HAW HAMBURG

Integration realer Angriffe in simulierte Echtzeit-Ethernet-Netzwerke

Echtzeit 2020

Sandra Reider, Philipp Meyer, Timo Häckel, Franz Korf und Thomas C. Schmidt

Department Informatik, HAW Hamburg

Security for **V**ehicular **I**nformation Forschungsprojekt

Gliederung

- Einleitung
- Einbindung von Angriffen in die Simulation
- Fallbeispiel DoS-Angriff
- Fazit und Ausblick

Einleitung

Fahrzeugnetzwerke

- Steigende Bandbreitenanforderungen
- Ethernet als Kommunikationsmedium angestrebt
- Steuergeräte haben Echtzeit-Anforderungen

Öffnung des Netzwerks nach außen

- Neue Angriffsmöglichkeiten

Einleitung

Neue Sicherheitskonzepte notwendig

Simulation der Netzwerke

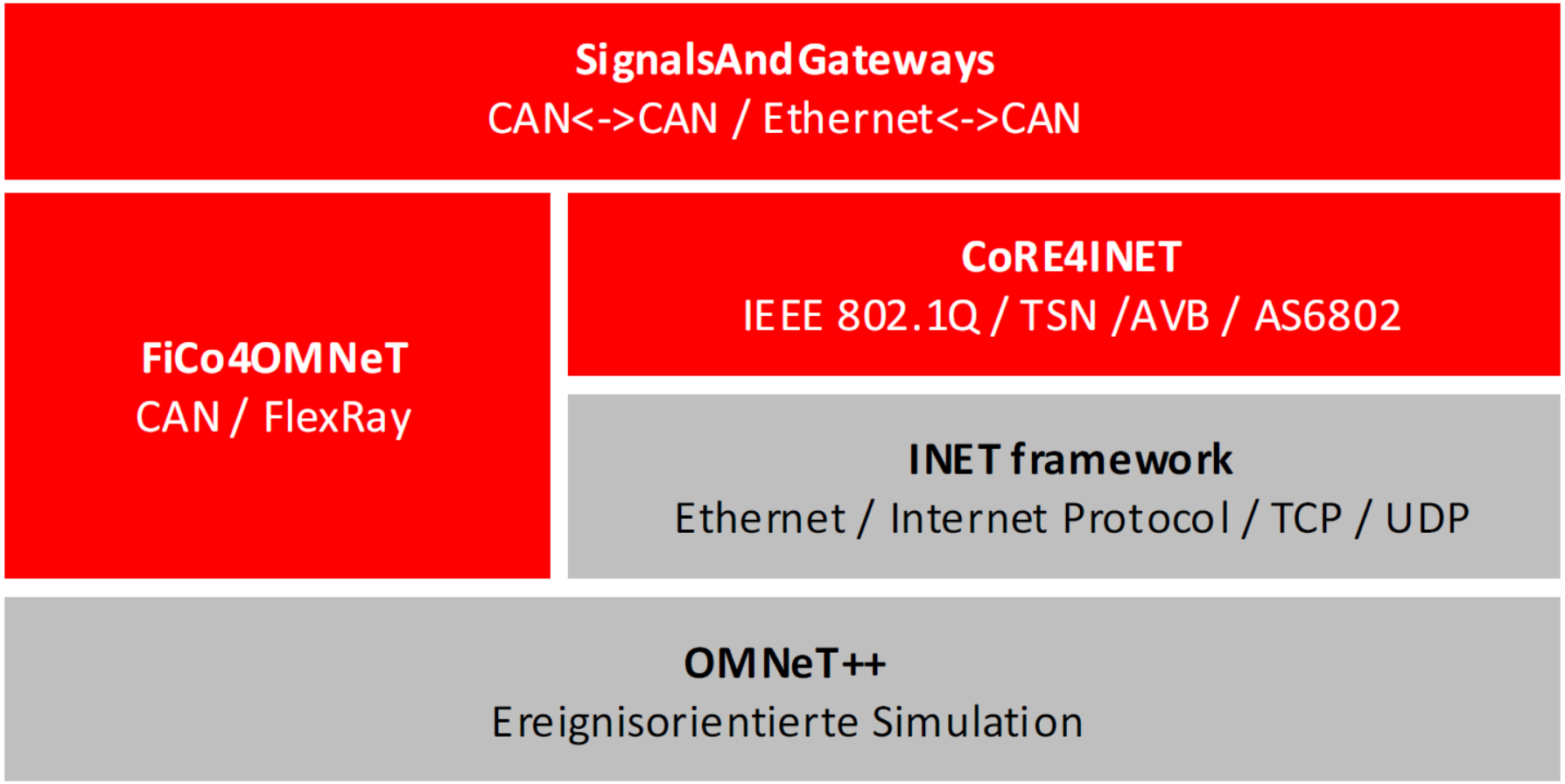
- Erleichtert Konfigurieren und Testen
- Auch Architekturen, für die keine Hardware existiert

