HAW
HAMBURG

Network Anomaly Detection in Cars based on Time-Sensitive Ingress Control

IEEE VTC2020-Fall, Online

Philipp Meyer, Timo Häckel, Franz Korf and Thomas C. Schmidt

Dept. Computer Science, HAW Hamburg, Germany

Communication over Real-time Ethernet research group

CoRE

Outline

I. Time-Sensitive Networking (TSN) in Cars

II. Detecting Network Anomalies with TSN

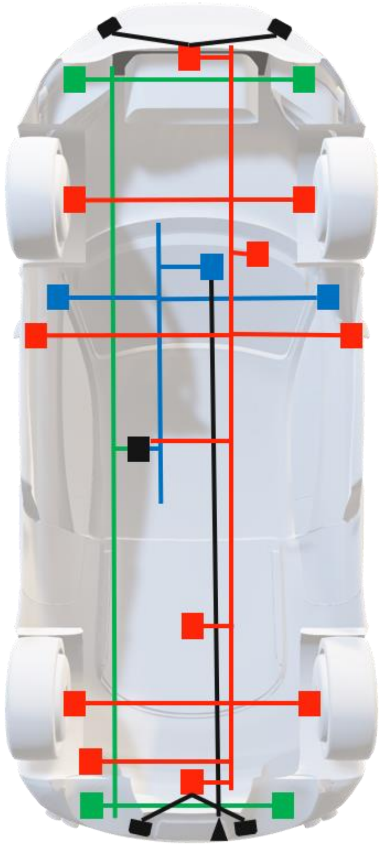
III. Automotive Case Study

IV. Conclusion & Outlook

I.

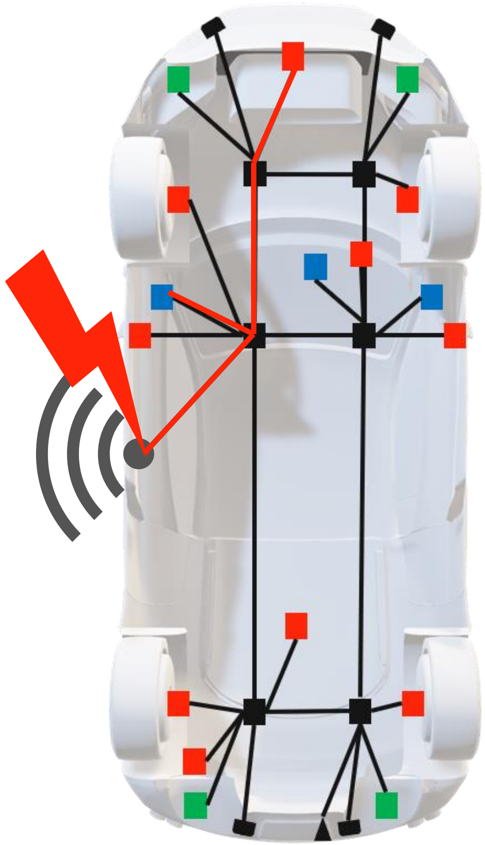
Time-Sensitive Networking (TSN) in Cars

Time-Sensitive Networking in Cars
Current Architecture



- Multitude of Electronic Control Units
- Connected over proprietary bus technologies
- In distinct Domains

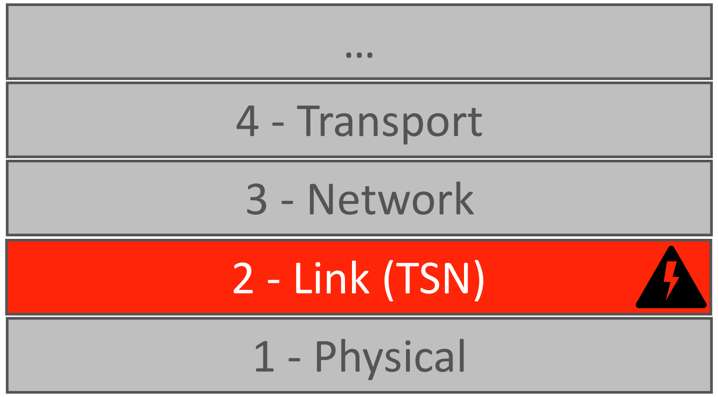
Time-Sensitive Networking in Cars
Future Architecture



