Secure and Autonomic Framework for SCHC Context Management in LoRaWAN-IPv6 Networks

Authors:

Maryam Hatami, Sandra Céspedes, J. William Atwood

IETF 121, Dublin, 02 Nov. 2024

Introduction

Starting point:

- LPWAN (LoRaWAN)
- IoT-specific communications
  - Small packet sizes
  - MAC-level addressing
  - Limited-scope security (manual keys)

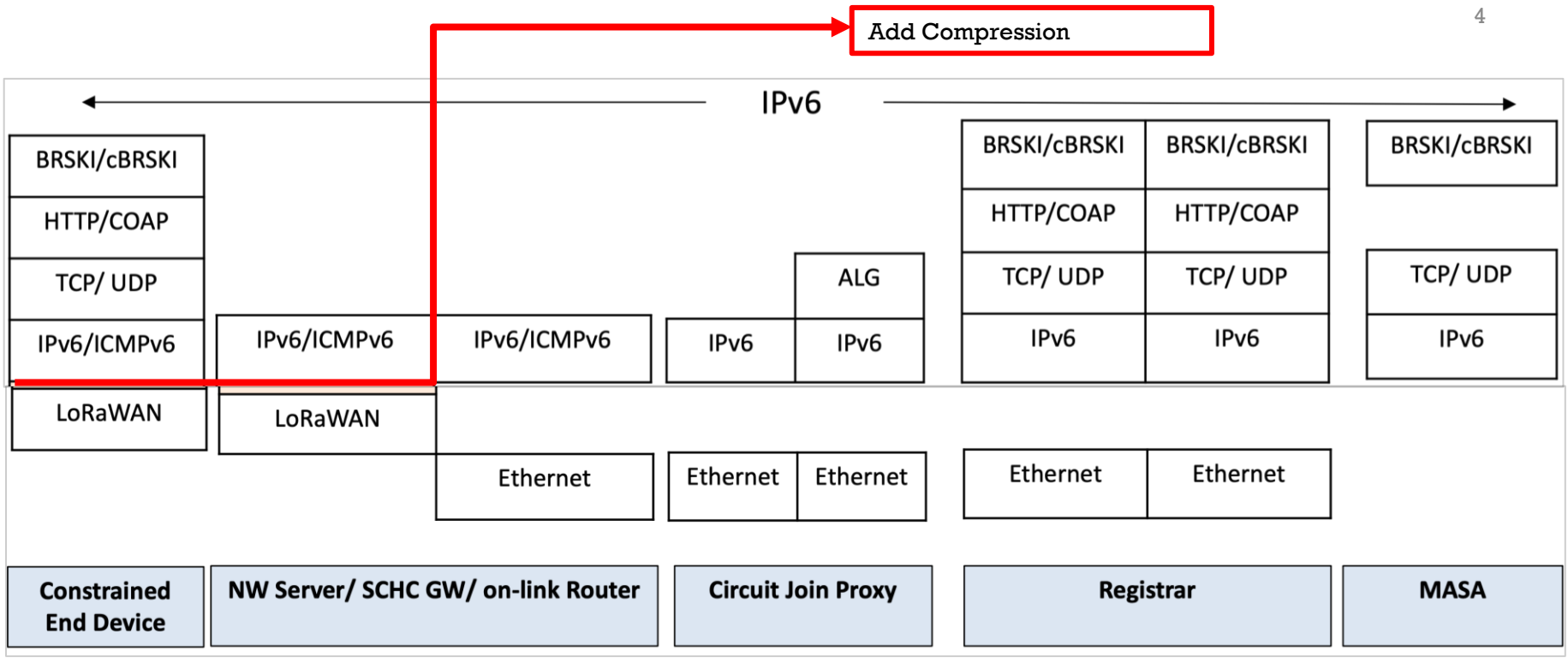
Ending point:

- IPv6-based autonomic network (ANIMA WG[1])
  - Large packets
  - Large addresses
  - Wide-scope security
  - Simple management

[1] https://datatracker.ietf.org/group/anima/about/

Introduction

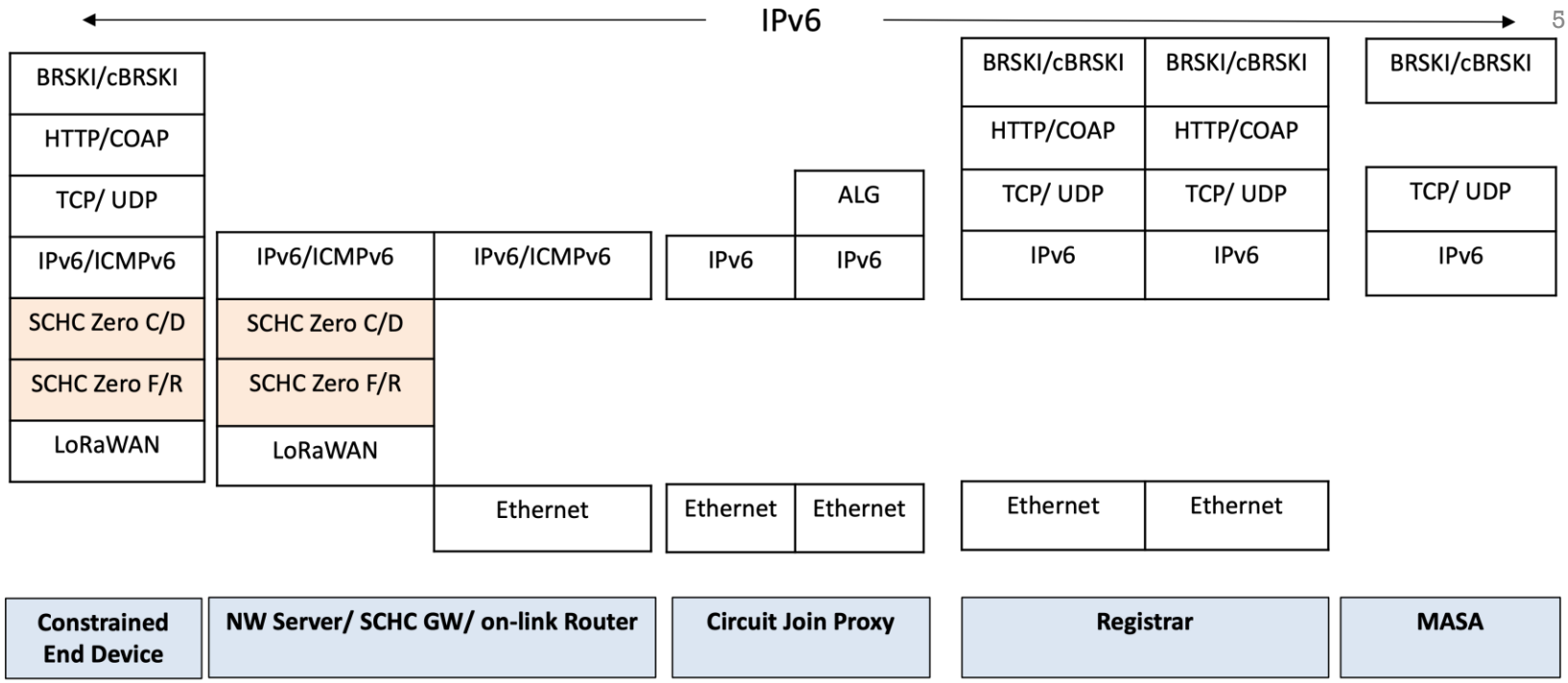
- Goal
  - Demonstrate that combining SCHC and ANIMA meets our goals and is feasible (does not take too long to set up)
- Approach
  - Assume an initial ruleset for SCHC (SCHC Zero)
  - Assume using ANIMA-required certificates
  - Calculate the time required for all the ANIMA onboarding message exchanges
  - MATLAB simulation