Simulation realer Angriffe

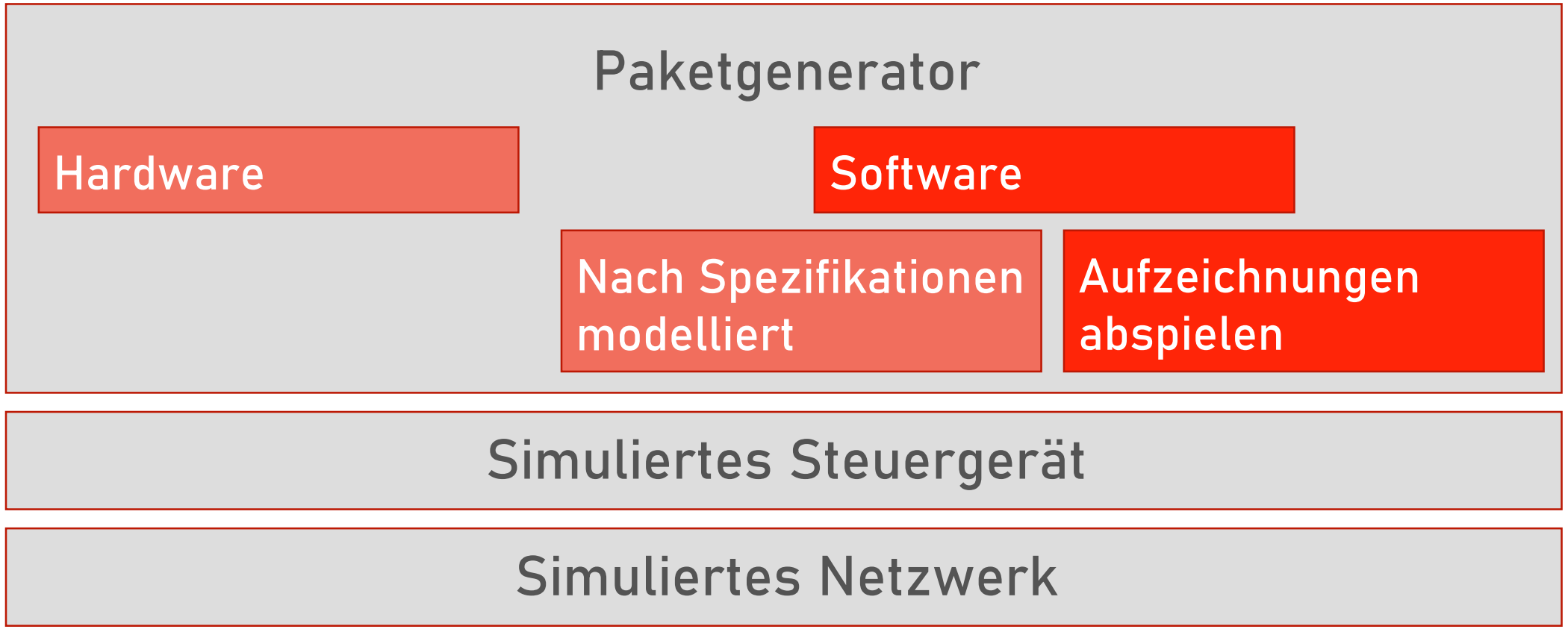
- Replizierbar
- Flexibel

Einbindung in die Simulation

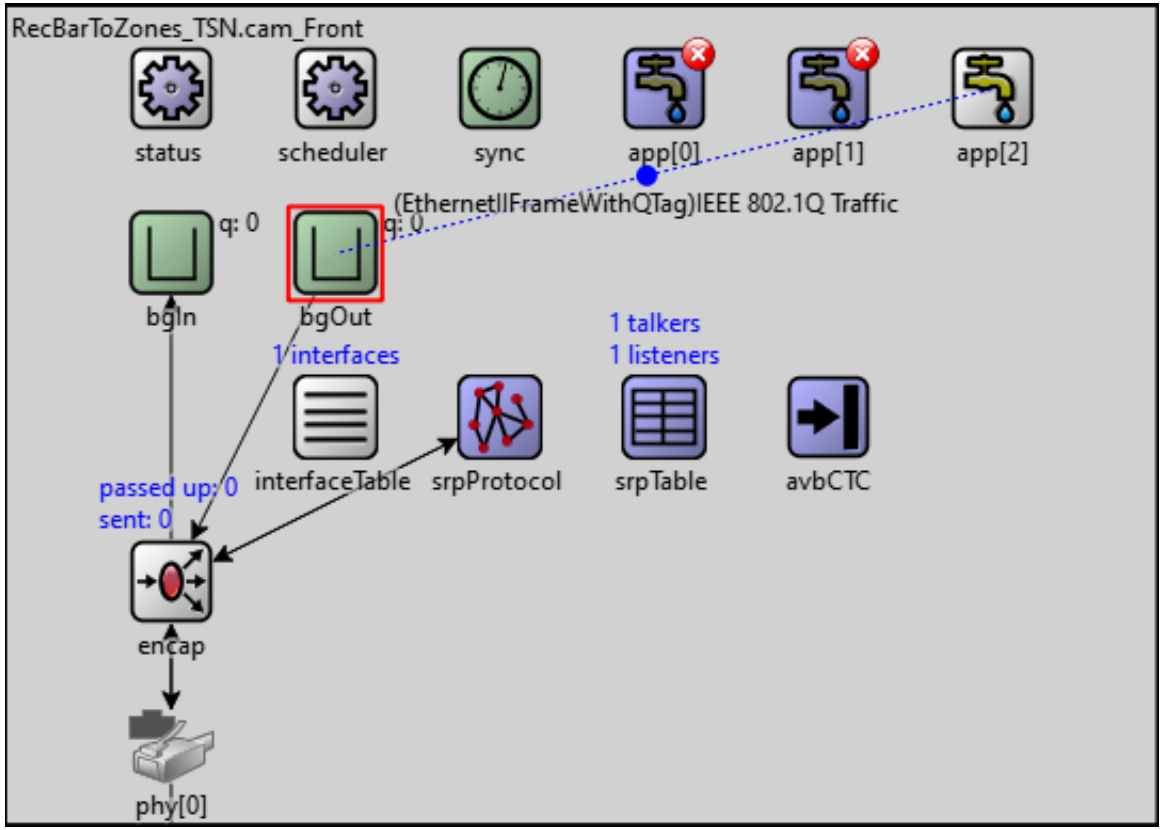
Verwendete Simulationsumgebung



Stimuligenerierung



Simuliertes Steuergerät



Paketgenerator – Datei einlesen

- Einspielen von Angriffen aus pcapng-Dateien
  - Weit verbreitet
  - Externe Angriffsmuster
  - Reproduzierbarkeit