- Flat Ethernet
- TSN deploys QoS on layer 2
- Integrated into global communication
- Attacks could result in fatal consequences

Time-Sensitive Networking in Cars
Anomaly Detection on the Link Layer

- Corruption can violate QoS and safety
  - Safety is dependent on QoS
  - Layer 2 guarantees QoS
- Fast and reliable on the lowest possible layer



…

4 - Transport

3 - Network

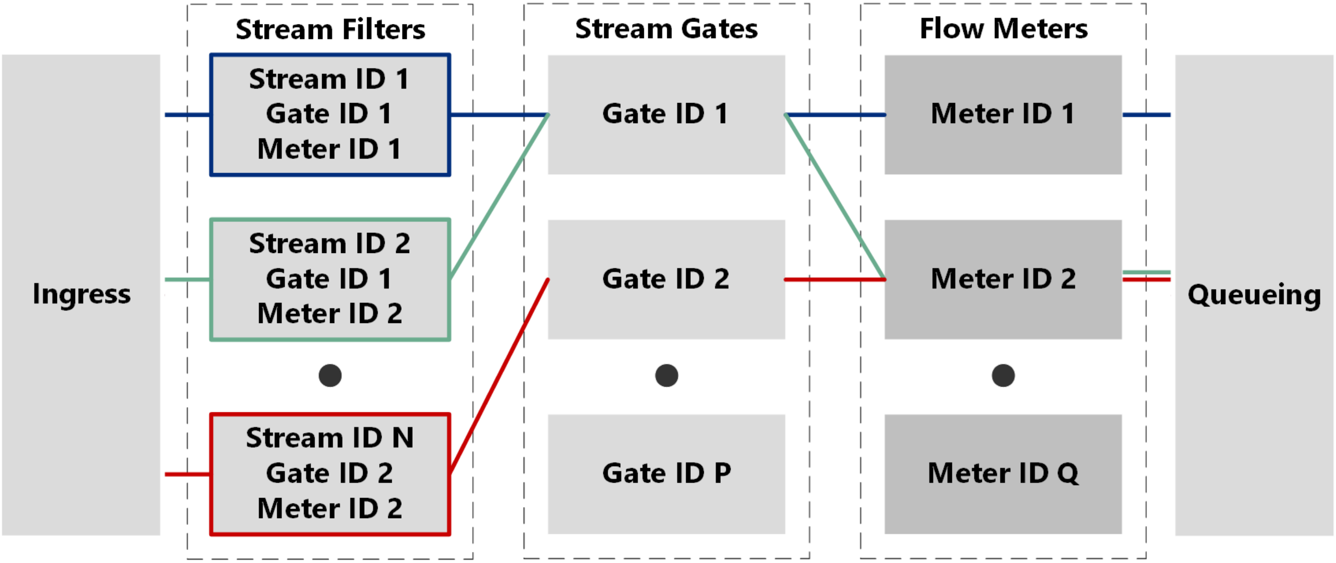
2 - Link (TSN) ⚠

1 - Physical

Multi-sided measures to secure layer 2 are needed.

Time-Sensitive Networking in Cars
Per-Stream Filtering and Policing (Qci)

- Network design specifies traffic
- Traffic behavior is known
- Qci enforces known traffic parameters



IEEE 802.1Q-2018 / IEEE 802.1Qci

The Qci configuration serves as an implicit description of regular traffic behavior on the link layer.

II.

