acklio

Massive IoT
Preserve the Internet with SCHC

Laurent Toutain

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Confidential Property of Acklio

At-a-Glance

CISCO

Internet of Things

Connected Means Informed

According to Cisco, 500 billion devices are expected to be connected to the Internet by 2030. Each device includes sensors that collect data, interact with the environment, and communicate over a network. The Internet of Things (IoT) is the network of these connected devices. These smart, connected devices generate data that IoT applications use to aggregate, analyze, and deliver insight, which helps drive more informed decisions and actions.

The IoT is a critical part of business strategies going forward. Based on an IDC study of 2300 executives in 15 countries, 48 percent of those surveyed have already deployed IoT solutions, and 58 percent said that the IoT is strategic to their business strategy (Figure 1).

Costs to maintain IoT

In 2030

60 devices

240 devices

Costs to maintain IoT

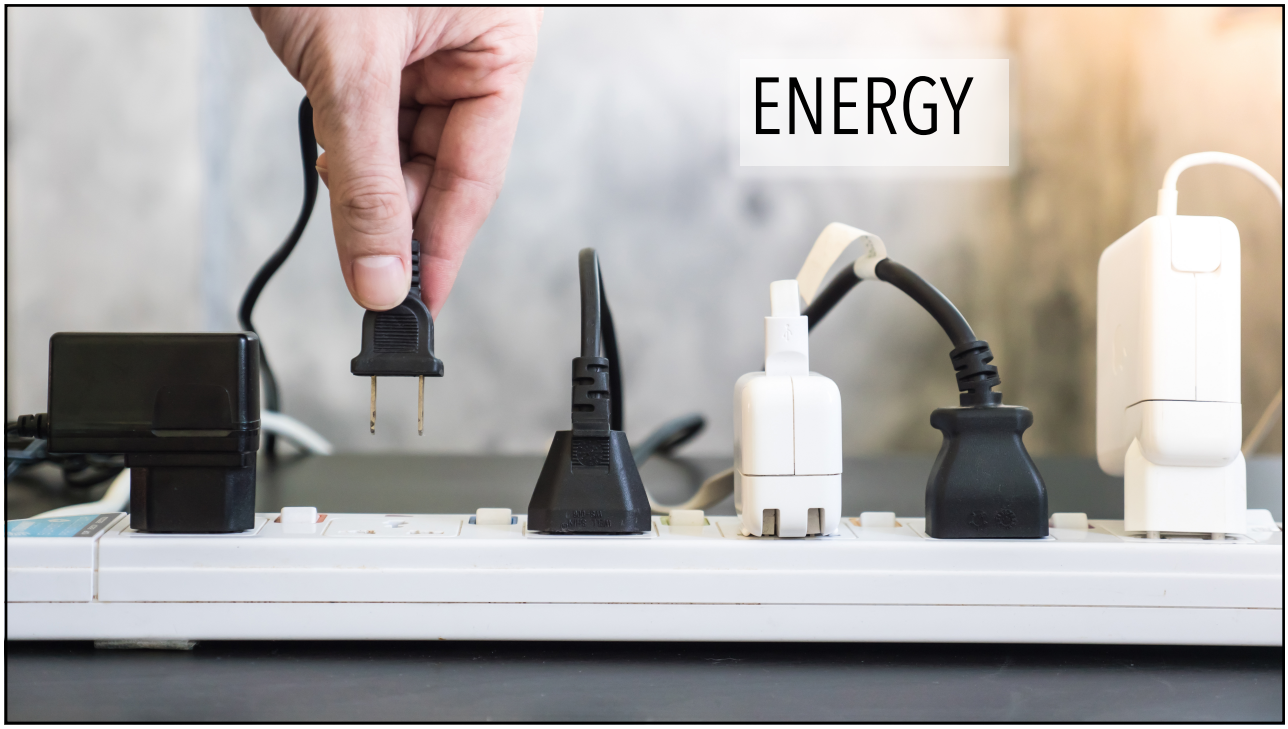
In 2030

60 devices

240 devices

4 hours

1 per day



LPWAN Capabilities (RFC 8376)

sigfox LoRaWAN

- Transmission power: 25 mW
- Battery lifetime: more than 10 years

- Throughput: 100 bit/s – 10 Kbit/s
- Frame size : 8 bytes to 200 bytes
- Range : 2 km urban – 30 km insight

- Unlicensed spectrum : 868 MHz (EU)
  - Duty cycle

Mainly uplink communications

3GPP A GLOBAL INITIATIVE LTE-M NB-IoT

- Transmission power: 100 mW
- Battery lifetime: more than 10 years

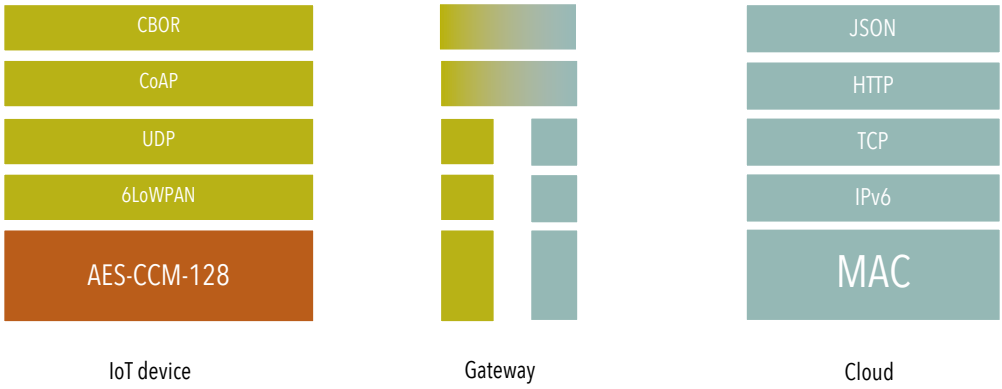
- Throughput: 200 bit/s – 10 Kbit/s
- Frame size : 1 600 Bytes
- Range : 2 km urban – 10 Km insight