Paketgenerator - Implementierung

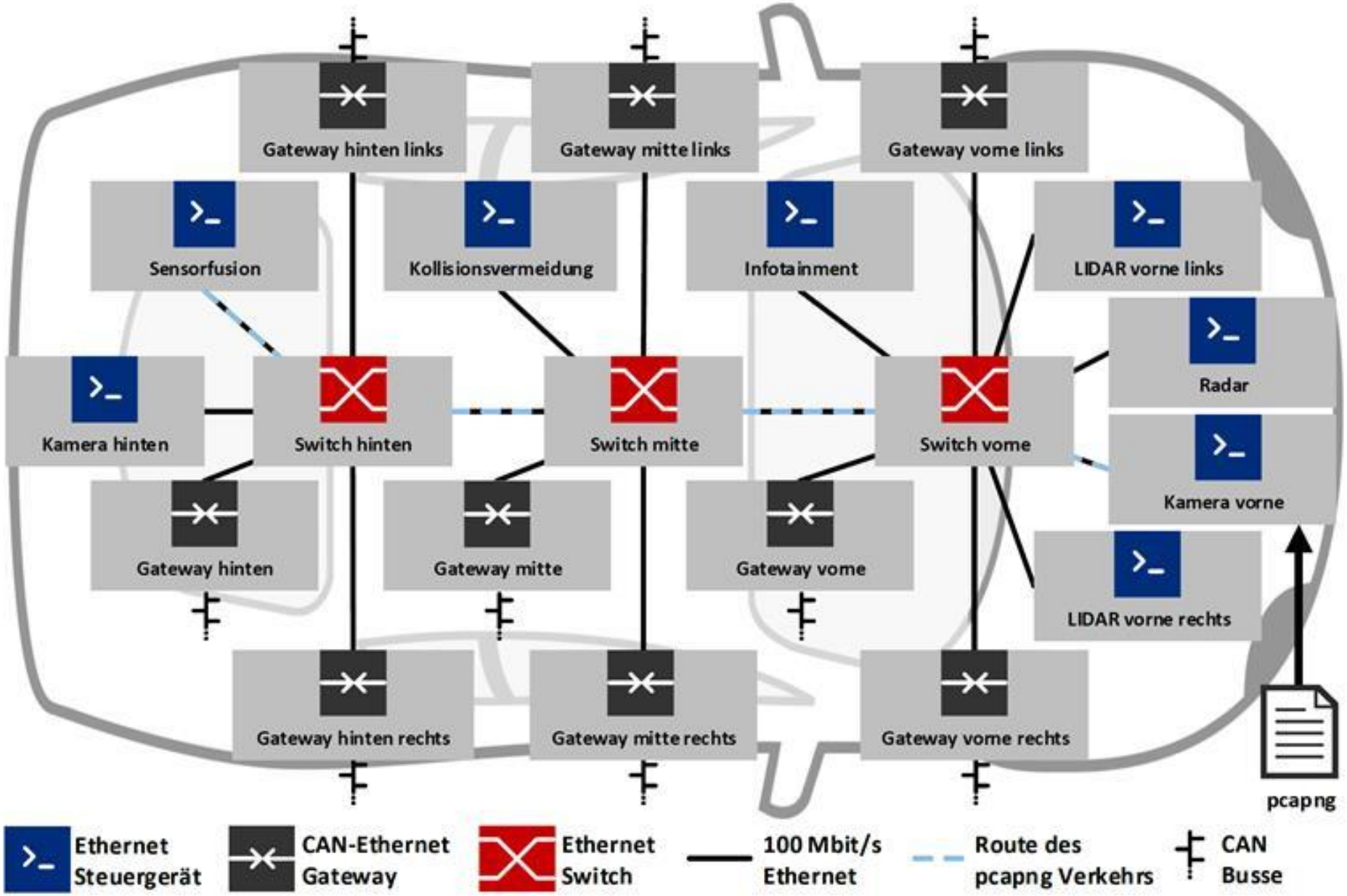
pcapng-Lesemodul

- Liest sequentiell und blockweise Dateien ein
- Schnittstellen für
  - Ethernet-Frames
  - Sendezeiten

Paketgenerator

- Einbindung in Steuergeräte:
  - Als einziger Generator
  - Gemeinsam mit anderen Generatoren
- Konfiguration:
  - Startzeit
  - Adressen
  - Vlan-Tag + Prioritäten