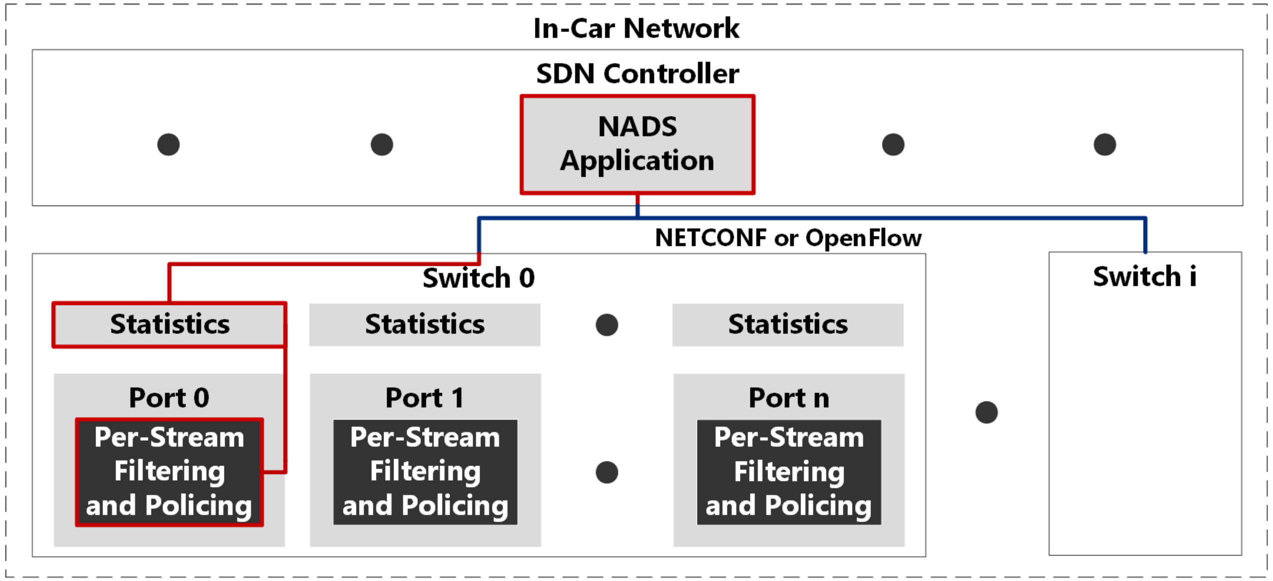
Detecting Network Anomalies with TSN

Detecting Network Anomalies with TSN
Network Anomaly Detection System (NADS)

1. A violation of a Qci rule indicates an abnormal behavior:
2. Anomaly indicators:
   - Frame drops
   - Missing frames
   - …
3. Indicators can remain free of false positives:
   - Frame drops never occur with valid behavior
   - …
4. Switches can communicate statistics to a central instance:
   - SDN controller
   - …

Detecting Network Anomalies with TSN Example

- Combine Qci & SDN into a NADS
- SDN controller application gathers Qci statistic
- Controller application enables further analysis