- Licensed spectrum : around 700 MHz

Bi-directional communications

Image by Andreas Lechner from Pixabay

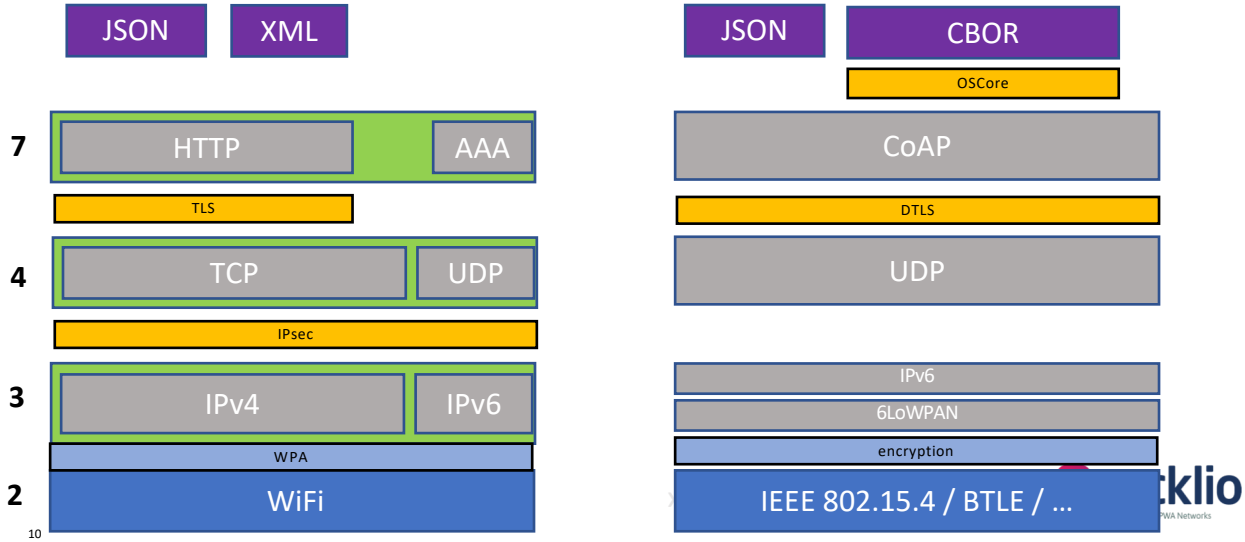
INTEROPERABILITY



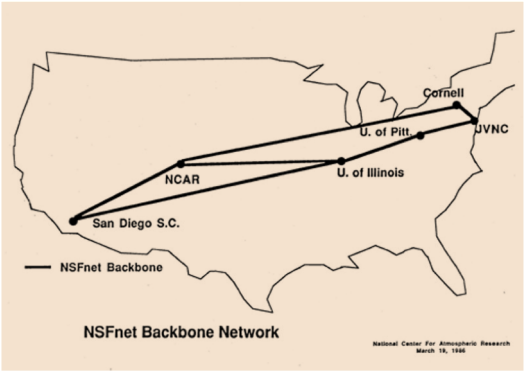
acklio
Unifying LPWA Networks

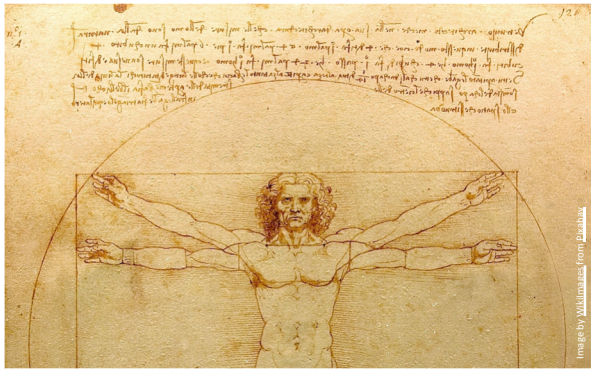
SECURITY

SECURITY


JSON
XML
JSON
CBOR
OSCore
7
HTTP
AAA
CoAP
TLS
DTLS
4
TCP
UDP
UDP
IPsec
3
IPv4
IPv6
IPv6
6LoWPAN
encryption
WPA
2
WiFi
IEEE 802.15.4 / BTLE / ...
10

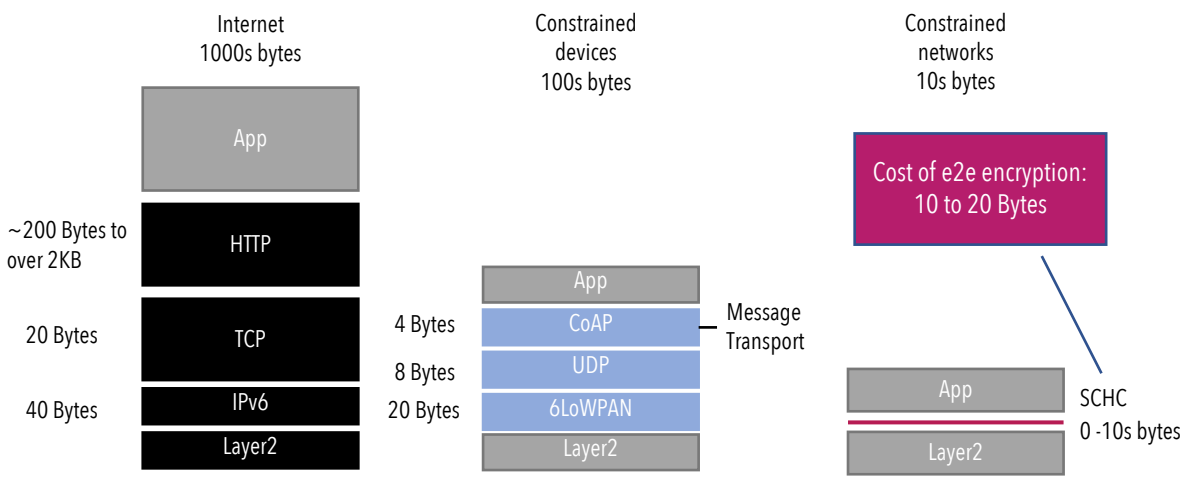
IP, Interoperability and Security generate too large messages for LPWAN.



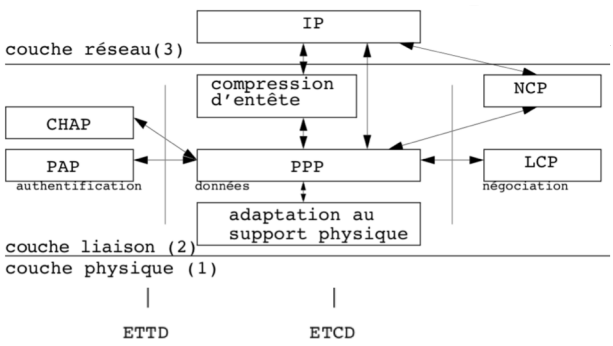


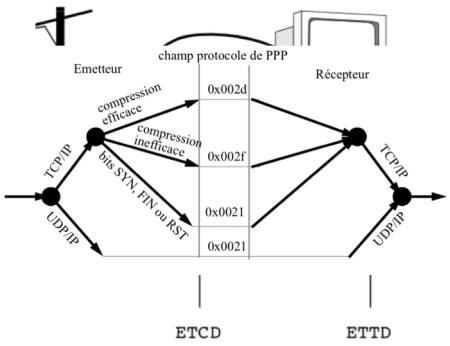
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

