HAW HAMBURG

Strategies for Integrating Control Flows in Software-Defined In-Vehicle Networks and Their Impact on Network Security

2020 IEEE Vehicular Networking Conference (VNC)
December 16–18, 2020 | Virtual Conference

Timo Häckel, Anja Schmidt, Philipp Meyer, Franz Korf, and Thomas C. Schmidt
Dept. Computer Science, Hamburg University of Applied Sciences, Germany

Contact: timo.haeckel@haw-hamburg.de

secVI

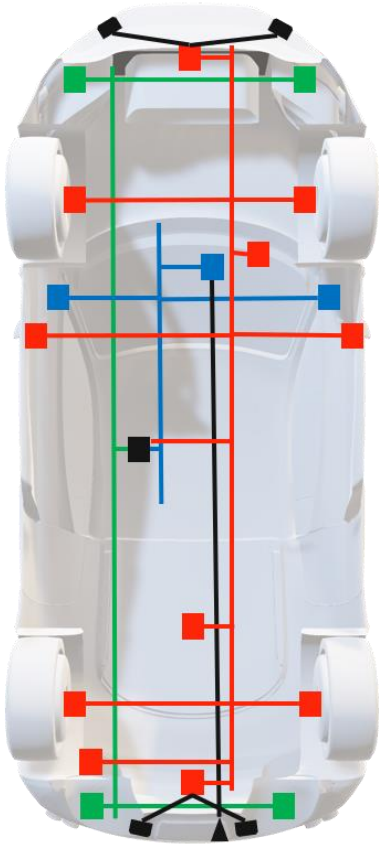
Outline

I. Evolution of In-Vehicle Networks
II. Design Space for Embedding Control Communication
III. Impact on Network Security
IV. Conclusion and Outlook

I.

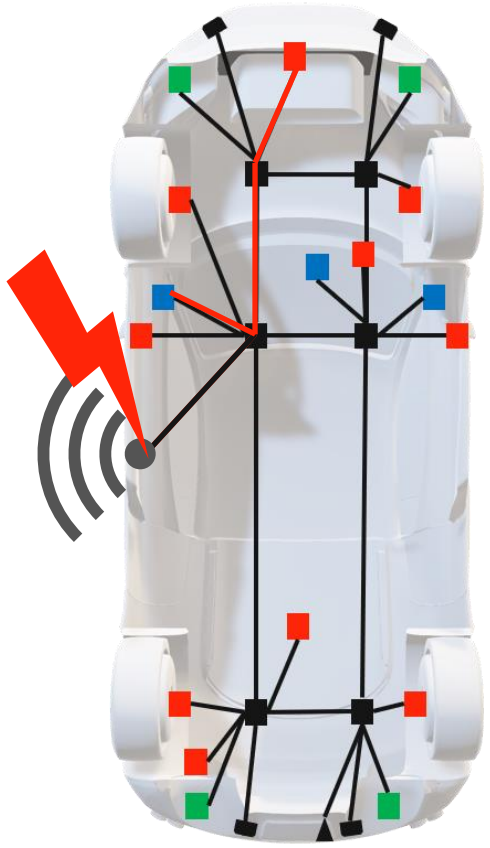
Evolution of In-Vehicle Networks

Current In-Vehicle Networks



- Multitude of Electronic Control Units (ECUs)
- Different bus technologies
- Central gateway separates bus domains
- Messages exchanged between ECUs are specified in the communication matrix

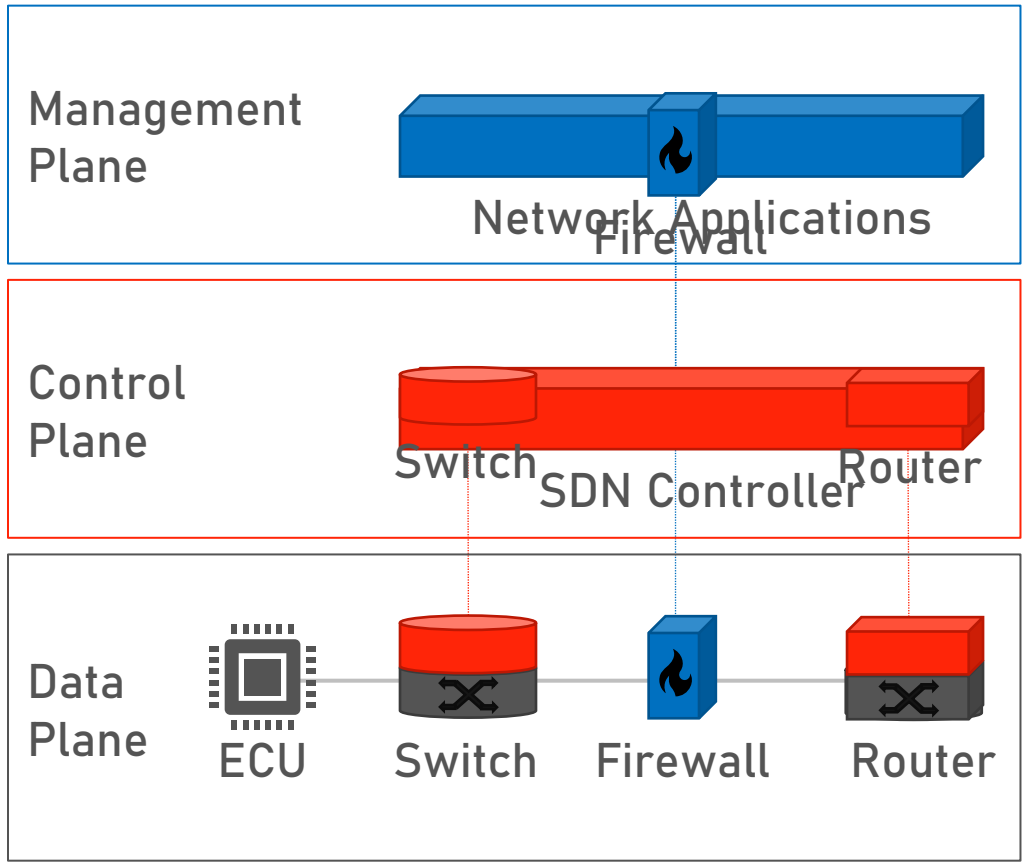
Future In-Vehicle Networks



- Evolution to Ethernet
- Gateways integrate legacy communication
- Time-Sensitive Networking (TSN) for QoS
- Integrated into global communication (V2X)
- Attacks could result in fatal consequences

→ **Opportunity to rethink network security**

Software-Defined Networking in Cars



- Separates data plane and control plane
- Central network control entity
- Secure dynamic traffic stearing
- OpenFlow pipeline matching all layer 2-4 packet header fields

→ **Trusted communication backbone**

Research Question

What is the most secure way to embed control communication in software-defined in-car networks?

II.

Design Space for Embedding Control Communication

Differentiating Two Types of Flows

Control Flow (CF)	Network Flow (NF)
• Logical, specified in communication matrix • Sequence of messages identified based on identifier, domain and priority • Sent from a single origin to one or multiple receivers	• Physical, matched in network devices • Sequence of packets identified based on packet header fields from layer 2 - 4 • Forwarded from a particular source to a destination

Embedding Strategies for Control Flows

Control flow context information from the communication matrix

Control Flow Identifier | **Control Flow Priority** | **Control Flow Domain** | **Sender** | **Receivers**

Hidden embedding

L2 - Ethernet IEEE 802.1Q (auto-generated)				L3 - IPv4			L4 - UDP		L5 - SOME/IP	
MAC Dst (6 Byte)	MAC Src (6 Byte)	802.1Q Tag (PCP, VID) (4 Byte)	EtherType (2 Byte)	DSCP (6 Bit)	IP Src. (4 Byte)	IP Dst. (4 Byte)	Src. Port (2 Byte)	Dst. Port (2 Byte)	Msg. ID (4 Byte)	Payload (0-1400 Byte)
			Ipv4	CF Priority	Sender	CF Domain	SOME/IP	SOME/IP	CF ID	Data

Exposed embedding

L2 - Ethernet IEEE 802.1Q				Data
MAC Dst (6 Byte)	MAC Src (6 Byte)	802.1Q Tag (PCP, VID) (4 Byte)	EtherType (2 Byte)	Payload (42 – 1500 Byte)
CF ID	Sender	CF Priority / CF Domain	Embedded Type	Data

Separating In-Vehicle Control Flows

	Exposed Embedding	Hidden Embedding	
Separation	**By Message**	**By Domain**	**By Topic**
Strategy	Exact identification of control flows	Domain bus concept	Group same sender & receivers
Embedded Information	ID, domain, sender, priority	Domain, sender, priority	Topic, sender, priority
Network Flow	Per control flow	Per domain and sender	Per topic and sender

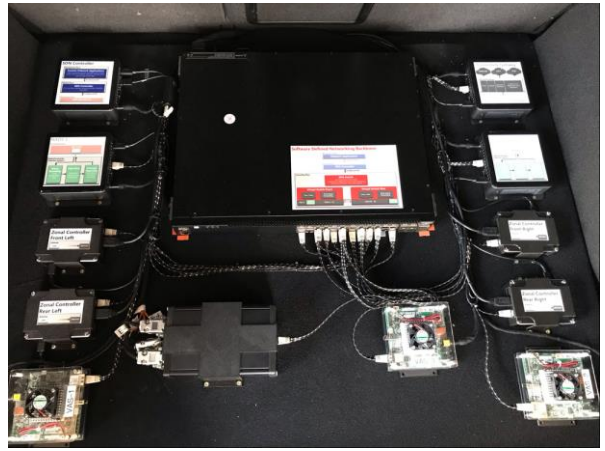
III.

Impact on Network Security

Prototype Car of the SecVI Project

- Real production car
- CAN network in domain architecture
- Software-defined Ethernet backbone

2016‘ Seat Ateca Prototype



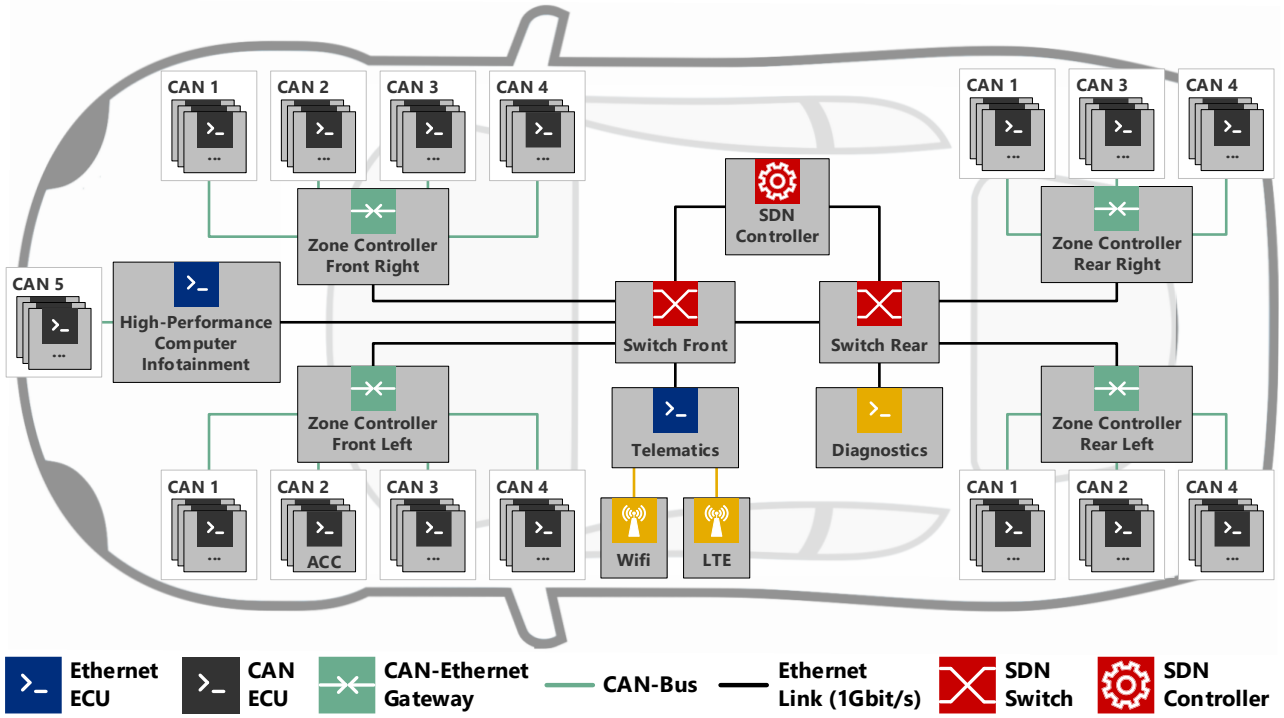
Installation in the trunk

→ SecVI demo here at VNC 2020

Demo: A Security Infrastructure for Vehicular Information Using SDN, Intrusion Detection, and a Defense Center in the Cloud
Philipp Meyer et al.

Evaluation Network

- Modern zone topology
- Zone controllers act as gateways for legacy
- Three different network configurations for separation concepts



Generated Network Flows

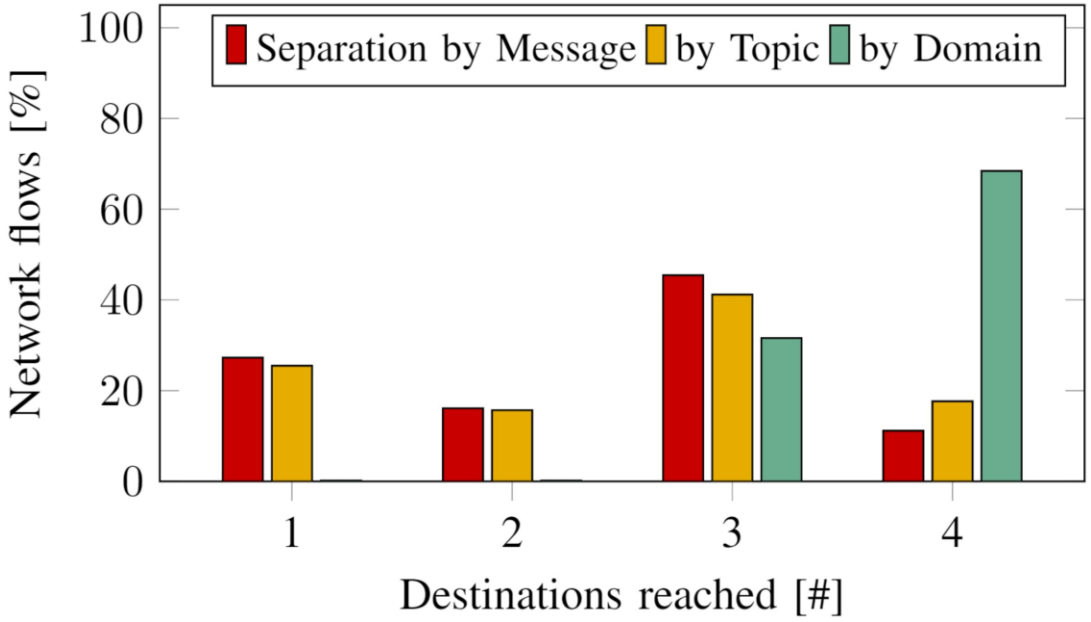
- Focus on CAN control flows transported via the backbone
- Network flows generated for a total of 242 control flows

Separation	# Generated Network Flows (with multiple Control Flows)	# Control Flows per Network Flow		
		Minimum	Average	Maximum.
By Message	242 (0)	1	1	1
By Domain	19 (19)	5	13	37
By Topic	102 (38)	1	3	17

→ **Ideal control flow separation with separation by message**

Destinations of Network Flows

- Separation by message
  - Serves as benchmark
- Separation by domain
  - No flows reach less than 3 destinations
  - Over 70% of all network flows reach all destinations
- Separation by topic
  - Approximation to benchmark



→ More fine-grained topics reduce cross communication

Impact on a Critical Control Flow

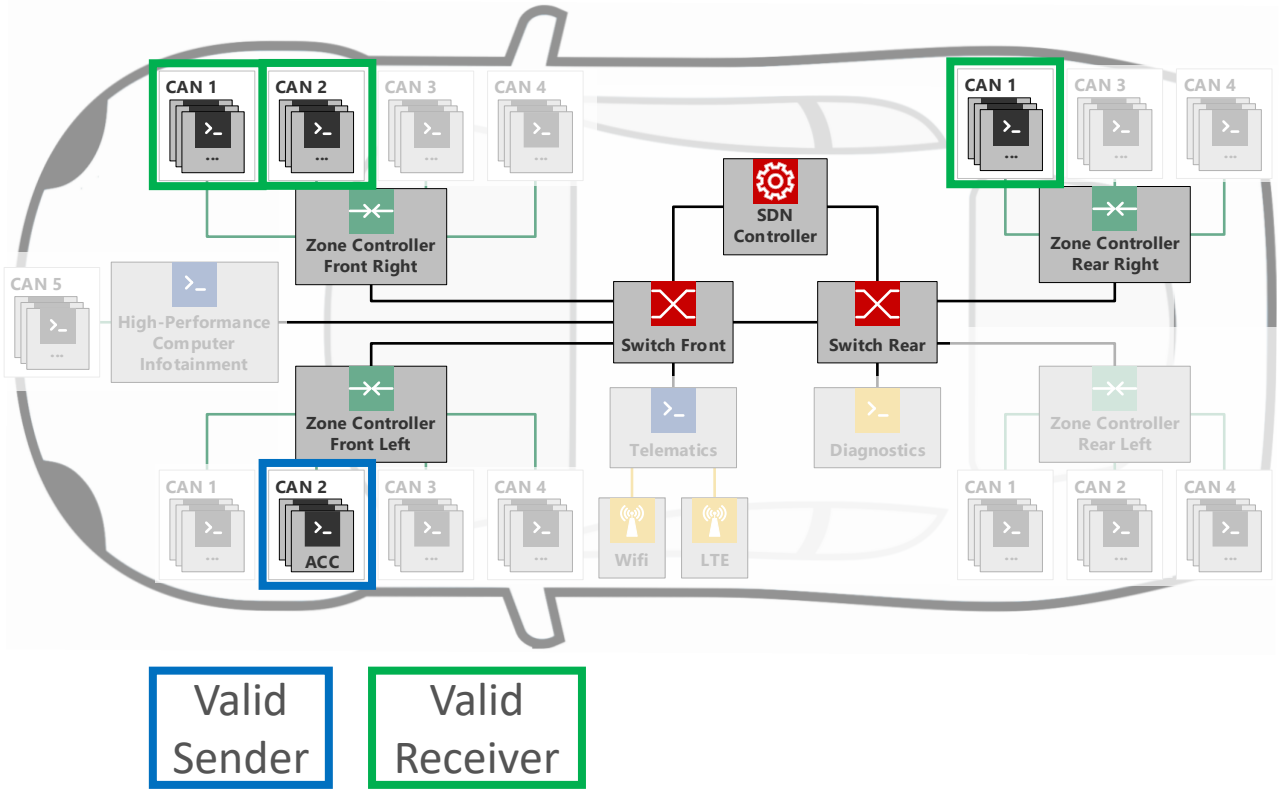
Acceleration Request

1 valid sender:

- Adaptive Cruise Control (ACC)

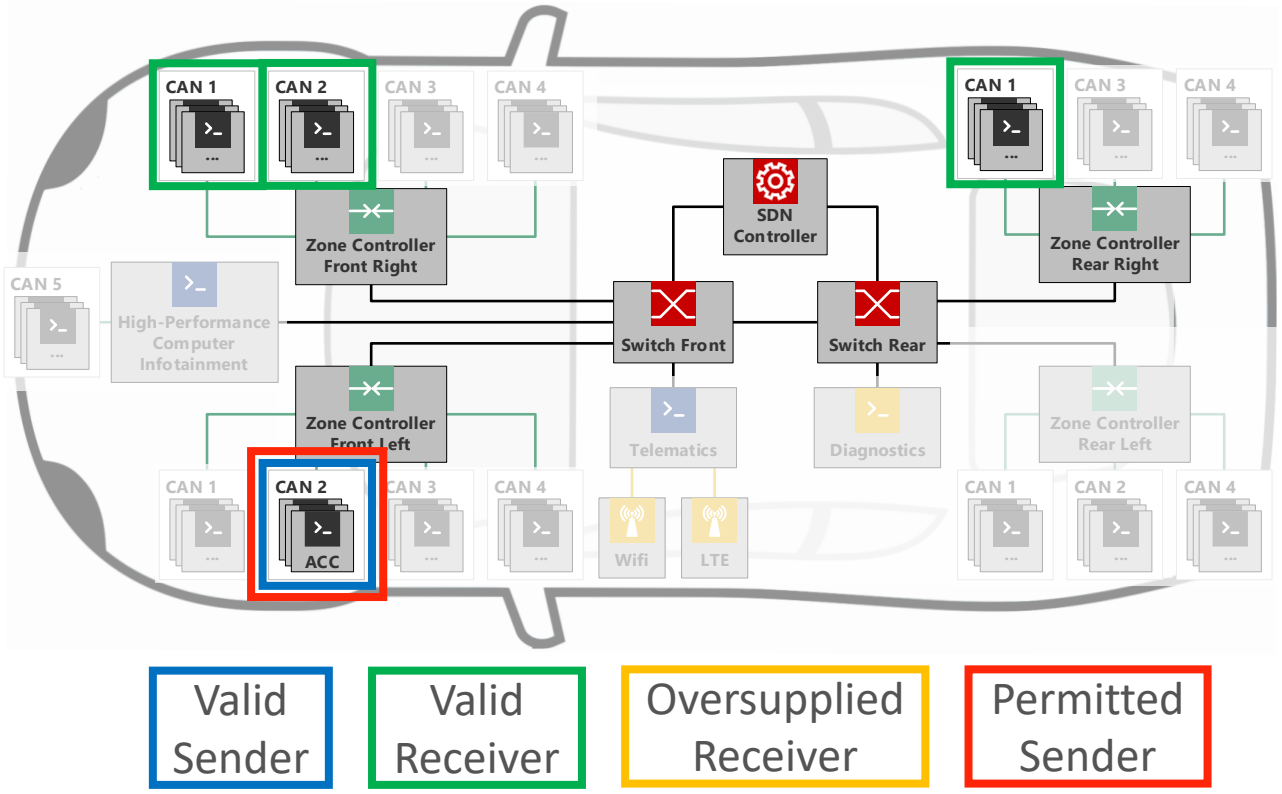
3 valid receivers:

- Engine,
- Transmission control
- Front Sensors ADAS



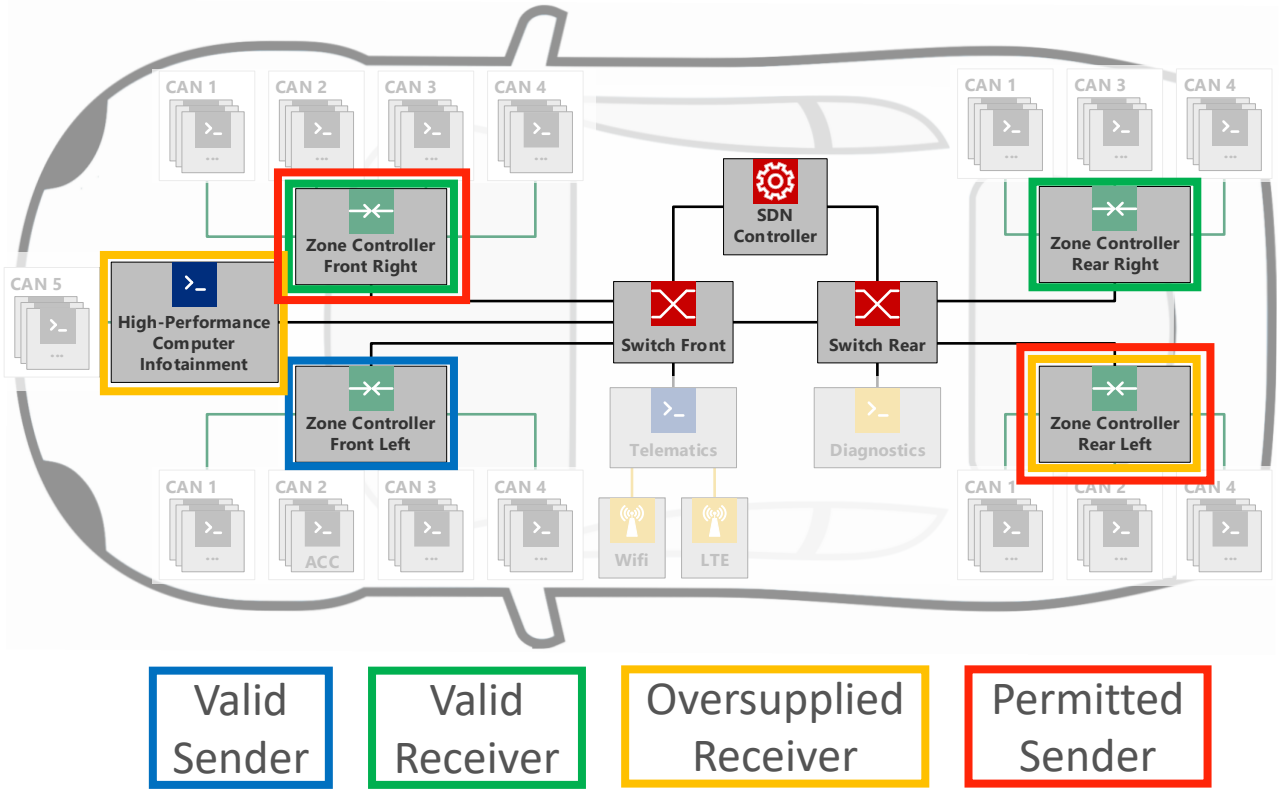
Attack Potential of CAN ECUs

- No protection on same physical CAN bus
- Gateways filter illegitimate messages
- 1 additional sender forwarded on the backbone
- Less devices per bus in zone topology



Attack Potential of Ethernet ECUs

Separation	Oversupplied Receivers	Permitted Senders
By Message	None	None
By Domain	HPC Infotainment, ZC Rear Left	ZC Rear Left, ZC Front Right
By Topic	HPC Infotainment	ZC Rear Left, ZC Front Right

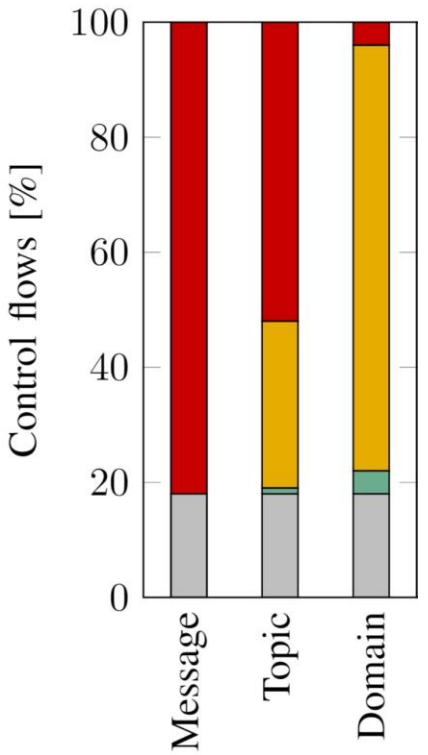


→ **Additional senders and receivers with hidden embeddings**

Impact of Control Flow Separation

Properties of a control flow (source to destination)

- Legitimate: Specified in communication matrix
- Received: Sent from the src and arrived at the dst
- Oversupplied: Received ∧ ¬Legitimate
- Permitted: Allowed to be sent ∧ ¬ Legitimate
- Forbidden: Not forwarded by the backbone
- No legitimate control flows are forbidden



→ **Only message separation enables precise access control**

Security Implications

Hidden embeddings

- Oversupplied control flows allow listening
- Permitted control flows allow manipulation and injection

→ Attacks easier as fewer devices are needed for advanced attacks

Exposed embeddings

- Ideal control flow separation
- Precise access control

→ Smaller attack surface as all original senders need to be under control

IV.

Conclusion and Outlook

Conclusion and Outlook

- Opportunity to define network security
- SDN enables a precise flow control from layer 2 to 4
- Embedding strategies have a big impact on network security
- Only exposed embeddings establish a trust zone in the network

Future work

- Advance security in cars with additional network intelligence

Acknowledgements

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

SPONSORED BY THE

Federal Ministry of Education and Research

secvi.inet.haw-hamburg.de