Chicago, March 23rd 2017

IPv6 over the TSCH mode of IEEE 802.15.4

Chairs:
Pascal Thubert
Thomas Watteyne

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

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- By participating with the IETF, you agree to follow IETF processes.
- If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.
- You understand that meetings might be recorded, broadcast, and publicly archived.

For further information, talk to a chair, ask an Area Director, or review the following:

- BCP 9 (on the Internet Standards Process)
- BCP 25 (on the Working Group processes)
- BCP 78 (on the IETF Trust)
- BCP 79 (on Intellectual Property Rights in the IETF)

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-98-6tisch?useMonospaceFont=true
** Recordings and Minutes are public and may be subject to discovery in the event of litigation.
*** From the Webex login

Agenda

9:30 Intro and Status (Chairs) [10min]

- Note-Well, Blue Sheets, Scribes, Agenda Bashing [5min]
- draft-ietf-6tisch-minimal-21, draft-ietf-6tisch-terminology-08, progress vs. charter [5min]

9:40 Security [70min]

- Presenting the drafts and the flow between them (Michael) [20min]
- draft-ietf-6tisch-dtsecurity-secure-join-01 (Michael) [15min]
- draft-ietf-6tisch-minimal-security-02 (Mališa) [15min]
- draft-richardson-6tisch-join-enhanced-beacon-01 [10min]
- draft-richardson-6tisch-minimal-rekey-01 [10min]

10:50 6top protocol draft-ietf-6tisch-6top-protocol-03 (Xavi) [15min]

11:05 Service Function 0 draft-ietf-6tisch-6top-sf0-03 (Diego) [15min]

11:20 Architecture draft-ietf-6tisch-architecture-11 (Pascal) [10min]

11:30 News from IEEE 802.15.4 (Pat) [15min]

11:45 Detnet backhaul draft-wang-detnet-backhaul-architecture-00 (Lun) [10min]

11:55 AOB [5min]

Volunteers

- notetaker 1: Dominique Barthel
- notetaker 2: Geraldine Texier
- notetaker 3: Francesca Palombini (?)
- notetaker 4: Alexander Pelov
- notetaker 5: Tero Kivinen
- notetaker 6: Xavi Vilajosana
- notetaker 7: Pascal Thubert
- Jabber scribe: Ines Robles, MCR

draft-ietf-6tisch-minimal-21

Draft 21: ready

OPSDIR Last Call Review (of -20): Ready

SECDIR Telechat Review (of -19): Has Issues

GENART Telechat Review (of -19): Ready

SECDIR Last Call Review (of -17): Serious Issues

GENART Last Call Review (of -17): Almost Ready

INTDIR Early Review (of -15): Ready with Nits

INTDIR Early Review (of -13): Ready

Milestones

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*

Update on Security work

presenter: Michael Richardson (SSW)
mcr@sandelman.ca

Update on security
Design team meetings

Meetings occurred:

2017-01-17, 2017-01-31, 2017-02-14,

2017-02-21 (extra), 2017-02-28.

2017-03-14 (cancelled)

Typically present:

Michael Richardson, Tero Kivinen, Pascal Thubert,

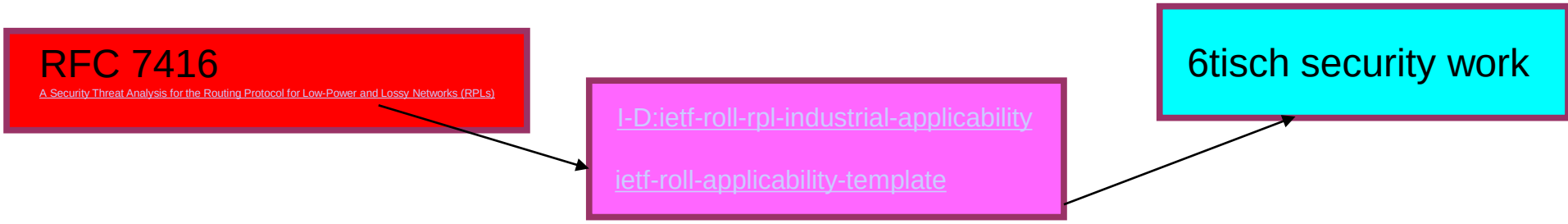
Thomas Watteyne, Mališa Vučinić, Göran Selander,

Toerless Eckert, Peter van der Stok

Recent minutes so far: https://www.ietf.org/mail-archive/web/6tisch-security/current/msg00661.html

Overview / Charter

- Charter says: “The WG will continue working on securing the join process and making that fit within the constraints of high latency, low throughput and small frame sizes that characterize IEEE802.15.4 TSCH”
- 6tisch itself is the embodiement of RPL Applicability Statement for Industrial Network, which includes statements about how L2 security is to be accomplished. This was a “promise” to the security area (director) going back to the beginning of RPL security.



The drafts

- draft-ietf-6tisch-minimal-security
  - This is the “one-touch” process: adopted Dec 2016
- draft-ietf-6tisch-dtsecurity-secure-join
  - This is the “zero-touch” process: adopted Dec 2016
- draft-richardson-6tisch-minimal-rekey
  - This the proposal for rekeying of both.
- draft-richardson-6tisch-join-enhanced-beacon
  - This is the proposal to add join info to EB.

Detailed issues on each draft follows this overview.

New Terminology

Joining Node (JN)

Join Coordinating Entity (JCE)

Join Assistant (JA)

Pledge

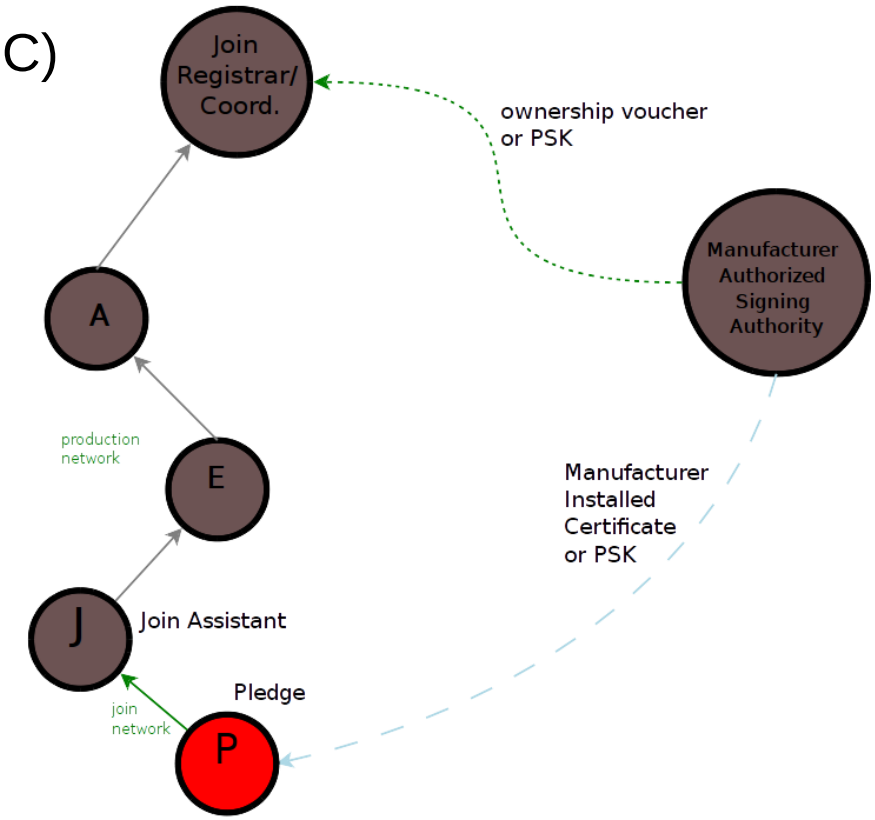
Join Registrar/Coordinator (JRC)

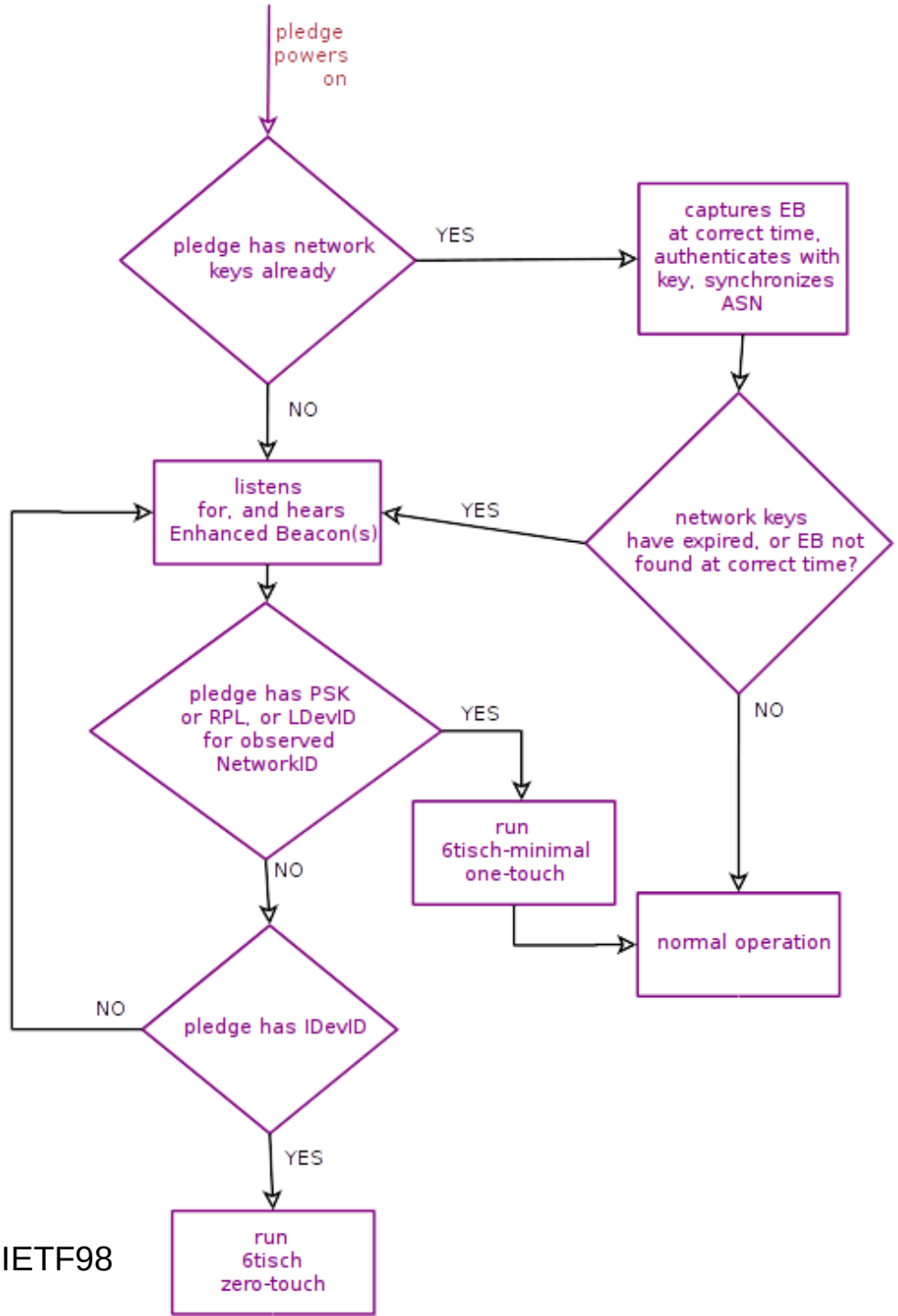
Join Proxy (JP)

Reference diagram and Common Terminology

- Join Coordination Entity (JCE) is now
  - Join Registrar/Coordinator (JRC)
- Join Proxy (JP)
- “New node” is Pledge (P)

- Manufacturer Authorized Signing Authority
  - ietf-anima-bootstrapping-keyinfra
- Voucher
  - Ietf-anima-voucher





Decision tree for Pledge Join

Constraints and Responses

Limited bandwidth	Small messages
Few broadcasts opportunities	Maximize use
DAG structure pushes traffic to root	Manage bandwidth
Limited energy in pledge	Maximize opportunities to sleep
Limited code space	Reuse code needed for applications

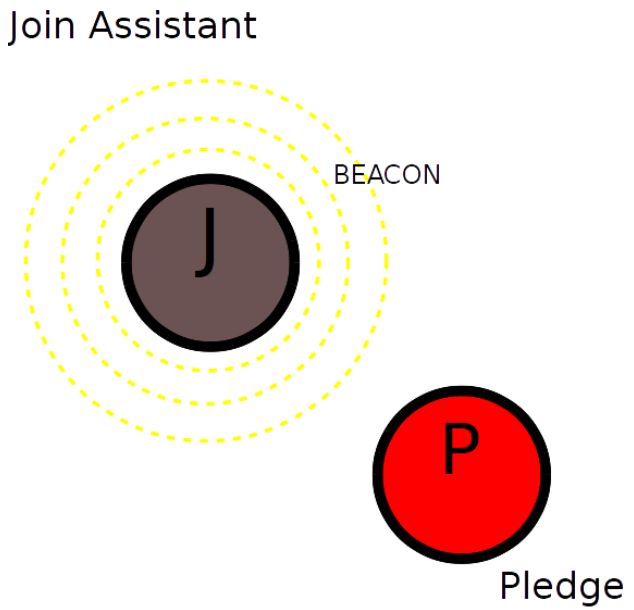
10,000ft view: 1. EB

Step 1: become aware of networks

This means to listen for Enhanced Beacons.

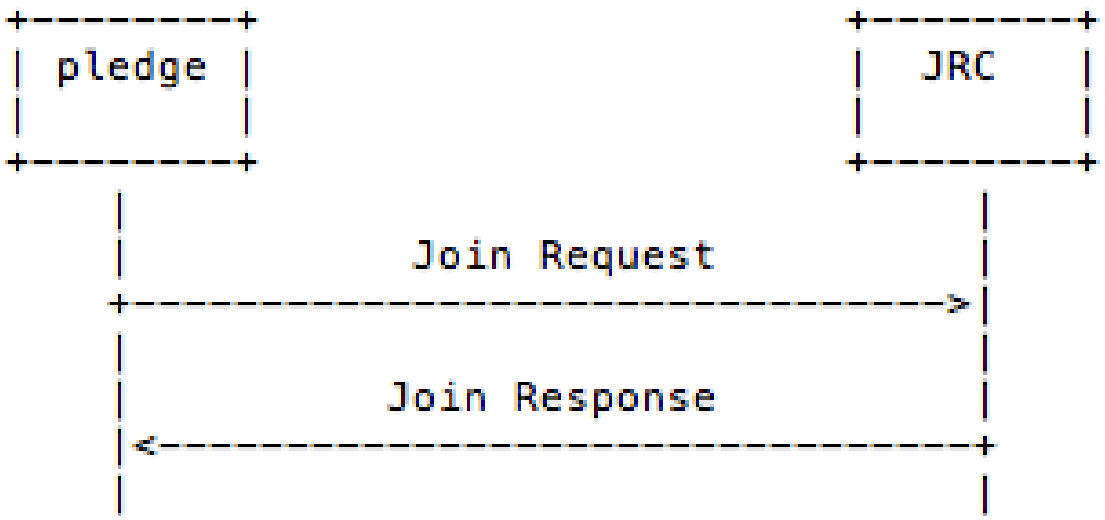
Must scan channels and frequencies!

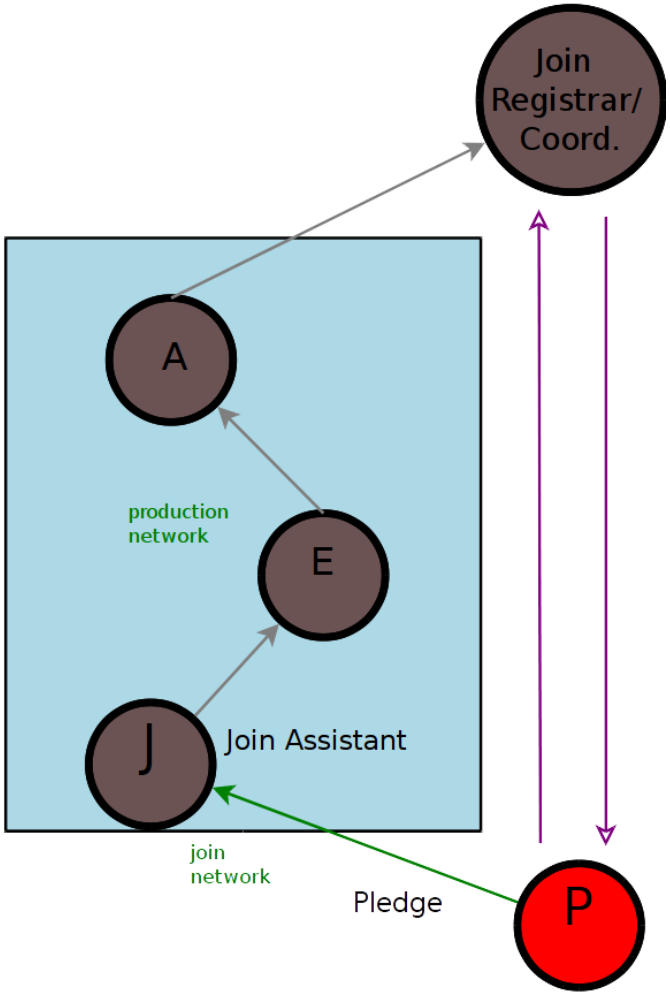
- May not be short!