For constrained networks

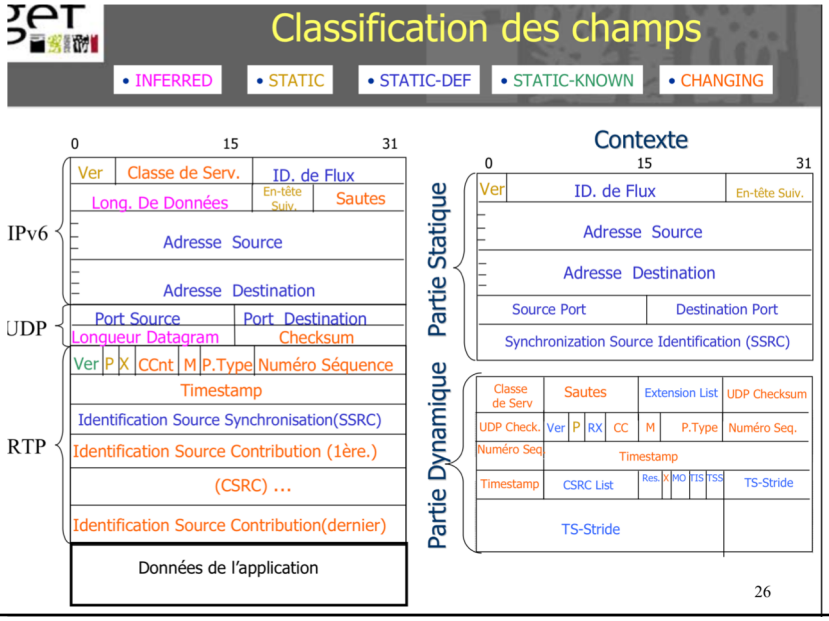


Compression mechanisms – VAN Jacobson

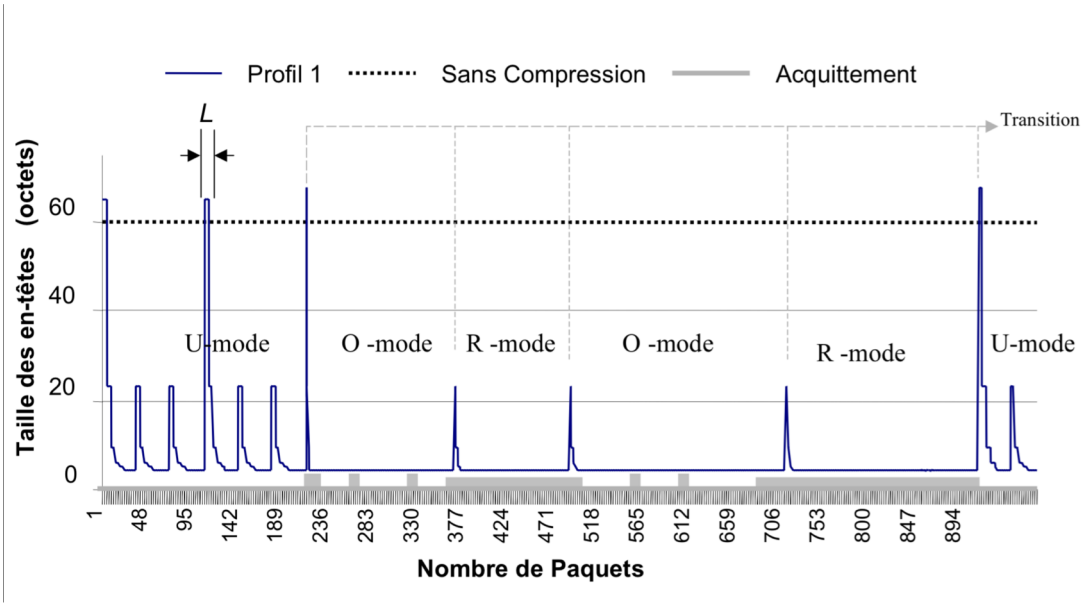




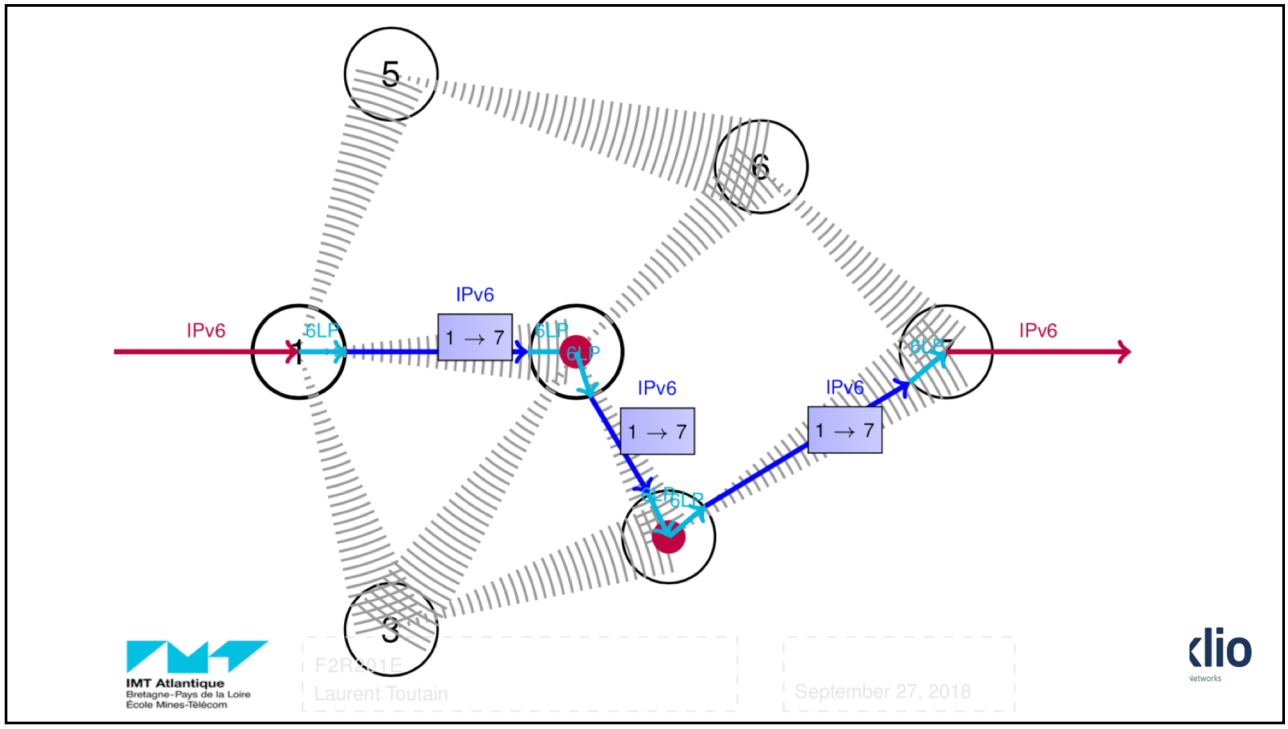
Compression mechanisms – ROHC

