

Secure In-Band Network Telemetry for the SCION Internet Architecture on Tofino

M.Sc. Robin Wehner
M.Sc. Lars-Christian Schulz

M.Sc. Tony John
Prof. Dr. David Hausheer

Structure

1. Motivation
2. The ID-INT Protocol
3. P4 Implementation & Performance Results on Tofino
4. Evaluation of ID-INT on Specific Use Case
5. Conclusion & Future Work

1. Motivation

- ❖ SCION is a path-aware Internet architecture
 - Challenge: How to select an appropriate path?

1. Motivation

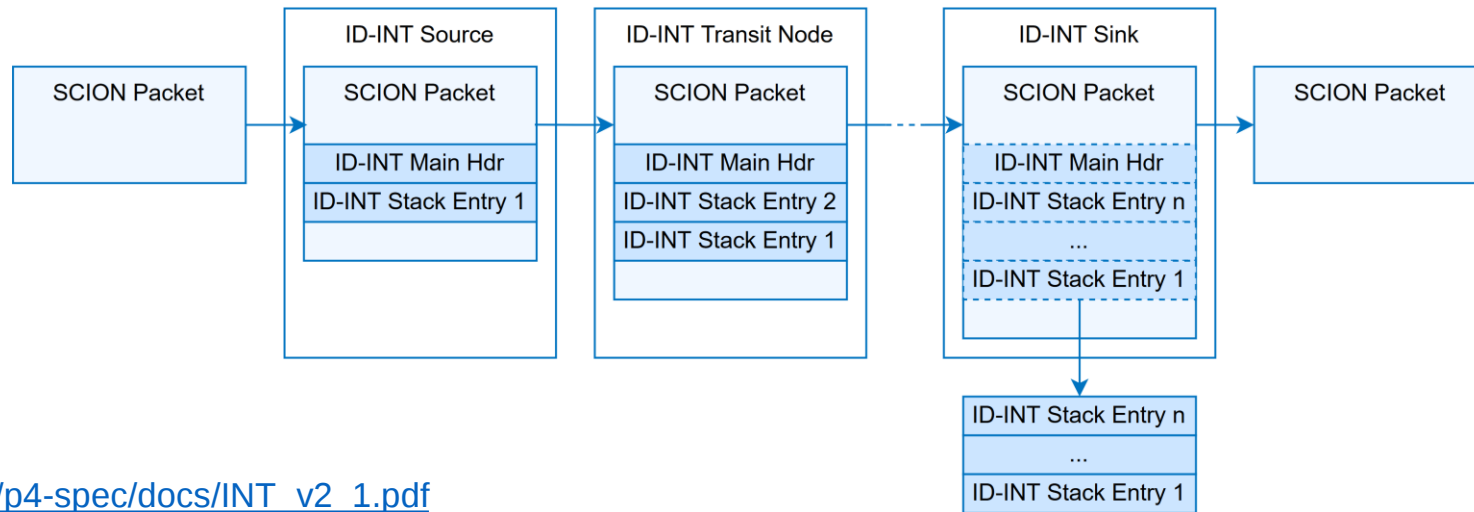
- ❖ SCION is a path-aware Internet architecture
 - Challenge: How to select an appropriate path?
- ❖ **General Approach:** End-2-end measurements
 - Useful for latency, bandwidth, jitter, etc.
 - Unprecise information on hop-by-hop latency
 - No information on internal router state (e.g. queue length)
 - Insufficient for certain applications that require more detailed network information to optimize path selection (e.g. congestion control)

1. Motivation

- ❖ SCION is a path-aware Internet architecture
 - Challenge: How to select an appropriate path?
- ✓ **Our Proposed Approach:** Inter-Domain In-band Network Telemetry (ID-INT)
 - Offers fine-granular metadata from inside the network
 - Implemented on Tofino
 - Hardware offers very precise network metadata (e.g. queue length)
 - High total throughput in combination with SCION border router