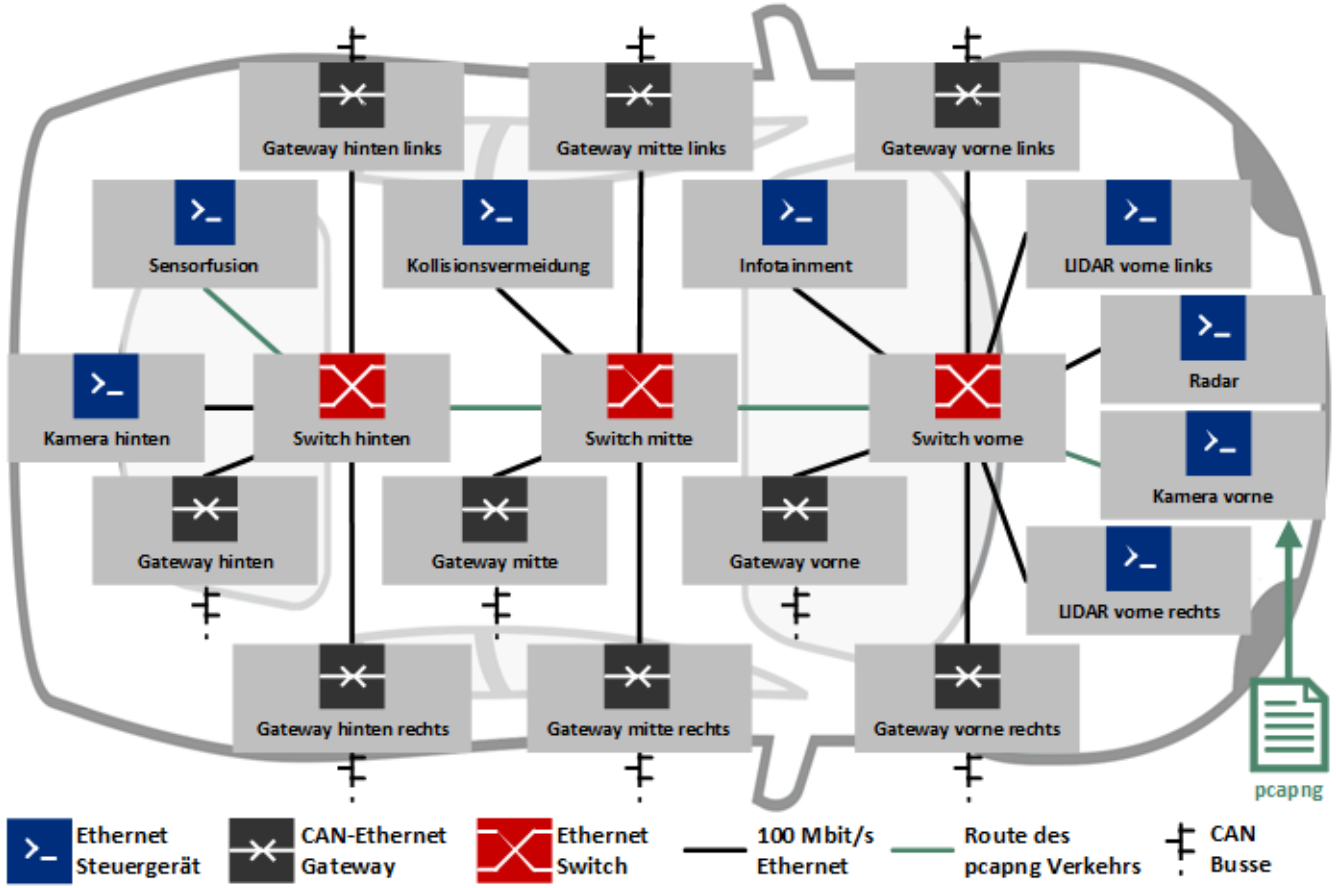
Fallbeispiel


Gateway hinten links
Gateway mitte links
Gateway vorne links
Sensorfusion
Kollisionsvermeidung
Infotainment
LIDAR vorne links
Radar
Kamera hinten
Switch hinten
Switch mitte
Switch vorne
Kamera vorne
Gateway hinten
Gateway mitte
Gateway vorne
LIDAR vorne rechts
Gateway hinten rechts
Gateway mitte rechts
Gateway vorne rechts
pcapng
Ethernet Steuergerät
CAN-Ethernet Gateway
Ethernet Switch
100 Mbit/s Ethernet
Route des pcapng Verkehrs
CAN Busse