Architecture

https://datatracker.ietf.org/doc/rfc8995/

https://www.ietf.org/archive/id/draft-ietf-anima-constrained-voucher-24.html



Architecture

SCHC Zero Example Rules

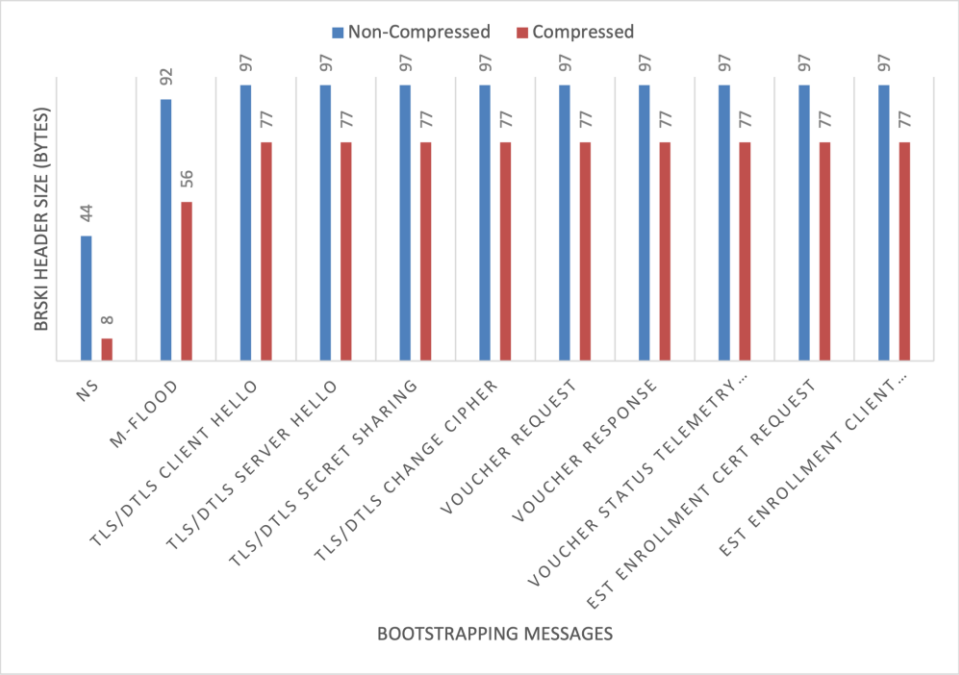
SCHC ZERO - IPV6 COMPRESSION

Field	Length (bits)	Target Value	MO	CDA
IPv6 version	4	6	equal	not sent
Traffic flow label	20	(e.g., 0x00000)	match map-ping	not sent
Next header	8	17 (UDP)	equal	not sent
Hop limit	8	1	equal	not sent
IPv6 App prefix	64	FE80::/64	equal	not sent
IPv6 DevIID	64	(derived from DevEUI 64)	ignore	DevIID
Destination address	128	-	ignore	sent

SCHC ZERO - UDP COMPRESSION

Field	Length (bits)	Target Value	MO	CDA
UDP dev port	16	-	equal	value sent
UDP app port	16	443 (DTLS)	equal	not sent
UDP length	16	-	ignore	compute-*
UDP checksum	16	-	ignore	compute-*