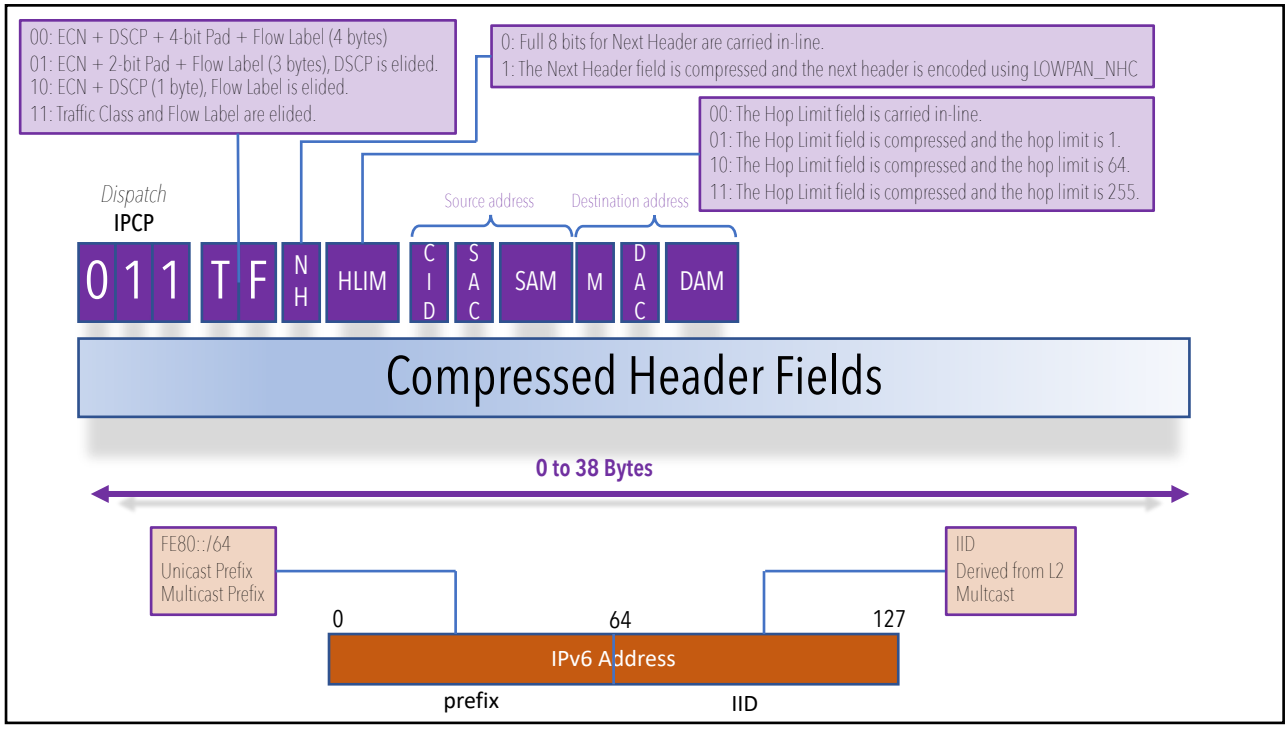


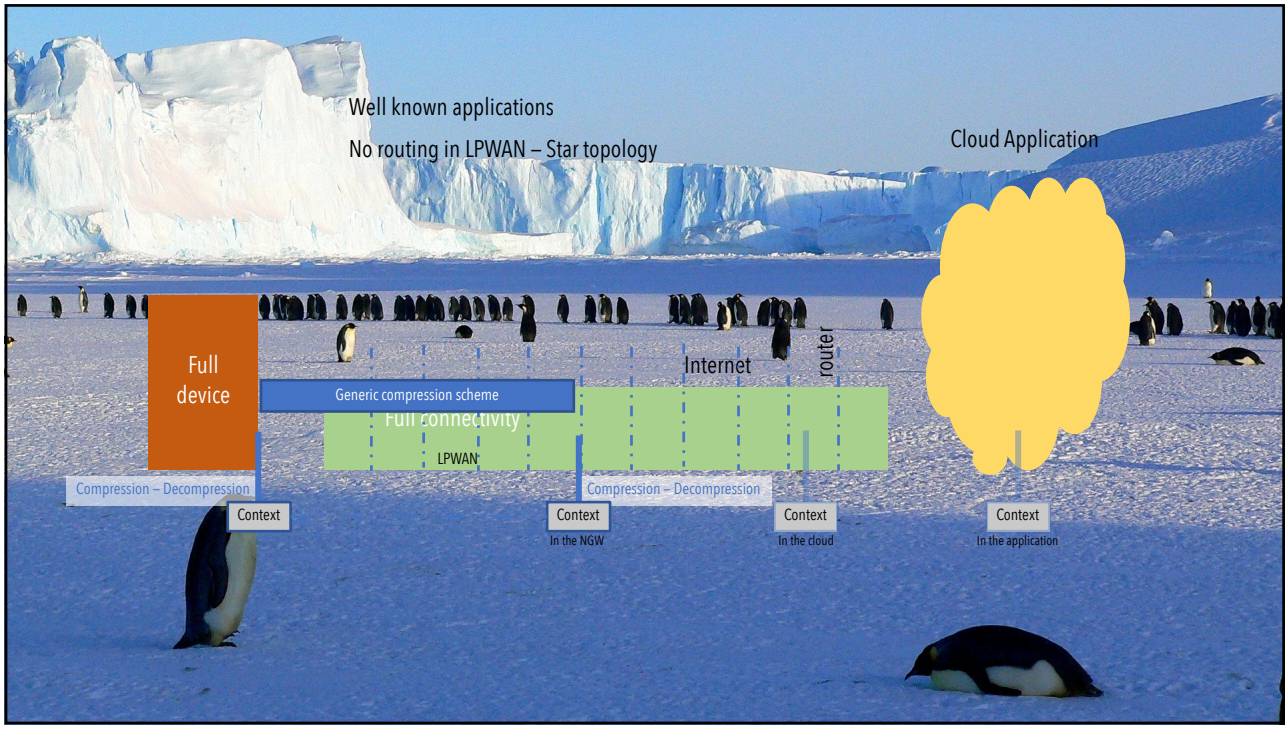
ROHC

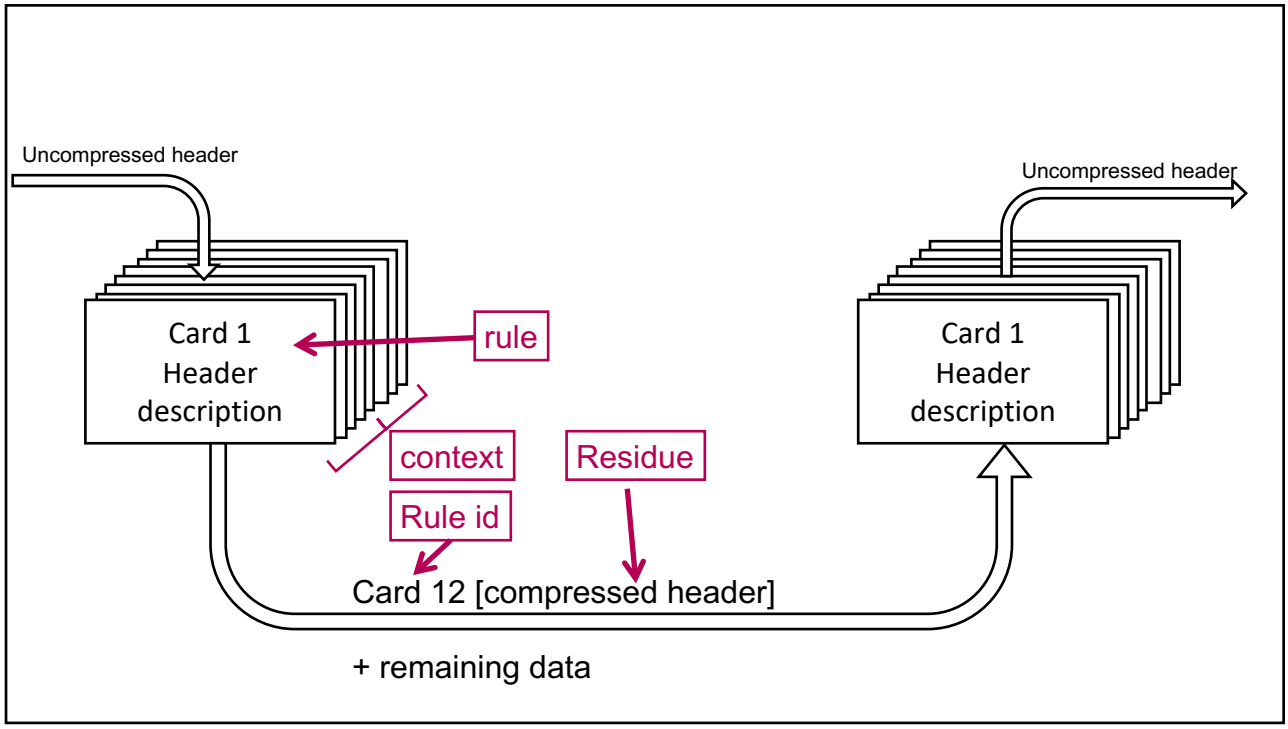


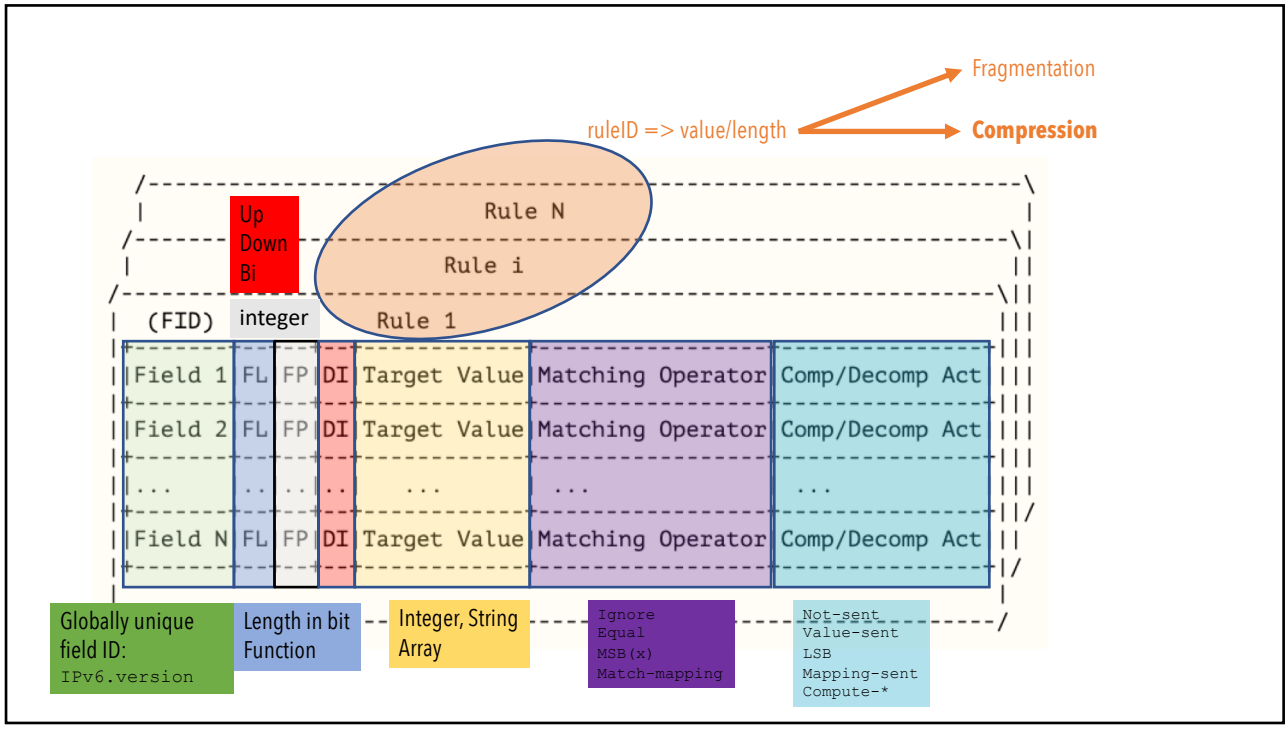
Couvreur, A., Ny, LM.L., Minaburo, A. et al. Telecommun Syst (2006) 31: 85. https://doi.org/10.1007/s11235-006-5524-z


5
6
3
IPv6
6LP
1 → 7
IPv6
IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom
Laurent Toutain
September 27, 2018
clio