10,000ft view: 2-minimal PSK, Join Request

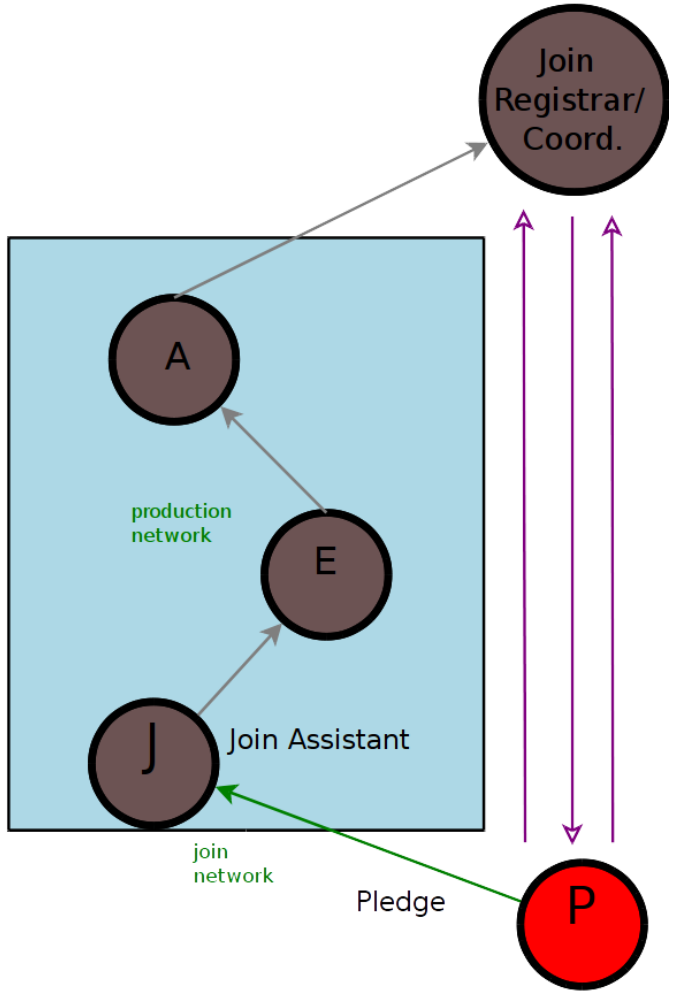
Step 2-psk: with PSK, two messages.





10,000ft view: 2-minimal with EDHOC for RPK, LDevID

Step 2-edhoc: with asym., three message exchange. U=pledge, V=JRC, then do Join Request.. (previous slide)




```
Party U                                                  Party V
   |                    S_U, N_U, E_U, EXT_1                    |
   +------------------------------------------------------------>|
   |                                                            |
   |  S_U, S_V, N_V, E_V, AEAD(EXT_2, ID_V, Sig(V; E_U, E_V))   |
   |<------------------------------------------------------------+
   |                                                            |
   |         S_V, AEAD(EXT_3, ID_U, Sig(U; E_V, E_U))           |
   +------------------------------------------------------------>|
   |                                                            |
```

10,000ft view: Join Proxy 1

IPIP mechanism - features

- Join Proxy encapsulates Link-Layer traffic in IPIP header.
  - (potentially, three IPIP headers to compress)
  - (6LoRH compresses IPIP!)
- JRC uses RH3 to and IPIP to send traffic back to Pledge.
  - See draft-ietf-roll useofrpl, section 6.3.

IPIP benefits

- Reuses existing routing code
- Could be used for any protocol (DTLS, etc.)
- Mechanism is specific to 6lowpan networks!

10,000ft view: Join Proxy 2

CoAP mechanism - features

- Alg gateway (changes srcip/dstip)
- Originally overloaded the ContextID (cid) to include the address of the pledge.
- Now uses new Stateless-Proxy: header, which JRC will echo.

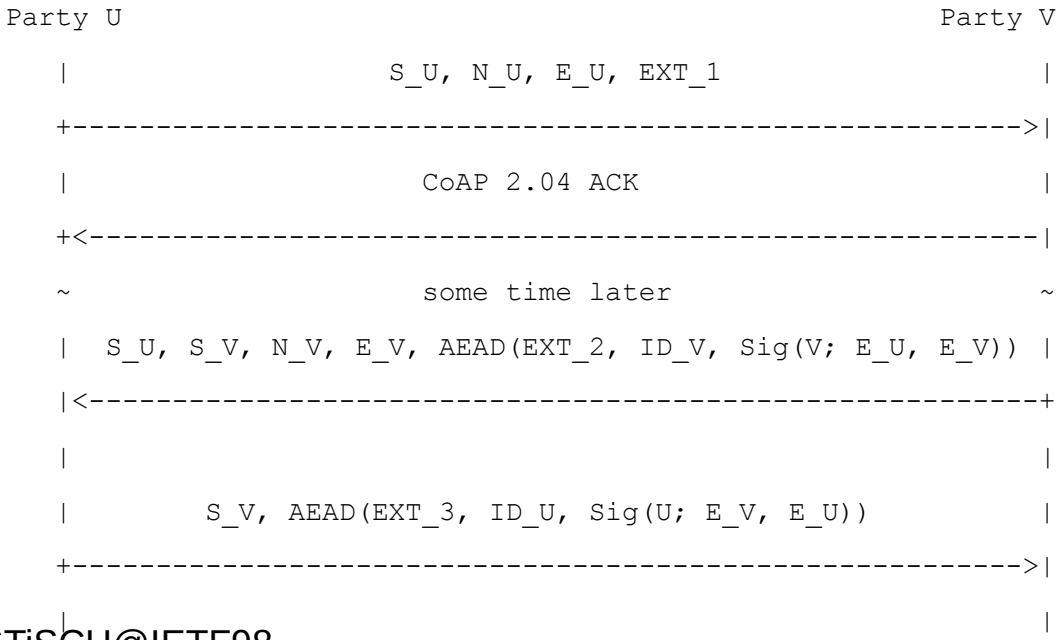
CoAP benefits:

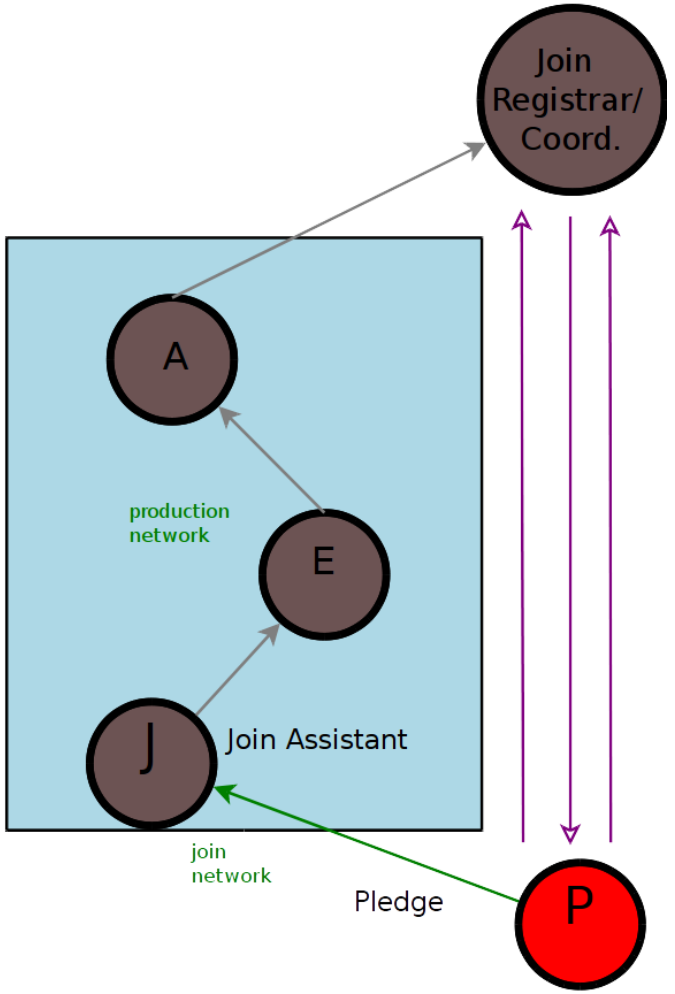
- Does all work in application code/OSCoap (above routing)
- Specific to CoAP
- Proxy has join specific algorithm gateway code.

10,000ft view: 2-zero touch notify to Join Proxy

Step 2-z: original idea was to use Neighbor Discovery, DAD to register to Proxy, and have Join Proxy communicate existence of pledge to JRC.

Step 2-z: new idea is to run process identical to 2-edhoc, but just to ACK message_1.





6tisch-dtsecurity-secure-join

presenter: Michael Richardson (SSW)
mcr@sandelman.ca

Status: 6tisch-dtsecurity-secure-join

- Goal
  - Reduce document scope to leverage minimal-security mechanisms, augmented with IDevID and voucher exchange.
  - Synchronize (push/pull!) with ANIMA voucher document
    - Vouchers in CWT rather than PKCS7 signed JSON.
- News
  - Document shrunk by 4 pages, moved some text to minimal-security.
- Next
  - Adopt/advance EDHOC. EALS could carry voucher?

Relationship to other work

- ANIMA BRSKI
  - RFC7030 (EST), HTTPS over TCP.
  - Zero-touch is re-interpretation of same mechanism.
  - Common JRC, MASA mechanism.
- EDHOC/OSCOAP
  - CoAP equivalent of IKEv2, but application layer.
  - Replaces DTLS as the security component.
- ANIMA Voucher
  - Currently PKCS7 (CMS) signed JSON.
    - Could become JWT, which eliminates some ASN.1 goo.
  - CWT is to JWT what CBOR is to JSON. CWT uses draft-ietf-cose-msg, which is in common with ACE and OSCOAP.
- EALS
  - New work by group led by Goeran, to merge EST and EDHOC.
  - Could carry vouchers within the EDHOC protocol.

Overview of Voucher work

- (ownership) Voucher document was adopted in ANIMA in Dec. 2016.
- Desire to make Voucher common across imprint protocols: one set of vendor tools across many product lines.

Renewals > Revocations

A) Long lifetime
Con: Requires revocation logic, services

MASA

Revoked!

Undefined
OCSP/CRL

B) Medium or Short lifetime
Con: Contiguous renewals

MASA

not renewed!
not renewed!

MASA

not renewed!
e.g. t > last-renewal-date

C) Short lifetime, non contiguous
Pro: A single flow, always exercised

Open (ANIMA) Issues

1. Does the voucher still need to support indirect issuer?

1. Need to support revocations of domain certificate?

1. PKCS#7 or something else, like CWT?

1. Is there a need for authority-key-identifier?

3. PKCS#7 or something else, like CWT?

Right now Voucher uses PKCS#7 for signing

- like SMIME with stapled certificate chain

Some would like to align it with CWT for ultra-small IoT devices

- but CWT is not a good match

Worry about in some future RFC instead?

Open Issues 1: How to tell Pledge to wait for join.

- Init bit in EB.
  - Requires message from Pledge/JP to JRC.
- Via OSCOAP initial exchange?
  1) Costs the pledge some entropy, and doing exponentiation sooner (potentially with a network that does not want it).
  2) Pledge must reveal it's identity somehow in this process, while SIGMA-I is actually designed to conceal it!

Open Issue 2

- How to carry voucher
  - OSCOAP, EALS includes proposal to put voucher into the key agreement protocol.
    - Plus: eliminates “provisional” state that BRSKI has to deal with.
    - Negative: may complicate protocol.
      - JRC has to know identity of pledge in order to produce correct voucher. If done inside protocol, pledge has to reveal; but since voucher is only thing preventing MITM, maybe pledge always is easily attacked
        - » Can be differences for active for passive eavesdropping!
      - Pledge could time out if JRC needs to consult human!
  - Or use OSCOAP to set up EST/CoAP mechanism, provisionally, and then send/receive voucher, and certificate, much like BRSKI.
    - See: email exchange https://www.ietf.org/mail-archive/web/6tisch/current/msg05020.html

Open Issue 2 (cont)

Then the JCE driven process should instead look like:

-

```
pledge                          JCE
       <--- CoAP GET /nonce-----
       ----- 200 OK, nonce ---->     [could be empty if nonce

       <--- CoAP POST /voucher--     {audit token or ownership voucher}
       ----- 200 OK------------>     [or 4xx or 5xx code! ]

       <--- CoAP POST /cacerts--     [block-transfer]  [maybe not??]
                                     (application/pkcs7-mime,
                                      CMC Simple PKI RESPONSE)
       ----200 OK-------------->

       <--- CoAP POST /csrattrs-     [ASN as per 7030]
       ----200 OK-------------->

       <--- CoAP GET  /csr------
       ----200 OK ---PKCS10 ----     [PKCS#10 Cert Req]

       <--- CoAP POST /cert-----     [PKCS7 Certificate]
       ----200 OK --------------
```

https://www.ietf.org/mail-archive/web/6tisch/current/msg05020.html

Ideal outcomes

- EDHOC/OSCOAP for key agreement.
- ANIMA adopts CWT as voucher format.
- Common JRC and MASA components
  - Can bootstrap non-constrained or constrained devices with same infrastructure.
- Zero-touch/one-touch choice orthogonal to question about bandwidth management.
- IPIP Join Proxy mechanism chosen as MTI for 6tisch, with identical option *optional* for ANIMA.

draft-ietf-6tisch-minimal-security

Mališa Vučinić, Inria
Jonathan Simon, Linear Technology
Kris Pister, UC Berkeley
Michael Richardson, Sandelman Software Works

Status

- News
  - draft-ietf-6tisch-minimal-security-02
  - Published on March 12th 2017
- Next
  - Stabilize the proxy mechanism
- Goal
  - Call for reviews

New Terminology

Joining Node (JN)

Join Coordinating Entity (JCE)

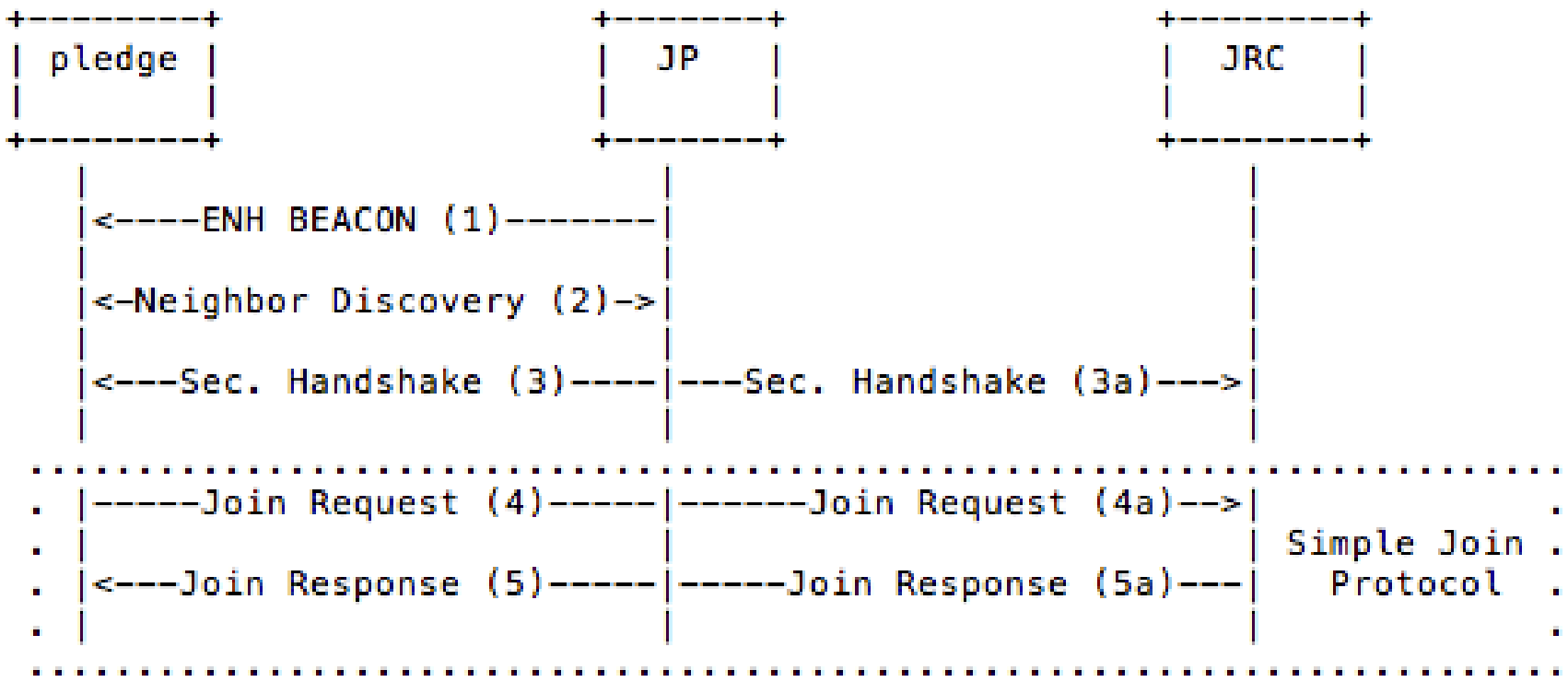
Join Assistant (JA)