pcapng-Dateien

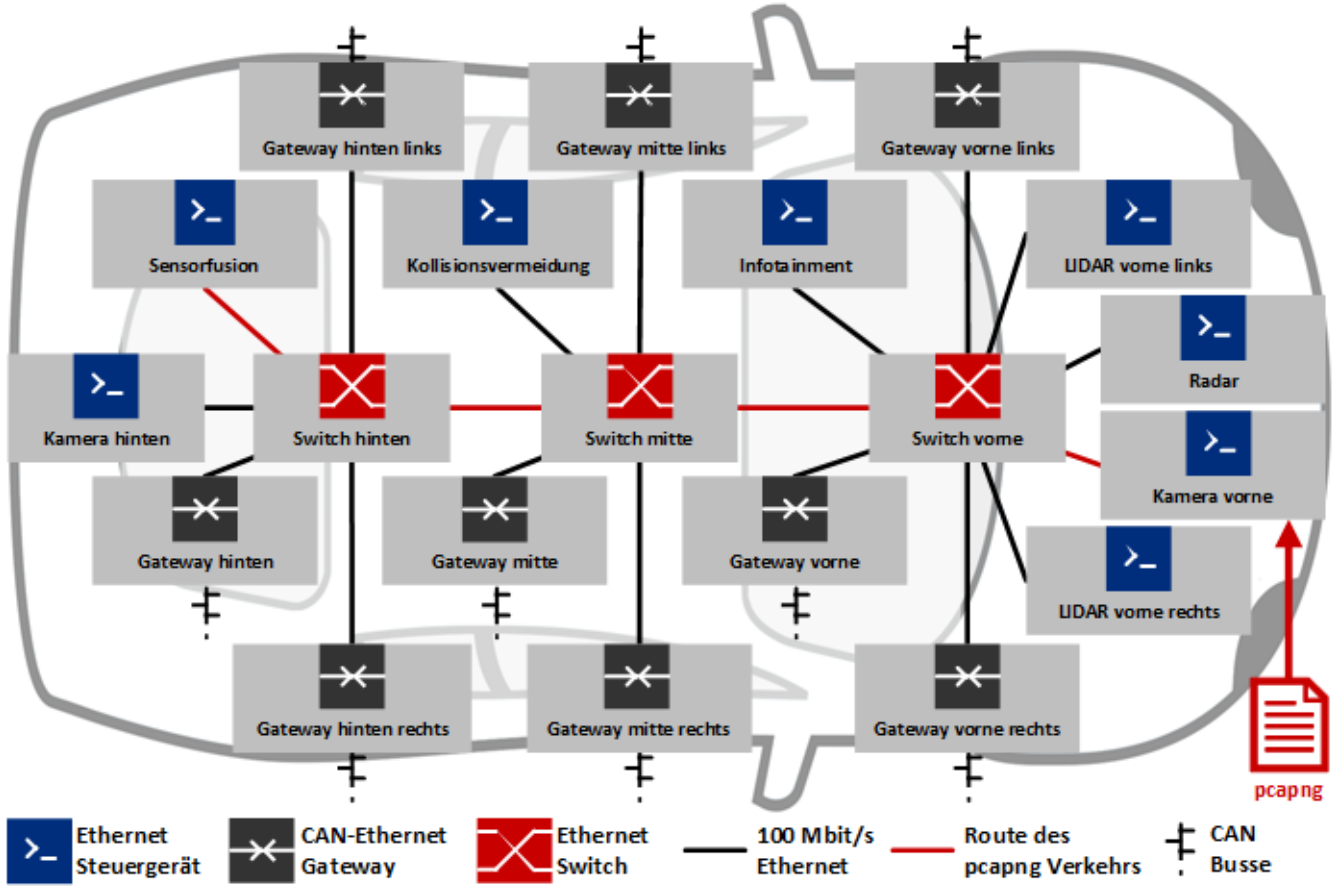
- Aufgezeichneter Datenverkehr aus Prototypnetzwerk
- Sender: vordere Kamera
- Empfänger: Sensorfusion
- Zwei Dateien (1 mit, 1 ohne Angriff)

