UNIVERSITÉ Concordia UNIVERSITY

GINA CODY SCHOOL OF ENGINEERING AND COMPUTER SCIENCE

# A Framework for Secure Autonomic IoT Device Management in Constrained Networks

Maryam Hatami[1], Sandra Céspedes [1], & J. William Atwood[1]

[1] Concordia University, Montreal, QC, Canada
email: maryam.hatami@concordia.ca

# Outline

- Introduction
- Related Work
- Proposed Framework
- Discussion
- Future Work

# Introduction

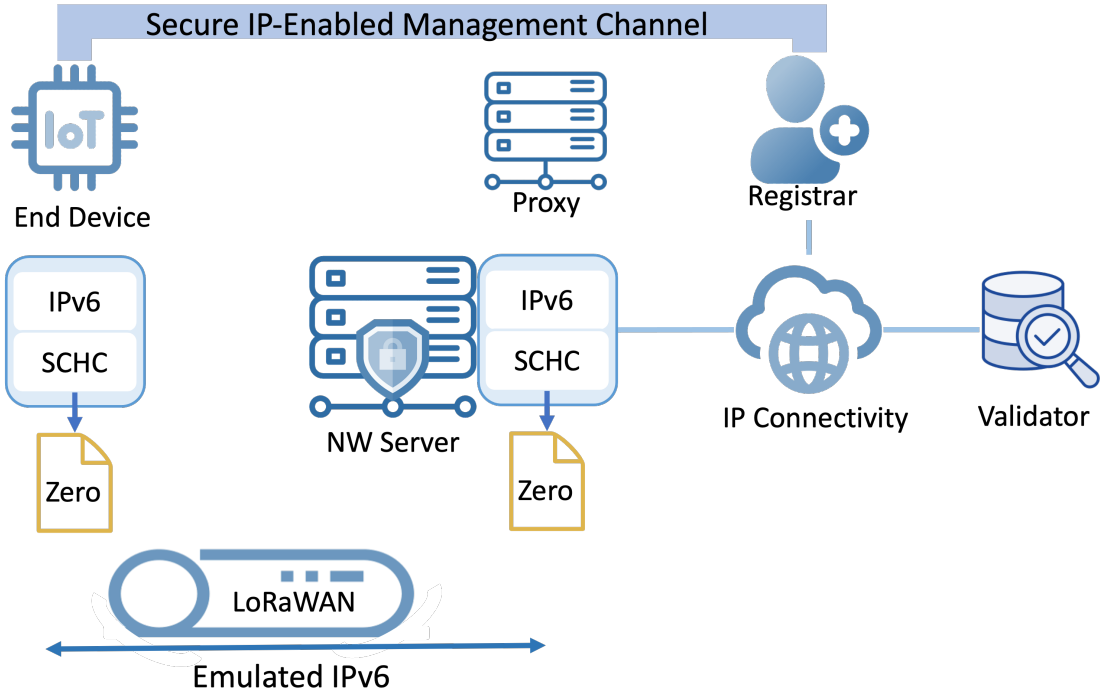
- **IoT growth demands scalable, secure onboarding**
- **Current solutions address either constrained or IP networks (not both)**
- **Our solution:** Bridge both worlds with **SCHC Zero + BRSKI**
- **LoRaWAN case study** shows feasibility
- **Goals:** Interoperability, minimal configuration, security

# Related Work

- **Autonomic Networking (ANIMA)**
  - Self-configuring, self-managing networks (RFC 8993, 8995)[1]
  - BRSKI enables zero-touch secure onboarding[2]
  - Establishes virtual out-of-band management plane (OAM)[2]
- **IoT Onboarding Solutions**
  - Existing approaches (LoRaWAN, CoAP, CBOR) limited to closed domains[3,]
  - Constrained BRSKI (cBRSKI) uses DTLS/CoAP but lacks compression [5,13]
  - Research gap: secure, scalable onboarding from constrained → IP networks