00: ECN + DSCP + 4-bit Pad + Flow Label (4 bytes)
01: ECN + 2-bit Pad + Flow Label (3 bytes), DSCP is elided.
10: ECN + DSCP (1 byte), Flow Label is elided.
11: Traffic Class and Flow Label are elided.
0: Full 8 bits for Next Header are carried in-line.
1: The Next Header field is compressed and the next header is encoded using LOWPAN_NHC
00: The Hop Limit field is carried in-line.
01: The Hop Limit field is compressed and the hop limit is 1.
10: The Hop Limit field is compressed and the hop limit is 64.
11: The Hop Limit field is compressed and the hop limit is 255.
Dispatch
IPCP
Source address
Destination address
0 1 1 T F NH HLIM CID SAC SAM M DAC DAM
Compressed Header Fields
0 to 38 Bytes
FE80::/64
Unicast Prefix
Multicast Prefix
IID
Derived from L2
Multcast
0
64
127
IPv6 Address
prefix
IID


Well known applications
No routing in LPWAN – Star topology
Cloud Application
Full device
Generic compression scheme
Full connectivity
LPWAN
Internet
router
Compression – Decompression
Context
Context
In the NGW
Compression – Decompression
Context
In the cloud
Context
In the application


Uncompressed header
Card 1
Header
description
rule
context
Rule id
Residue
Card 12 [compressed header]
+ remaining data
Uncompressed header
Card 1
Header
description

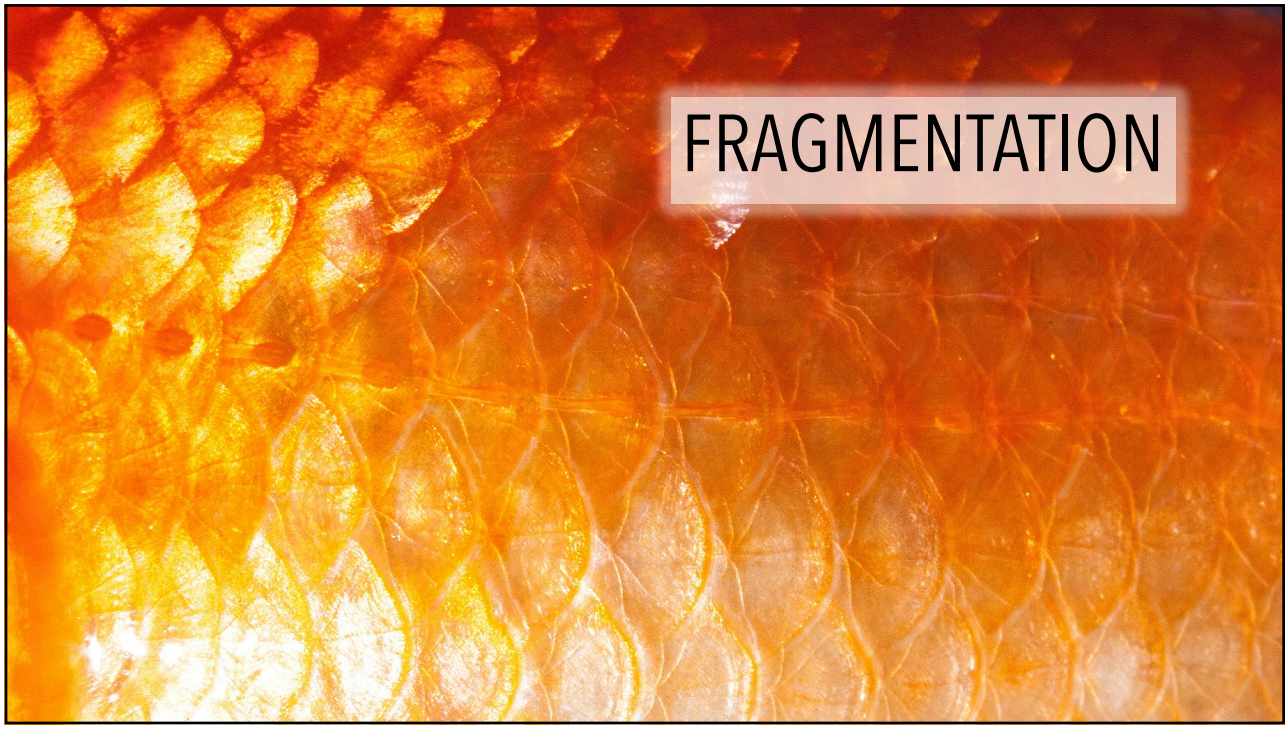


IPv6 | UDP | CoAP | Data

V DS. FL Len. NH HL Source Address Destination Address S port. D Port. Len. Chk Sum T tlk C Mid Tk Options

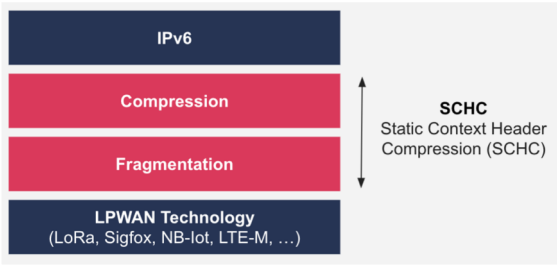
```
60031299003011 1e2001066073013728 10bb6cc6ca9ff7f3 2001042011010001000000000000185 d509 1633 0030 8612 4102 000e 17b36d7372 03746d70 06414243443d3d 46696e73696465ff 831903f41a00029e62191898
60043608001511 1e2001066073013728 10bb6cc6ca9ff7f3 2001042011010001000000000002365723 d509 1633 0015 71f3 4102 000f 18b5414c455254 ff f5
```

RULE 12	FL	Pos	Dir	Target Value	Matching Operator	CDA	Frame 1	Frame 2
IPv6.version	4	1	bi	6	Equal	Not-sent	--	--
IPv6.DiffServ	8	1	bi	00	Equal	Not-sent	--	--
IPv6.Flow Label	20	1	bi	00000	Equal	Not-sent	--	--
IPv6.Length	16	1	bi		Ignore	Compute-length	--	--
IPv6.Next Header	8	1	bi	11	Equal	Not-sent	--	--
IPv6.Hop Limit	8	1	up	30	Equal	Not-sent	--	--
IPv6.Hop Limit	8	1	dw	1	Ignore	Not-sent	--	--
IPv6.Dev Prefix	64	1	bi	0x200106607301372 8	Equal	Not-sent	--	--
IPv6.Dev IID	64	1	bi	0x10bb6cc6ca9ff7f3	Equal	Not-sent	--	--
IPv6.App Prefix	64	1	bi	0x200104201101000 1	Equal	Not-sent	--	--
IPv6.App IID	64	1	bi	[0x185, 0x2365723]	Match-mapping	Mapping-sent	0b0	0b1
UDP.Dev Port	16	1	bi	0xd509	Equal	Not-sent	--	--
UDP.App Port	16	1	bi	0x1633	Equal	Not-sent	--	--
UDP.Length	16	1	bi		Ignore	Compute-length	--	--
UDP.Checksum	16	1	bi		Ignore	Compute-checksum	--	--
CoAP.version	2	1	bi	1	Equal	Not-sent	--	--
CoAP.Type	2	1	up	1 (NON)	Equal	Not-sent	--	--
CoAP.TKL	4	1	bi	0x00	MSB(7)	LSB	0b1	0b1
CoAP.Code	8	1	Up	2 (POST)	Equal	Not-sent	--	--
CoAP.MID	16	1	Bi	0x0000	MSB(12)	LSB	0xe	0xf
CoAP.Token	Tkl	1	Bi		Ignore	Value-sent	0x17	0x18
CoAP.Uri-path	Var	1	Up	["msr", "ALERT"]	Match-mapping	Mapping-sent	0b0	0b1
CoAP.Uri-path	Var	2	Up	[None, "tmp"]	Match-mapping	Mapping-sent	0b1	0b0
CoAP.Uri-path	Var	3	Up		Ignore	Value-sent	0b0110"inside"	0b0000
CoAP.end option	8	1	Up	0xFF	Equal	Not-sent	--	--
							68 bits	20 bits