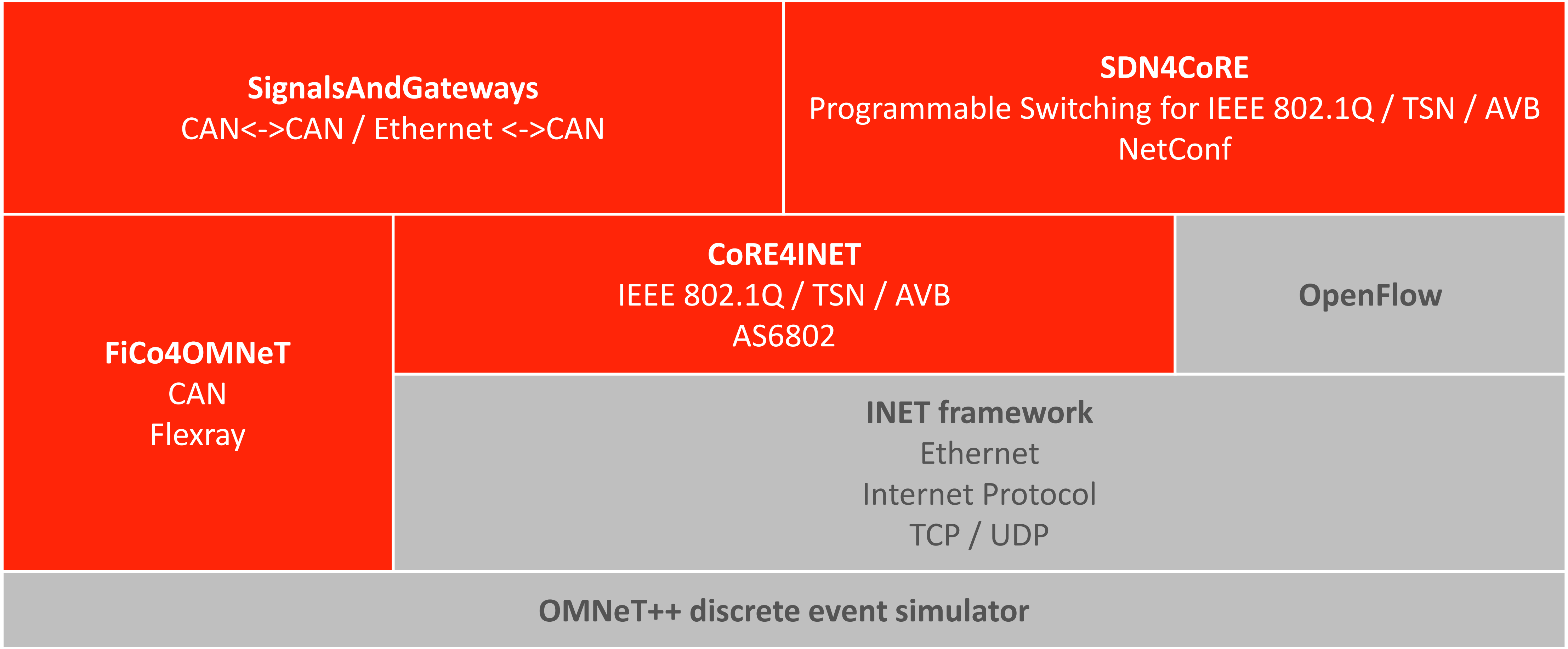


Qci misbehavior is traced without additional hardware.

III.

Automotive Case Study

Automotive Case Study
Simulation Environment (github.com/CoRE-RG)



SignalsAndGateways
CAN<->CAN / Ethernet <->CAN

SDN4CoRE
Programmable Switching for IEEE 802.1Q / TSN / AVB
NetConf

FiCo4OMNeT
CAN
Flexray

CoRE4INET
IEEE 802.1Q / TSN / AVB
AS6802

OpenFlow

INET framework
Ethernet
Internet Protocol
TCP / UDP

OMNeT++ discrete event simulator

Automotive Case Study Topology

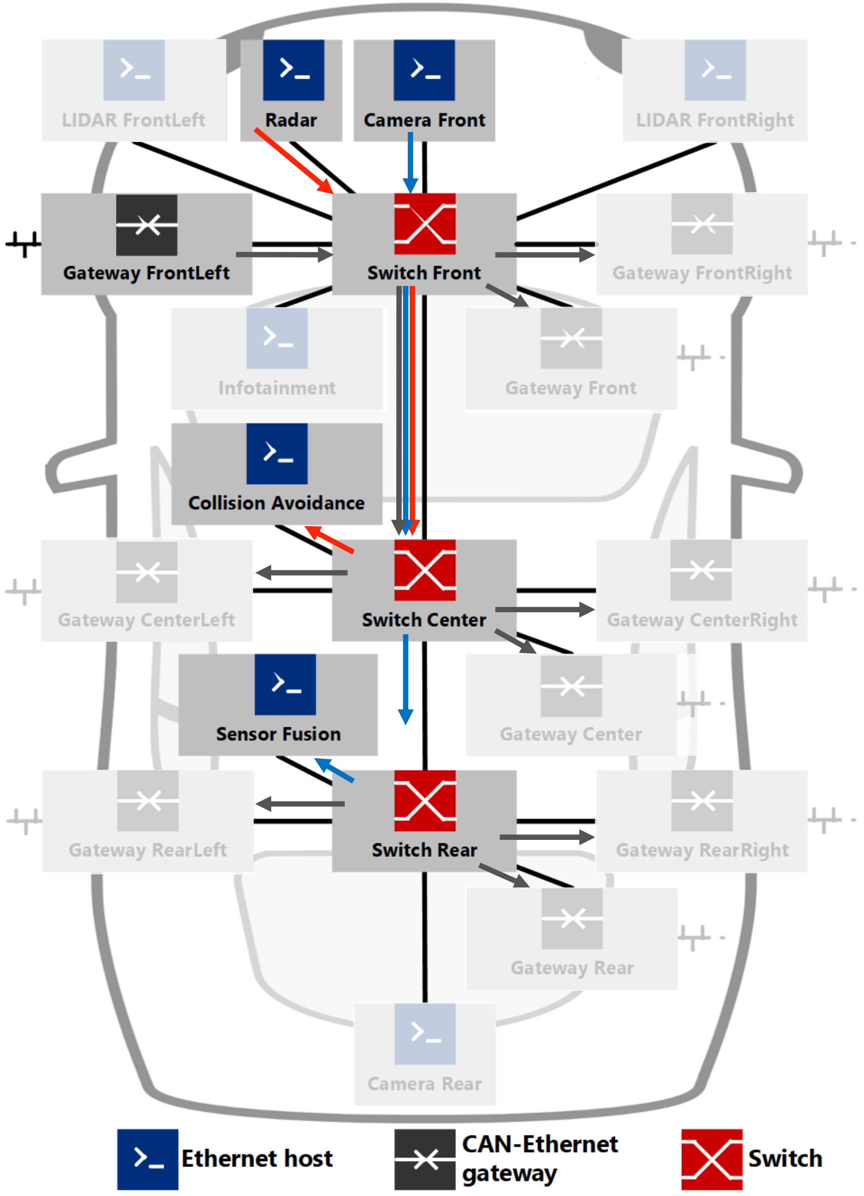
- Based on real in-car communication matrix
- Zonal 100 Mbit/s Ethernet topolgy
- TSN fowarding & filtering on each port
- **Anomaly indicator:** Dropping of frames

Observed Backbone Communication

- Synchronos safety critical
- Asynchronus data stream
- CAN tunneling

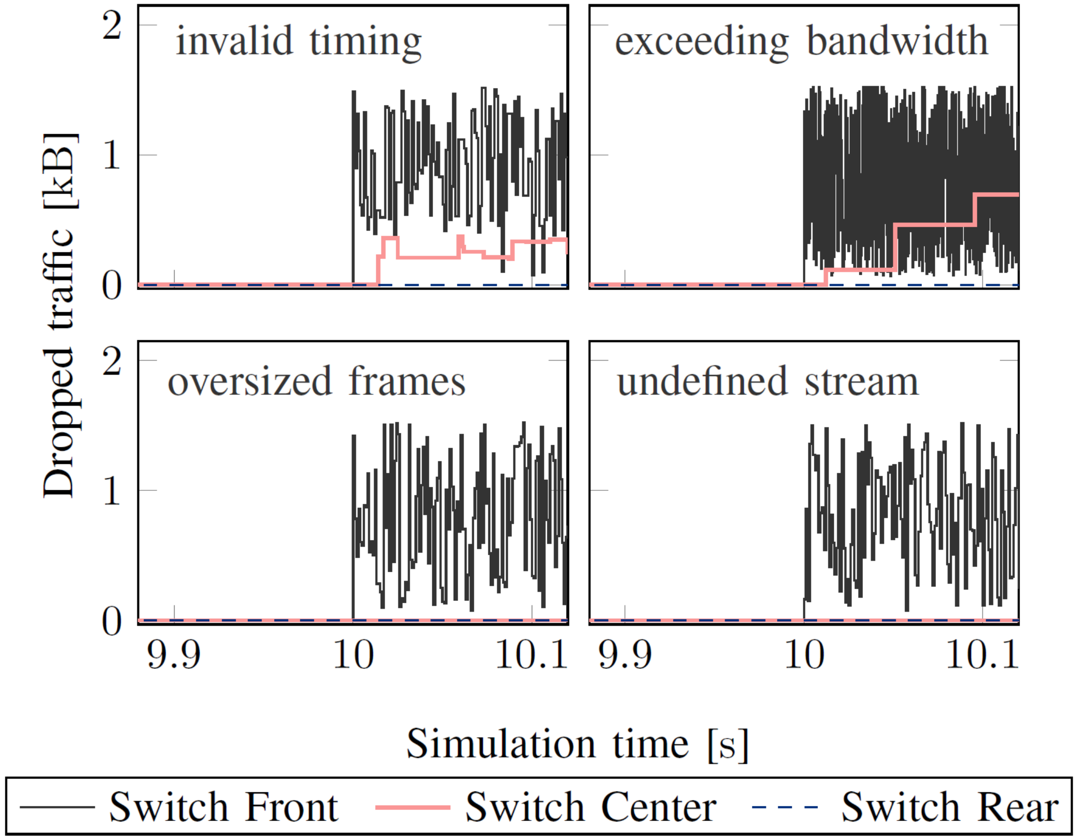
Qci configuration

- Timing
- Bandwidth
- Frame size
- Undefined streams will be dropped



Case Study Detection

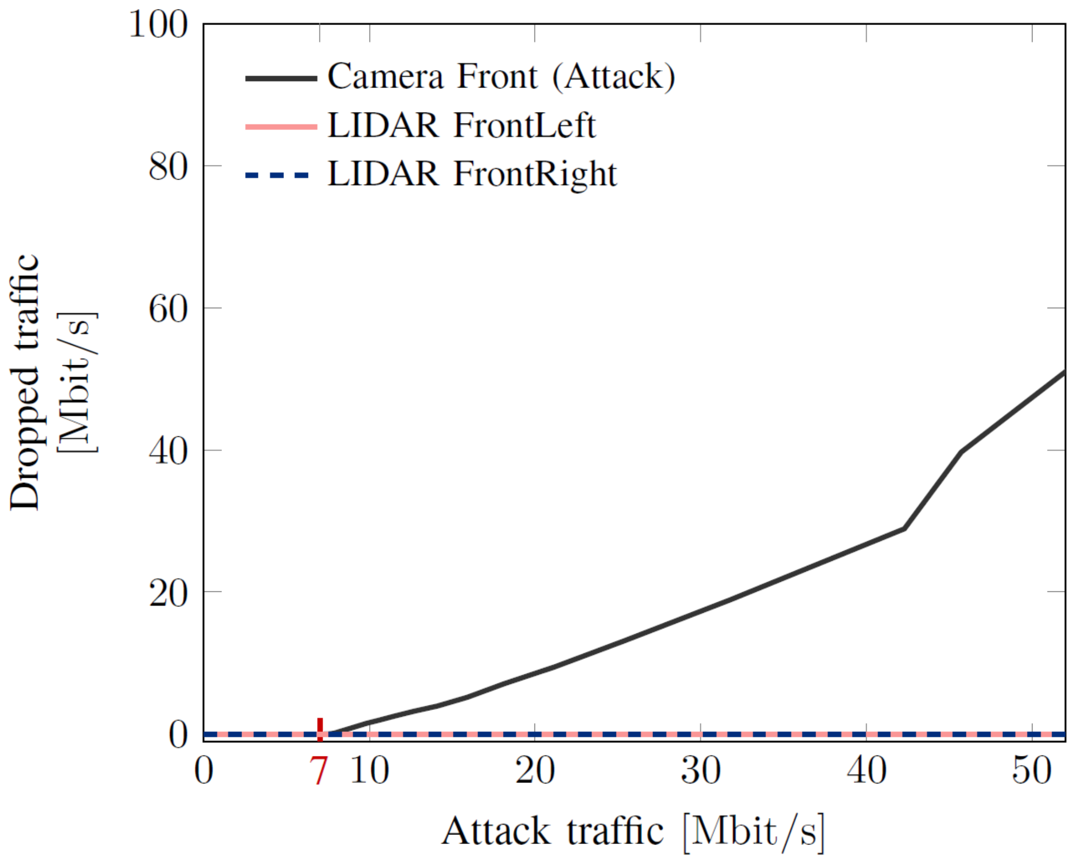
- Attack:
  - Source is the original sender
  - Frame injection (DoS)
  - Uniformly distributed size
  - Starts at 10s
- Demonstrates detection of invalid behavior for individual streams



There are no false positive anomaly detections.

Case Study False Negatives

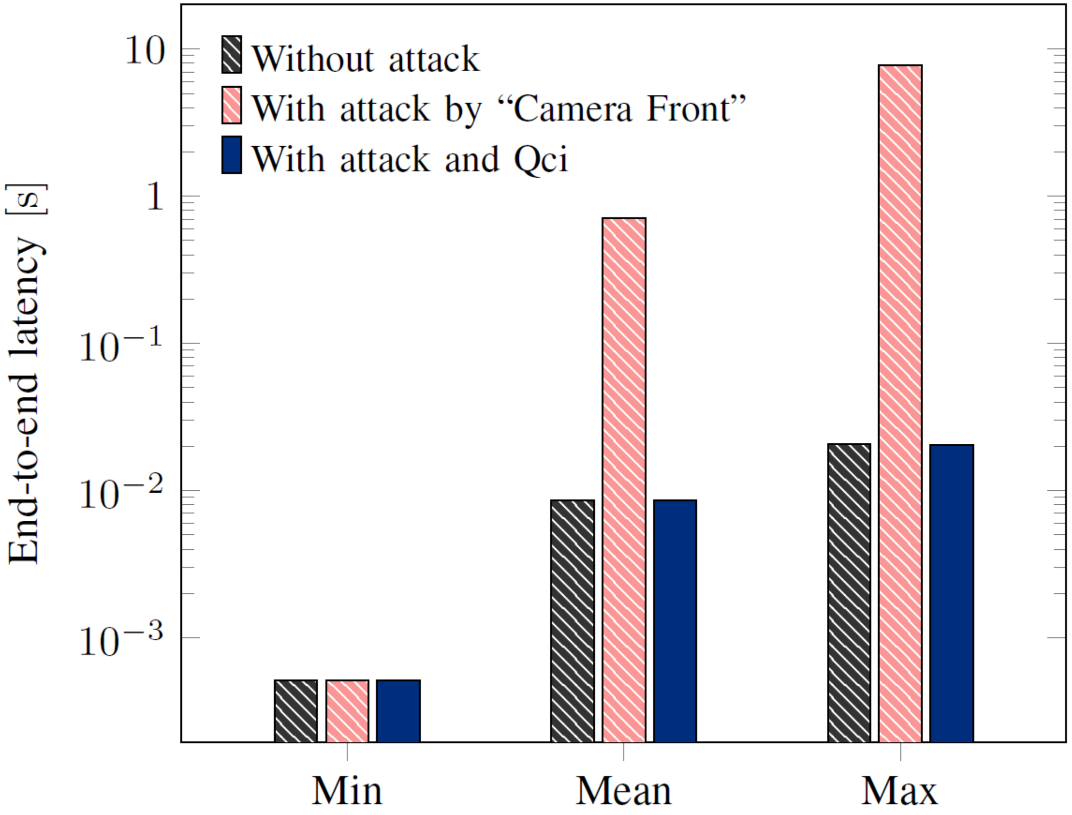
- Stream bandwidth is 7 Mbit/s
- Dropped traffic is related to the attack bandwidth
- No frame drops below 7 Mbit/s



There are false negatives.

Case Study Mitigation

- Ingress filtering & policing:
  - Drops invalid/surplus frames
- SDN controller:
  - Reconfigure or disable flows
  - Reconfigure TSN forwarding and ingress control



LIDAR FrontLeft data stream

IV.

Conclusion

Conclusion

- More efficient on the lowest possible layer
- Link-layer anomaly detection with Qci
- Can perform with zero false positive detections
- Does not require additional hardware
- Mitigation advantages through Qci & SDN

In the future:

- New or correlated meters can reduce false negatives
- Further evaluate benefits and limits

Acknowledgements

This work is funded by the German Federal Ministry of Education and Research (BMBF) within the SecVI project.

secVI

secvi.inet.haw-hamburg.de

SPONSORED BY THE

Federal Ministry
of Education
and Research