2. ID-INT Design

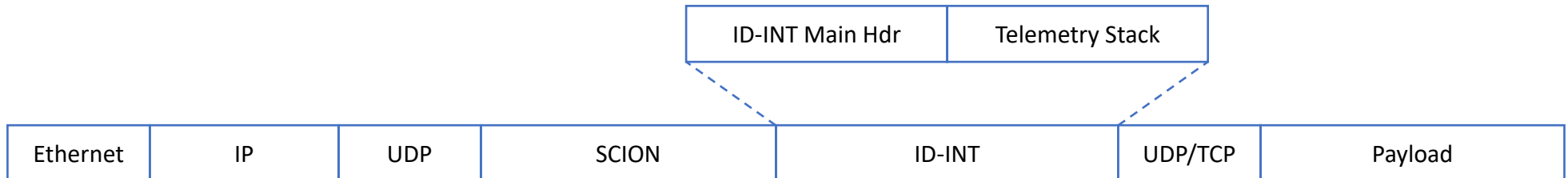
- ❖ Based on P4.org INT standard's INT-MD operational mode [1]
- ❖ Extends standard INT to support inter-domain environments by adding verifiable MACs to each stack entry
- ❖ Leverages the capabilities of SCION PKI and DRKey



[1] https://p4.org/p4-spec/docs/INT_v2_1.pdf

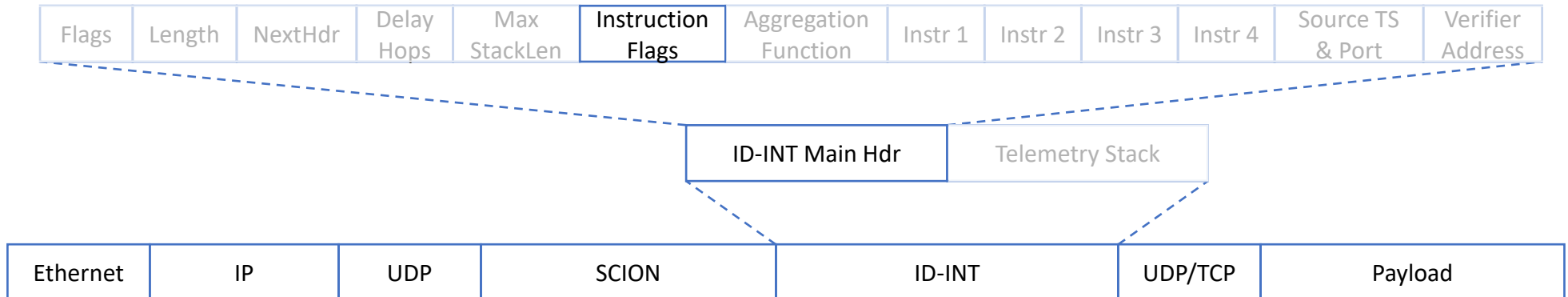
2. ID-INT Header Design

- ❖ SCION extension that is inserted after SCION headers



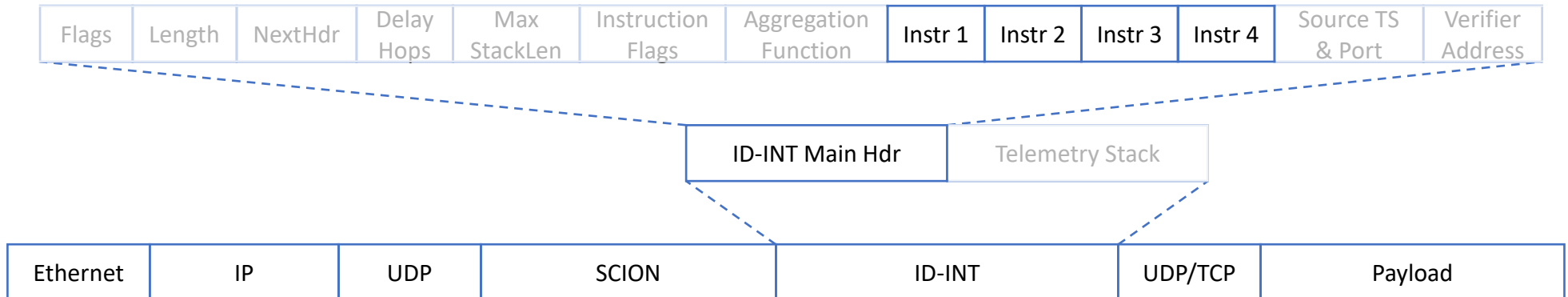
2. ID-INT Header Design

- ❖ Supports aggregation of metadata, **fixed** and flexible metadata
 - **Node Localization:** Node ID, Node Count, Ingress/Egress Interface ID