SCHC

Static Context Header Compression *[chic]



IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Image by skeeze from Pixabay

Why fragmentation?

- **If compression is not enough:**
  - Large payload
  - Very limited frame size
- **Necessary for key exchanges:**
  - Based on random values
- **New services:**
  - Logs vs events
  - Optimize transmissions and privacy
- **Firmware updates**
- …

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Image by skeeze from Pixabay

Efficient fragmentation for LPWAN Networks

- **Small overhead**
  - Use Rule ID
  - Different fragmentation parameters: error rate, packet size,...
- **Padding management**
  - Max Overhead : 7 bits
- **Traffic asymmetry**
  - Ack and retransmission are optimized
- **Simple implementation**
  - Few synchronization during the exchange
- **MTU change**

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Image by skeeze from Pixabay

3 fragmentation modes

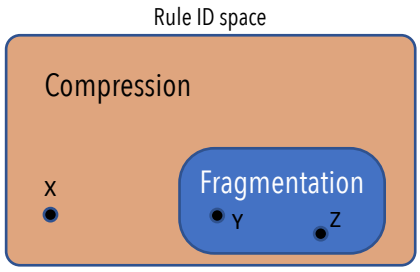
No Ack:
- Fragments are sent, last one contains a MIC to check fragment losses

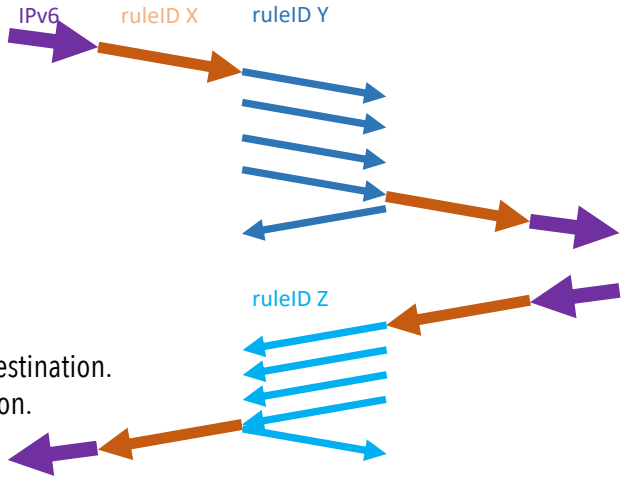
Ack-always:
- Packets are divided into windows
- Each window is acked

Ack-on-Error:
- Packets are divided into windows and tiles
- Last packet is acked
- Extra ack are sent only if some fragments are lost

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Image by skeeze from Pixabay

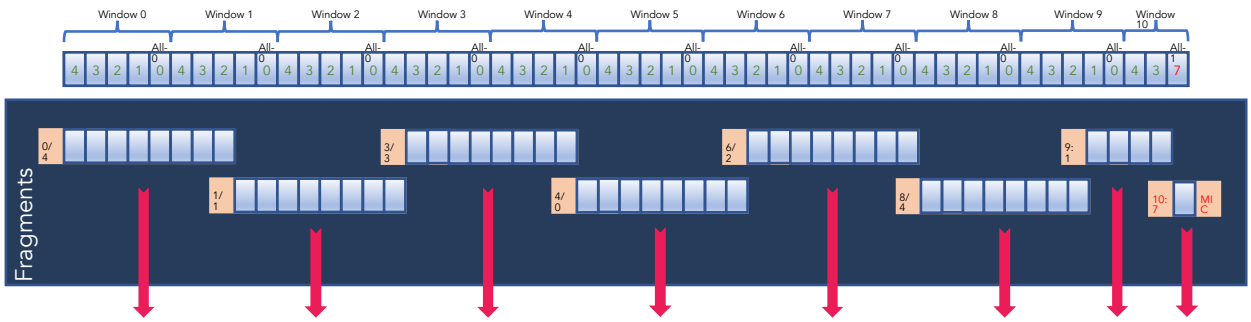




Compression rules are bi-directional:
- Use dev and App address, not source and destination.
- Up and down attribute to assign to a direction.

Fragmentation rules are unidirectional:
- Other direction may be used for ack.

acklio
Unifying LPWA Networks



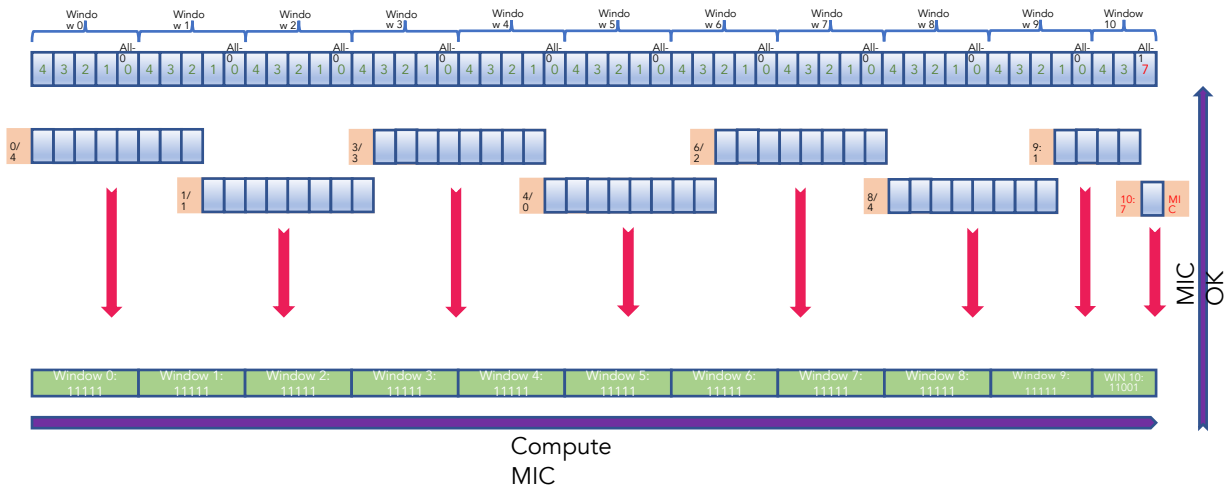
1) Define a Tile size compatible with the smallest frame
   - Ex: 9 bytes for LoRaWAN in the US

