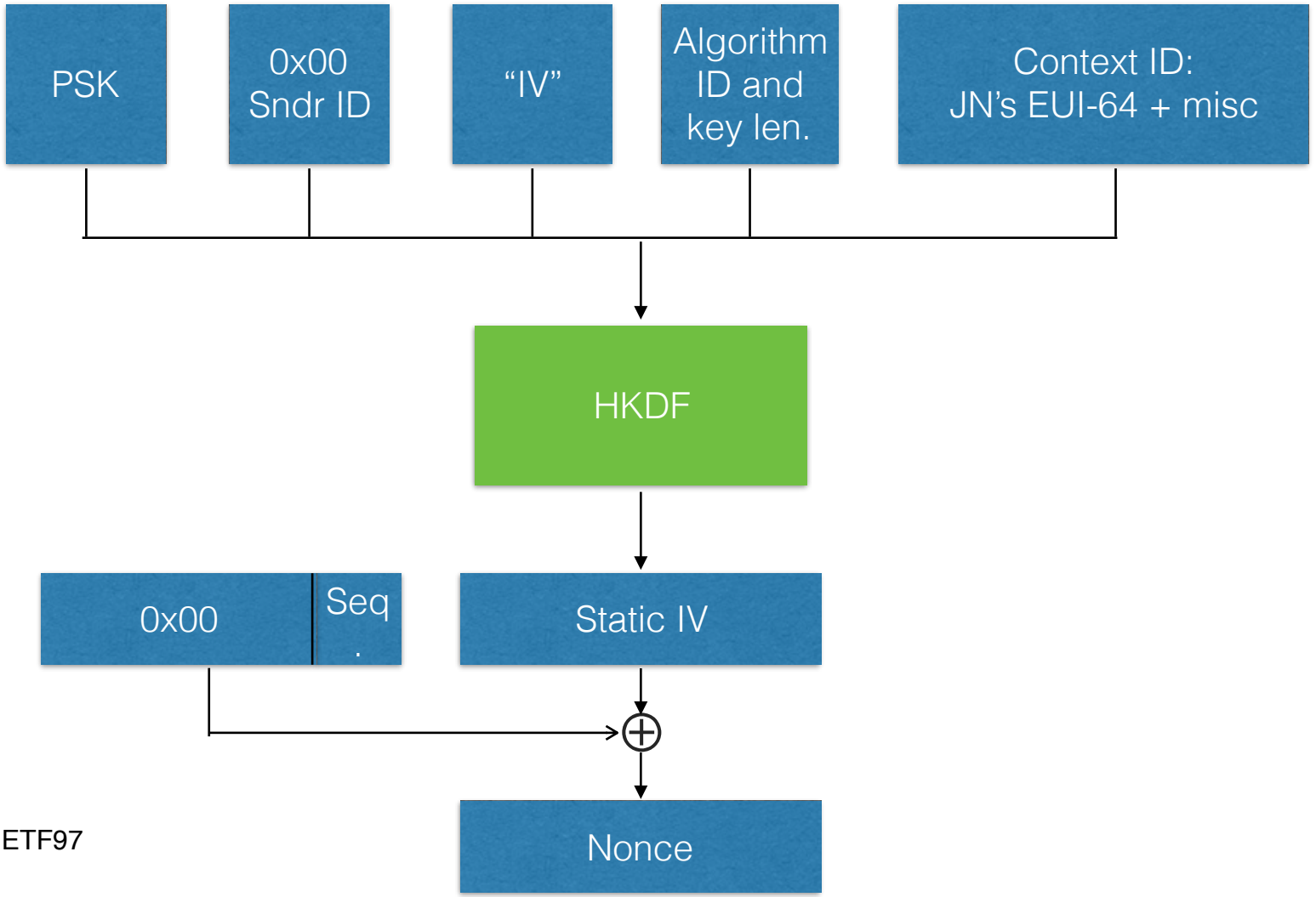
uses EDHOC [draft-selander-ace-cose-ecdhe-03]

Figure 1: Message sequence for join protocol.