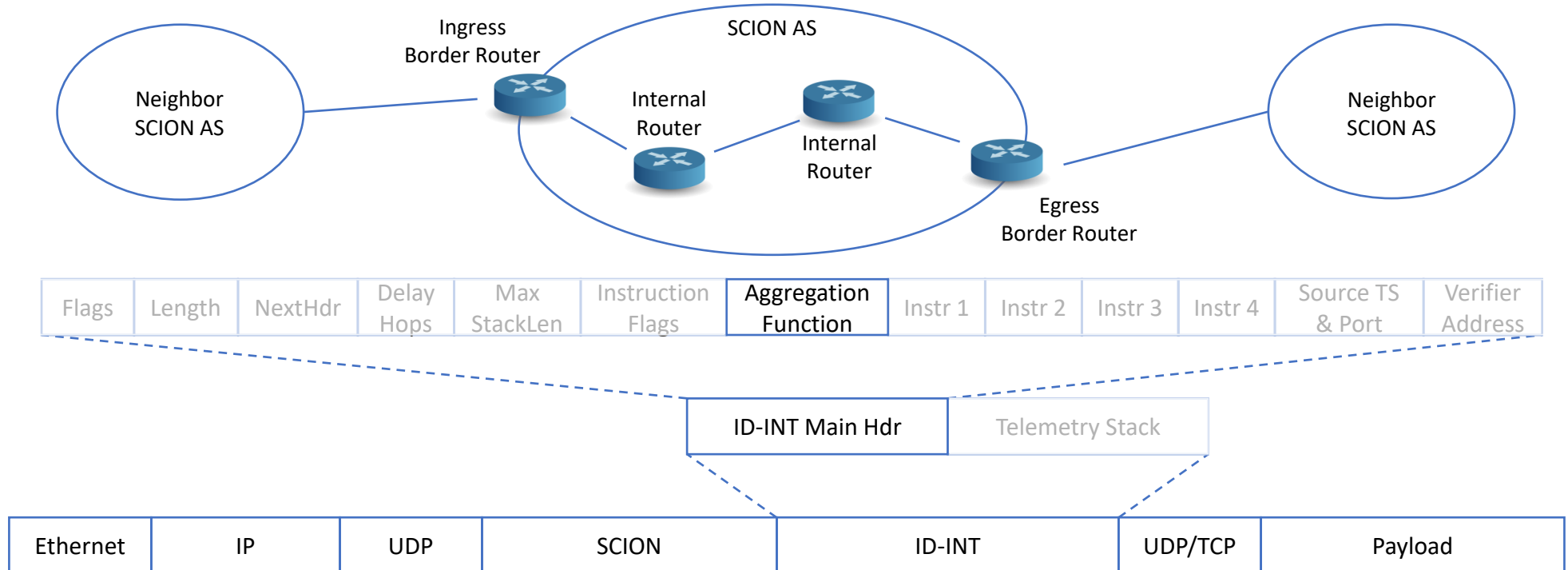
2. ID-INT Header Design

- ❖ Supports aggregation of metadata, fixed and **flexible** metadata
 - **Node Telemetry:** Timestamps, Queue ID, Instantaneous Queue Lengths, Ingress Port, *Device Type, Fan speed, Total Power Draw, Ingress/Egress Interface Speed, Uptime, Ingress/Egress SCION Interface Packet/Drop/Byte Count, Ingress/Egress Total Packet/Drop/Byte Count, ...*