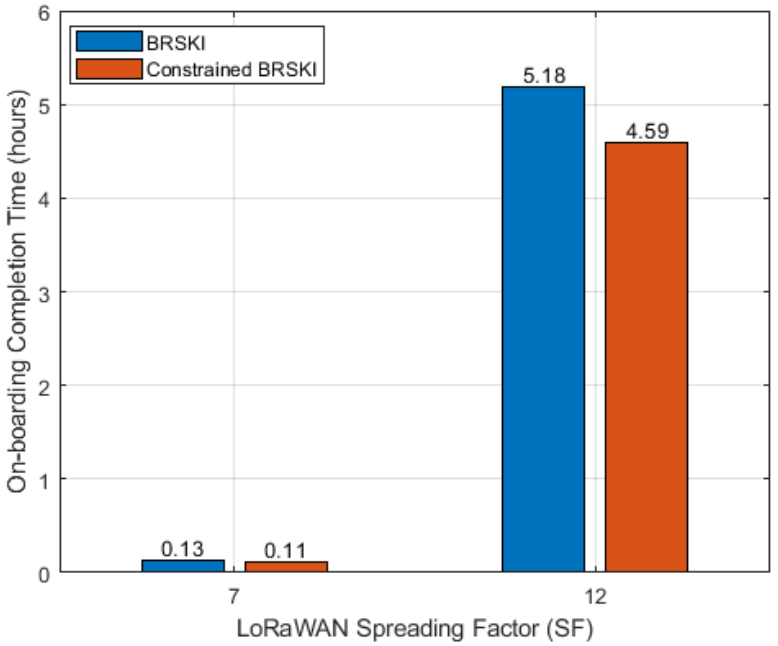
Results



Result

- Packet Header Compression on ANIMA On-boarding messages

Results



Result

- Onboarding time is feasible:
  - 0.11 - 0.13 hour for Spreading Factor 7 (best case)
  - 4.59 - 5.18 Hour for Spreading Factor 12 (worst case)

Conclusion

- IoT device is securely managed
- Now possible to update
  - SCHC rules
  - Basic software
  - Application software
  - While ensuring the identity of the device
- Now possible to attach a globally-routable IPv6 address, if necessary.

Next Steps

- Implement on a real testbed and simulate the network architecture
- Measure Energy efficiency
- Continue the work with SCHC Context Update

Questions and Comments?

Appendix

ANIMA
Exchanged Messages

BRSKI VS CBRSKI COMPRESSED PACKET SIZES

Packet Type	BRSKI Header (B)	cBRSKI Header (B)	BRSKI Payload (B)	cBRSKI Payload (B)
Neighbor Solicitation (NS)	8	8	20	20
M-Flood	56	34	53	53
TLS/DTLS client hello	77	37	186	186
TLS/DTLS server hello	77	37	70	70
TLS/DTLS secret sharing	77	37	3061	3061
TLS/DTLS change cipher	77	37	149	149
Voucher request	77	37	1576	978
Voucher response	77	37	1180	298
Voucher status telemetry	77	37	114	114
EST enrollment cert request	77	37	678	678
EST enrollment client cert	77	37	4246	4246

ANIMA
Exchanged Messages

Table 7.1: On-boarding messages that require SCHC Zero context

Message	Headers	Fields to be compressed by SCHC Zero
SLAAC	IPv6 header	IP Version, traffic flow label, Next Header, Hop limit, IPv6 app prefix, IPv6 DevIID, Destination address
	ICMPv6	ICMPv6 code , ICMPv6 type
M-Flood	IPv6 header	IP Version, traffic flow label, Next Header, Hop limit, IPv6 app prefix, IPv6 DevIID, Destination address
	UDP	UDP Dev Port, UDP App Port, UDP Length, UDP Checksum
TLS Handshake	IPv6 header	IP Version, traffic flow label, Next Header, Hop limit, IPv6 app prefix, IPv6 DevIID, Destination address
DTLS Handshake/Voucher/EST	IPv6 header	IP Version, traffic flow label, Next Header, Hop limit, IPv6 app prefix, IPv6 DevIID, Destination address
	UDP	UDP Dev Port, UDP App Port, UDP Length, UDP Checksum

ANIMA
Exchanged Messages

Table 7.2: SLAAC SCHC rules

Field	Length (bits)	Target Value	Matching Operator	CDA
IPv6 version	4	6	equal	not sent
Traffic flow lable	20	(e.g., 0x00000)	match mapping	mapping-sent
Next header	8	58 (ICMPv6)	equal	not sent
Hop limit	8	1	equal	not sent
IPv6 App prefix	64	FE80::/64	equal	not sent
IPv6 DevIID	64	(derived from DevEUI 64) calculate in AS	ignore	DevIID
Destination address	128	FF02::1:FF00:0000/104 (Solicited-node multicast address)	equal	not sent

Table 7.3: SLAAC next header SCHC rules

Field	Length (bits)	Target Value	Matching Operator	CDA
ICMPv6 type	8	135 (NS)	equal	not sent
ICMPv6 code	8	0	equal	not sent