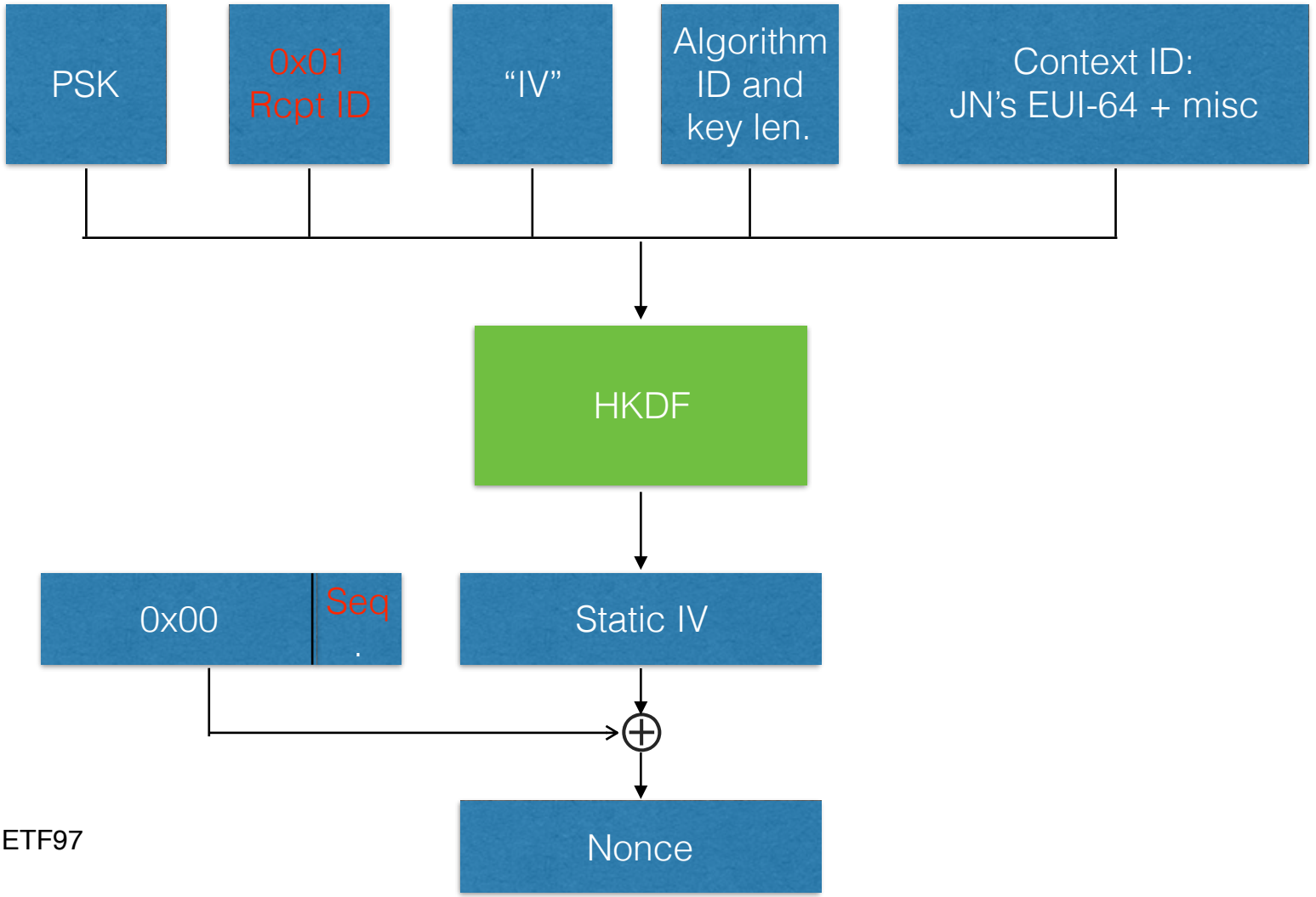
Protocol Specification

- Implemented with CoAP
  - JN is a CoAP client, JCE a server
- JA is a CoAP proxy
  - Stateless using app-level info
  - Agnostic of the routing protocol (mode)
- E2E encryption *through JA* using OSCOAP + COSE
- Actual “traffic keys” and nonces are derived from PSK

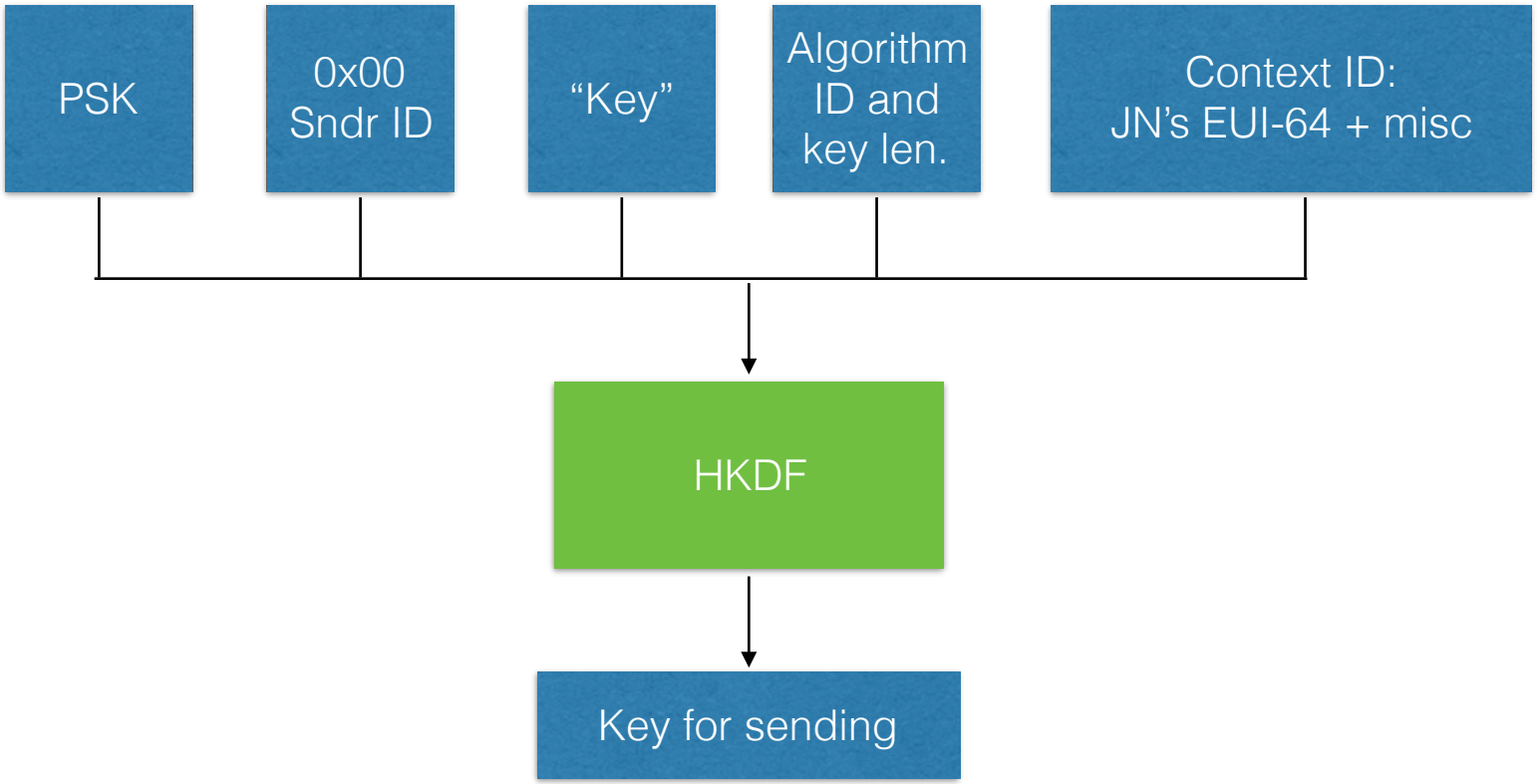
Nonce generation at JN



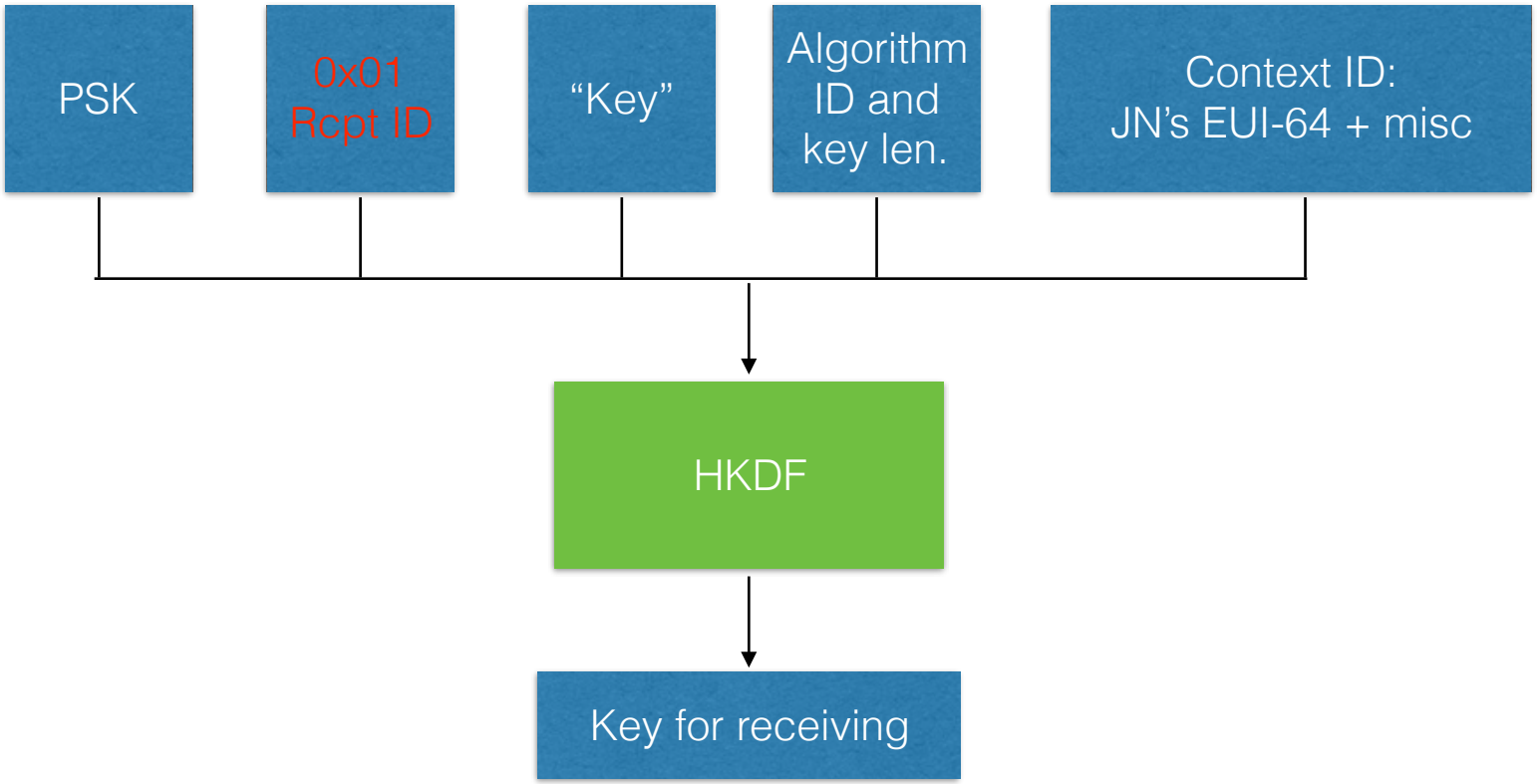
Nonce generation at JCE



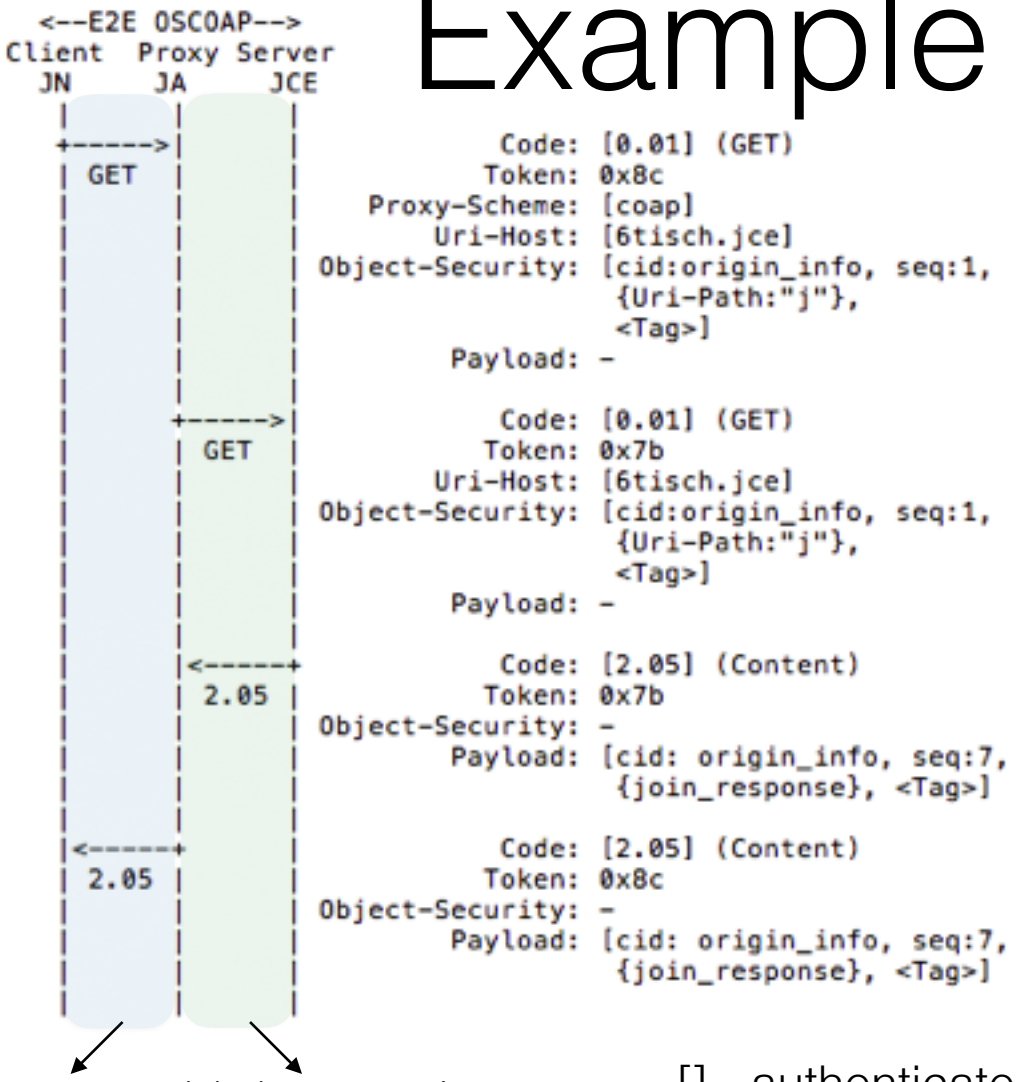
Key generation at JN



Key generation at JN



Example (PSK)




```
origin_info:

[
     h'00170d00060d9f0e', / JN's EUI64 /
     49152, / JN's UDP source port /
     0x8c   / JN's CoAP token /
]
```

Encodes to 15 bytes

```
join_response:
[
    [   / COSE Key Set array with a single key /
        {
            1:4, / key type symmetric /
            -1:h'e6bf4287c2d7618d6a9687445ffd33e6' / key value /
        }
    ],
    h'af93' / assigned short address /
]
```