pcapng-Datei ohne Angriff



- Videostrom

pcapng-Datei mit DoS-Angriff



- Videostrom
- Zusätzlich 67834 minimale UDP-Pakete/s

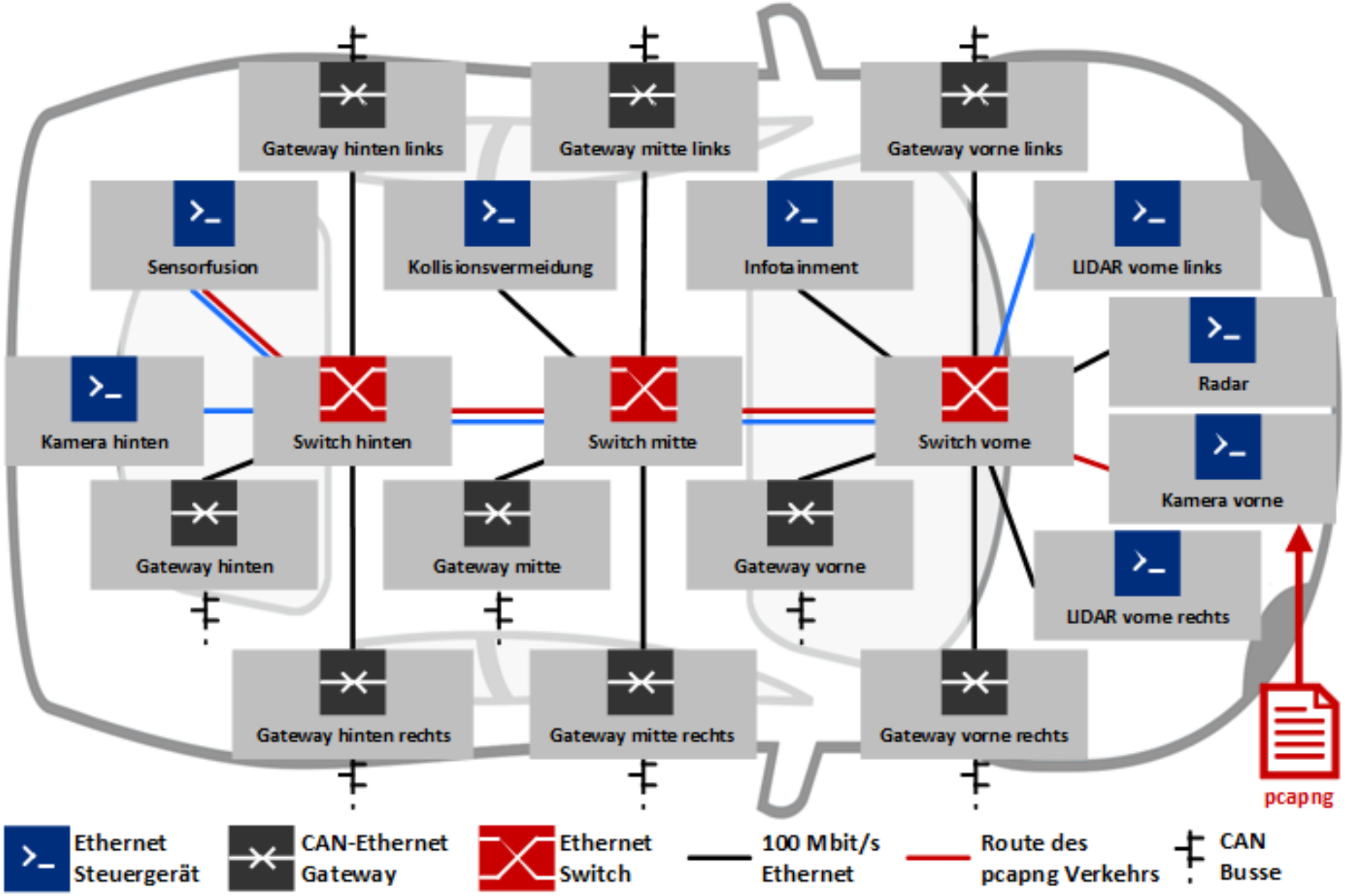
Konfiguration

- Kamera sendet nur Datenpakete aus pcapng-Dateien
- Datenpakete sind überpriorisiert
- Paketgeneratoren anderer Steuergeräte sind nach Spezifikation modelliert
- 500 ms Simulationsdauer

Ergebnisse

	Paketanzahl		Linkauslastung	
	Ohne Angriff	DoS-Angriff	Ohne Angriff	DoS-Angriff
Kamera – vorderer Switch	40	33814	0.88%	39.66%
Hinterer Switch - Sensorfusion	539	34304	13.09%	51.87%