2) Define a max tile number and number in decreasing order
   - All-0: End of window, All-1: End of Packet

3) Number windows

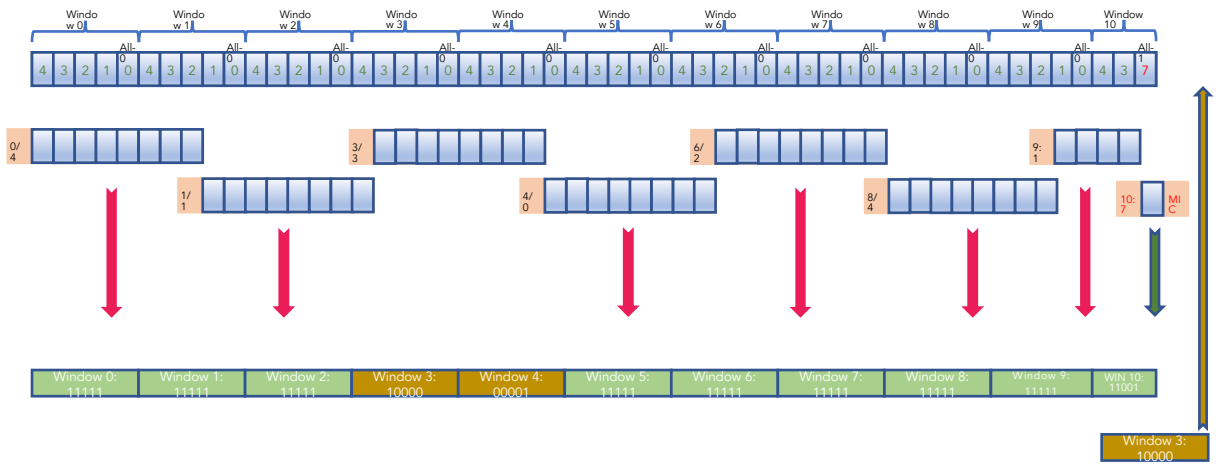
4) Send fragments with a integer number of tiles

Confidential Property of Acklio



4) Compute bitmap for each window
5) Receive All-1
6) Verify MIC
7) Send back MIC OK

Confidential Property of Acklio



4) Compute bitmap for each window
5) Receive All-1
6) Some fragments are missing
7) Send first non full window bitmap

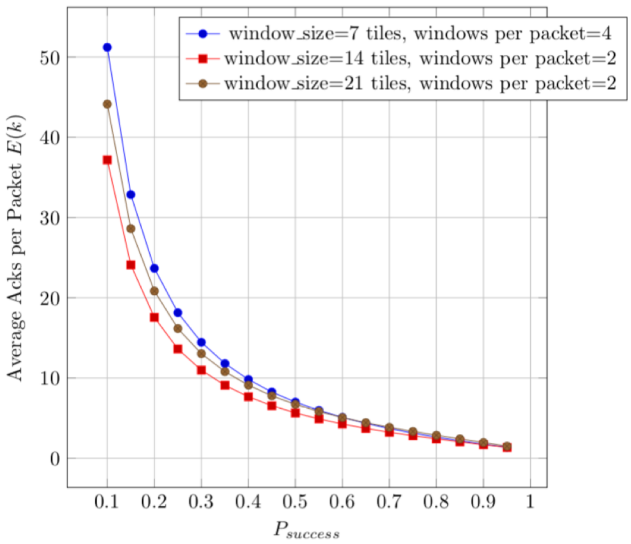
Confidential Property of Acklio

Performances

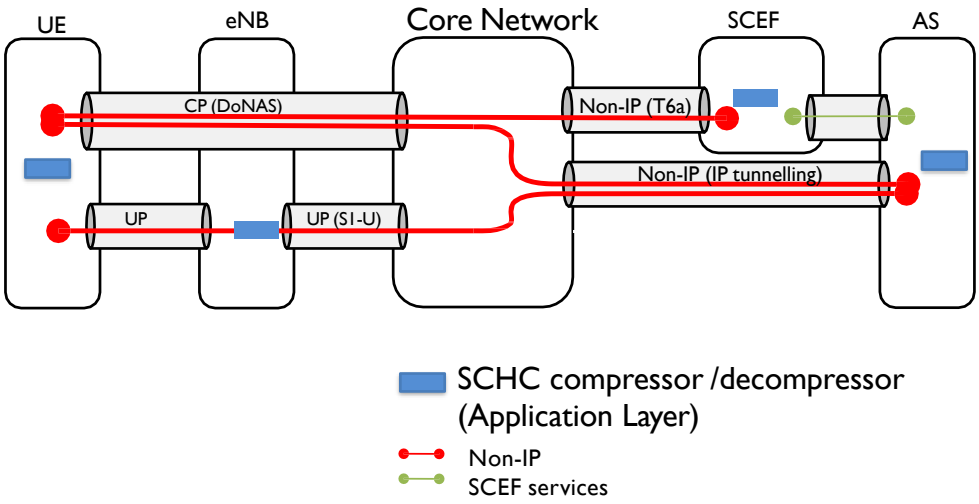
Average Acks per Packet vs. P success

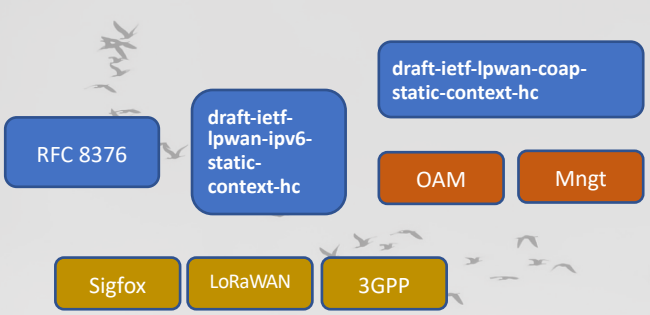
Fragment size = 200 bytes
Tile size = 49 bytes
Packet size = 1280 bytes

No error, just a small ack: MIC OK



SHCH as application layer packets





SCHC'N

https://github.com/openschc

SCHC integrates Billions on devices into the Internet for a better interoperability and security.