Pledge

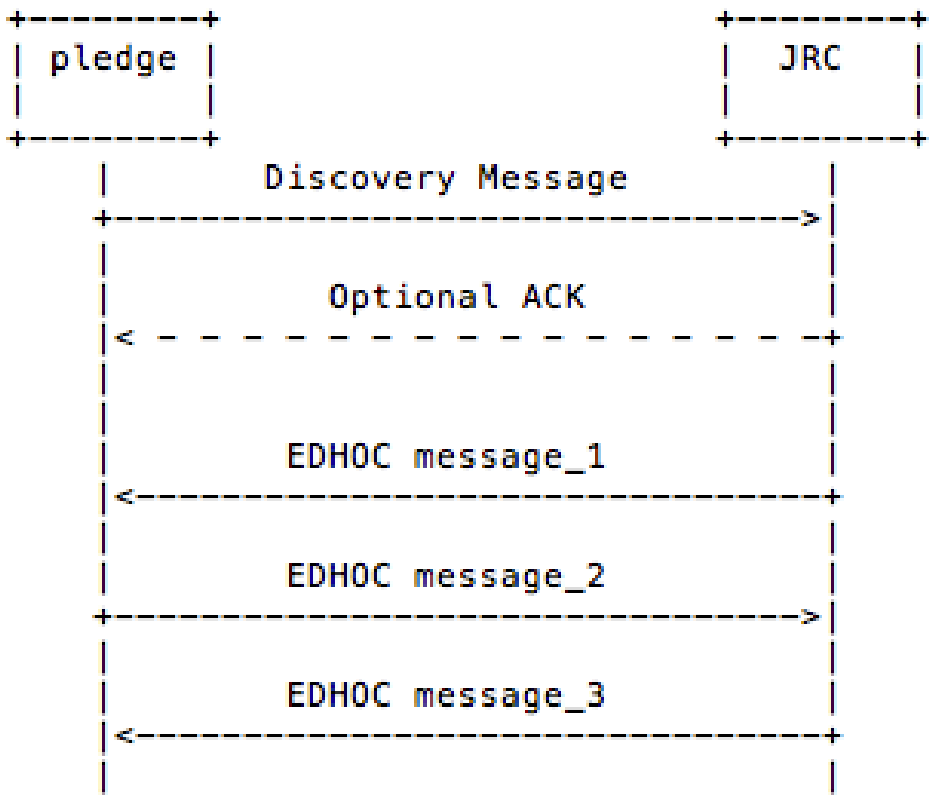
Join Registrar/Coordinator (JRC)

Join Proxy (JP)

Join Process Overview

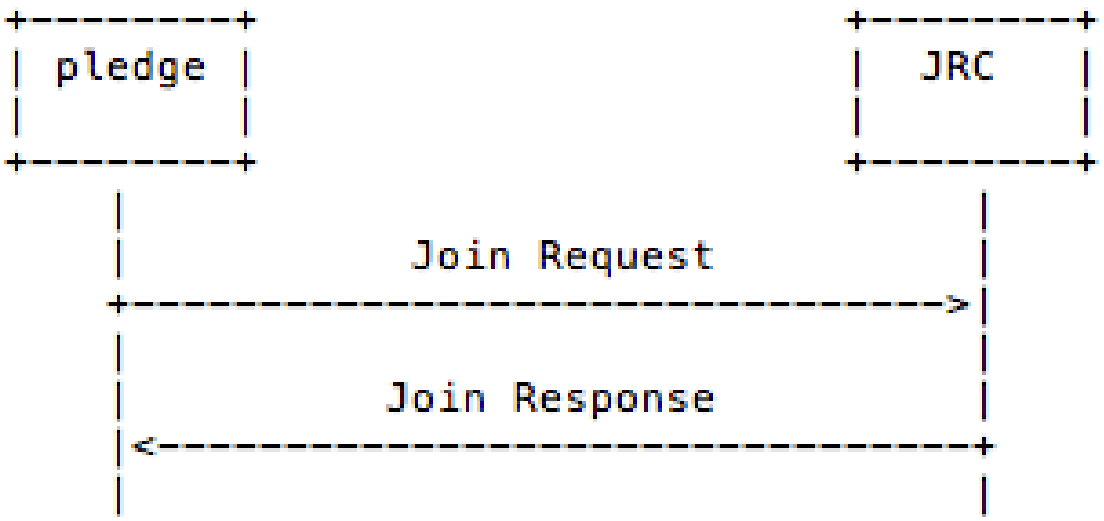


Security Handshake



- Optional with PSKs
- Mandatory with asymmetric keys

Simple Join Protocol



- Can be run directly with PSKs
- Preceded by security handshake in case of asymmetric keys

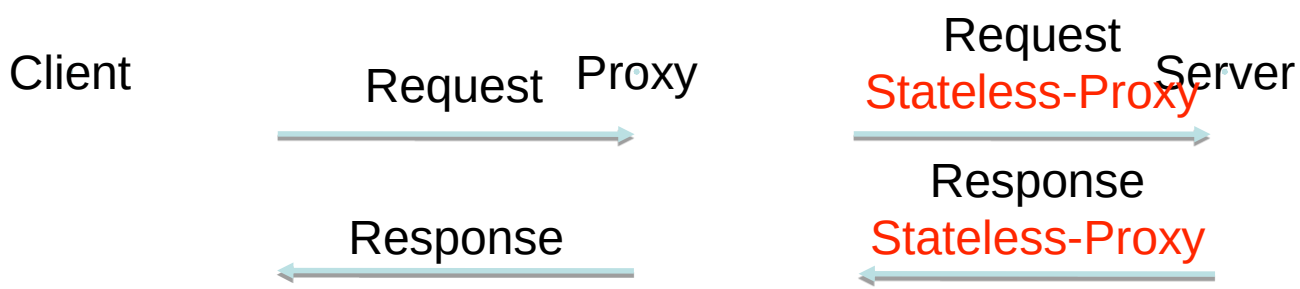
Operation of Join Proxy 1/2

- Problem: State-fullness of a CoAP proxy leads to easy DoS attacks
- Solution: New CoAP option carrying state between Proxy and Server

No.	C	U	N	R	Name	Format	Length
TBD	x		x		Stateless-Proxy	opaque	1-255

C=Critical, U=Unsafe, N=NoCacheKey, R=Repeatable

Figure 2: Stateless-Proxy CoAP Option



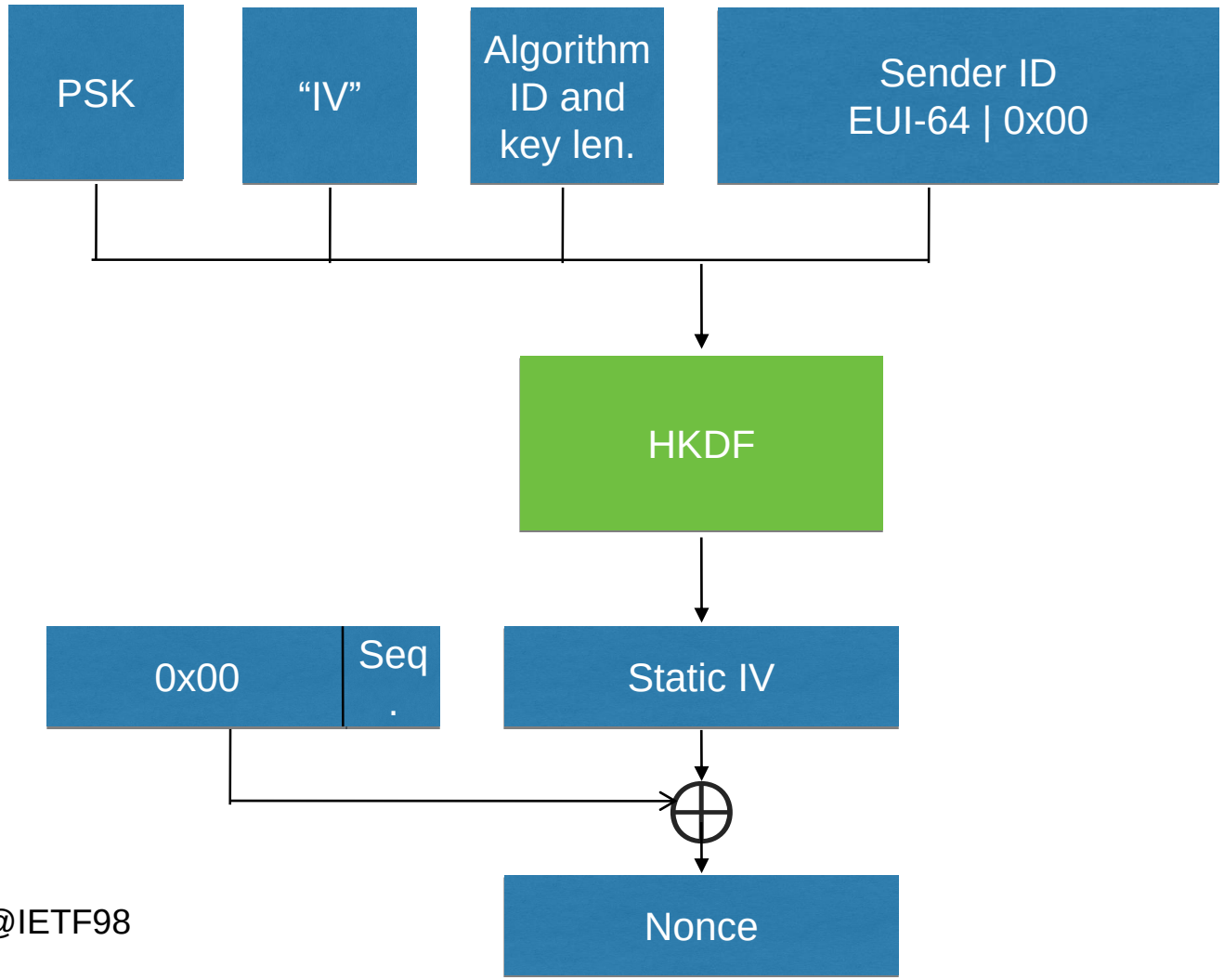
Operation of Join Proxy 2/2

- IP-in-IP encapsulation as an alternative
- Problem: Results in **3** IP headers downwards in case of non-storing RPL (MUST in minimal)
- Can all three headers be compressed?
  - By how much?

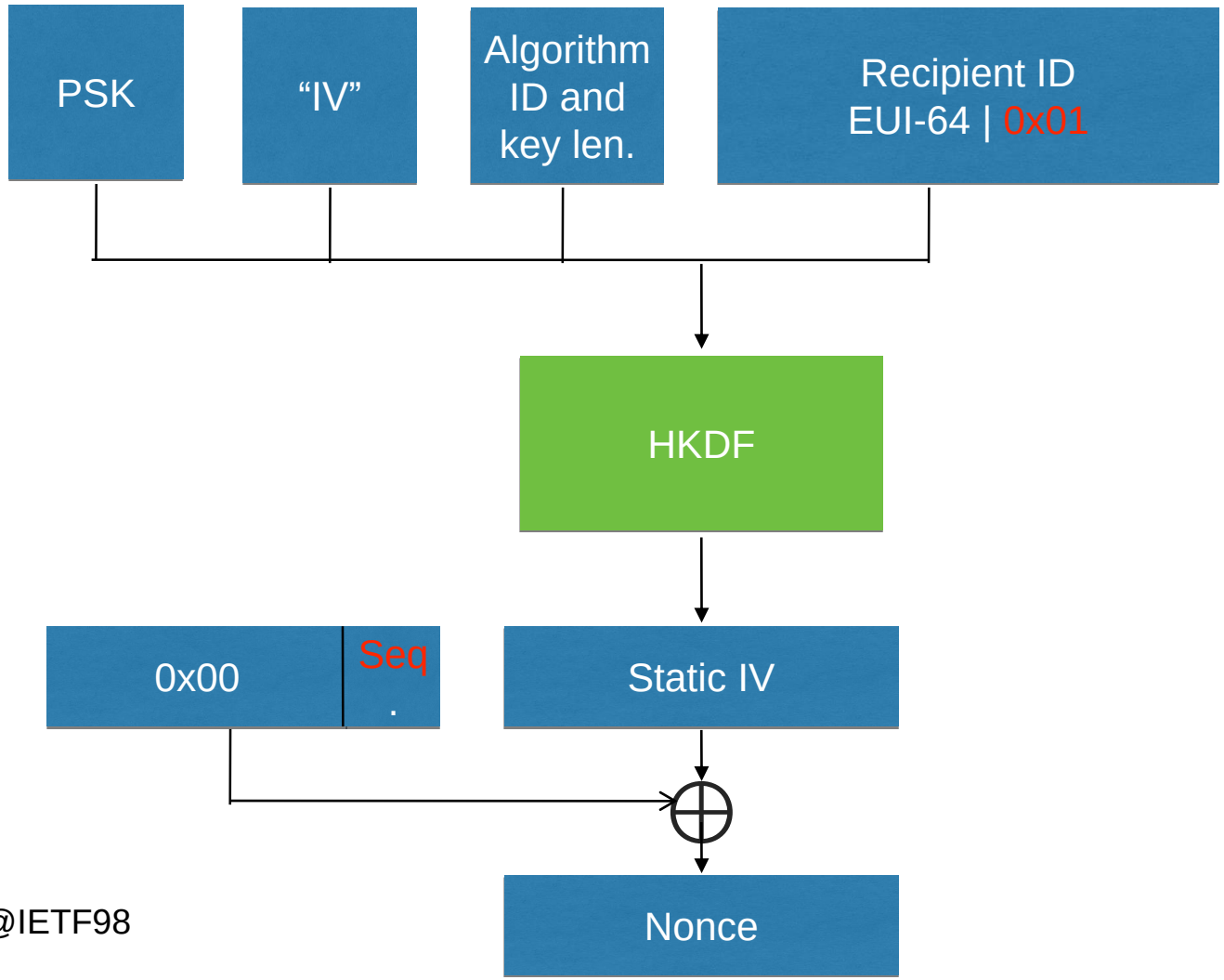
Misc Updates

- Editorial restructure
- Tracking of EDHOC and OSCOAP
- Extended join response structure
  - Lease time for short addresses
  - 15.4 security parameters
- Section on rekeying
  - Out of scope but can be done with the Simple Join Protocol
  - Idea: How about using CoAP Observe option with initial Join Request for rekeying?
- Alignment with latest changes to minimal

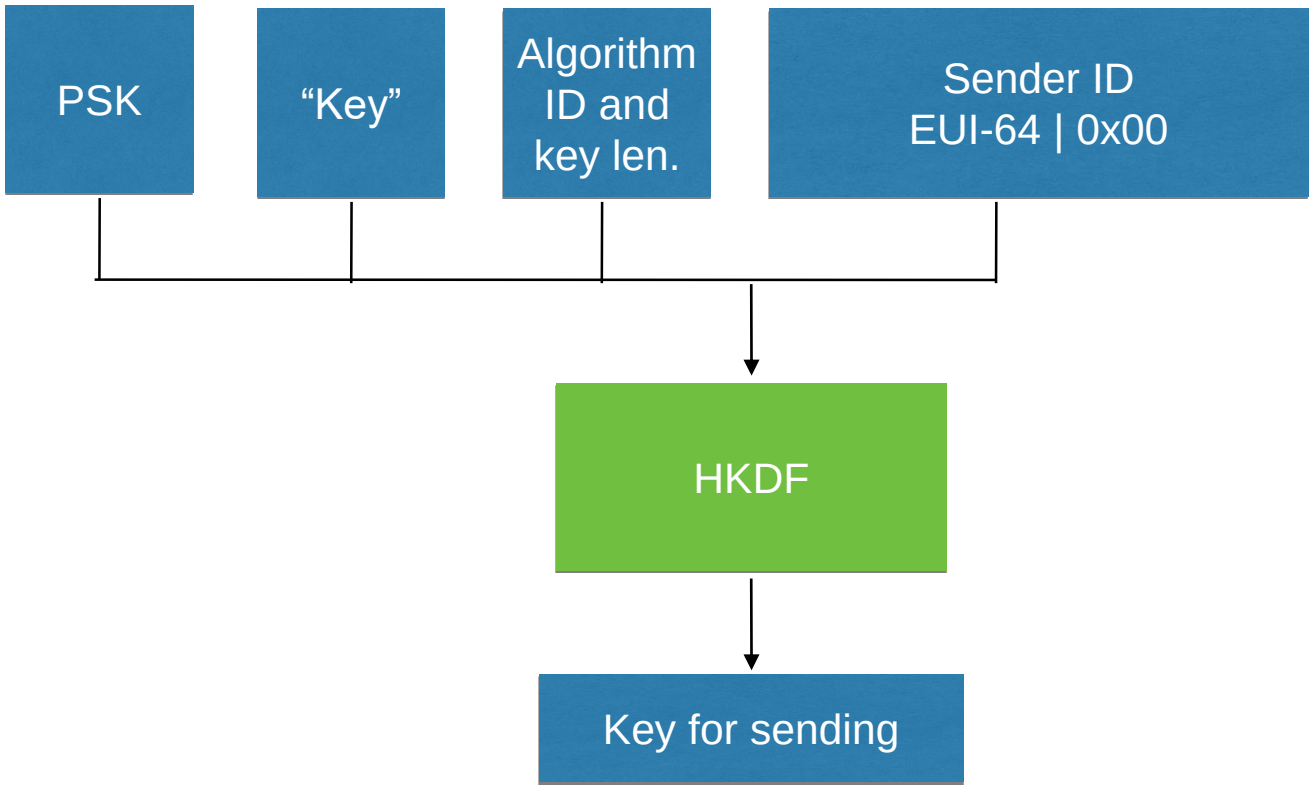
Nonce Generation at Pledge



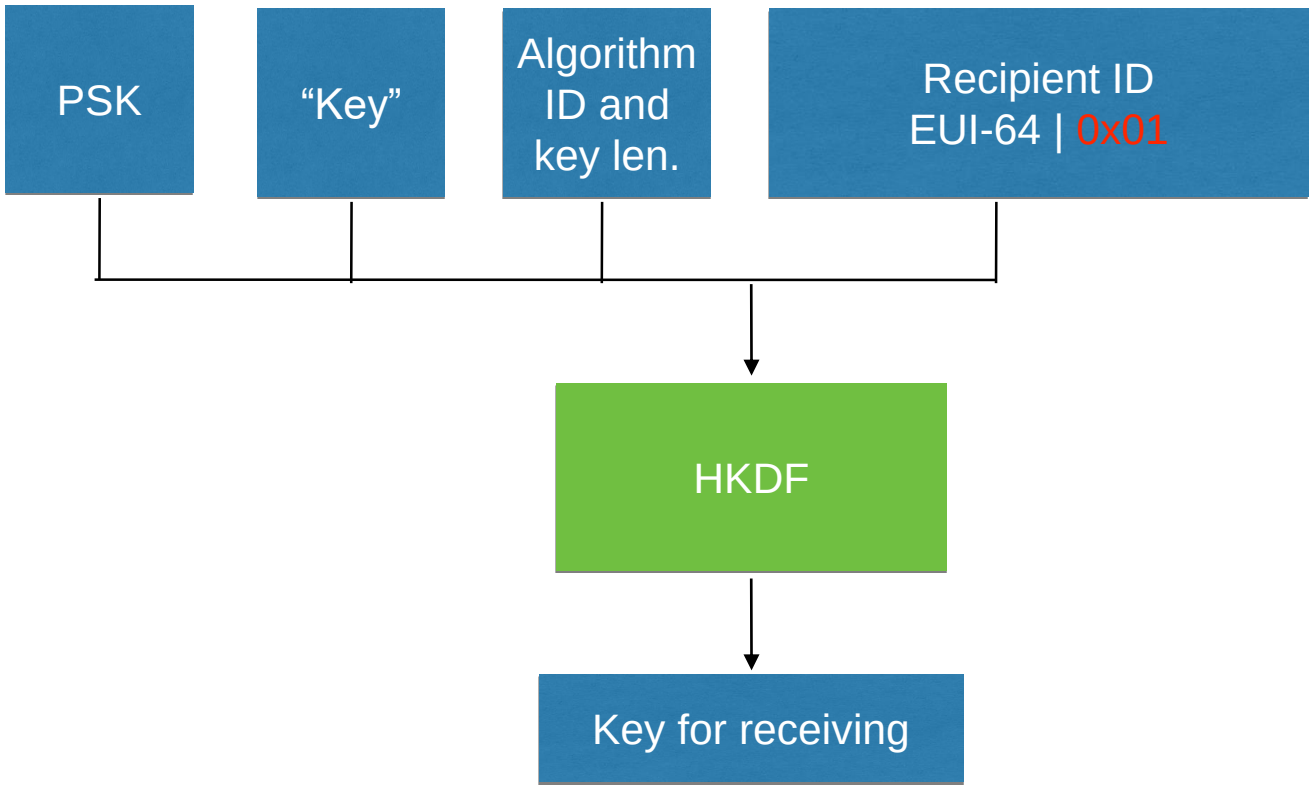
Nonce Generation at JRC



Key Generation at Pledge



Key Generation at Pledge



Conclusion

- PSK variant stable
  - Proceed to implementation
- Asymmetric-key variant under discussion
  - Who/how initiates the handshake?
- Proxy operation under discussion
- Seeking reviews to progress the draft

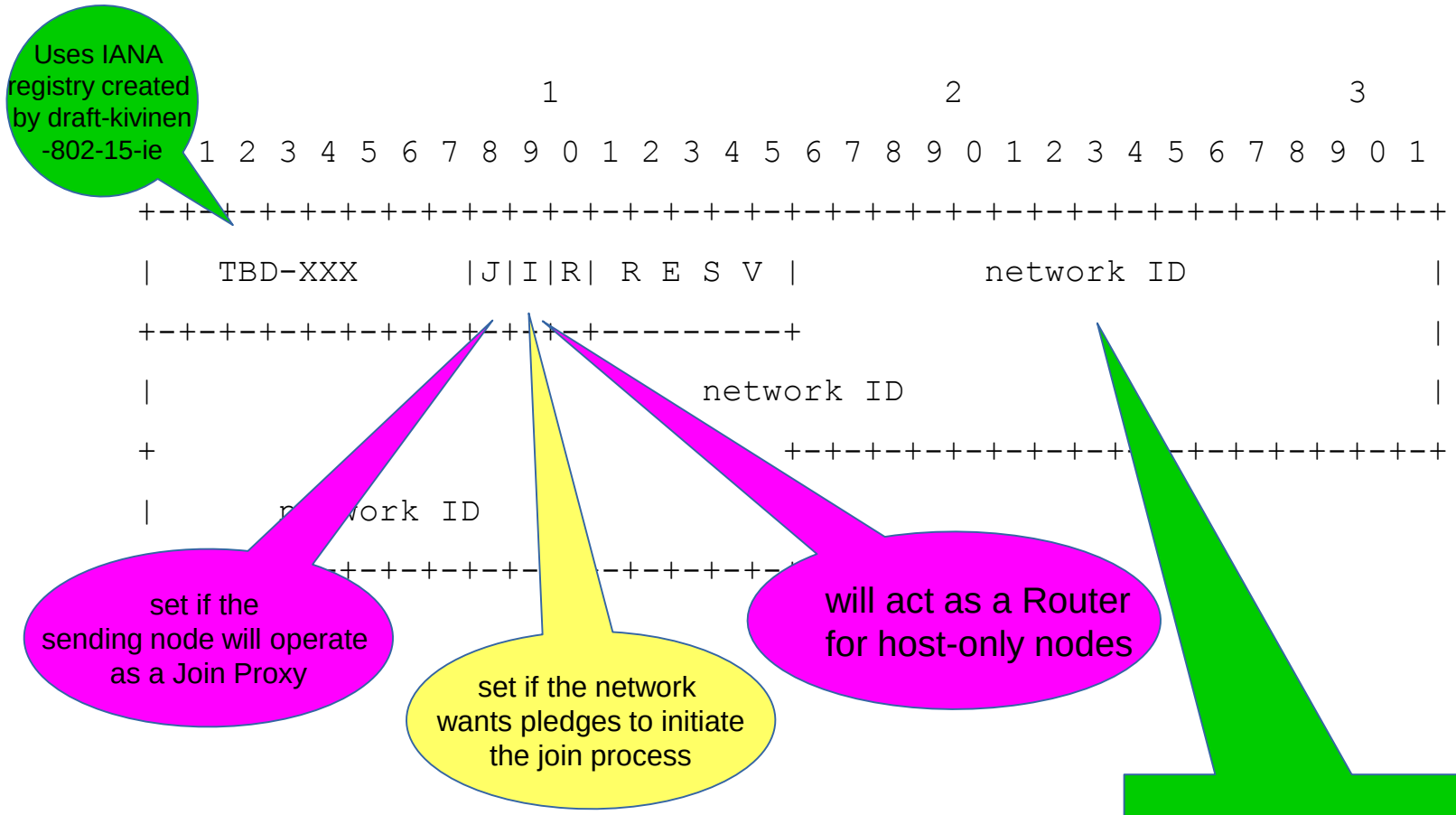
Richardson-6tisch-join-enhanced-beacon

presenter: Diego Dujovne and
Michael Richardson

Status: 6tisch-join-enhanced-beacon

- Goal
  - Standards track definition of extension to Enhanced Beacon to support join needs.
- News
  - How much advice should this document give about finding the Enhanced Beacon?
- Next
  - If this is the right approach, then the WG should adopt this document.

Overview: draft-richardson-6tisch-join-enhanced-beacon



Details: 6tisch-join-enhanced-beacon

J: if bit not set, then announcer not willing to act as proxy. Used when JP is overloaded, or if JP if too many nearby Join Proxy.

R: announcer accepts unicast router solicitations from host-only nodes.

I: initiate flag causes pledge to start EDHOC exchange, rather than wait for JRC to contact it. May be eliminated!

NetworkID: allows a pledge to collect announcements from multiple Join Proxy, and permits long-sleeping node to quickly identify potential Enhanced Beacons to validate.

Thoughts: 6tisch-join-enhanced-beacon

What else could go in EB?

Are there scheduler things that would fit here?

- Would existing IE for 6p work just fine?
- What would be **inappropriate**?

Reminder: EB is **not** encrypted.

Could we put PIO?

- Probably not!
- Lack of encryption would leak too much information.
- Useful only for non-RPL leaf nodes (aka “hosts”)

Questions: 6tisch-join-enhanced-beacon ?

- Thoughts on adoption?

6tisch-minimal-rekey

presenter: Michael Richardson (SSW)
mcr@sandelman.ca

Status: 6tisch-minimal-rekey

- Goal
  - Standards track definition of management interface for rekey operations.
- News
  - Just created.
- Next
  - Fill in some details, get some yang review, some co-authors, and ask for adoption in June.

draft-richardson-6tisch-minimal-rekey

- Moved rekey from minimal to new document.
  - Provides for CoMI managed access to keys.
  - Rekey is managed by slow process of JRC reaching out to all nodes and writing new keys.
    - Provision of new keys includes timeout on old key, after switch-over.
  - Nodes accept traffic from old keys and new keys, uses old keys for transmission until use of new key is seen.
    - Switch over from old to new keys triggers expiration of old keys based upon timers.
- Short addresses are also managed in this interface, short addresses timeout based upon ASN.
  - JRC can garbage collect short-addresses by initiate rekey.
- SEEKING WG adoption and co-authors.

Issues with Rekey

1) Are we using two keys (K1/K2), or one key?

802.15.4 has secKeyId space for 255 keys.

Is that 127 pairs, or 255 keys?

1) Transition to new key leaves window during which old key can be used.

This matters if rekey is to remove malicious node from network.

Extra Slides

draft-richardson-6tisch-join-enhanced-beacon

- Need for definition of extension to enhanced-beacon made clear by join process.
  - Uses IANA registry created by draft-kivinen-802-15-ie
- Includes some bits to help hosts (aka non-RPL leaf nodes) to find correct network, and give hint about using unicast Router Solitications.
- Network ID is based upon SHA256 of DODAGID to identify network.
- Notes that EB is not encrypted, so inappropriate to put much information in.
- Has bit to indicate if sender is available as a Join Proxy; L3 address is implied by SLAAC configuation of Link-Local address from EUI-64 of sender.

SEEKING WG adoption and co-authors.
Authors: Diego Dujovne and Michael Richardson

draft-ietf-6tisch-6top-protocol

Qin Wang
Xavier Vilajosana
Thomas Watteyne

Status

- Stable document.
  - New version published the 27th of March
  - Major reordering and clean up
  - Added command for relocation of cells
  - STATUS renamed to COUNT
- Next
  - Ready for Last Call?

Reordering

Changes

- Full reordering of commands
  - Put together frame format and description of the operation
- Renamed STATUS to COUNT
- Removed cell suggestion example (was confusing)

Next Steps

- Authors looking for feedback
  - Important is relation with SF0.
  - Are there any functionalities missing?
- Ask for Last Call

draft-ietf-6tisch-sf0-03

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

Status

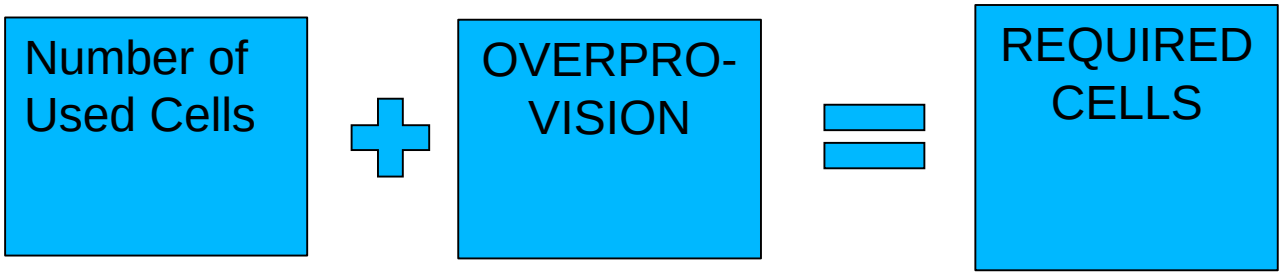
- Goal: Provide a simple distributed Scheduling Function according to the requirements of the 6P draft
- Changes:
  - Changed Estimation Algorithm
  - Fixed Typos
  - Added statistics calculations
- Next

Status

- Next:
- Change to Experimental RFC
- Timeout discussion

Cell Estimation Algorithm

- Changed to Alternative 3 presented at IETF97:

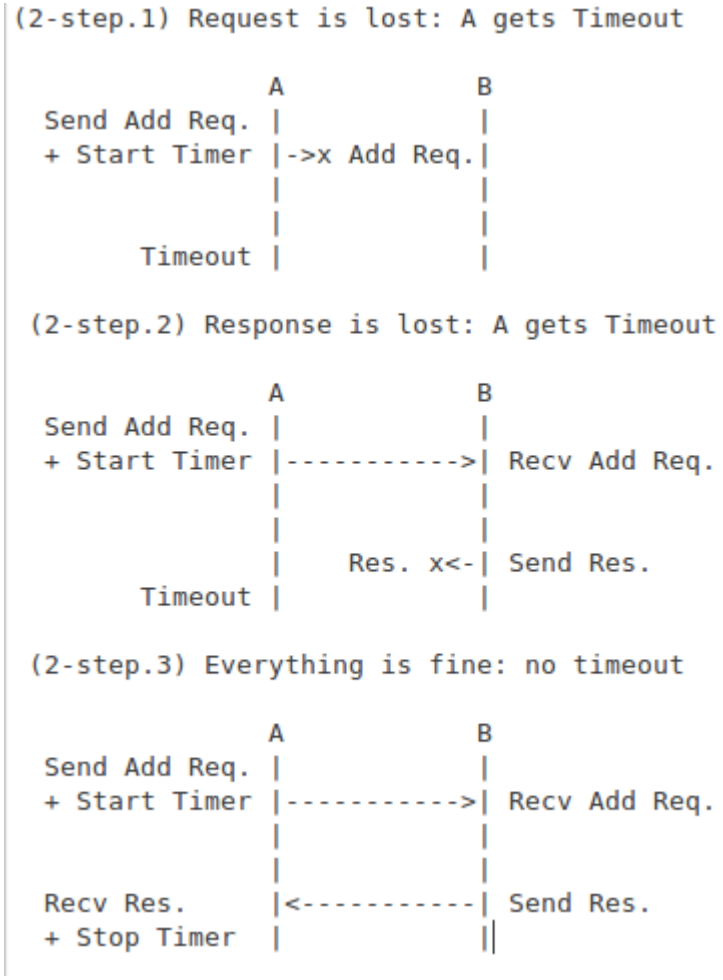


- SF0 is based on a neighbor-to-neighbor negotiation.
- We do not know if the incoming requested add/delete cell destination is the local node or if it will be routed to another neighbor
- Including it would add unnecessary uncertainty, resulting in possible under- or over-provisioning.
- OVERPROVISION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

PDR Calculation

- Added PDR Calculation:
- “Packet Delivery Rate (PDR) is calculated per cell, as the quotient of the number of successfully delivered packets to 10, for the last 10 packet transmission attempts, without counting retransmissions.”
- Is 10 a good value for the sliding window? Shall leave the value as implementation-specific?

Timeout Calculation



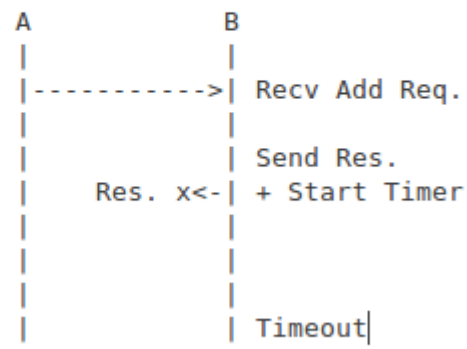
- Yasuyuki´s proposal without MAC-level timeout (Dec 12/2016)
- Requires 6P modification.

Timeout Calculation

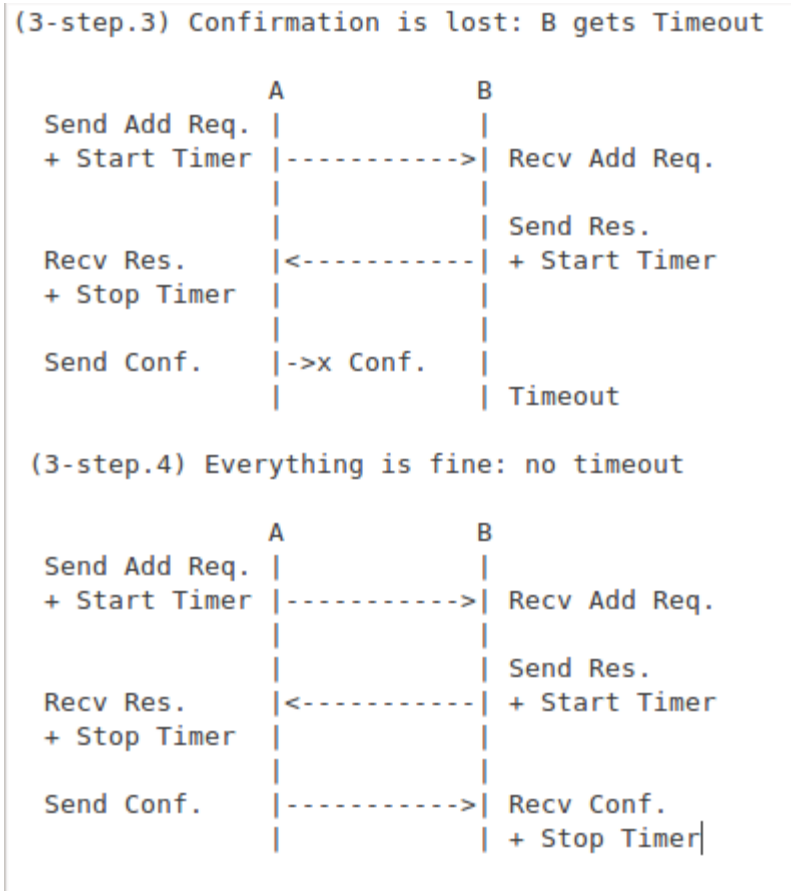
(3-step.1) Request is lost: A gets Timeout

Same as (2-step.1)

(3-step.2) Response is lost: A and B gets Timeout



Timeout Calculation



Typos and text changes

- Eliminated the term “effectively” from “effectively used cells”. Now we have only non-allocated, allocated and used cells, following Randy´s and Yasuyuki´s comments.
- Forced Deletion: Implementation Specific

Cell Relocation

- PDR_THRESHOLD: Defined as a percentage of the average of the PDR of the rest of the scheduled cells,
- SF0 relocates each of the cell(s) to a number of available cells selected randomly.
- PDR_THRESHOLD is out of the scope of this document and it is implementation-dependent.

Questions

- Do you agree on leaving PDR_THRESHOLD as implementation-specific?
- Do you agree in leaving “Forced Deletion” as implementation-specific?
- Shall we leave the number of average elements on the PDR calculation as implementation-specific?

Future

- Fixed typos (“effectively” is still on the text at least once)
- Change to Experimental RFC:
  - We need simulations and experimental results to validate the proposed algorithms.
  - There is a paper on the topic, but it does not use the current estimation algorithm.
- Timeout discussion: Do we adopt the former proposal?

draft-ietf-6tisch-architecture

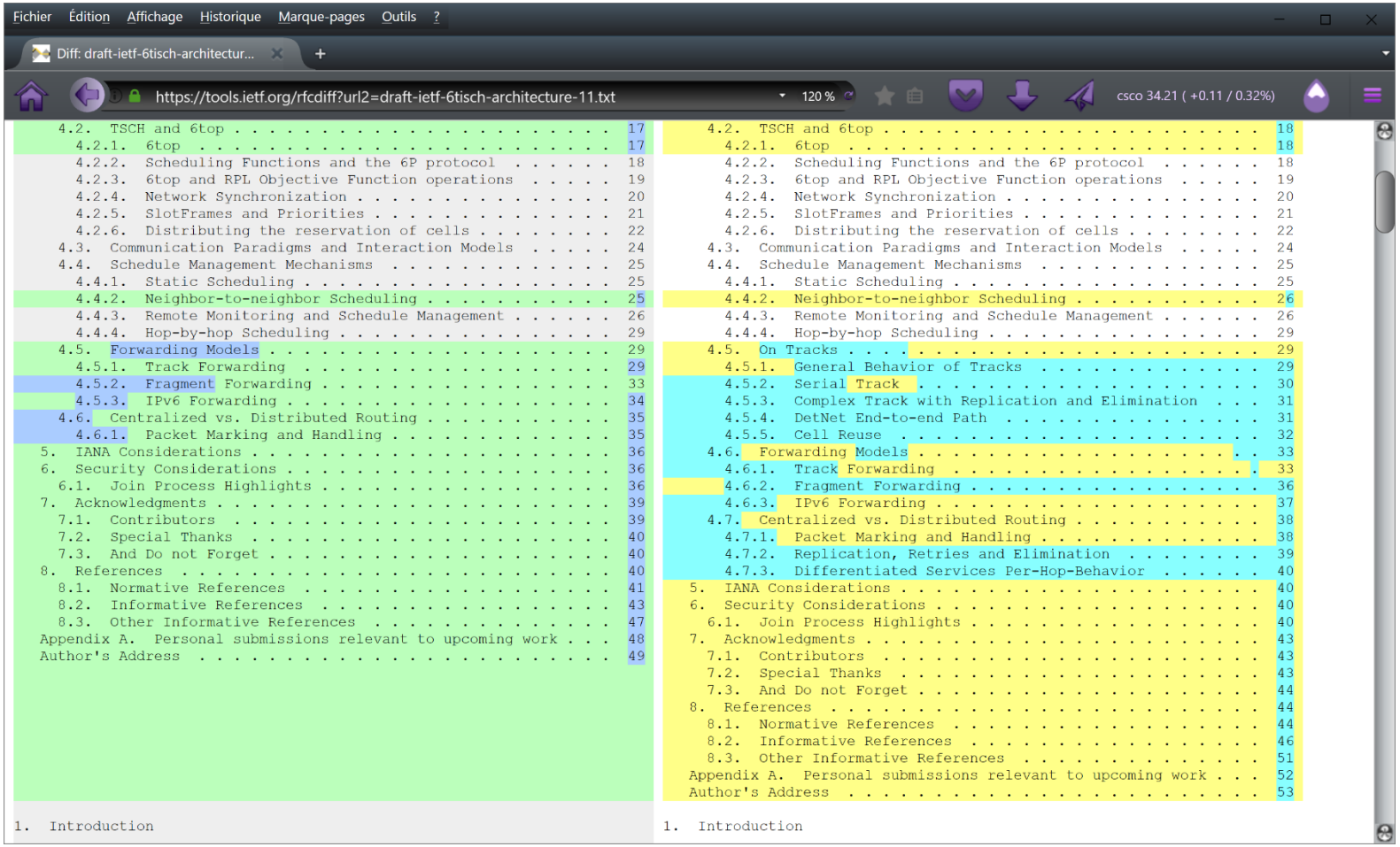
P. Thubert, Ed.

Status

- draft-ietf-6tisch-architecture-11
  - Published January 27, 2017
  - Incorporate text on tracks
  - from 6tisch-for-detnet draft

- Goal
  - Keep it active for potential rechartering

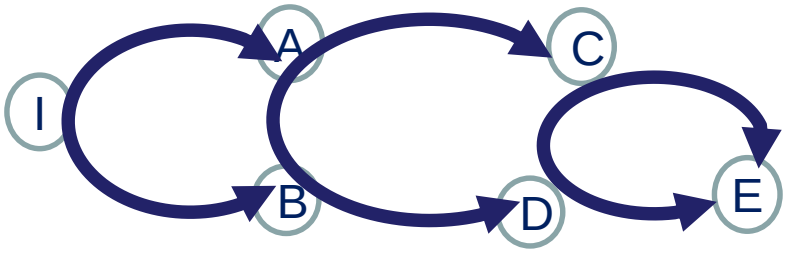
Diffs


Fichier Édition Affichage Historique Marque-pages Outils ?
Diff: draft-ietf-6tisch-architectur...
https://tools.ietf.org/rfcdiff?url2=draft-ietf-6tisch-architecture-11.txt
120 %
csco 34.21 (+0.11 / 0.32%)
4.2. TSCH and 6top . . . 17
4.2.1. 6top . . . 17
4.2.2. Scheduling Functions and the 6P protocol . . . 18
4.2.3. 6top and RPL Objective Function operations . . . 19
4.2.4. Network Synchronization . . . 20
4.2.5. SlotFrames and Priorities . . . 21
4.2.6. Distributing the reservation of cells . . . 22
4.3. Communication Paradigms and Interaction Models . . . 24
4.4. Schedule Management Mechanisms . . . 25
4.4.1. Static Scheduling . . . 25
4.4.2. Neighbor-to-neighbor Scheduling . . . 25
4.4.3. Remote Monitoring and Schedule Management . . . 26
4.4.4. Hop-by-hop Scheduling . . . 29
4.5. Forwarding Models . . . 29
4.5.1. Track Forwarding . . . 29
4.5.2. Fragment Forwarding . . . 33
4.5.3. IPv6 Forwarding . . . 34
4.6. Centralized vs. Distributed Routing . . . 35
4.6.1. Packet Marking and Handling . . . 35
5. IANA Considerations . . . 36
6. Security Considerations . . . 36
6.1. Join Process Highlights . . . 36
7. Acknowledgments . . . 39
7.1. Contributors . . . 39
7.2. Special Thanks . . . 40
7.3. And Do not Forget . . . 40
8. References . . . 40
8.1. Normative References . . . 41
8.2. Informative References . . . 43
8.3. Other Informative References . . . 47
Appendix A. Personal submissions relevant to upcoming work . . . 48
Author's Address . . . 49
1. Introduction
4.2. TSCH and 6top . . . 18
4.2.1. 6top . . . 18
4.2.2. Scheduling Functions and the 6P protocol . . . 18
4.2.3. 6top and RPL Objective Function operations . . . 19
4.2.4. Network Synchronization . . . 20
4.2.5. SlotFrames and Priorities . . . 21
4.2.6. Distributing the reservation of cells . . . 22
4.3. Communication Paradigms and Interaction Models . . . 24
4.4. Schedule Management Mechanisms . . . 25
4.4.1. Static Scheduling . . . 25
4.4.2. Neighbor-to-neighbor Scheduling . . . 26
4.4.3. Remote Monitoring and Schedule Management . . . 26
4.4.4. Hop-by-hop Scheduling . . . 29
4.5. On Tracks . . . 29
4.5.1. General Behavior of Tracks . . . 29
4.5.2. Serial Track . . . 30
4.5.3. Complex Track with Replication and Elimination . . . 31
4.5.4. DetNet End-to-end Path . . . 31
4.5.5. Cell Reuse . . . 32
4.6. Forwarding Models . . . 33
4.6.1. Track Forwarding . . . 33
4.6.2. Fragment Forwarding . . . 36
4.6.3. IPv6 Forwarding . . . 37
4.7. Centralized vs. Distributed Routing . . . 38
4.7.1. Packet Marking and Handling . . . 38
4.7.2. Replication, Retries and Elimination . . . 39
4.7.3. Differentiated Services Per-Hop-Behavior . . . 40
5. IANA Considerations . . . 40
6. Security Considerations . . . 40
6.1. Join Process Highlights . . . 40
7. Acknowledgments . . . 43
7.1. Contributors . . . 43
7.2. Special Thanks . . . 43
7.3. And Do not Forget . . . 44
8. References . . . 44
8.1. Normative References . . . 44
8.2. Informative References . . . 46
8.3. Other Informative References . . . 51
Appendix A. Personal submissions relevant to upcoming work . . . 52
Author's Address . . . 53
1. Introduction

Tests done Using Tracks

Radios are lossy, but they are also inherently broadcast:
Use that latter property as a compensation for the former

1. Multipath Tracks with the general shape of a cord ladder



2. Control the replication and elimination to save energy
3. Use intelligent flooding leveraging broadcast properties

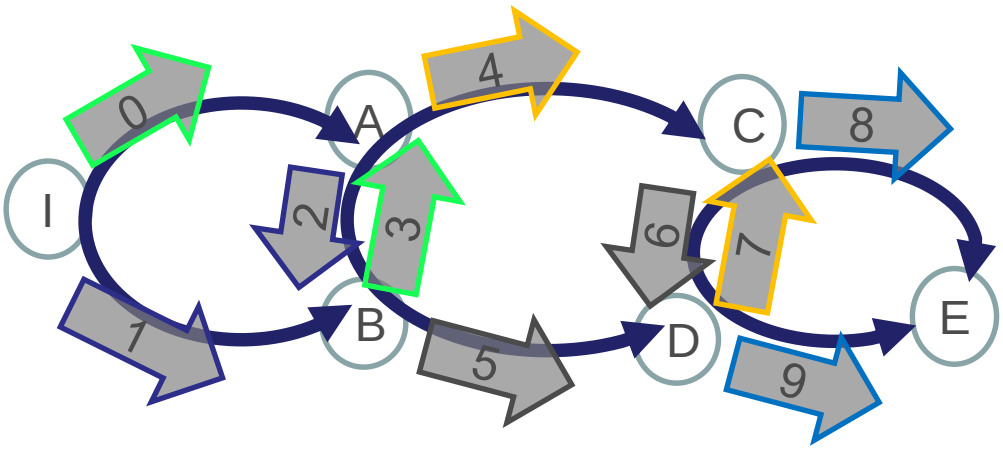
Goals: minimize energy, minimize latency, optimize delivery and avoid 4 losses in a row

https://datatracker.ietf.org/doc/draft-thubert-6lo-bier-dispatch/

Test1: Flooding an ARC chain

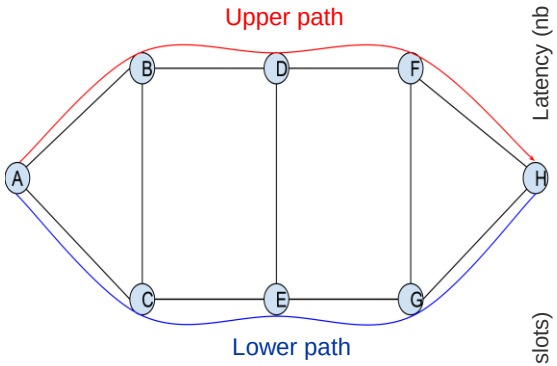
Using ARC chains and multipath scheduling

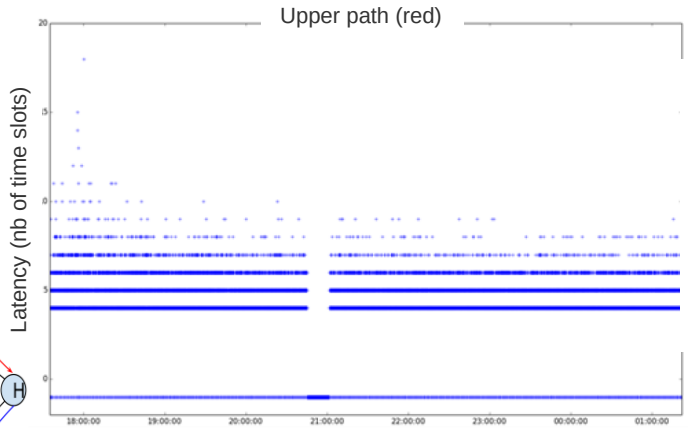
Assigning Time Slot and configuring replication and elimination, each packet with 2 receive opportunities
Time slots taken from a schedule shared with IP/6TiSCH

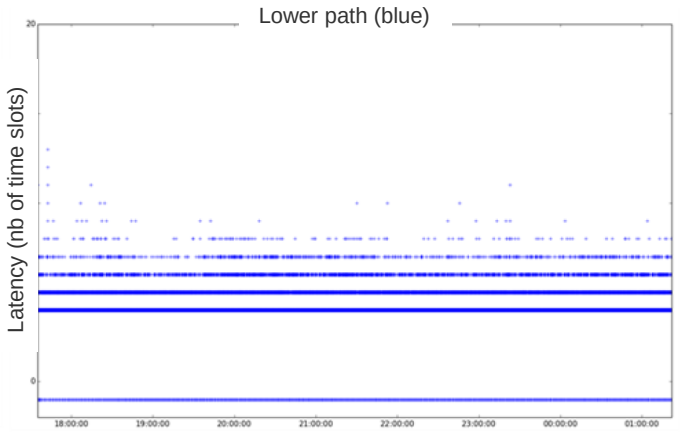


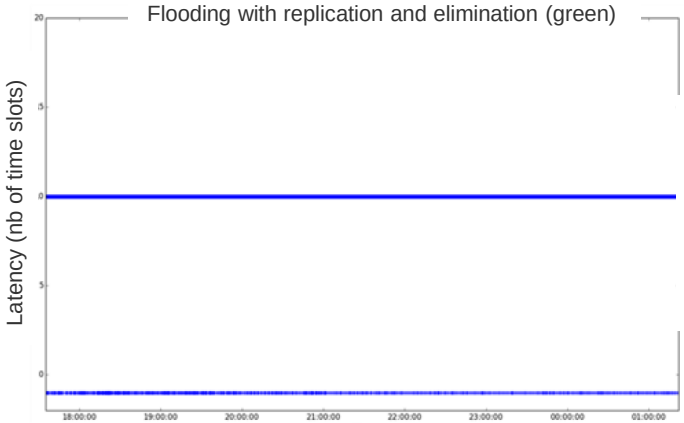
timeSlot	Adjacency
0	I->A
1	I->B
2	A->B
3	B->A
4	A->C
5	B->D
6	C->D
7	D->C
8	C->E
9	D->E

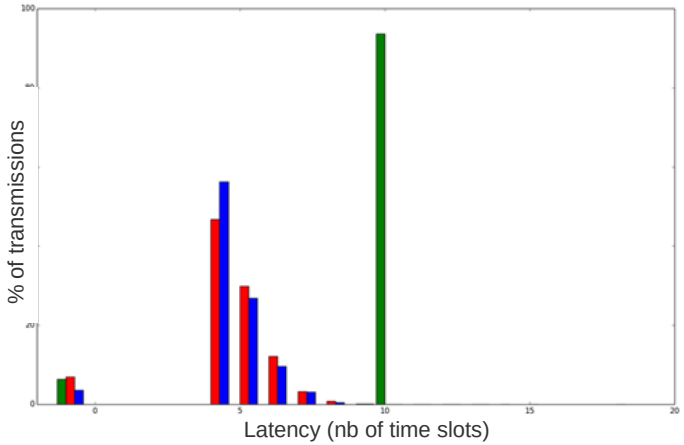
Test1: Replication and Elimination vs. Serial Path







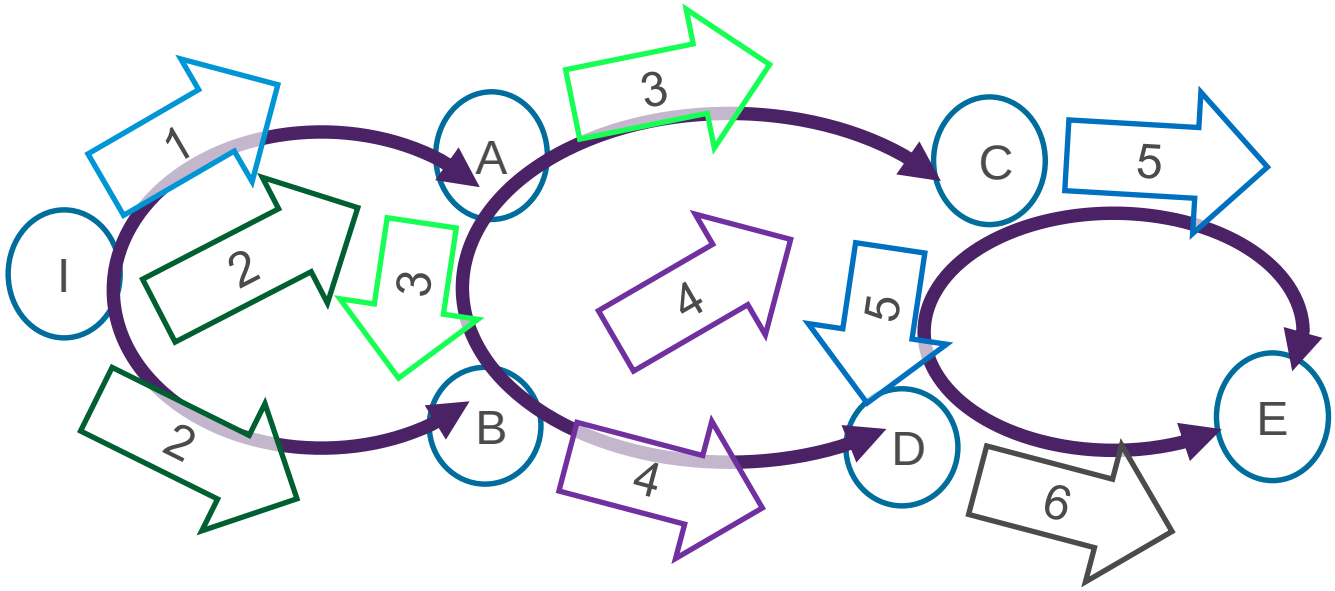




Test 2 controlling unicast in the ARC chain

Dynamic (in band) control of the replication and elimination operation with BIER

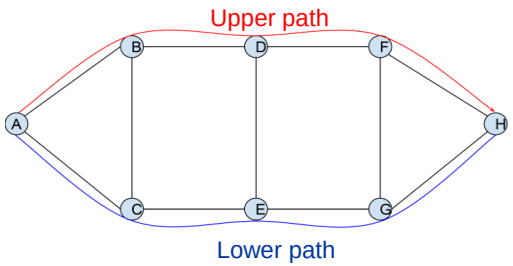
Segment Activity is controlled in band with packet header
Knowledge of ownership is programmed in the devices

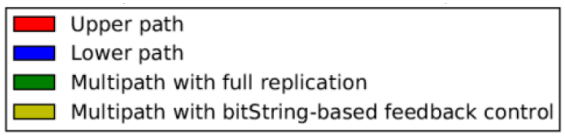


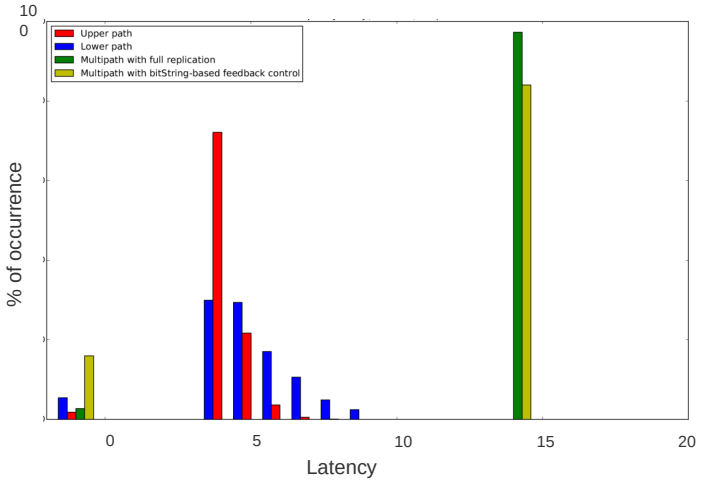
ctrl #	Adjacency	Owner
1	I->A(,B)	I
2	I->B,A	I
3	A->C,B	A
4	B->D,C	B
5	C->D,E	C
6	D->E	B

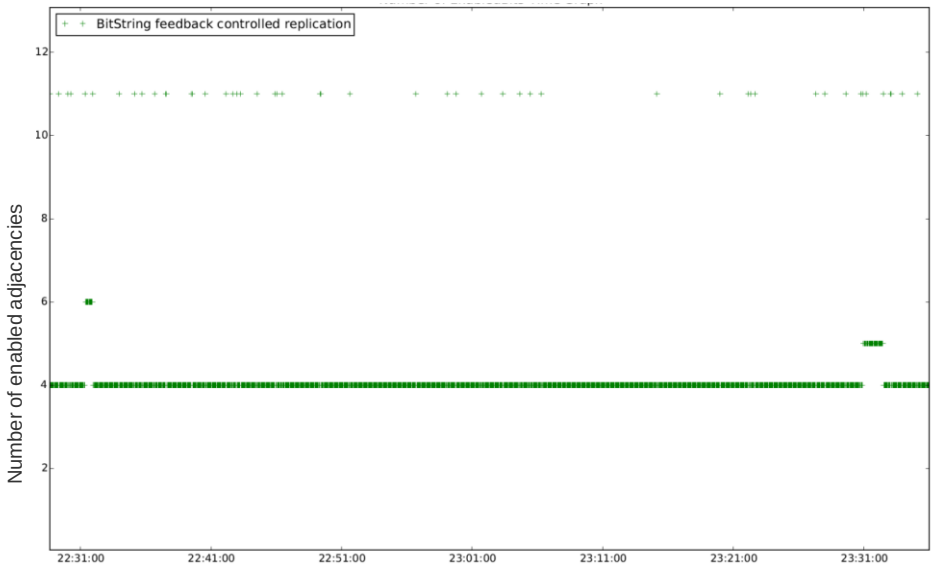
https://datatracker.ietf.org/doc/draft-thubert-6lo-bier-dispatch/

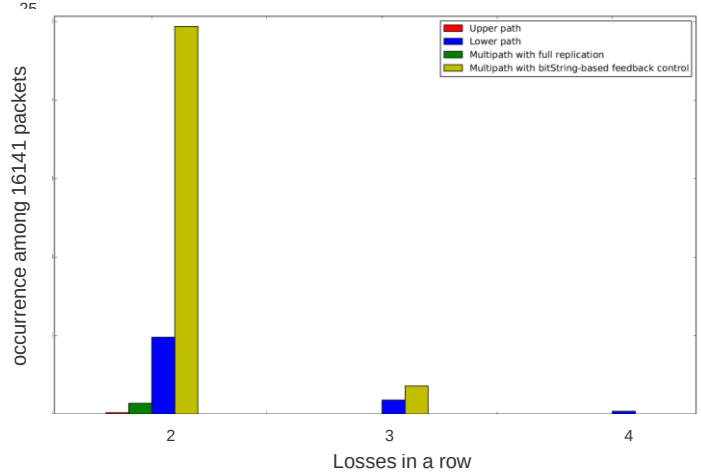
Test 2: Energy Saving









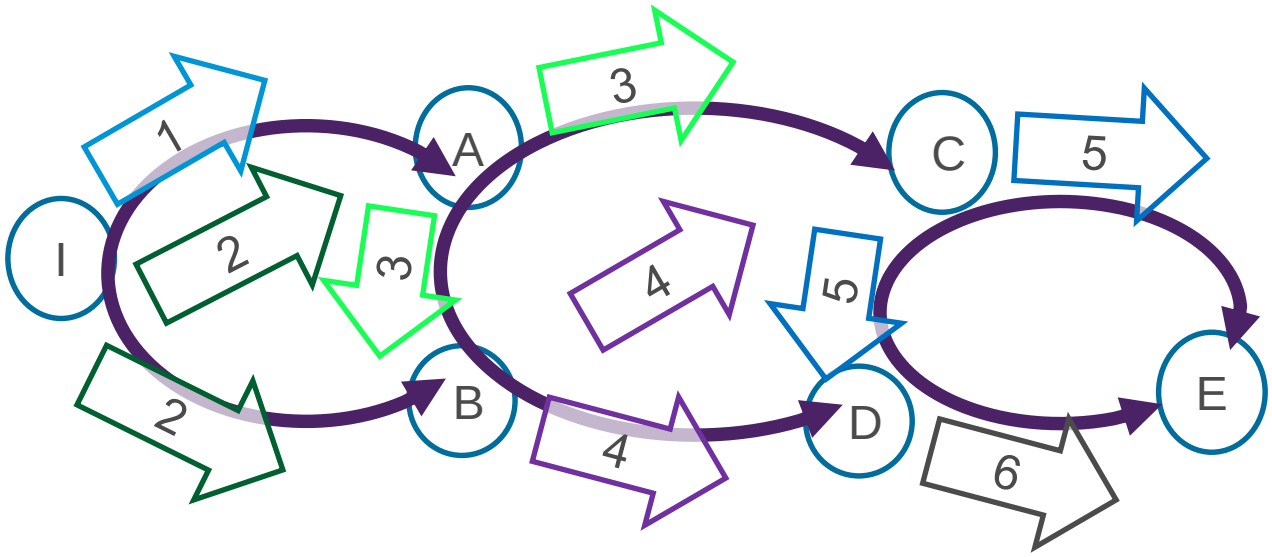


https://datatracker.ietf.org/doc/draft-thubert-6lo-bier-dispatch/

Test 3: Controlling bicasting in the ARC chain

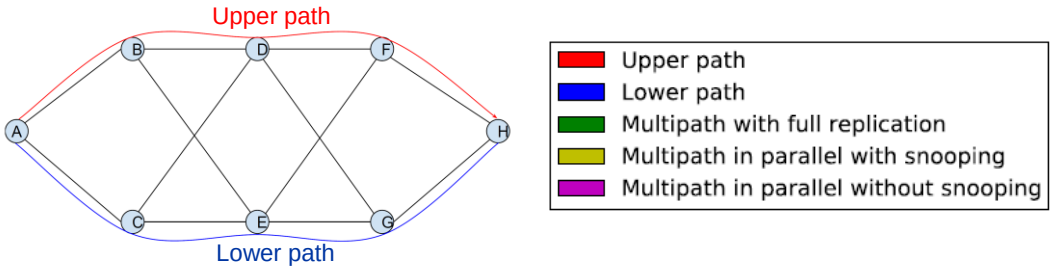
Collaborative overhearing to improve latency while preserving energy

Use RPL non storing mode to expose topology
Enables and schedules >1 downstream listeners



ctrl #	Adjacency	Owner
1	I->A(,B)	I
2	I->B,A	I
3	A->C,B	A
4	B->D,C	B
5	C->D,E	C
6	D->E	B

Test 3: Improved latency using collaboration



Multipath with full replication:

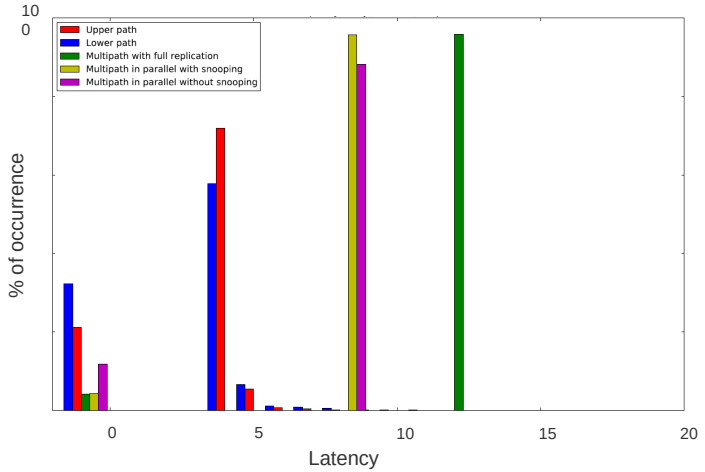
0	1	2	3	4	5	6	7	8	9	10	11
A --> B	A --> C	B --> E	B --> D	C --> E	C --> D	D --> G	D --> F	E --> G	E --> F	F --> H	G --> H

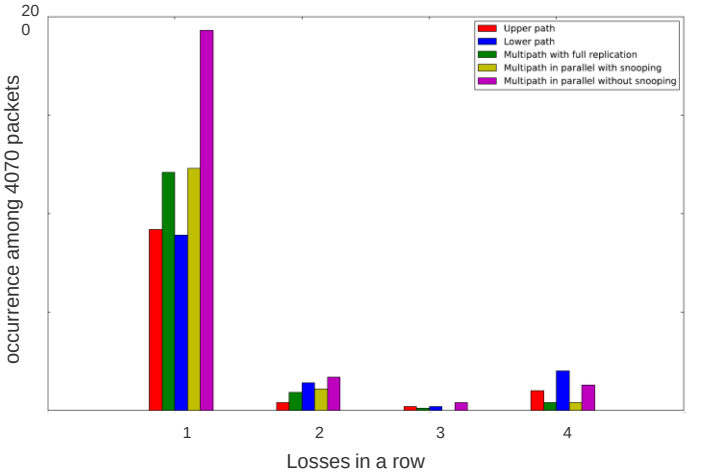
Multipath in parallel with snooping:

0	1	2	3	4	5	6	7	8	9	10	11
A --> B,C	A --> C,B	B --> E,D	C --> E,D	D --> G,F	E --> G,F	F --> H	G --> H				

Multipath in parallel without snooping:

0	1	2	3	4	5	6	7	8	9	10	11
A --> B	A --> C	B --> D	C --> E	D --> F	E --> G	F --> H	G --> H				





IEEE 802.15.4 and related standards update

- IEEE 802.15.4 - amendments, corrigendum, and revision
- IEEE 802.15.9 – Key Management Protocol
- IEEE 802.15.10 – Layer 2 Routing
- IEEE 802.15.12 – Upper Layer Interface to 802.15.4

IEEE 802.15.4 Approved Amendments

(Latest Revision: IEEE 802.15.4-2015)

IEEE Std 802.15.4n: IEEE Standard for Low-Rate Wireless Networks - Amendment 1: **Physical Layer Utilizing China Medical Bands**

IEEE Std 802.15.4q: IEEE Standard for Low-Rate Wireless Networks - Amendment 2: **Ultra-Low Power Physical Layer**

IEEE Std 802.15.4t: IEEE Standard for Low-Rate Wireless Networks – Amendment 4: **Higher Rate (2 Mb/s) Physical (PHY) Layer**

IEEE Std 802.15.4u: IEEE Standard for Low-Rate Wireless Networks- Amendment 3: **Use of the 865 MHz to 867 MHz Band in India**

IEEE 802.15.4 amendments in process

IEEE Std 802.15.4s: IEEE Standard for Low-Rate Wireless Networks: **Amendment Enabling Spectrum Resource Measurement Capability**

- spectrum resource measurements, such as packet error ratio, delay, etc,
- information elements and data structures to capture these measurements,
- procedures for collecting and exchanging spectrum resource measurement information with higher layers or other devices.

IEEE Std 802.15.4v: IEEE Standard for Low-Rate Wireless Networks: **Amendment Enabling/Updating the Use of Regional Sub-GHz Bands**

- 870-876 MHz & 915-921 MHz bands in Europe,
- 902-928 MHz band in Mexico,
- 902-907.5 MHz & 915-928 MHz bands in Brazil,
- 915-928 MHz band in Australia/New Zealand and Asian regional frequency bands that are not in IEEE Std 802.15.4-2015.

IEEE 802.15.4 Corrigendum

- Two corrections for IEEE 802.15.4-2015 are:
  1. 64-bit MAC address transmission order
     - Transmission order was reversed from earlier standards, this will be corrected, i.e. changed back to original order
  2. Missing value for CID in CCM* Nonce for TSCH mode
     - IEEE 802.15 CID is called out to be inserted into the nonce when using the short address in TSCH mode
     - IEEE 802.15 CID has been approved by IEEE Registration Authority (IEEE RA) with an assigned value of: BA-55-EC
- Estimated approval date is February, 2018

IEEE 802.15.4 Revision

- Changes include:
  - Roll-up of 6 amendments
  - Inclusion of corrigenda and other corrections
  - Correct ambiguities and violations of IEEE style guide
  - Other?
- Major effort will start in July 2017
- Estimated approval date is May, 2019

IEEE 802.15.9 Key Management Protocol (KMP)

- Recommended practice for message exchange framework using information elements (IE) as the transport method for KMP datagrams.
- Guidelines for IEEE 802.15.4 usage of some existing KMPs such as: IEEE 802.1X/MKA, HIP, IKEv2, PANA, Dragonfly, IEEE 802.11/4WH, IEEE 802.11/GKH, ETSI TS 102 887-2.
- Defines a general purpose multiplexed (MPX) data service
- Defines a fragmentation and re-assembly protocol for payloads unable to fit in a single MAC frame.

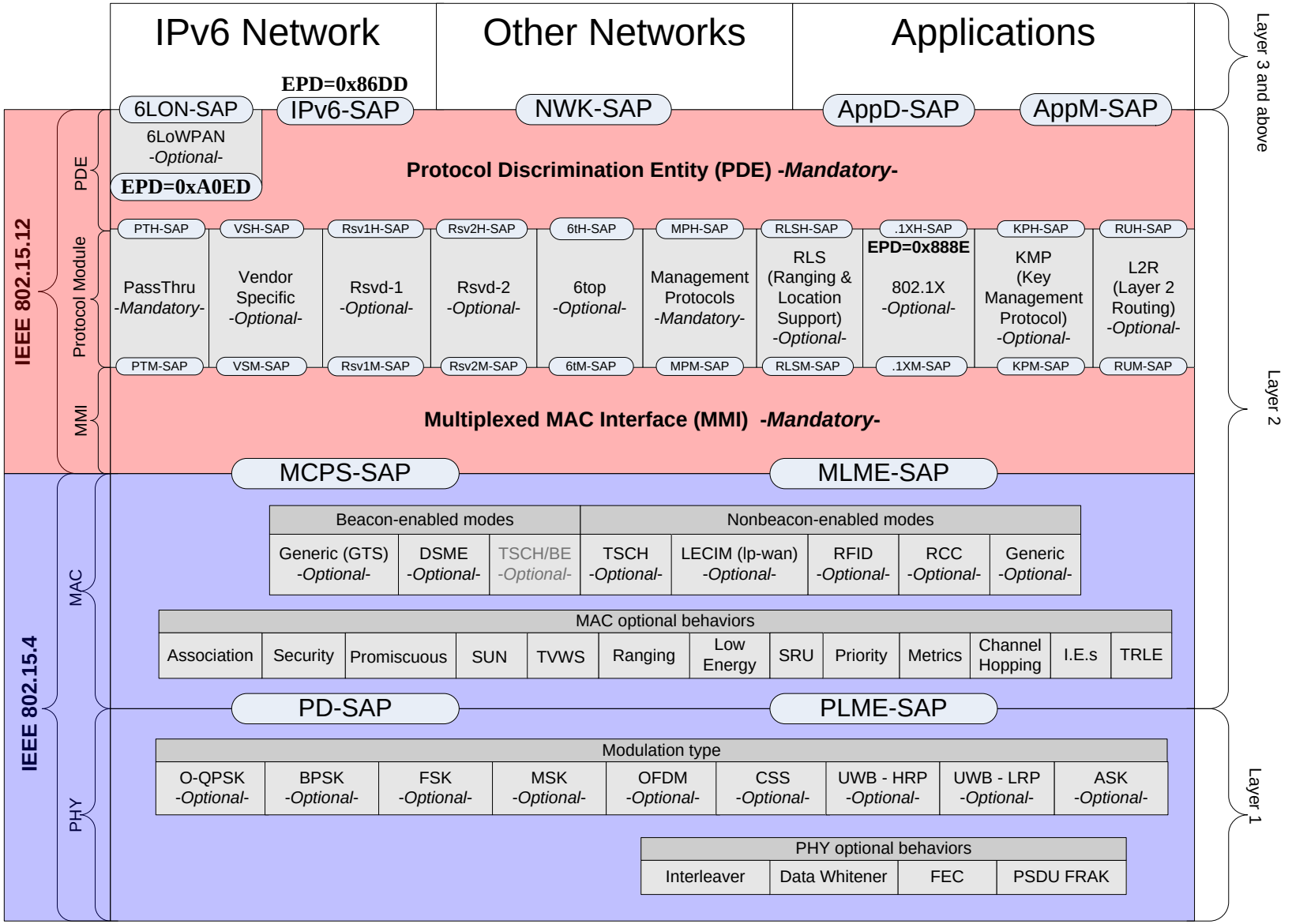
IEEE 802.15.10 Layer 2 Routing (L2R)

- Recommended Practice for L2R:
  - Defines protocols that route packets in a dynamically changing (order of a minute) 802.15.4 network
  - Extends the area of coverage as the number of nodes increase
  - Supports Data Concatenation
  - Supports small, medium and large scale networks
- Overview Tutorial on IEEE 802.15.10:https://mentor.ieee.org/802.15/dcn/17/15-17-0205-00-0010-overview-tutorial-on-802-15-10.pptx

IEEE 802.15.12 Upper Layer Interface for IEEE 802.15.4

- 802.15.12 Presentation to 6tisch was done 3 February https://mentor.ieee.org/802.15/dcn/17/15-17-0113-00-0012-802-15-12-conceptual-overview.pptx.
- Purpose:
  - Reduction of the complexity in configuring and using the 802.15.4 device
  - Addition of higher layer protocol identification
  - Fragmentation of L3 datagrams
  - Harmonization of L2 protocols
  - Management of 802.15.4 managed objects
- Updates since then:
  - Configuration
  - Network Management

IEEE 802.15.12 paired with IEEE 802.15.4



IEEE 802.15.12 Upper Layer Interface

Configuration

- Approved the concept of profiles where a profile defines all configuration parameters (i.e. data objects) necessary for IEEE 802.15.4 operation,
- Management protocol module would store/access the profile(s) for the IEEE 802.15.4 device and implement them into the device when instructed by a higher layer app or by another protocol module,
- Yang data model initially selected using a format of JSON or XML,
- Growing consensus is that a protocol such as Netconf could provide necessary functionality to extract or install the configuration parameters in an efficient manner, yielding a full, formal application programming interface (API).

Network Management

- Create data objects related to network performance, including those created by IEEE 802.15.4s,
- Leveraging Configuration, would use Netconf with Yang data modeling.

IEEE 802.15.12 Participation

- To complete 802.15.12 in a timely fashion additional participation is requested
- Participation can be via email, conference calls, conference attendance, or all of the above
- Email reflector: stds-802-15-12@listserv.ieee.org
- Conference call: will be set-up
- Conferences:
  - May 7-12, 2017, Daejeon Convention Center, Daejeon Korea, *802 Wireless Interim Session.*
  - July 9-14, 2017, Estrel Hotel and Convention Center, Berlin, Germany, *802 Plenary Session.*
  - September 10-15, 2017, Hilton Waikoloa Village, Kona, HI, USA, *802 Wireless Interim Session.**

Backhaul Networks

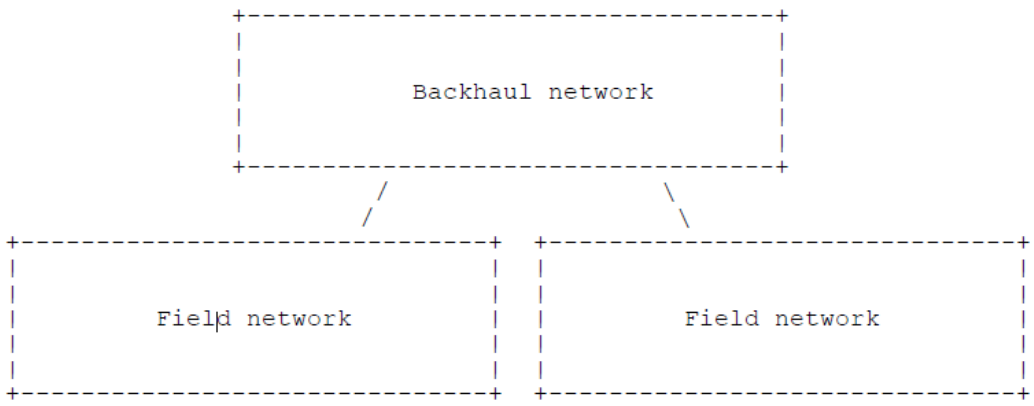
draft-wang-detnet-backhaul-architecture-00

Heng Wang, Ping Wang , Lun Shao
wangheng@cqupt.edu.cn, wangping@cqupt.edu.cn, yjssslcqupt@163.com
Chongqing University of Posts and Telecommunications, China

Chicago, March 28, 2017

Network Structure

- A typical deterministic industrial field networks - backhaul networks structure.
- End-to-end joint scheduling of the cross-network data streams

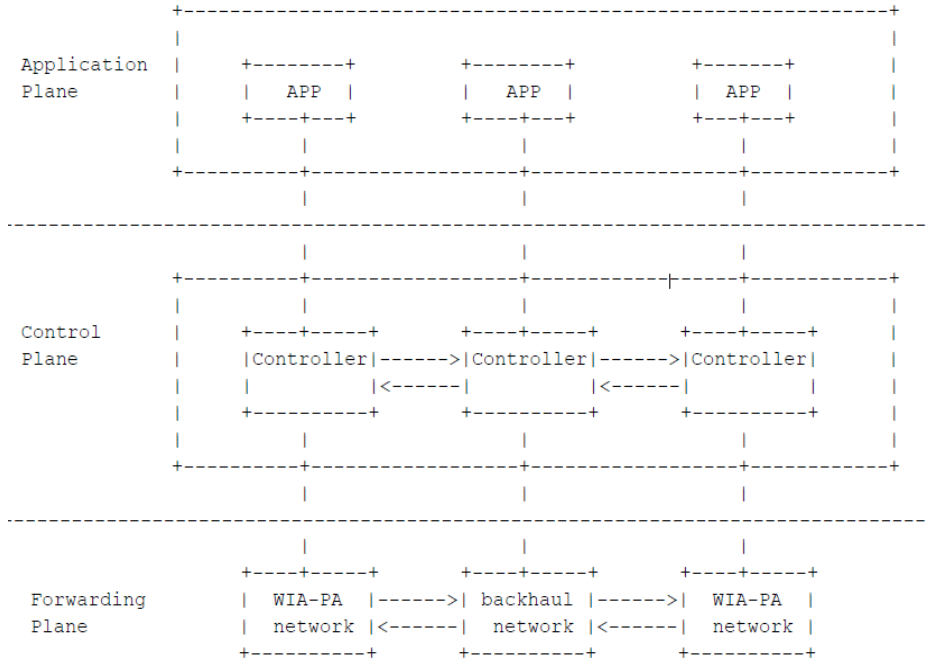


Joint Scheduling Architecture

- Control Plane
  - There are many network controllers in the network, which together constitute the control plane for the whole industrial network.
- No uniform standard
  - There is not a unified standard of joint architecture of multiple controllers in the industry at present.
- The main frameworks
  - Distributed architecture.
  - Centralized architecture.

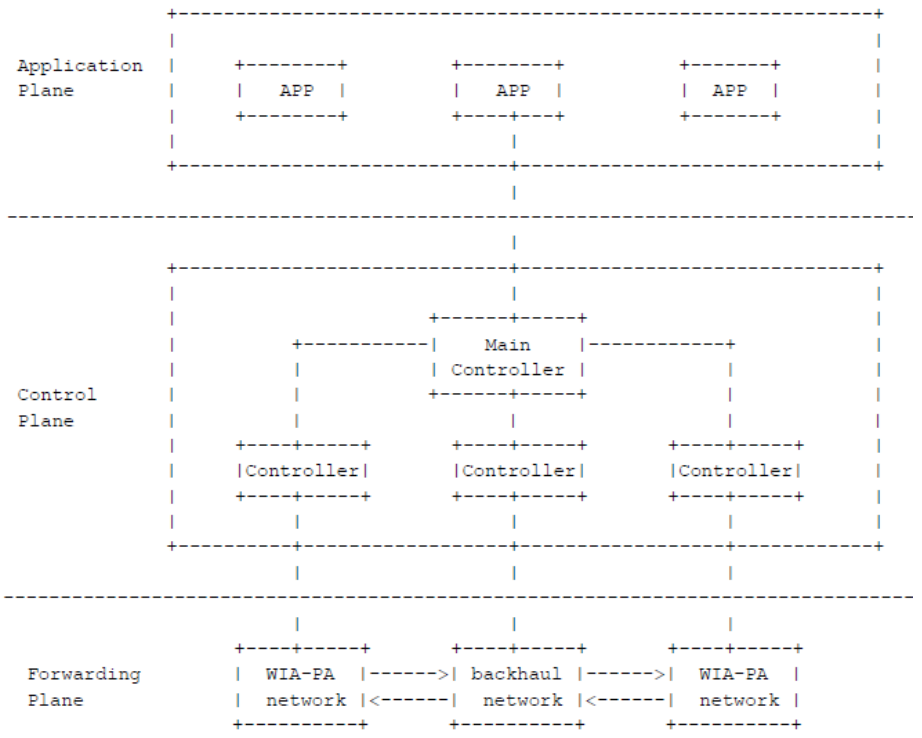
Joint Scheduling Architecture

- Distributed Architecture
  - East-West architecture.
  - The status of all network controller is equal.
- Disadvantages
  - Need to extend the east-west interface;
  - Maintain a global network topology in each controller.



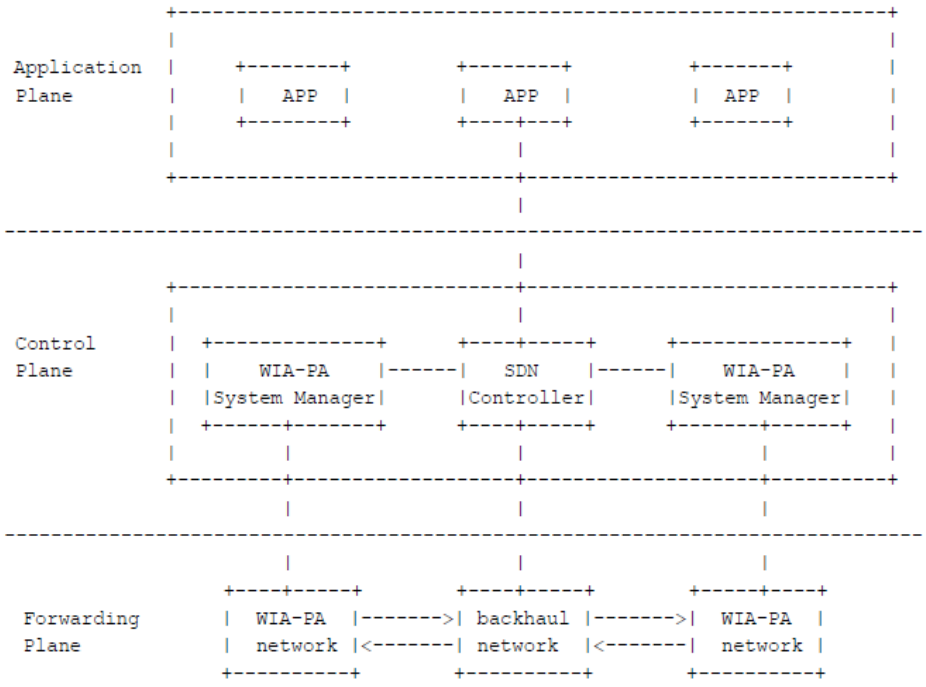
Joint Scheduling Architecture

- Centralized Architecture
  - Vertical multi-level architecture;
  - One is the basic control plane composed of a variety of network controllers;
  - Another part is a network controller composed of the main controller.
- Disadvantages
  - The scale of the network is not very large;
  - A single SDN controller is sufficient to meet the control demands of industrial backhaul network.



Joint Scheduling Architecture

- Control plane
  - WIA-PA System Manager, SDN controller.
  - Joint scheduler is integrated into the SDN controller in the form of plugin.
  - Establishing a connection with the SDN controller.
  - Directly calling the corresponding module of SDN controller.
- Joint Scheduling Architecture
  - Deterministic networks and deterministic Ethernet-based networks are jointly scheduling.
  - Control and scheduling for the entire industrial network by joint scheduler, so as to provide a real-time protection for each data stream.



Joint Scheduling Architecture

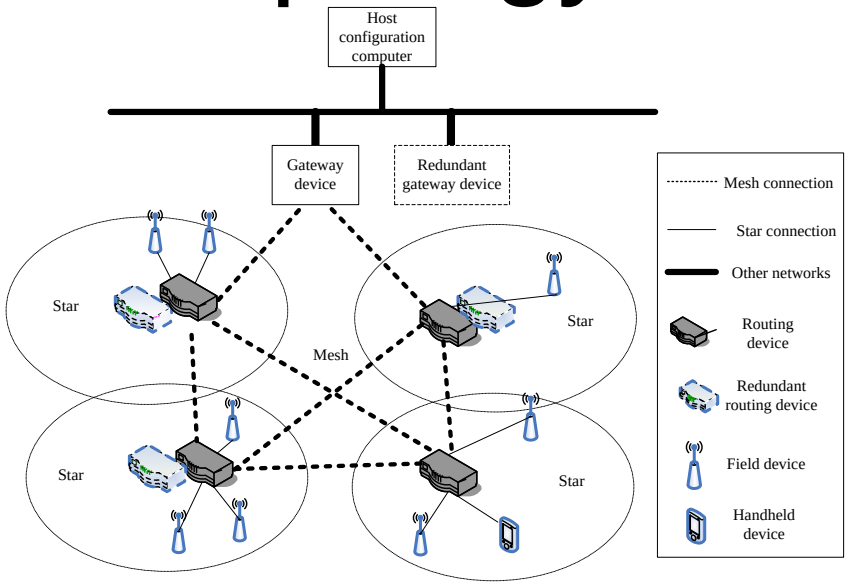
- Joint Scheduling Scheme
  - Firstly, adding scheduling scheme based on SDN in industry backhaul network.
  - Secondly, conducting an optimization for original WIA-PA scheduling scheme enables scheduling scheme based on WIA-PA networks plays together joint scheduler, and scheduling scheme can simultaneously apply to two non-adjacent domains.
  - Thirdly, due to the specificity of cross-border transmission services, the joint scheduling scheme for WIA-PA network VCR_ID and Route ID is reclassified.
  - Finally, In order to identify the field device on different network domains and domain, the network identifier (PAN_ID) is applied to the joint scheduling scheme to identify WIA-PA network.

Introduction for WIA-PA Networks

WIA-PA network topology

- A hierarchical network topology that combines star and mesh.

- WIA-PA specifies five types of devices:
  - Host configuration computer;
  - Gateway;
  - Routing device;
  - Field device;
  - Handheld device.

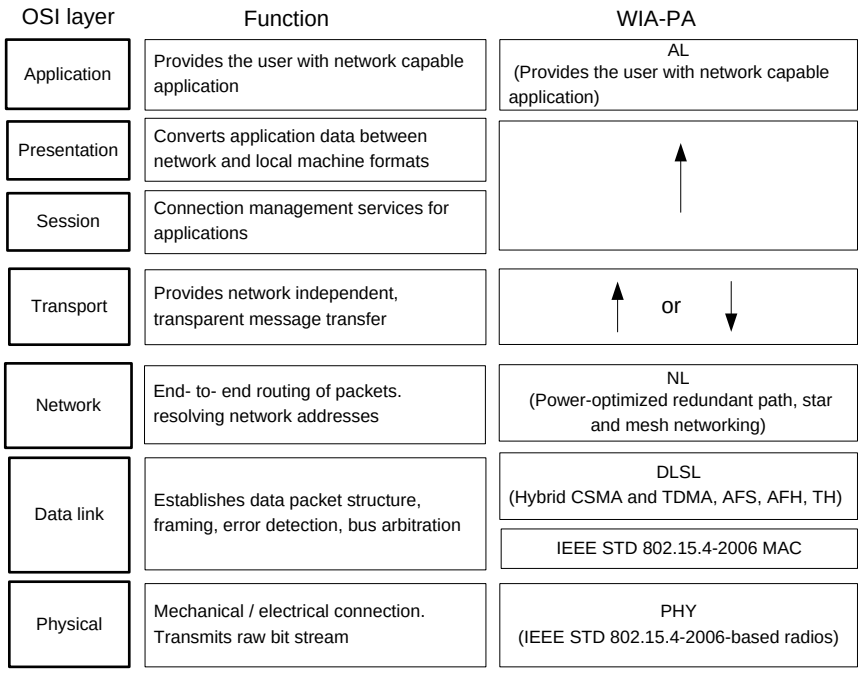


An example of WIA-PA physical topology

Protocol architecture

- The WIA-PA protocol architecture defines
  - Data Link Sub-Layer (DLSL);
  - Network Layer (NL);
  - Application Layer (AL);
  - Physical layer (PHY);
  - Medium Access Control sub-layer (MAC).

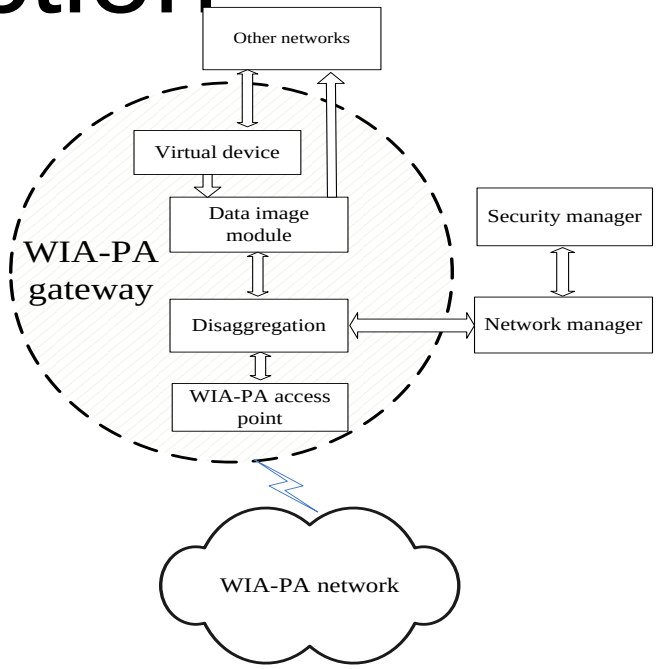
Its PHY and MAC are based on IEEE STD 802.15.4-2006.



OSI basic reference model mapped to WIA-PA

Interconnection

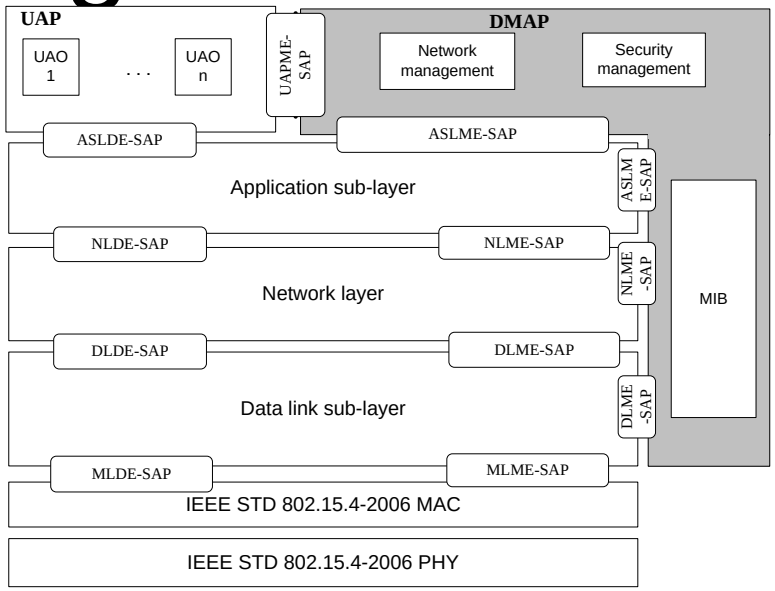
- The WIA-PA network interconnects with other networks through the WIA-PA gateway:
  - communication to the WIA-PA NM and SM;
  - exchange information between devices;
  - connect other networks.



The architecture of WIA-PA gateway

System management

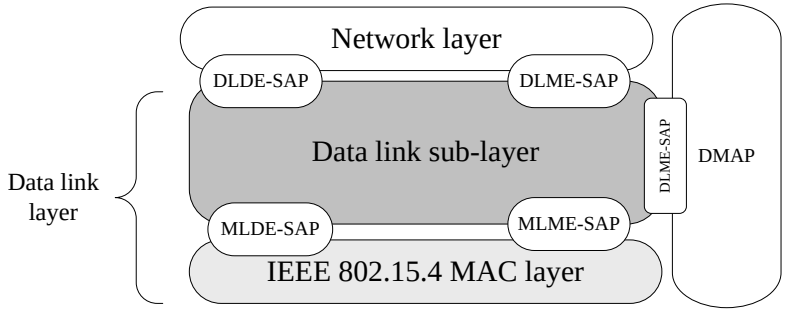
- Network management, security management.
- The network management functions include:
  - Joining and leaving the network;
  - Network address allocation;
  - Routing configuration;
  - Communication resource configuration;
  - …



DMAP in system management

Data link layer

- Guarantee communication.
- The DLL extends the IEEE STD 802.15.4-2006 superframe structure.
- Support certain key functions:
  - Frequency hopping;
  - Retransmission;
  - Time Division Multiple Access (TDMA);
  - Carrier Sense Multiple Access (CSMA).

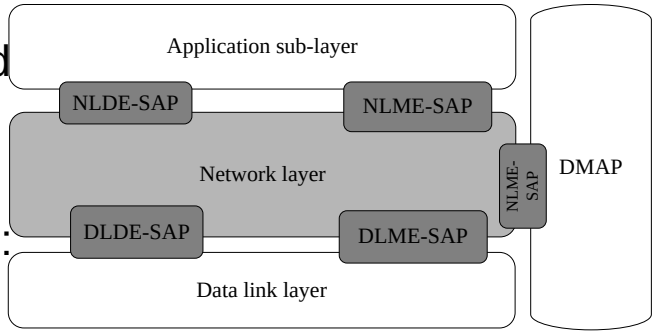


WIA-PA DLL protocol stack

- The WIA-PA DLL includes the following parts:
  - The IEEE STD 802.15.4-2006 MAC.
  - The DLSL.

Network layer

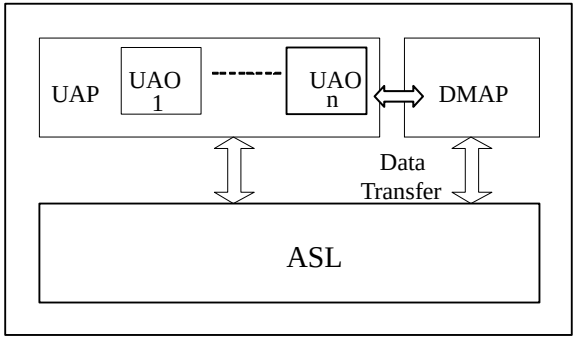
- The Network Layer Data Entity(NLDE) provides the service interface;
- The (Network Layer Management Entity)NLME provid the service interfaces.
- The NL is designed to perform the following functions:
  - Addressing,
  - Routing,
  - Communication resource allocation,
  - Packet lifecycle management,
  - Management for device joining and leaving network,
  - End-to-end network performance monitoring, and
  - Fragmentation and reassembly.



WIA-PA network layer protocol stack

Application Layer

- AL defines:
  - application objects,
  - communication services.
- UAP
  - collecting process data;
  - processing collected process data;
  - computing and generating output data ;
  - generating and reporting alarm;
  - ….
- ASL
  - provides end-to-end transparent data services for UAP, and it supports C/S, P/S, and R/S data transmissions.



AL structure

Aggregation and disaggregation

- Data aggregation
  - reduce the data communication frequency.
- Packet aggregation
  - reduce the number of packets from the routing device to the gateway;

- Disaggregation
  - implemented by gateway device,
  - notify the DGO in its DMAP to disaggregate the packets.
  - DMAP sends the disaggregated packets to UAOs.

Thanks!

Heng Wang, Ping Wang, Lun Shao
wangheng@cqupt.edu.cn, wangping@cqupt.edu.cn, yjssslcqupt@163.com
Chongqing University of Posts and Telecommunications, China

Chicago, March 28, 2017