# Proposed Framework

- **Overview:**
  - Enables secure onboarding using SCHC rules + BRSKI
  - Uses pre-installed certs, no runtime config needed
- **SCHC Zero Context:**
  - Compresses SLAAC, M-Flood, UDP, TLS/DTLS from device startup
- **Protocol Flow:**
  - NS → M-Flood → TLS → Voucher → EST
  - Proxy relays messages to registrar
- **Transport:**
  - DTLS/UDP recommended over TCP due to LoRaWAN constraints



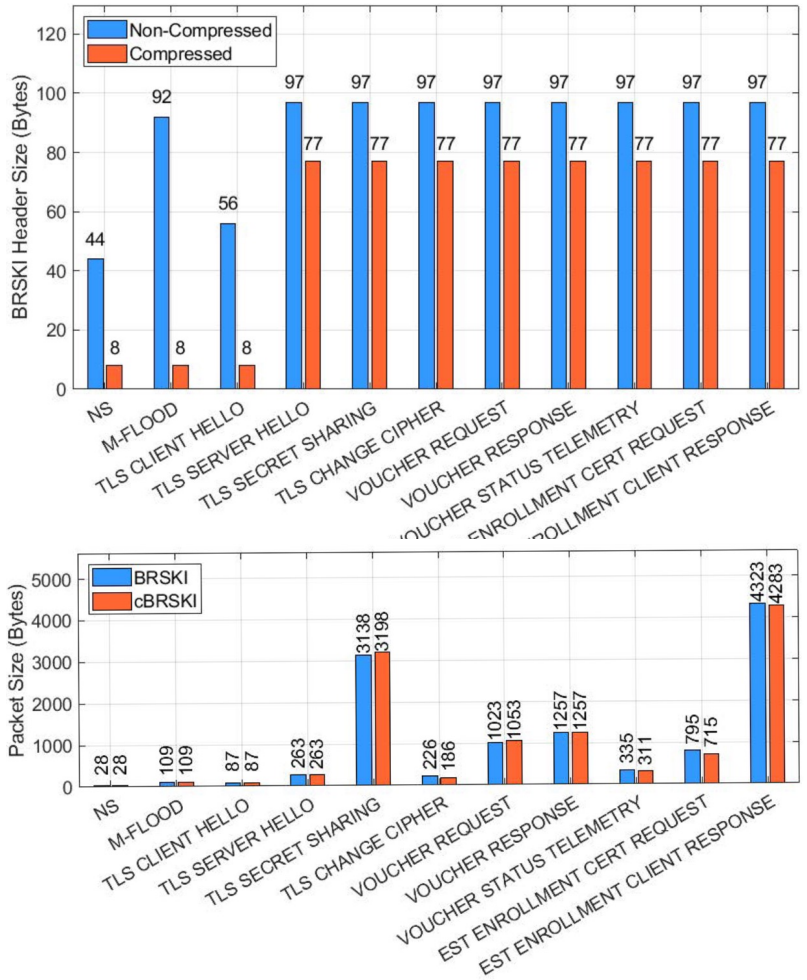
# Discussion - SCHC Zero: Predefined Context Fields

- **Messages & Fields Compressed:**
  - SLAAC: IPv6 & ICMPv6 headers
  - M-Flood: IPv6 & UDP headers
  - TLS / DTLS / EST: IPv6 & UDP headers
- Covers all BRSKI-related messages to support early device communication over LoRaWAN/IP.

| **Message** | **Header** | **Fields Compressed by *SCHC Zero*** |
|---|---|---|
| SLAAC | IPv6 | IP Version, Traffic Flow Label, Next Header, Hop Limit, IPv6 App Prefix, IPv6 DevIID, Destination Address |
| | ICMPv6 | ICMPv6 Code, ICMPv6 Type |
| M-Flood | IPv6 | 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 | IP Version, Traffic Flow Label, Next Header, Hop Limit, IPv6 App Prefix, IPv6 DevIID, Destination Address |
| DTLS Handshake / Voucher / EST | IPv6 | 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 |

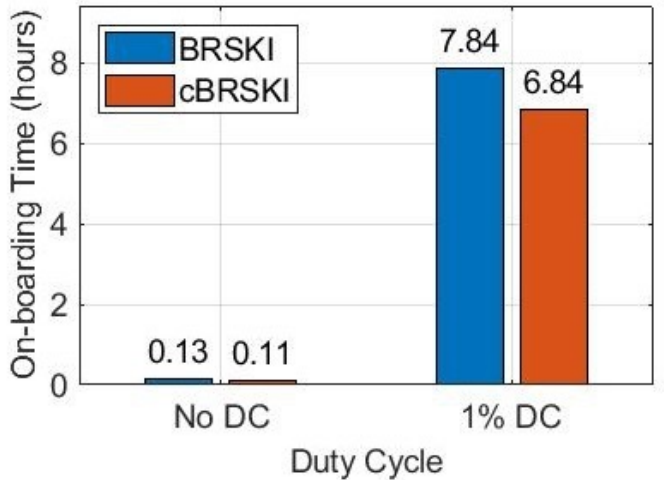
# Discussion - SCHC Zero Compression Gains

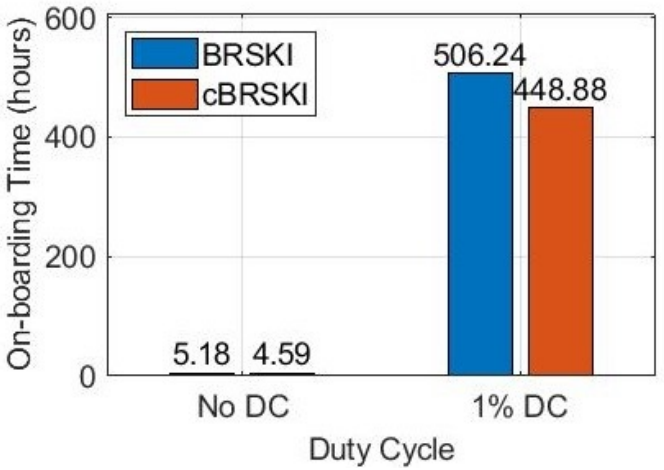
- **Header Size Savings (Top Chart):**
  - NS: 44B → 8B, M-Flood: 92B → 56B
    TLS/DTLS: 97B → 77B (up to 48% reduction)
- **Packet Size (Bottom Chart):**
  - cBRSKI is often smaller than BRSKI
    ex: EST Response: 4323B → 4283B



# Discussion - Onboarding Time Analysis

- **Best Case (SF7):**
  - No DC → BRSKI: 0.13h, cBRSKI: 0.11h
    1% DC → BRSKI: 7.84h, cBRSKI: 6.84h
- **Worst Case (SF12):**
  - No DC → BRSKI: 5.18h, cBRSKI: 4.59h
    1% DC → BRSKI: 506h, cBRSKI: 449h



# Future Work

- Implement framework on real LoRaWAN hardware
- Deeper security analysis and performance benchmarking
- Extend framework to other non-IP constrained networks (e.g., PPP, BLE)

# References

[1] IETF ANIMA Working Group. 2020. "**Autonomic Networking Integrated Model and Approach (ANIMA).**" Working Group Charter charter-ietf-anima-02. Internet Engineering Task Force. https://datatracker.ietf.org/wg/anima/about/ Active Working Group

[2] Max Pritikin, Michael Richardson, Toerless Eckert, Michael H. Behringer, and Kent Watsen. 2021. "**Bootstrapping Remote Secure Key Infrastructure (BRSKI).**" RFC 8995. doi:10.17487/RFC8995

[3] The Things Network. 2024. LoRaWAN Architecture. https://www.thethingsnetwork.org/docs/lorawan/architecture/ Accessed: 2025-04- 07.

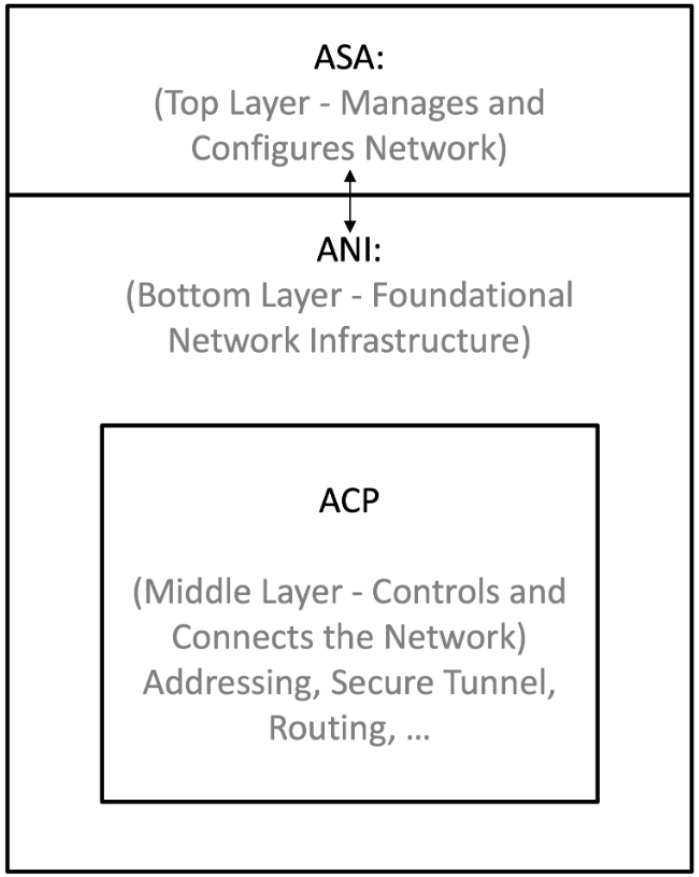
[4] Samira Afzal, Laisa CC De Biase, Geovane Fedrecheski, William T Pereira, and Marcelo K Zuffo. 2022. "**Analysis of Web-Based IoT through Heterogeneous Networks: Swarm Computing over LoRaWAN.**" Sensors 22, 2 (2022), 664.

[5] Michael Richardson, Peter Van der Stok, Panos Kampanakis, and Esko Dijk. 2024. "**Constrained Bootstrapping Remote Secure Key Infrastructure (cBRSKI).**" Internet-Draft draft-ietf-anima-constrained-voucher-25. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-anima-constrained-voucher/ Work in Progress.

[6] Eric Rescorla, Hannes Tschofenig, and Nagendra Modadugu. 2022. "**The Datagram Transport Layer Security (DTLS) Protocol**" Version 1.3. RFC 9147. doi:10.17487/RFC9147

# Thanks!

# Autonomic Node Architecture



# SCHC

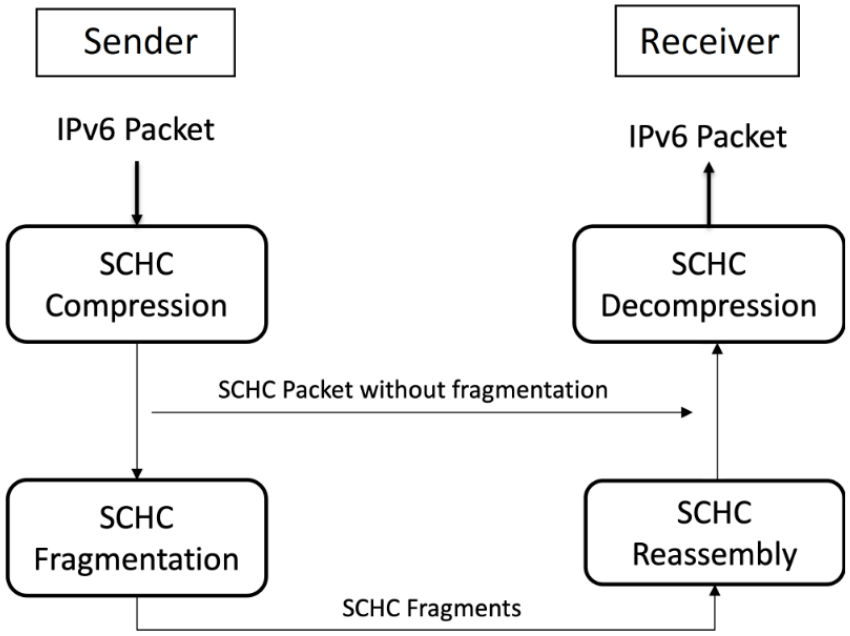



Figure 2.9: SCHC Stack Flow. Adapted from [2]

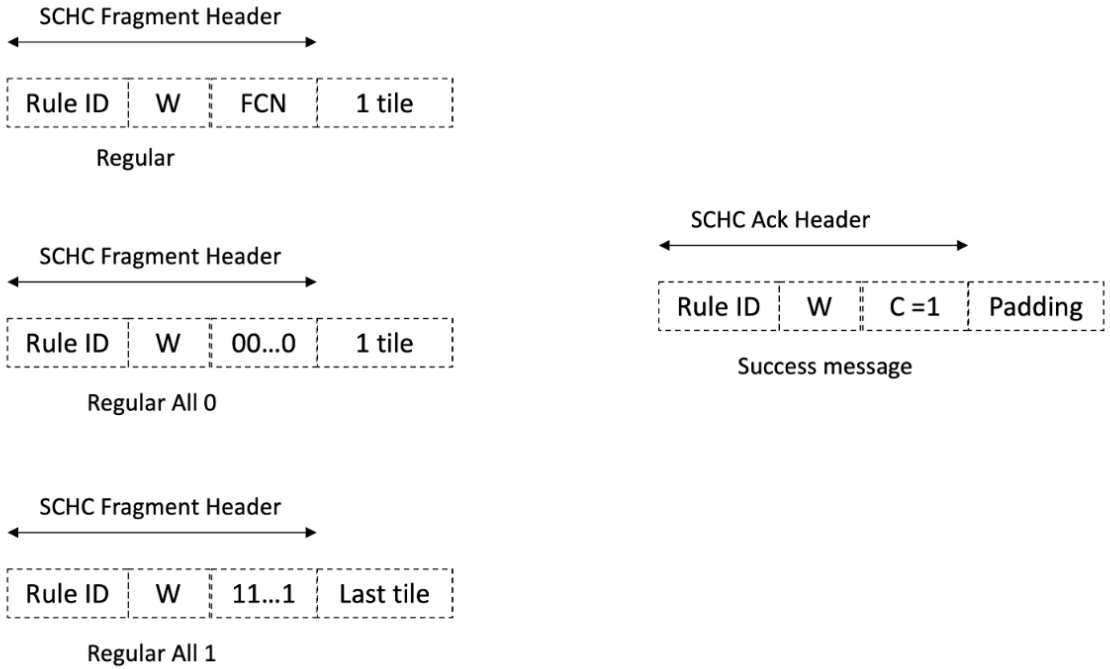



Figure 2.10: SCHC Fragment. Adapted from [2]

# BRSKI

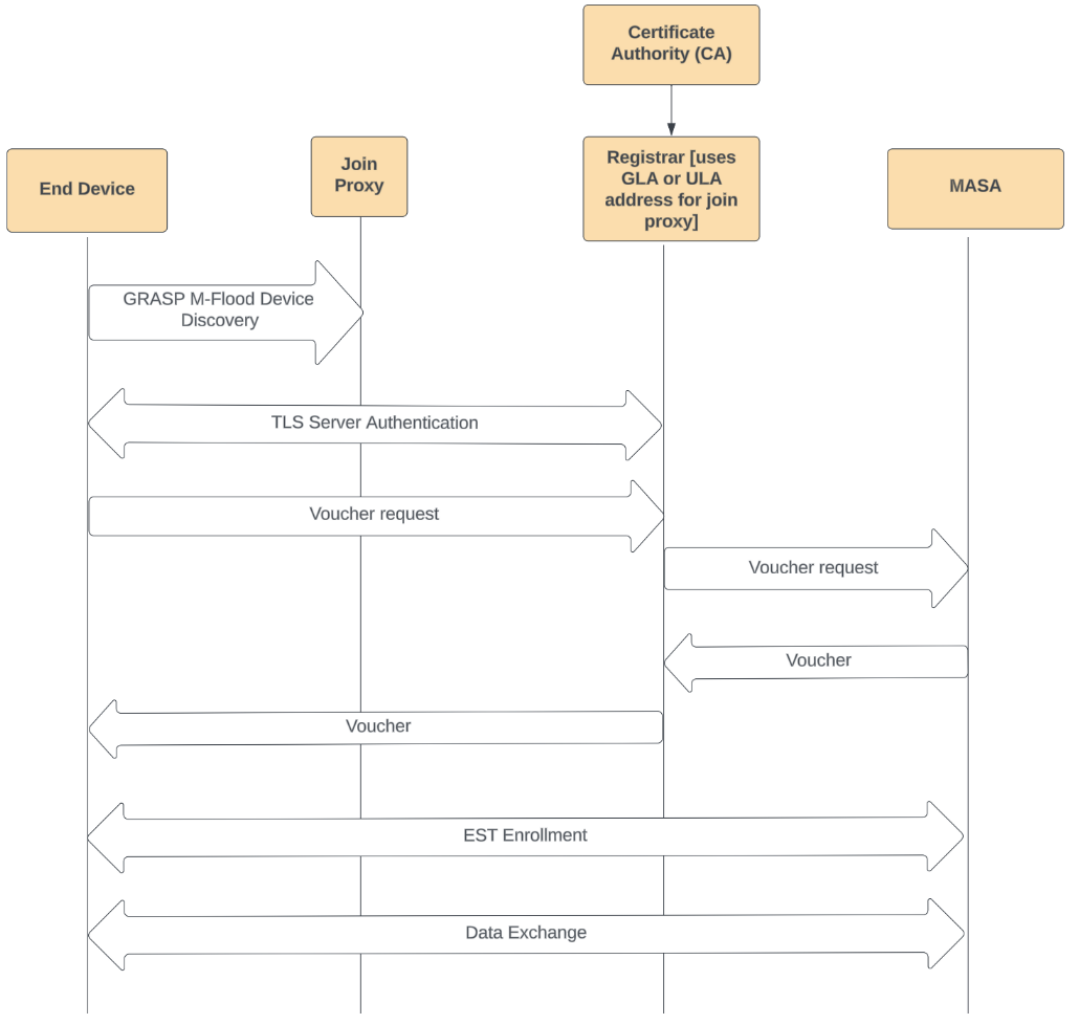



Figure 3.6: BRSKI Architecture

# System Network Stack Design

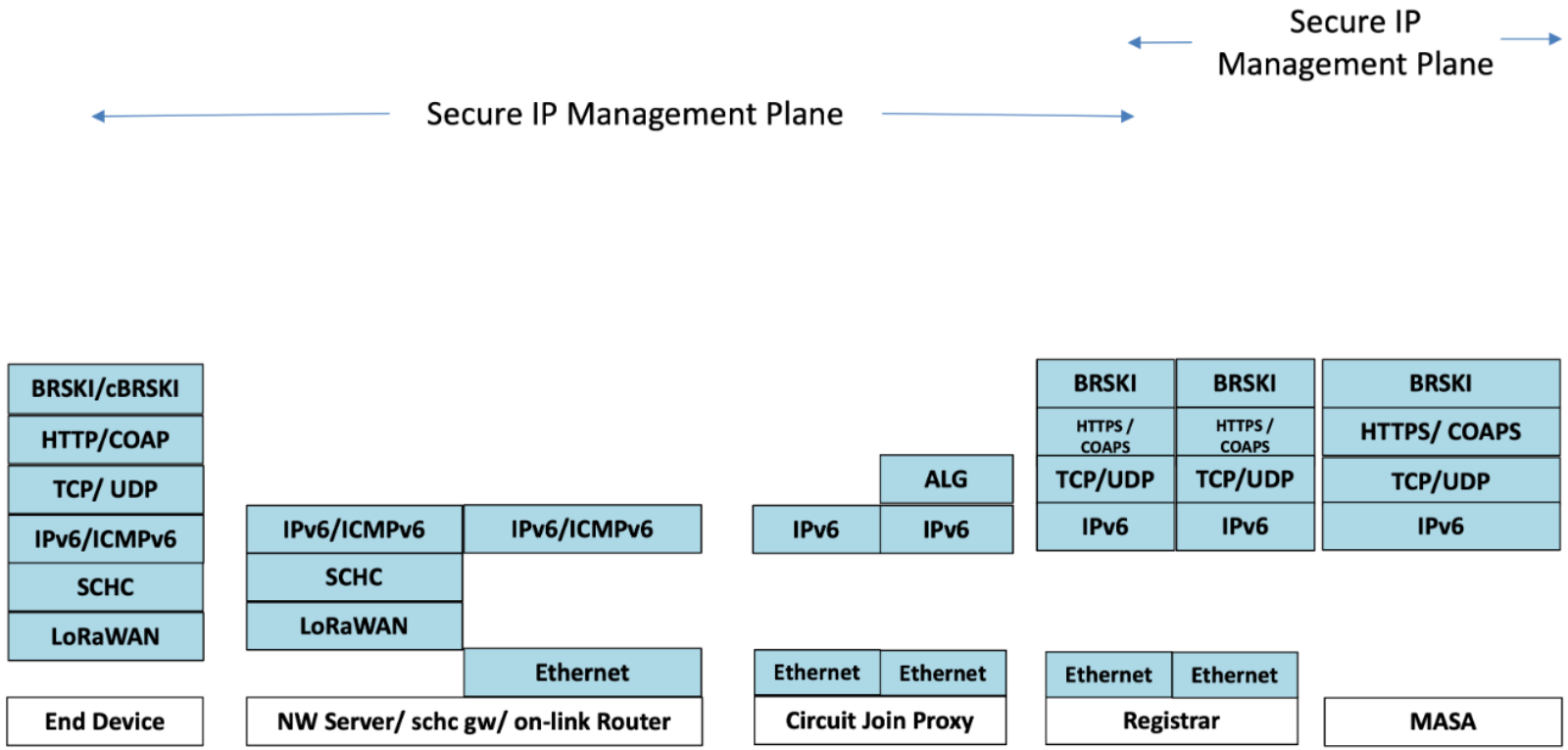



Figure 6.6: System Network Stack Design Management Plane Establishment

# Message exchanges

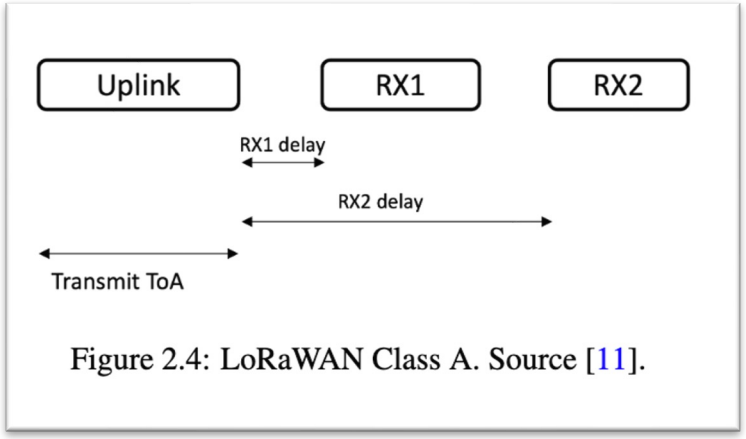



Figure 2.4: LoRaWAN Class A. Source [11].

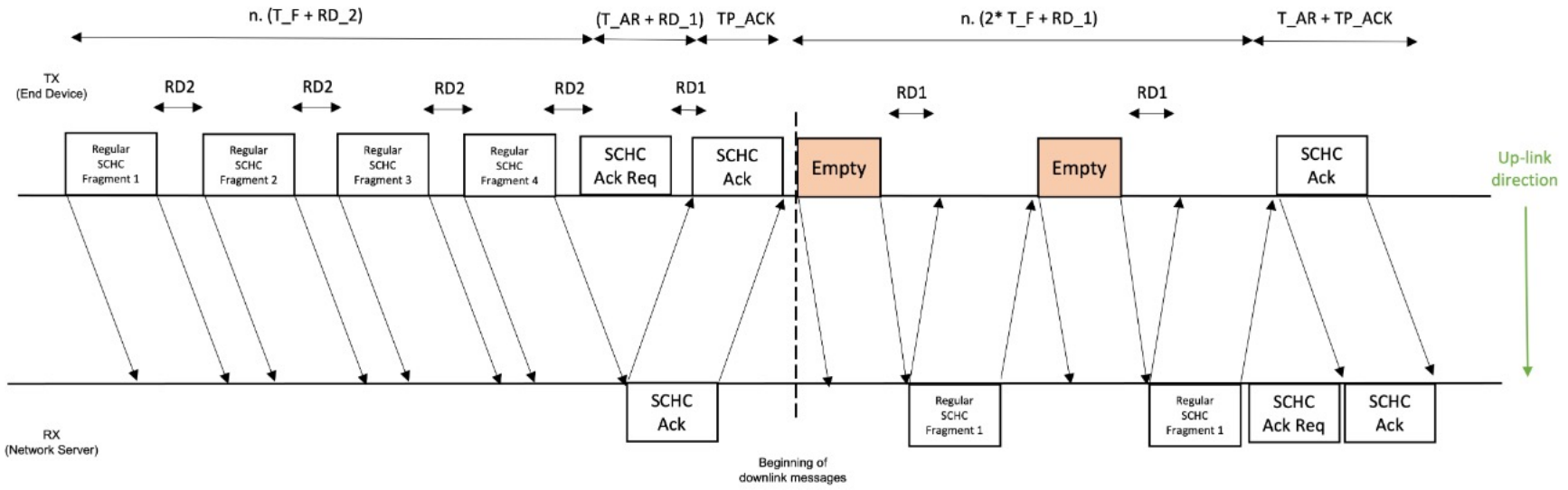



Figure 7.1: Up link and Down link messages in LoRaWAN using SCHC Fragmentation. Adapted from [2].

# SCHC Zero Context

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 |

# SCHC Zero Context

Table 7.5: MFLOOD next header SCHC rules

| Field | Length (bits) | Target Value | Matching Operator | CDA |
|---|---|---|---|---|
| UDP dev port | 16 | 7017 (GRASP listen port) | equal | value sent |
| UDP app port | 16 | - | ignore | value sent |
| UDP length | 16 | - | ignore | compute-* |
| UDP checksum | 16 | - | ignore | compute-* |

Table 7.4: M-Flood IPv6 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 | 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) calculate in AS | ignore | DevIID |
| Destination address | 128 | FF02::1:FF00:0000/104 (Solicited-node multicast address ) | equal | not sent |

# SCHC Zero Context

Table 7.7: DTLS IPv6 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 | 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) calculate in AS | ignore | DevIID |
| Destination address | 128 | - | ignore | sent |

Table 7.8: DTLS next header SCHC rules

| Field | Length (bits) | Target Value | Matching Operator | 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-* |