Encodes to 26 bytes

link local commun.

global comm. using pre-existing routes

[] - authenticated

{} - encrypted

draft-richardson-6tisch-dtsecurity-secure-join

Michael Richardson

Status

- Goal: securing the join process
  - Aligning as much as possible with ANIMA and NETCONF WG, while adapting to limits of constrained devices and networks
- News:
  - dtsecurity-secure-join-01 posted last week.
  - draft-richardson-6lo-ra-in-ie posted last week: discussion says do not make a general mechanism, but an RA specific mechanism, and that this work is within the 6tisch charter. To be revised ASAP.
  - Also contribution: draft-vucinic-6tisch-minimal-security-00
  - Nov. 8 security design team meeting did not happen (my fault), and will be rescheduled.
  - Security design team meetings to resume Nov. 29 (one week of rest)

The cast

Manufacturer

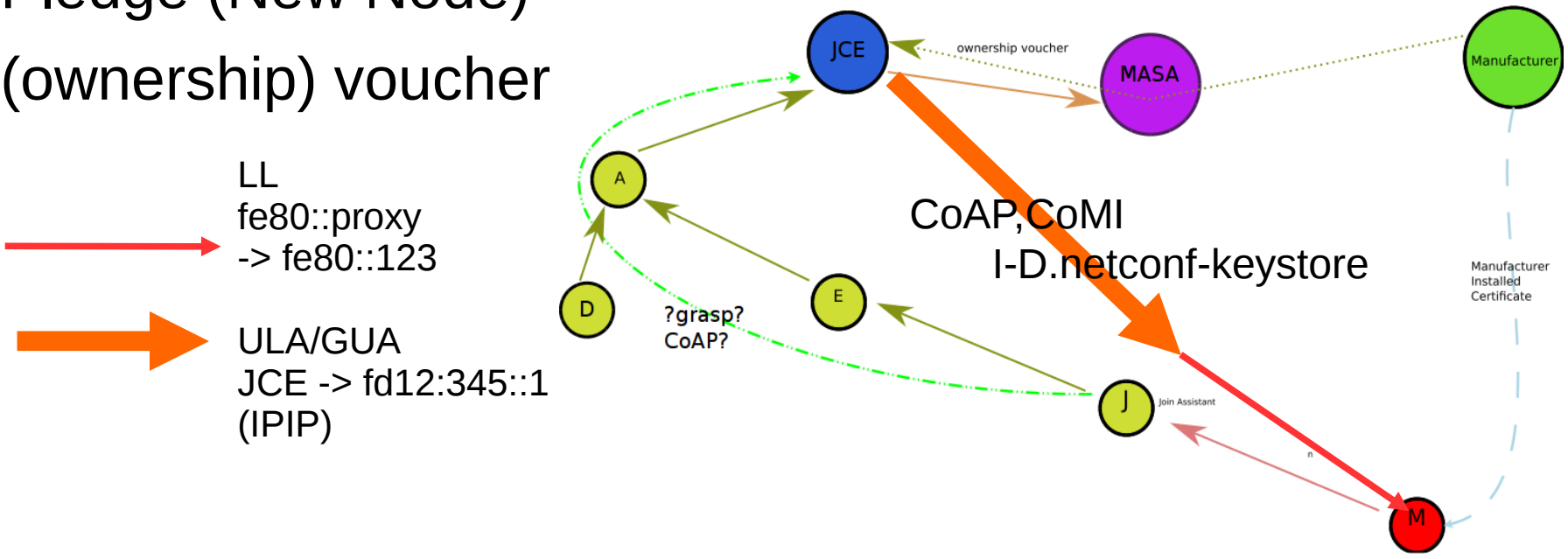
Manufacturer Authorized Signing Authority (MASA)

JCE (Registar)

Join Assistant (Proxy)

Pledge (New Node)

(ownership) voucher



The ANIMA cast

Manufacturer

Manufacturer Authorized Signing Authority (MASA)

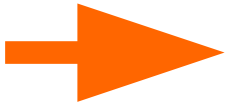
Registar

Join Assistant/Proxy

New Node (pledge)

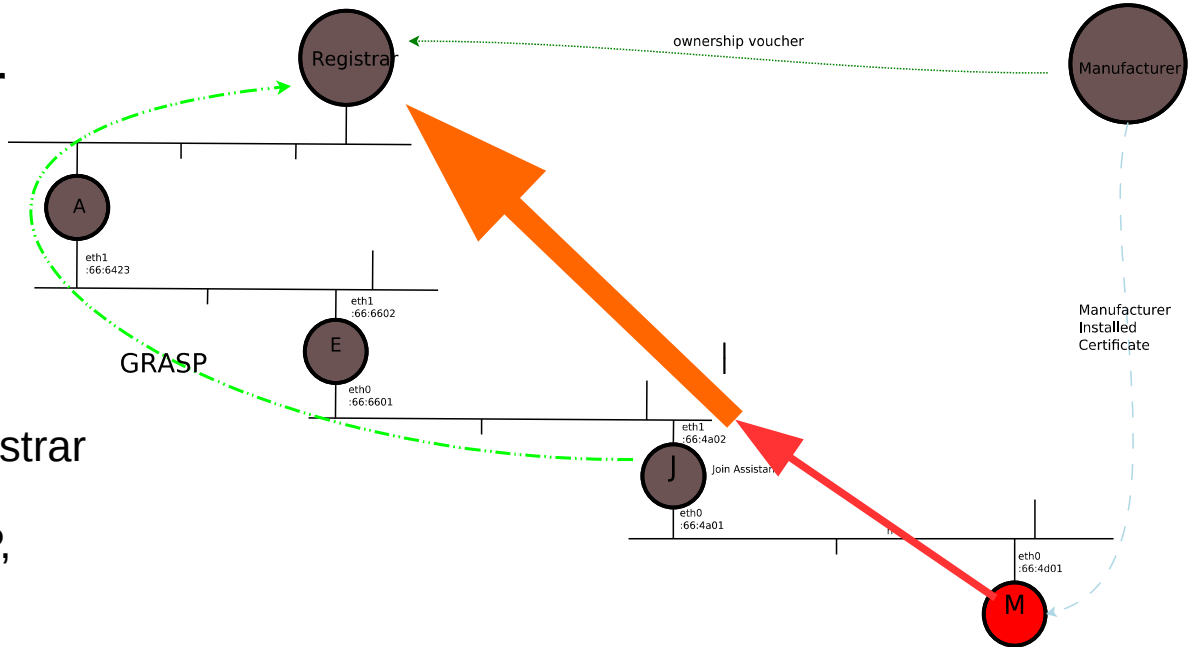
(ownership) voucher

LL
fe80::123->fe80::proxy



ULA
fd12:345::1-> registrar

(circuit proxy, IPIP, ~~NAT66~~)



Manufacturer

- The manufacturer installs a keypair during the manufacturing process.

Manufacturer Authorized Signing Authority (MASA)

- The MASA provides a signed artifact (that can be verified via a chain of trust to the manufacturer) about the ownership of the device.

Join Coordination Entity (JCE)

- The Join Coordination Entity, (Registrar in ANIMA terminology) decides which pledges to enroll.
- The JCE initiates the enrollment process, controls the order of enrollment based upon a device ID.
- The JCE also manages the rekeying of nodes.

Join Assistant (JA)

- The Join Assistant statelessly forwards packets to the pledge.
  - It is proposed to do this via IPIP encapsulation.
  - It could be done via EDHOC CoAP relaying as described in 6tisch-minimal instead.
- JA functionality is intended to be a small as possible, and reuse as much code/mechanism as possible.

Pledge

- This is the new device.
- It has an IDevID installed by the manufacturer.
- It has the manufacturer and/or MASA public key in it’s trusted store.

Audit vs **Ownership** Voucher

YANG description

```
module: ietf-voucher
  +--rw voucher
     +--rw assertion
     +--rw trusted-ca-certificate
     +--rw certificate-id
     |  +--rw cn-id?    string
     |  +--rw dns-id?   string
     +--rw unique-id*
     +--rw nonce
     +--rw created-on
     +--rw expires-on
     +--rw revocation-location
     +--rw additional-data
```

[**Audit** | Ownership]
trust anchor for Registrar
id of Registrar

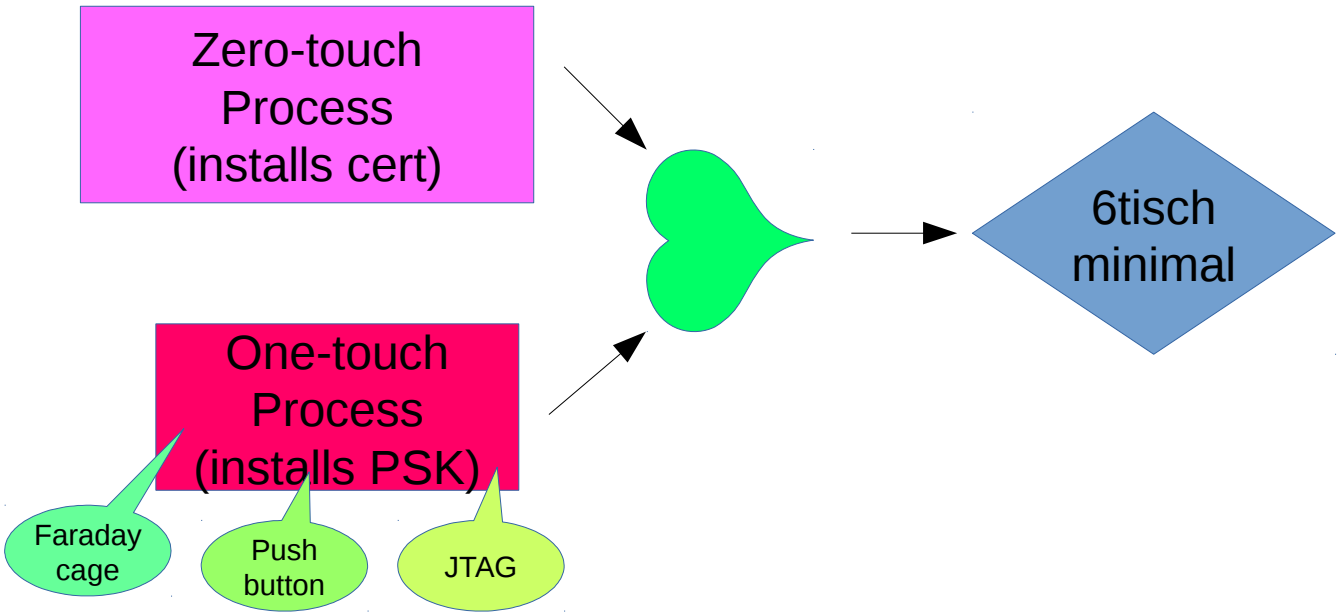
id of Pledge
Real Time Clock proofing
if RTC available on Pledge
if RTC available on Pledge
under consideration
future proofing

[Audit | **Ownership**]
trust anchor for Registrar
id of Registrar

id of Pledge
Real Time Clock proofing
if RTC available on Pledge
if RTC available on Pledge
under consideration
future proofing

6tisch-minimal integration

Goals of integration:
1. Zero-touch installs new credentials (certificate, but could also be PSK)
2. 6tisch-minimal arranges for keys



Issues and planned changes

1) GRASP requires TCP --- this is a problem, need to replace it.
2) EDHOC vs DTLS. Pick ONE.
3) Integrating this process with 6tisch-minimal
4) How many documents?
5) Ra-in-ie document will be updated to be Router Advertisement only
6) Where to do ownership voucher work (ANIMA, NETCONF, 6tisch?)
7) Would like a consensus call on use of “outgoing” (PCE->Pledge) method.
   - Are there implementers that would like the certificate renewal state machine to reside in the mote, rather than in the PCE?

AOB