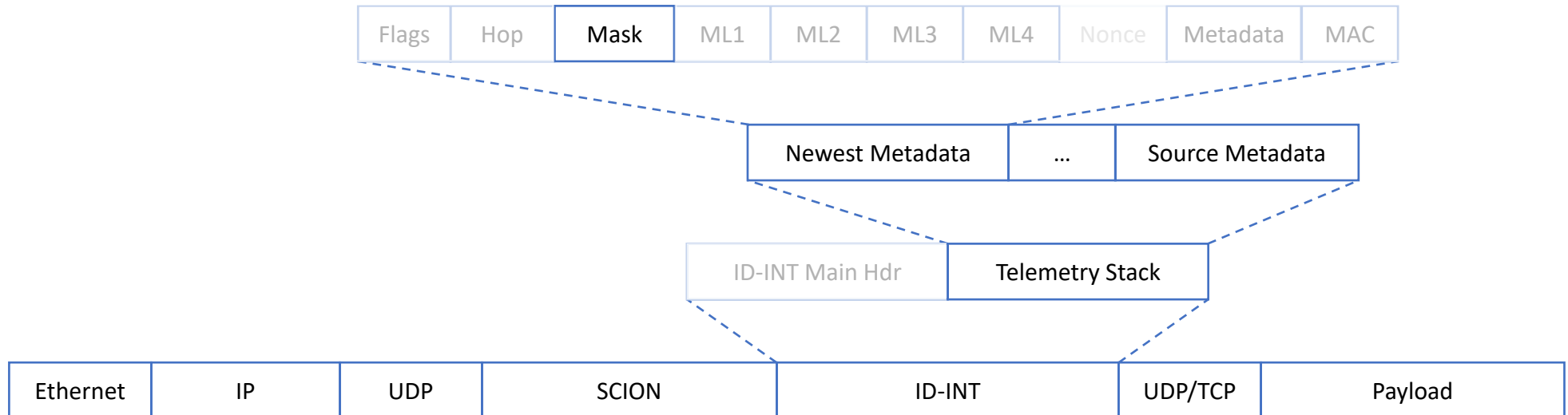
2. ID-INT Header Design

- ❖ Supports **aggregation** of metadata, fixed and flexible metadata



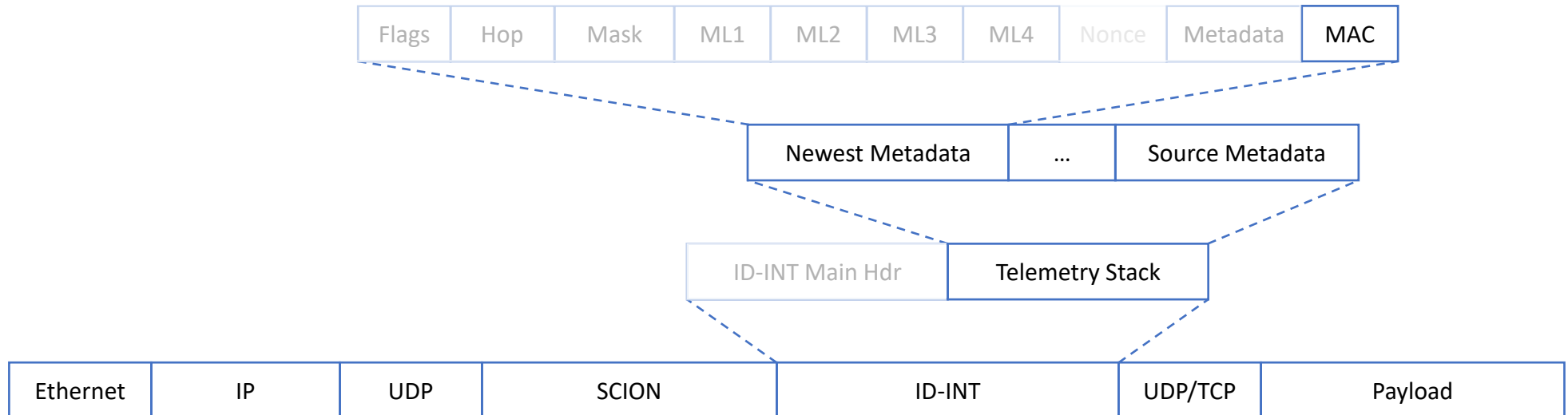
2. ID-INT Header Design

- ❖ Unsupported metadata is **not added to the stack**
- ❖ Stack entry size 8-64 Byte
- ❖ Telemetry entries are cryptographically secured by AES-CMAC



2. ID-INT Header Design

- ❖ Unsupported metadata is not added to the stack
- ❖ Stack entry size 8-64 Byte
- ❖ Telemetry entries are **cryptographically secured by AES-CMAC**



2. ID-INT Header Design

- ❖ Unsupported metadata is not added to the stack
- ❖ Stack entry size 8-64 Byte
- ❖ Telemetry entries are **cryptographically secured by AES-CMAC**
 - Derived with DRKey:
 - Used to create symmetrical AS-AS level keys in SCION
 - AES as pseudo-random derivation function

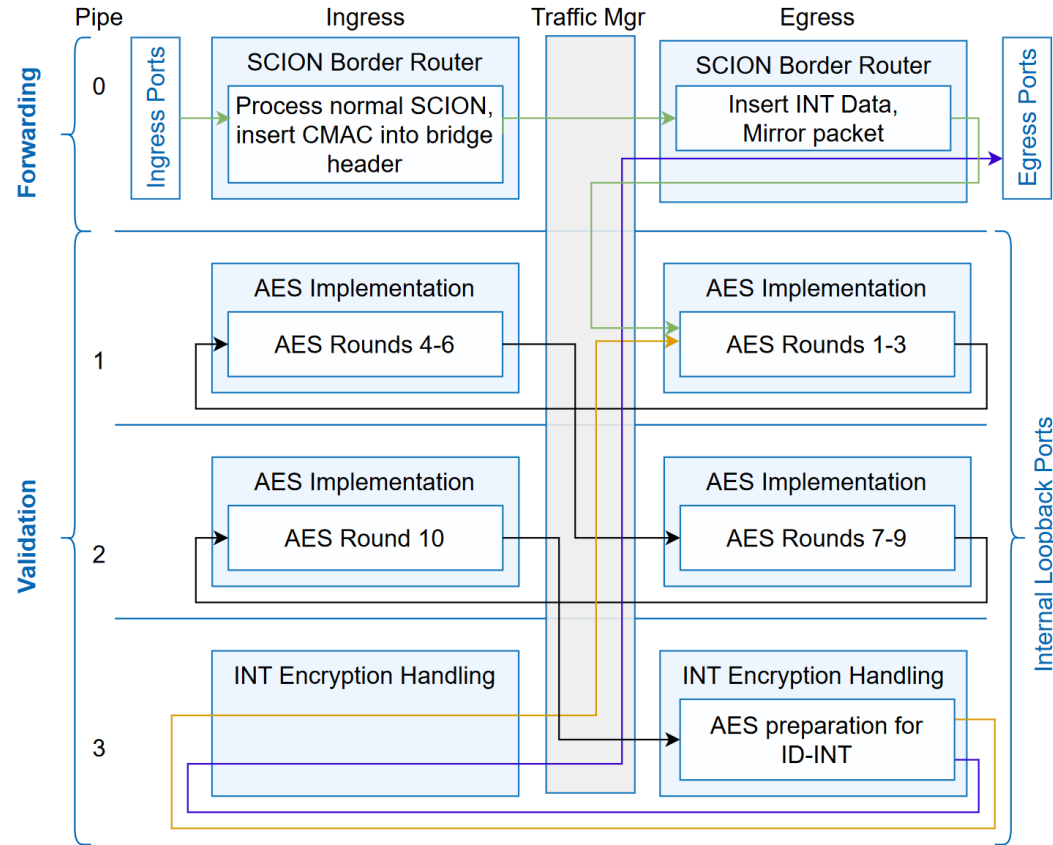
3. P4 Implementation & Performance Results on Tofino

- ❖ Extends the SCION Border Router implemented in P4 for Tofino 2 [2]
- ❖ Tofino's pipes 0 & 3 manage SCION and ID-INT processing
- ❖ Tofino's pipes 1 & 2 do AES calculations
 - SCION Hop Field validation
 - ID-INT MAC calculation → Done with an AS-AS level key
 - DRKey derivation (uses AES as pseudo-random function in SCION)

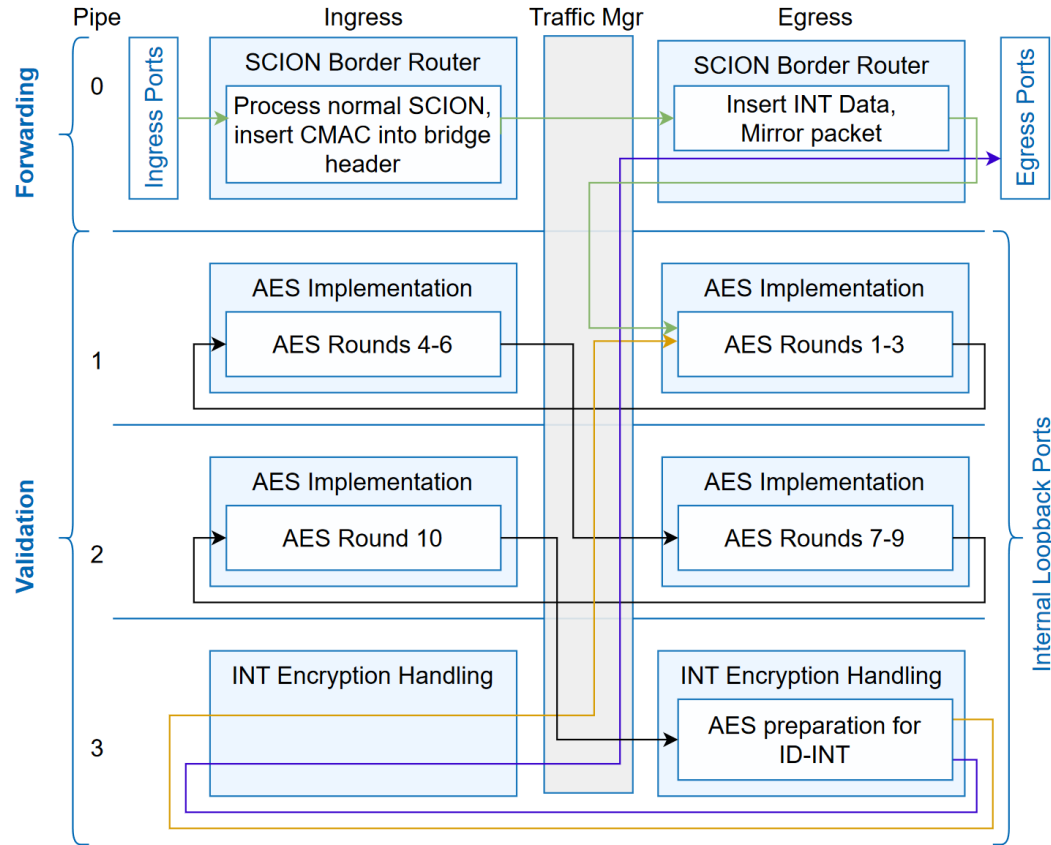
[2] Lars-Christian Schulz, Robin Wehner, and David Hausheer. 2023. **Cryptographic Path Validation for SCION in P4**. In *Proceedings of the 6th on European P4 Workshop (EuroP4 '23)*. <https://doi.org/10.1145/3630047.3630190>

Code: <https://github.com/netsys-lab/scion-p4>

3. P4 Implementation & Performance Results on Tofino



3. P4 Implementation & Performance Results on Tofino

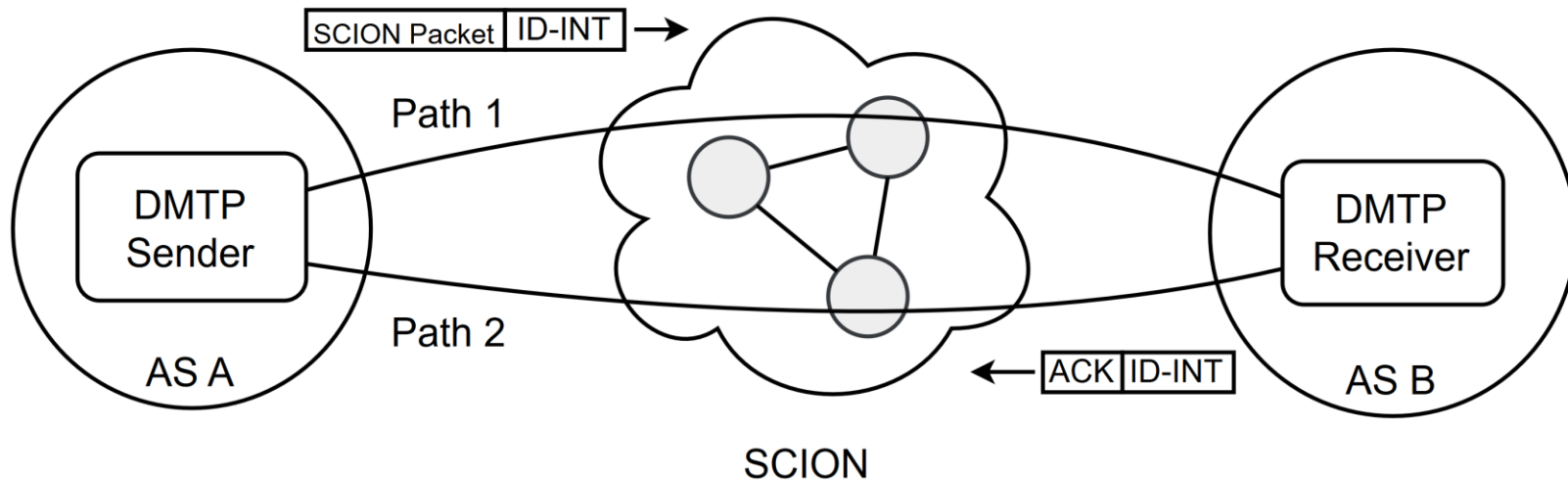


Performance Observations:

- ❖ 3-38 pipeline passes
- ❖ Best case: 400 Gbps per port
- ❖ Worst Case: 33.33 Gbps per port
- ❖ Regular case: 66-100 Gbps per port
- ❖ ID-INT may not be included in every packet or could be rate limited depending on use case
 - Avg.: Close to 400 Gbps

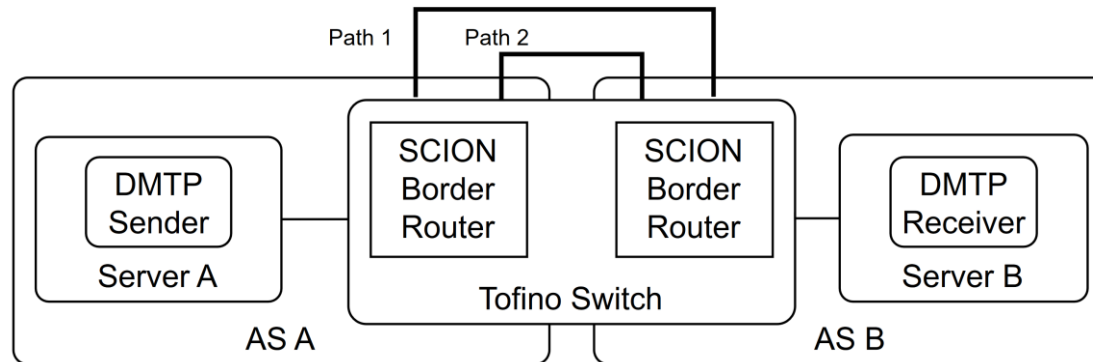
4. Evaluation of ID-INT on DMTP as Specific Use Case

- ❖ To prove effectiveness of ID-INT for SCION routing, DMTP [3] is deployed
- ❖ Integrated ID-INT into DMTP to select paths based on live statistics



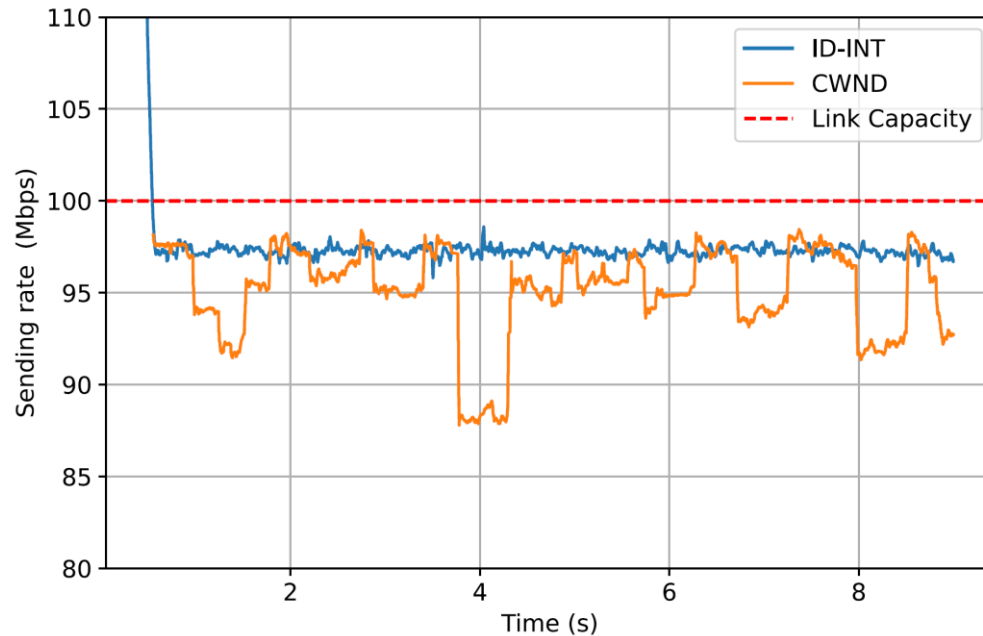
4. Evaluation of ID-INT on DMTP as Specific Use Case

- ❖ Evaluation setup used Tofino as 2 routers and a server that ran two SCION end hosts
- ❖ Primarily used instantaneous queue length in Tofino as metric
- ❖ Bottleneck inside the Tofino introduced to simulate link congestion



4. Evaluation of ID-INT on DMTP as Specific Use Case

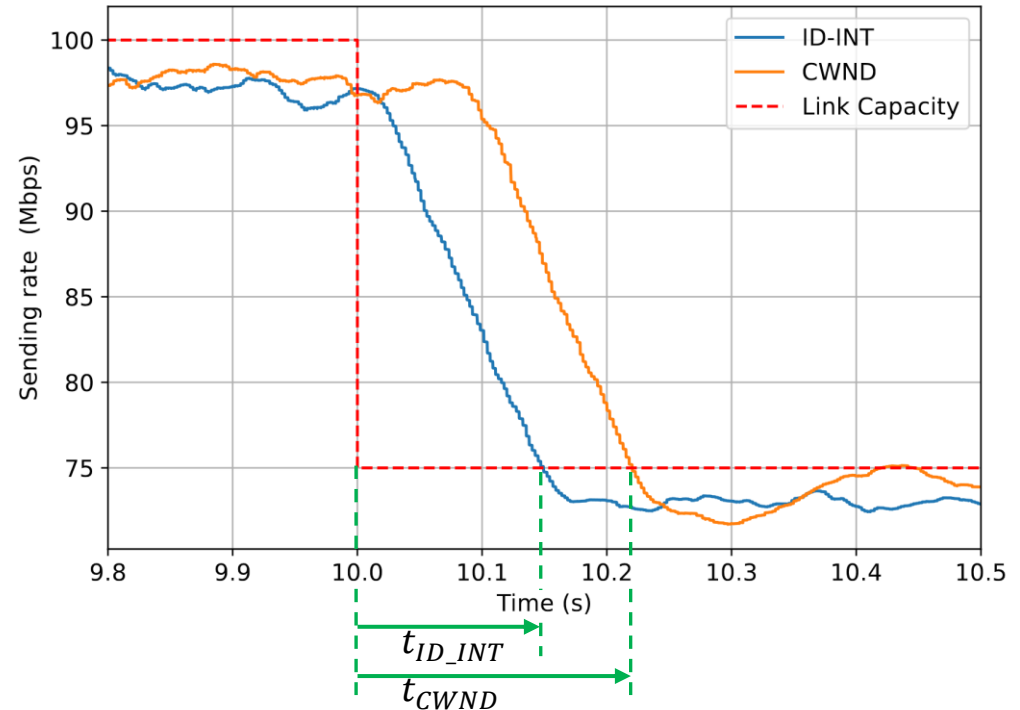
- ❖ With constant link capacity of 100 Mbps, the sending rate was more stable using the live metrics of ID-INT



4. Evaluation of ID-INT on DMTP as Specific Use Case

- ❖ When dropping the link capacity to 75 Mbps, ID-INT allows a 35 % faster reaction to the changed network conditions

- In multipath scenario, switching to a different path as a failover would be done faster



5. Conclusion & Future Work

- ❖ First hardware implementation of ID-INT enables fine-granular metadata collection for networks under various administrations
- ❖ ID-INT proved its effectiveness in assisting path selection of DMTP in terms of
 - More constant sending rates
 - Faster reaction times and failover under changing network conditions.

5. Conclusion & Future Work

- ❖ First hardware implementation of ID-INT enables fine-granular metadata collection for networks under various administrations
- ❖ ID-INT proved its effectiveness in assisting path selection of DMTP in terms of
 - More constant sending rates
 - Faster reaction times and failover under changing network conditions.
- ❖ Add missing features to current implementation
- ❖ Implement ID-INT on NetFPGA & XDP and compare performance and available metadata

Thanks for your attention!

Paper: Wehner, R., John, T., Schulz, L.C., Hausheer, D.: **Secure In-Band Network Telemetry for the SCION Internet Architecture on Tofino**. In: *7th European P4 Workshop (EuroP4'24)* (2024)
<https://ieeexplore.ieee.org/document/10858524>

E-Mails: robin.wehner@ovgu.de