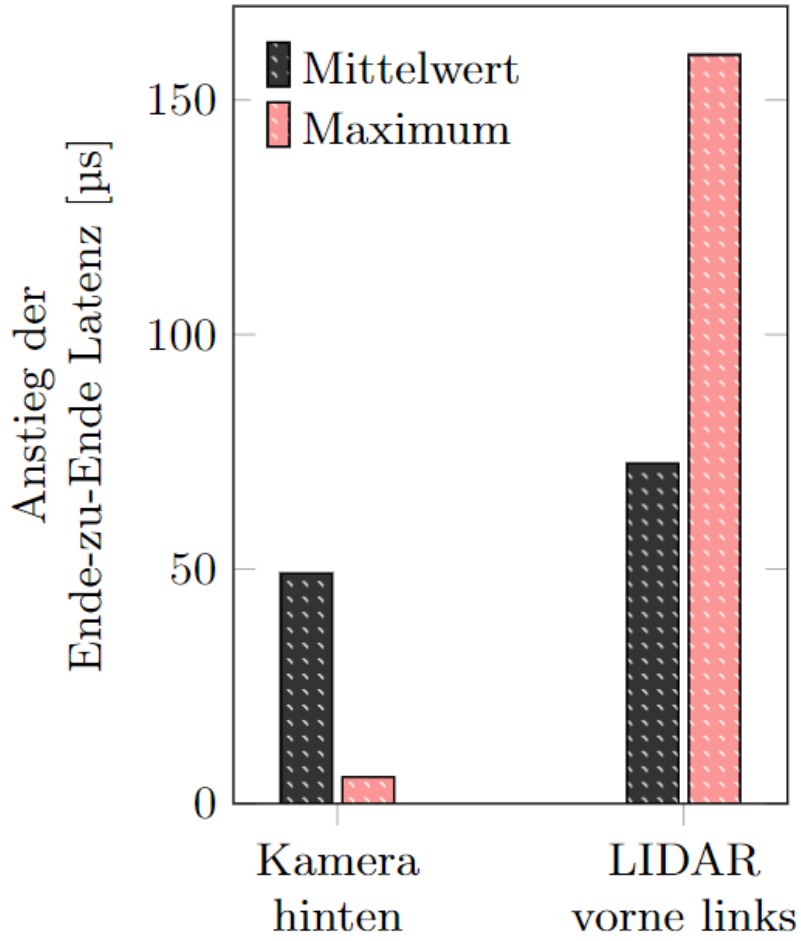
Keine Paketverluste


Gateway hinten links
Gateway mitte links
Gateway vorne links
Sensorfusion
Kollisionsvermeidung
Infotainment
LIDAR vorne links
Radar
Kamera hinten
Switch hinten
Switch mitte
Switch vorne
Kamera vorne
Gateway hinten
Gateway mitte
Gateway vorne
LIDAR vorne rechts
Gateway hinten rechts
Gateway mitte rechts
Gateway vorne rechts
pcapng
Ethernet Steuergerät
CAN-Ethernet Gateway
Ethernet Switch
100 Mbit/s Ethernet
Route des pcapng Verkehrs
CAN Busse

Ergebnisse

Anstieg der Ende-zu-Ende-Latenzen

- LIDAR vorne links - Sensorfusion:
  - Konkurriert an drei Links
- Hintere Kamera - Sensorfusion:
  - Konkurriert an einem Link



Fazit und Ausblick

Fazit

Simulation mit aufgezeichnetem Datenverkehr verwendbar für:

- Testen von Sicherheitsmechanismen
- Testen von Architekturen ohne verfügbare Hardware
- Simulation mit konkreteren Stimuli

Ausblick

- Erweiterung der Funktionalität:
  - Dateien periodisch einspielen
  - Filtern der Datenpakete

- Anwendung der Angriffssimulation:
  - Wirksamkeit von Mechanismen zur Anomalieerkennung untersuchen

Fragen?

Veröffentlichung unter: https://github.com/CoRE-RG

Danksagung:

Diese Arbeit wurde im Rahmen des SecVI-Projektes vom Bundesministerium für Bildung und Forschung gefördert.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung