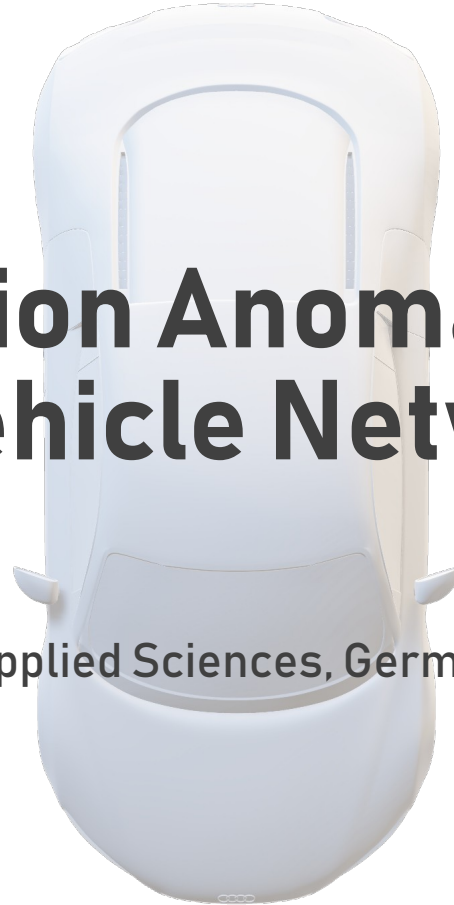


Detecting Communication Anomalies in Time-Sensitive In-Vehicle Networks

Status Report PhD Project @ TU Dresden - 21.10.2026

Philipp Meyer – philipp.meyer@haw-hamburg.de

Faculty of Computer Science, Hamburg University of Applied Sciences, Germany

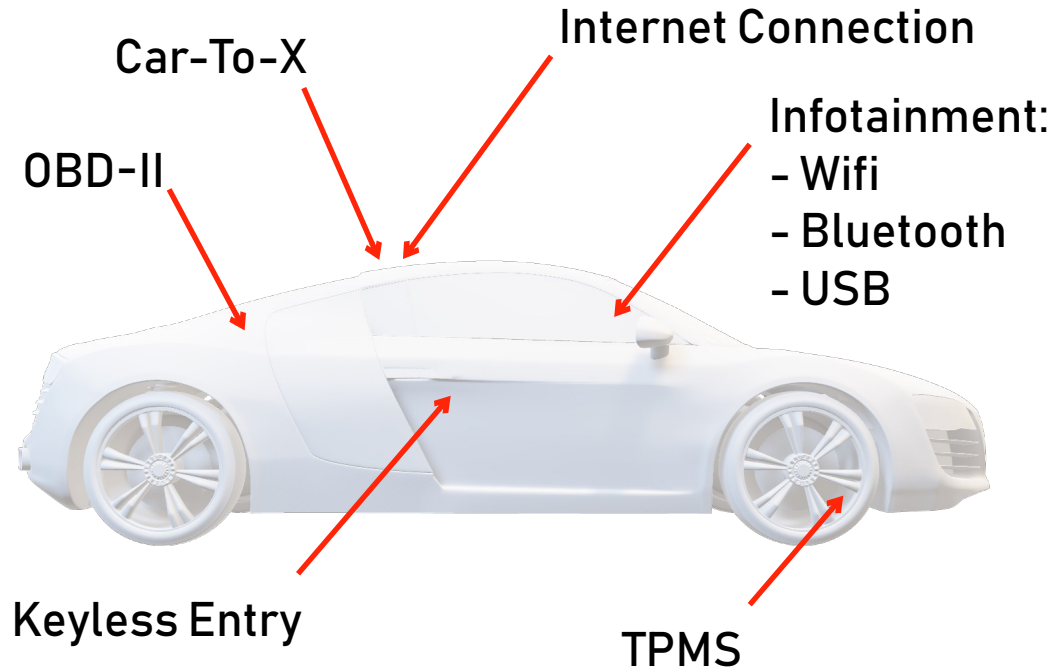


Vulnerability of In-Vehicle Networks

Why do vehicles need on-board network anomaly detection?

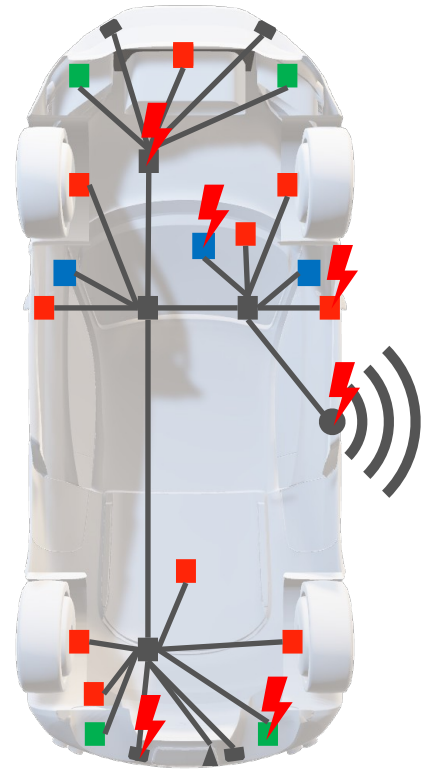


External Interfaces of Vehicles



In-Vehicle Networks (IVNs)

- New vehicles employ Ethernet backbones
- Interface are on-board network participants
- Attacks can spread over the network
- Remote threat to in-vehicle communication
- Increasing number of CVEs (>1500 since 2021) and new incidents (494 in 2025)
- 22% of those incidents involved car system manipulation and control of vehicle systems

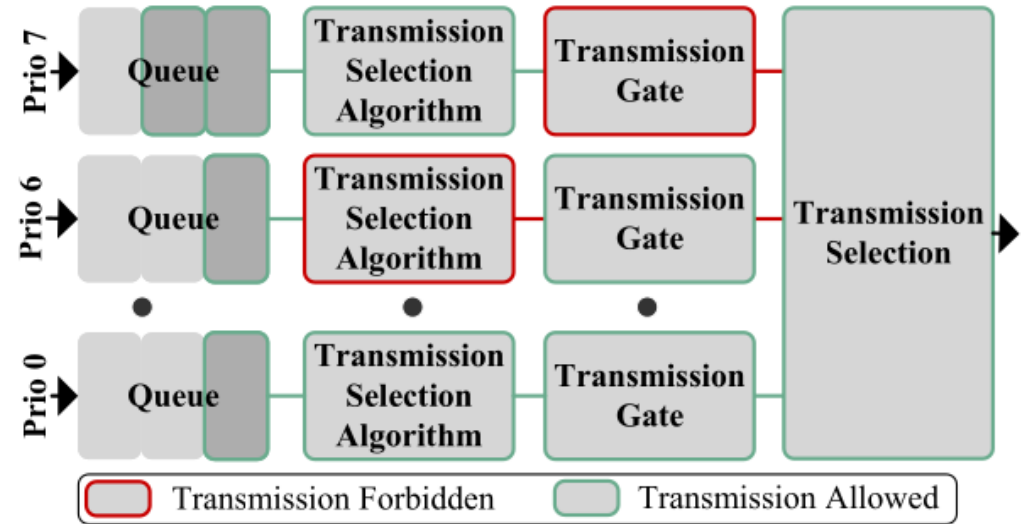


The Role of Anomaly Detection

- Key part of a comprehensive security architecture
- Detecting and reporting misbehavior:
 - Enables countermeasures
 - Uncovers complex relationships and root causes
 - Helps to converge risks to an acceptable level
- Return to a safe state after corruption

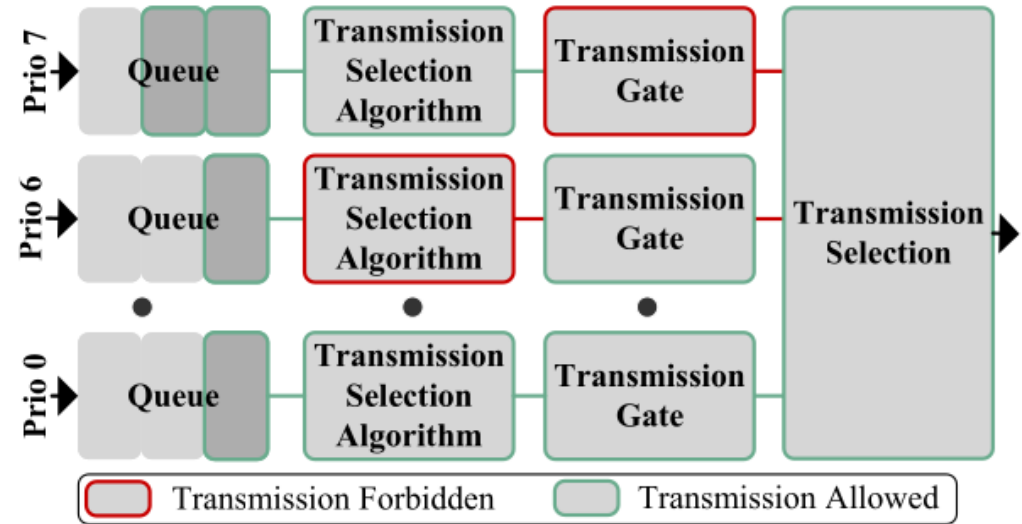
Time-Sensitive Networking (TSN)

- Implements QoS
- 8 traffic classes
- Priority selection
- Individual shaping
- Time division
- Concurrent impact



Promising Characteristics of TSN

- Shaping enforces distinct per-stream behavior
 - Time slots
 - Limited bursts
 - Upper bandwidth bounds
- Anomaly detection that “knows” per-stream behavior promises viable classification of deviations



Research Questions and Outline

1. What defines realistic in-vehicular networking data and what lessons can be learned from real-world prototypes?

2. How to build a systematic assessment framework integrating available data sources, a complete attack model, and detection systems?

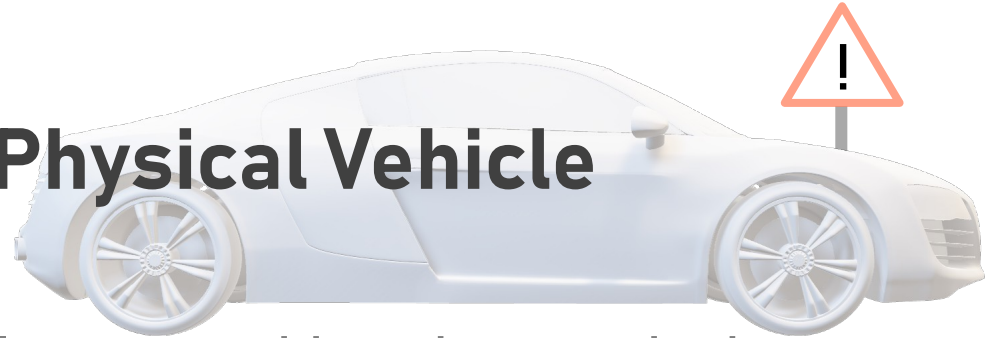
3. Can integrated indicators of TSN be exploited for anomaly detection?

4. Will behavioral metrics form clusters of benign TSN stream patterns for dedicated anomaly detection?

[3] P. Meyer, T. Häckel et al., “Demo: A Security Infrastructure for Vehicular Information Using SDN, Intrusion Detection, and a Defense Center in the Cloud,” in 2020 IEEE Vehicular Networking Conference (VNC) (IEEE VNC 2020), virtual, Dec. 2020, pp. 1–2.

[9] T. Häckel, P. Meyer et al., “A Multilayered Security Infrastructure for Connected Vehicles – First Lessons from the Field,” Presented at IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), May 2022.

Data and Lessons from Physical Vehicle Demonstrators



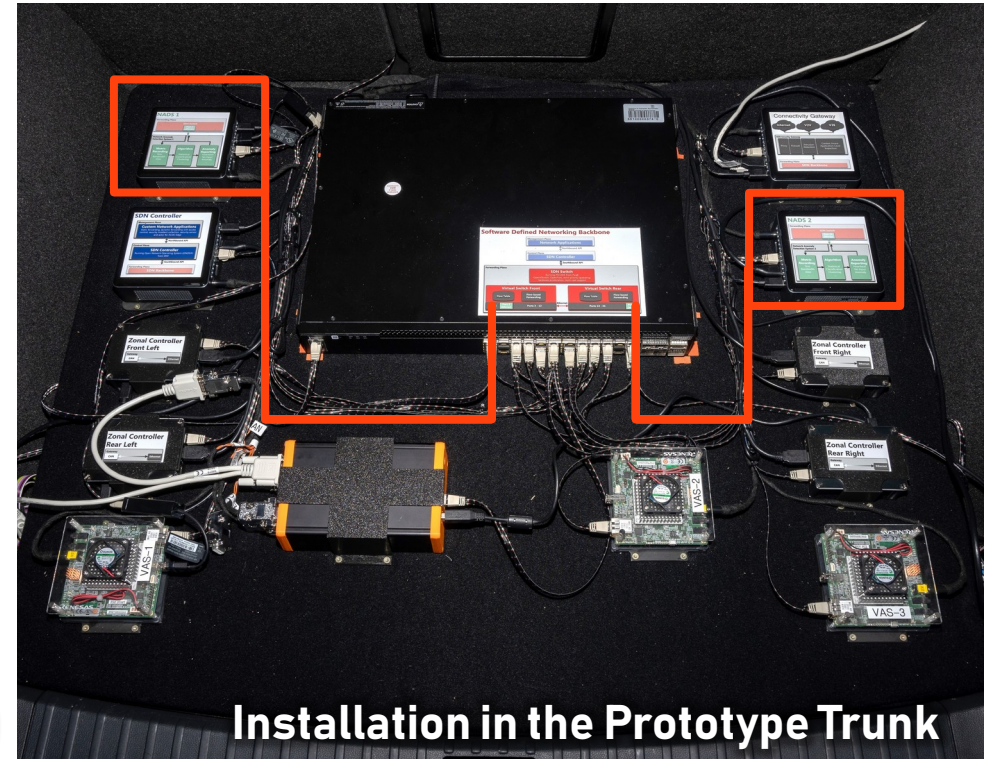
What defines realistic in-vehicular networking data and what lessons can be learned from real-world prototypes?

Idea

Access to future IVN architectures

- Combine a real IVN with future architectures
- Get realistic communication data
- First IVN anomaly detection evaluations
- Foundation for subsequent work

SecVI Demonstrators



Extracted Data

Formal:

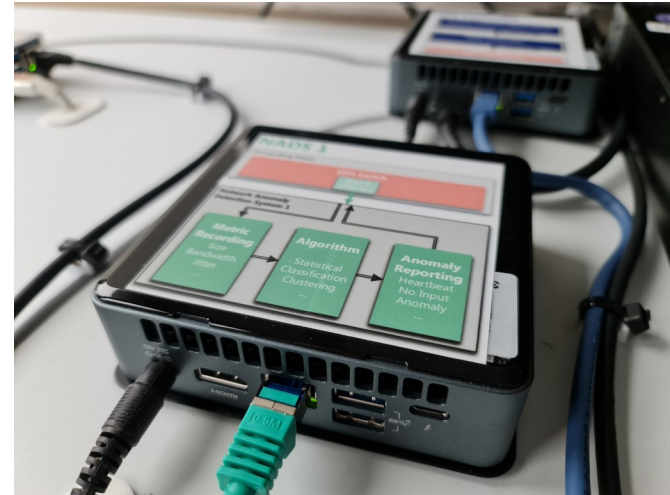
- Communication matrix
- Protocol stack
- Traffic characteristics

Experimental:

- CAN-Bus traces
- Sensor traces
- Ethernet mirror traces
- Evaluation results

Early Anomaly Detection Setup

- Selected streams
- One process per stream
- Bandwidth and avg frame size
- Public algorithms



Results from the Field

- 0.0009 – 0.02% FP rate during 8h operation
- 5 – 26% FN rate during Attacks
- Even low FP rates are too high for local countermeasures
- ~0.25s interval for fault detection
- ~0.3s interval for local countermeasures
- ≥ 2.7 s interval for remote countermeasures
- But local countermeasures are crucial for vehicle safety

Lessons Learned from the Field

- Evaluation is limited by available hardware
- Data is limited by available workforce
- Comparability limited by level of control
- Realism is still limited by artificial misbehavior

Summary

1. What defines realistic in-vehicular networking data and what lessons can be learned from real-world prototypes?
 - Pre-defined streams with heterogeneous QoS requirements
 - Highly valuable source for benign data
 - Deep knowledge about the environment and requirements
 - Minimizing FPs is crucial for local countermeasures
 - There are major hurdles for comprehensive evaluations

[4] P. Meyer, F. Korf, T. Steinbach, and T. C. Schmidt, "Simulation of Mixed Critical In-vehicular Networks," in Recent Advances in Network Simulation, A. Virdis and M. Kirsche, Eds., in EAI/Springer Innovations in Communication and Computing, Springer International Publishing, 2019.

[6] P. Meyer, T. Häckel, T. Lübeck, F. Korf, and T. C. Schmidt, "A Framework for the Systematic Assessment of Anomaly Detectors in Time-Sensitive Automotive Networks," in Proc. of the IEEE Vehicular Networking Conference (VNC), Kobe, Japan: IEEE, May 2024, pp. 57–64.

[8] S. Reider, P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "Integration realer Angriffe in simulierte Echtzeit- Ethernet-Netzwerke," in Echtzeit 2020, in Informatik aktuell. Wiesbaden: Springer Vieweg, Jan. 2021, pp. 51–60.

A Framework for the Systematic Assessment of In-Vehicle Network Anomaly Detectors

How to build a systematic assessment framework integrating available data sources, a complete attack model, and detection systems?



Idea

Simulation-based Data Generation

- Access to data beyond demonstrator access
- Projection of misbehavior to holistic classes
- As domain independent as possible
- Automatic labeling to enable large datasets
- Adaptable anomaly detection with comparable results
- Modular and extensible implementations

Limits of Available Datasets

- Datasets must match with the deployment environment
- Public dataset lack features of the IVN environment
 - Protocols
 - Attacks
 - Data
- Public datasets for IVNs focus on specific misbehavior
- Major challenge is the representation of attacks

Fundamental Link-Layer Anomalies

Valid



Manipulation



Elimination



Reordering



Injection

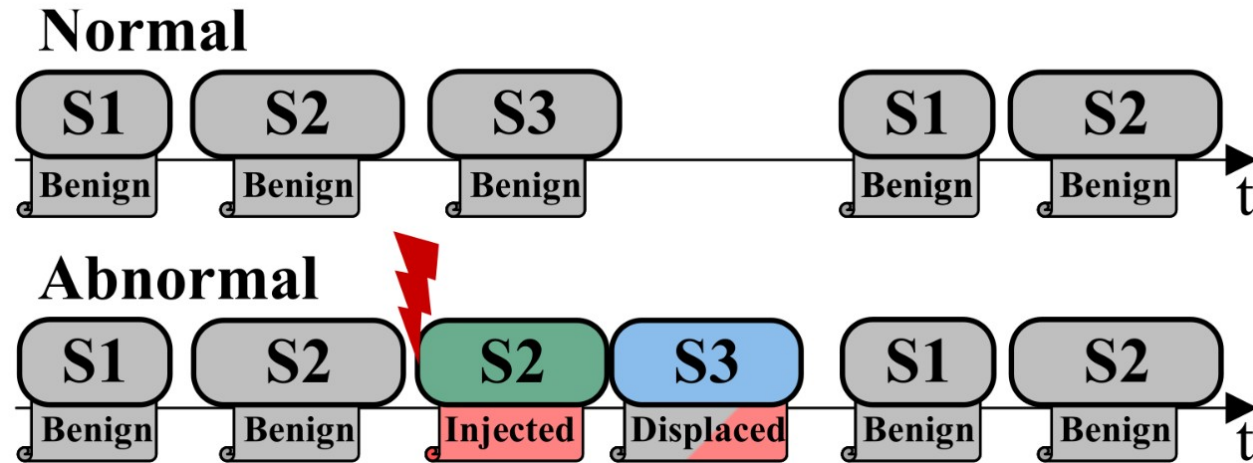


Rescheduling



- All anomalies are build of at least one fundamental anomaly

Cascading Effects of Anomalies



Open Source Building Blocks

Network Anomaly Detection System

new

PyNADS

Inputs (raw socket, scapy, pcapng, ...) / Filtering / Metrics (bandwidth, jitter, ...) /
Algorithms (isolation forrest, auto encoder, mean shift, ...) / Reporting

In-Vehicular Network Simulation

FiCo4OMNeT

CAN /
Flexray

extended

CoRE4INET

TTE / AVB / TSN / Anomalies

new

NIDSDatasetCreation

Anomalies / Labeling

INET 3.x

Ethernet / IP / TCP

INET 4.x

Ethernet / TSN / IP / TCP

OMNeT++

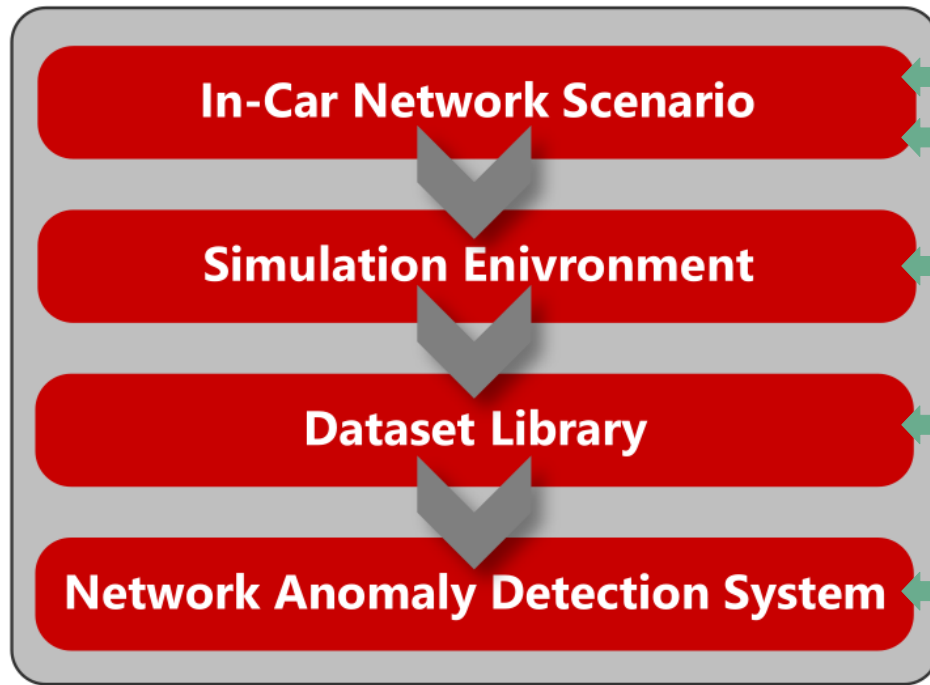
All Frameworks
available Open Source at



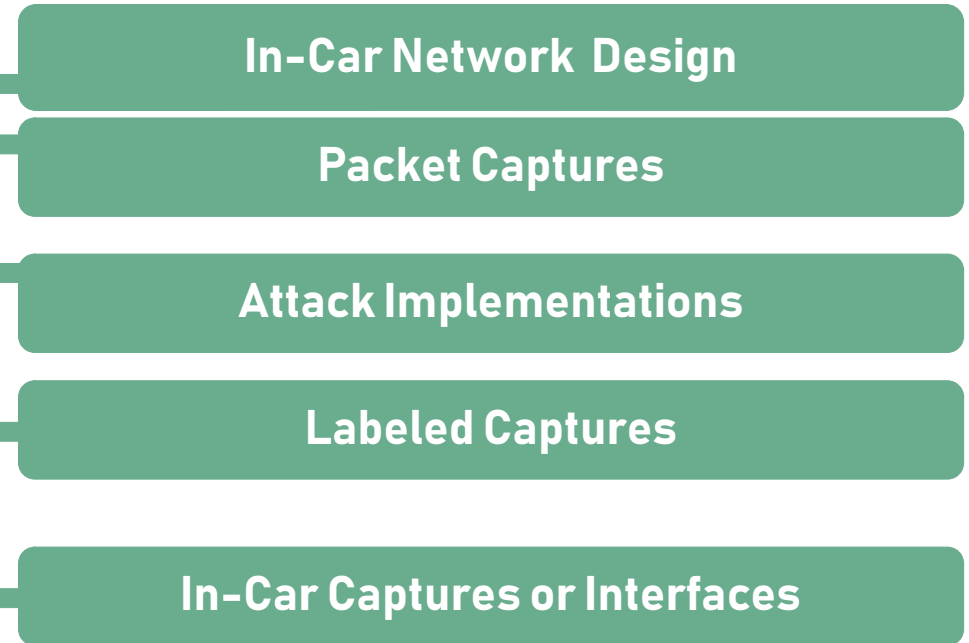
<https://github.com/CoRE-RG>

Assessment Framework

Workflow



Optional Real-world input



Labeled Network Traces

frame.interface_description contains eth0 && udp.port == 1200							
No.	Time	Source	Destination	Protocol	Length	Comment	
171389	1.997005	10.0.0.1	224.0.0.12	UDP	102	BENIGN	
171469	1.998005	10.0.0.1	224.0.0.12	UDP	102	BENIGN	
171553	1.999009	10.0.0.1	224.0.0.12	UDP	102	BENIGN	
171906	2.001004	10.0.0.1	224.0.0.12	UDP	102	BENIGN - switchFrontLeft_SManualSteer_DELAY	
171991	2.002006	10.0.0.1	224.0.0.12	UDP	102	BENIGN - switchFrontLeft_SManualSteer_DELAY	
172080	2.003023	10.0.0.1	224.0.0.12	UDP	102	DELAYED - switchFrontLeft_SManualSteer_DELAY	
172154	2.004003	10.0.0.1	224.0.0.12	UDP	102	BENIGN RECOVERED - switchFrontLeft_SManualSteer_DELAY	
172160	2.004009	10.0.0.1	224.0.0.12	UDP	102	BENIGN - switchFrontLeft_SManualSteer_DELAY	
172243	2.005008	10.0.0.1	224.0.0.12	UDP	102	BENIGN - switchFrontLeft_SManualSteer_DELAY	
172325	2.006009	10.0.0.1	224.0.0.12	UDP	102	BENIGN - switchFrontLeft_SManualSteer_DELAY	
> Packet comments							
> Frame 172080: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface eth0, id 3 (inbound)							
> Ethernet II, Src: 0a:aa:00:00:00:17 (0a:aa:00:00:00:17), Dst: IPv4mcast_0c (01:00:5e:00:00:0c)							
> 802.1CB Redundancy Tag, SEQ: 2002							
> 802.1Q Virtual LAN, PRI: 6, DEI: 0, ID: 1							
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 224.0.0.12							
> User Datagram Protocol, Src Port: 1027, Dst Port: 1200							
> Data (46 bytes)							

Summary

2. How to build a systematic assessment framework integrating available data sources, a complete attack model, and detection systems?

- Combining real-world input with simulation
- Fundamental link-layer anomalies
- Automated labeling
- Modular network anomaly detection framework

[2] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, “DoS Protection through Credit Based Metering – Simulation Based Evaluation for Time-Sensitive Networking in Cars,” in Proceedings of the International OMNeT++ Community Summit, M. Zongo et al. Eds., in EPiC Series in Computing, vol. 66. EasyChair, Sep. 2019, pp. 52–59.

[4] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, “Network Anomaly Detection in Cars based on Time-Sensitive Ingress Control,” in Proc. of the IEEE Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada: IEEE Press, Oct. 2020.

[5] P. Meyer, T. Häckel, S. Reider, F. Korf, and T. C. Schmidt, “Network Anomaly Detection in Cars: A Case for Time-Sensitive Stream Filtering and Policing,” Computer Networks, vol. 255, no. 110855, pp. 1–13, Dec. 2024,

[7] P. Meyer, T. Lübeck, T. Häckel, F. Korf, and T. C. Schmidt, “Anomaly Detection in Real-Time Networks Using Asynchronous Traffic Shaping,” in Proc. of the IEEE Vehicular Technology Conference (VTC2025-Fall), Chengdu, China: IEEE, Oct. 2025, pp. 1–7

[10] T. Lübeck, P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, “Asynchronous Traffic Shaping and Redundancy: Avoiding Unbounded Latencies in in-Car Networks,” in Proc. of the 16th IEEE Vehicular Networking Conference (VNC), Porto, Portugal: IEEE, Jun. 2025, pp. 1–8

An Integrated Detection Approach for TSN

Can integrated indicators of TSN be exploited for anomaly detection?



Idea

Integrated TSN Monitoring

- Use internal statistics of TSN protocols that handle ingress traffic in switches:
 - Per-Stream Filtering and Policing (PSFP)
 - Asynchronous Traffic Shaping (ATS)
- Re-use existing configurations when possible
- Target indicators that are free of false-positives

Open Source Building Blocks

Network Anomaly Detection System

new

PyNADS

Inputs (raw socket, scapy, pcapng, ...) / Filtering / Metrics (bandwidth, jitter, ...) /
Algorithms (isolation forrest, auto encoder, mean shift, ...) / Reporting

In-Vehicular Network Simulation

FiCo4OMNeT

CAN /
Flexray

extended

CoRE4INET

TTE / AVB / TSN / Anomalies

new

NIDSDatasetCreation

Anomalies / Labeling

INET 3.x

Ethernet / IP / TCP

INET 4.x

Ethernet / TSN / IP / TCP

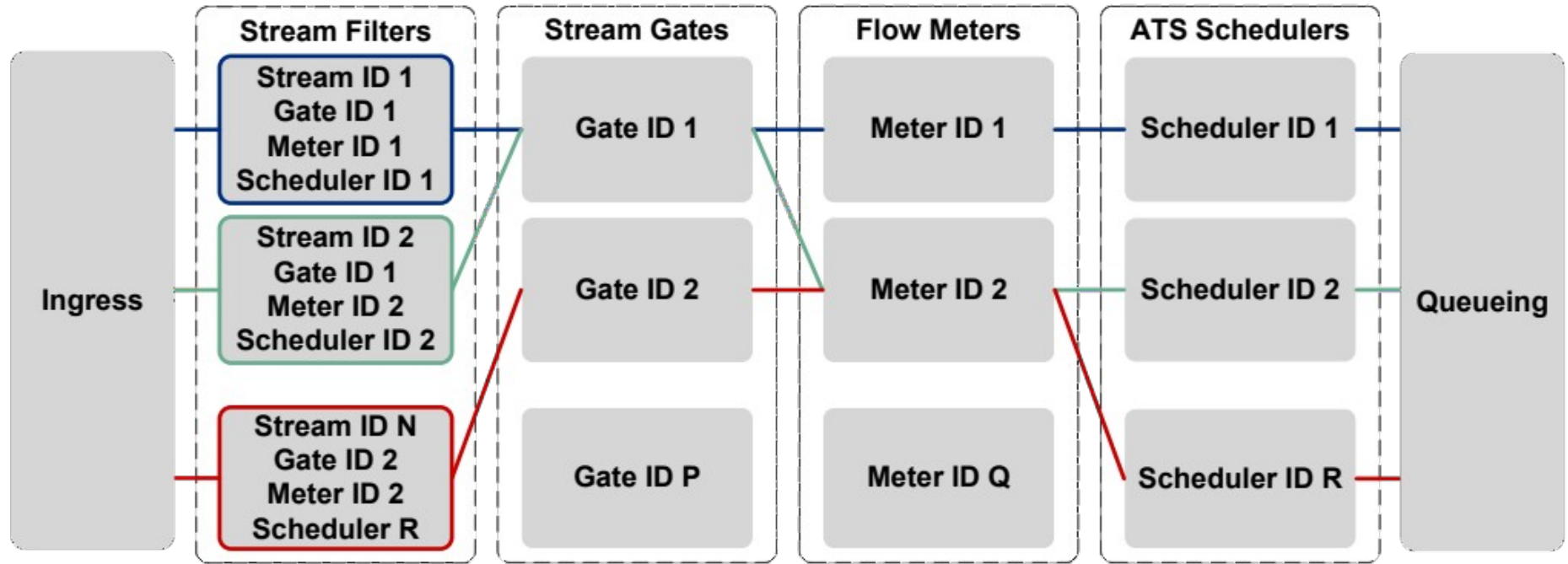
OMNeT++

All Frameworks
available Open Source at

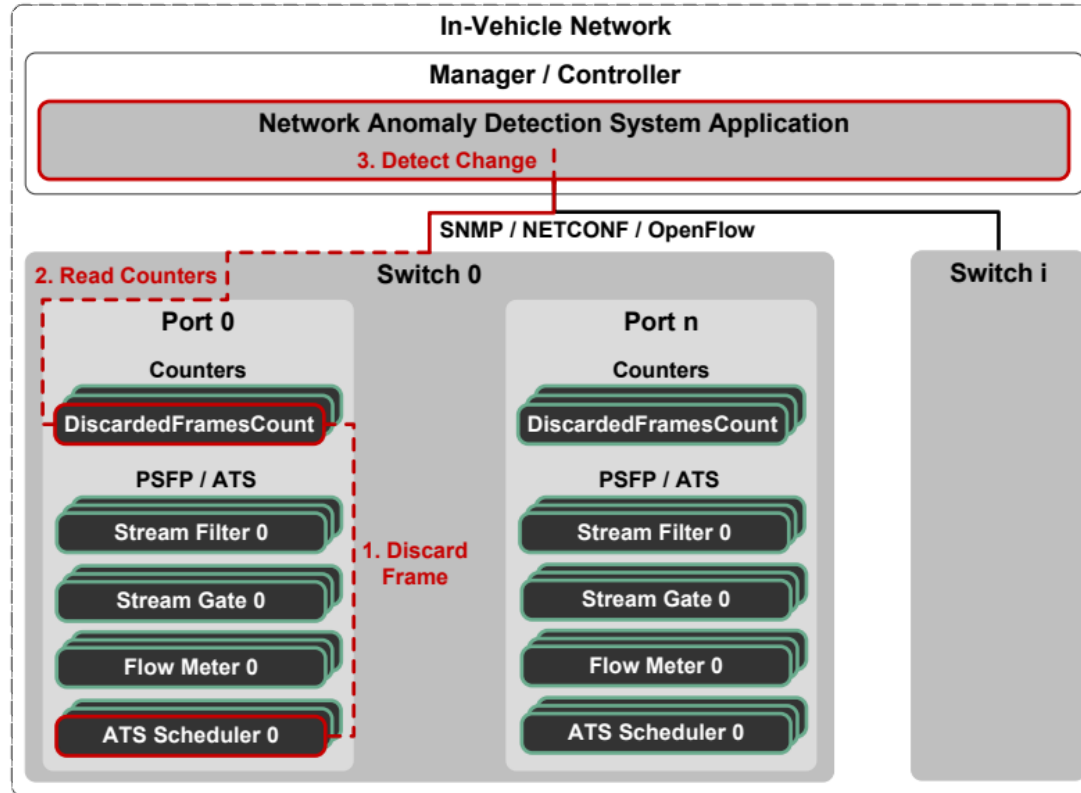


<https://github.com/CoRE-RG>

Per-Stream Filtering and Policing and Asynchronous Traffic Shaping

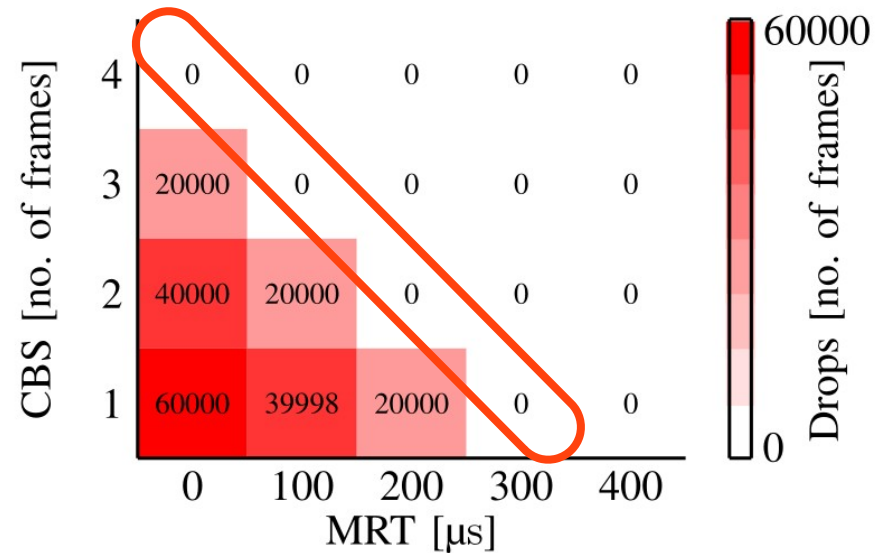


Concept

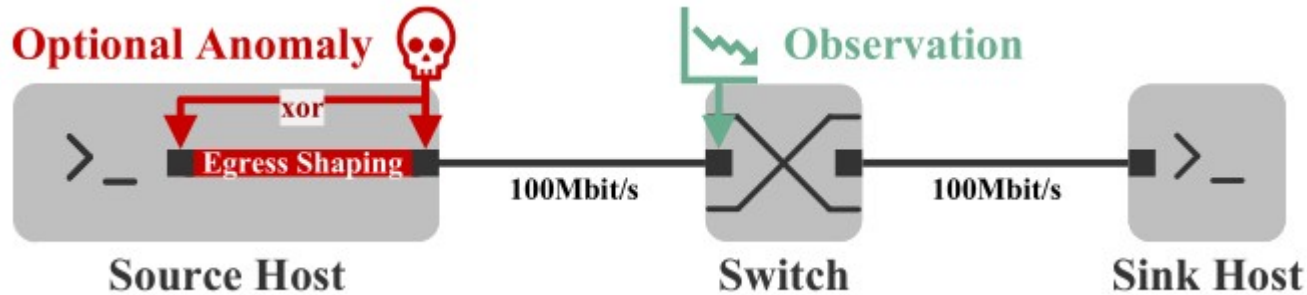


Correct Configuration

- Precise TSN configuration
- Mostly required for QoS
- Dependent on IVN design



Microbenchmarks



- Three observed streams
- Five traffic classes (including background traffic)
- Fundamental anomalies at two layers

Microbenchmarks

Result Matrices

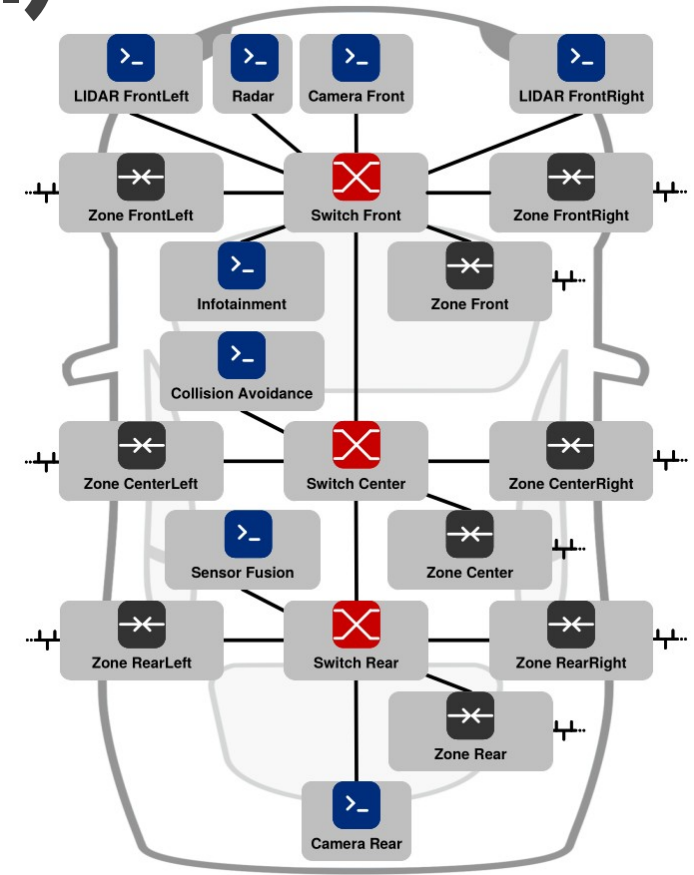
Traffic pattern	Elimination			Injection			Manipulation			Reordering			Rescheduling		
	TP	FN	R	TP	FN	R	TP	FN	R	TP	FN	R	TP	FN	R
Application Layer Corruption															
Timed control traffic	6645	1	1.0	6818	2598	0.72	5356	1254	0.81	1	6634	0.0	4	6621	0.0
Shaped data stream	22	7986	0.0	9180	228	0.98	7266	741	0.91	3420	4588	0.43	1977	6030	0.25
Prioritized CAN tunnel	0	6664	0.0	9145	263	0.97	6489	173	0.97	0	6659	0.0	0	6657	0.0
Link Layer Corruption															
Timed control traffic	5656	0	1.0	8701	706	0.92	4606	1073	0.81	5617	0	1.0	4382	1253	0.78
Shaped data stream	28	7980	0.0	9083	325	0.97	7270	725	0.91	1983	6025	0.25	2356	5639	0.29
Prioritized CAN tunnel	0	5616	0.0	9204	207	0.98	5584	165	0.97	0	5696	0.0	0	5692	0.0

Microbenchmarks Results

- Elimination hard to detect
 - ▶ Exclusive time slots enable detection
- Egress shaping masks anomalies
 - ▶ ATS deployment prevents masking
- Tendency to anomalies that increase resources
- Not a single FP detection in any evaluation

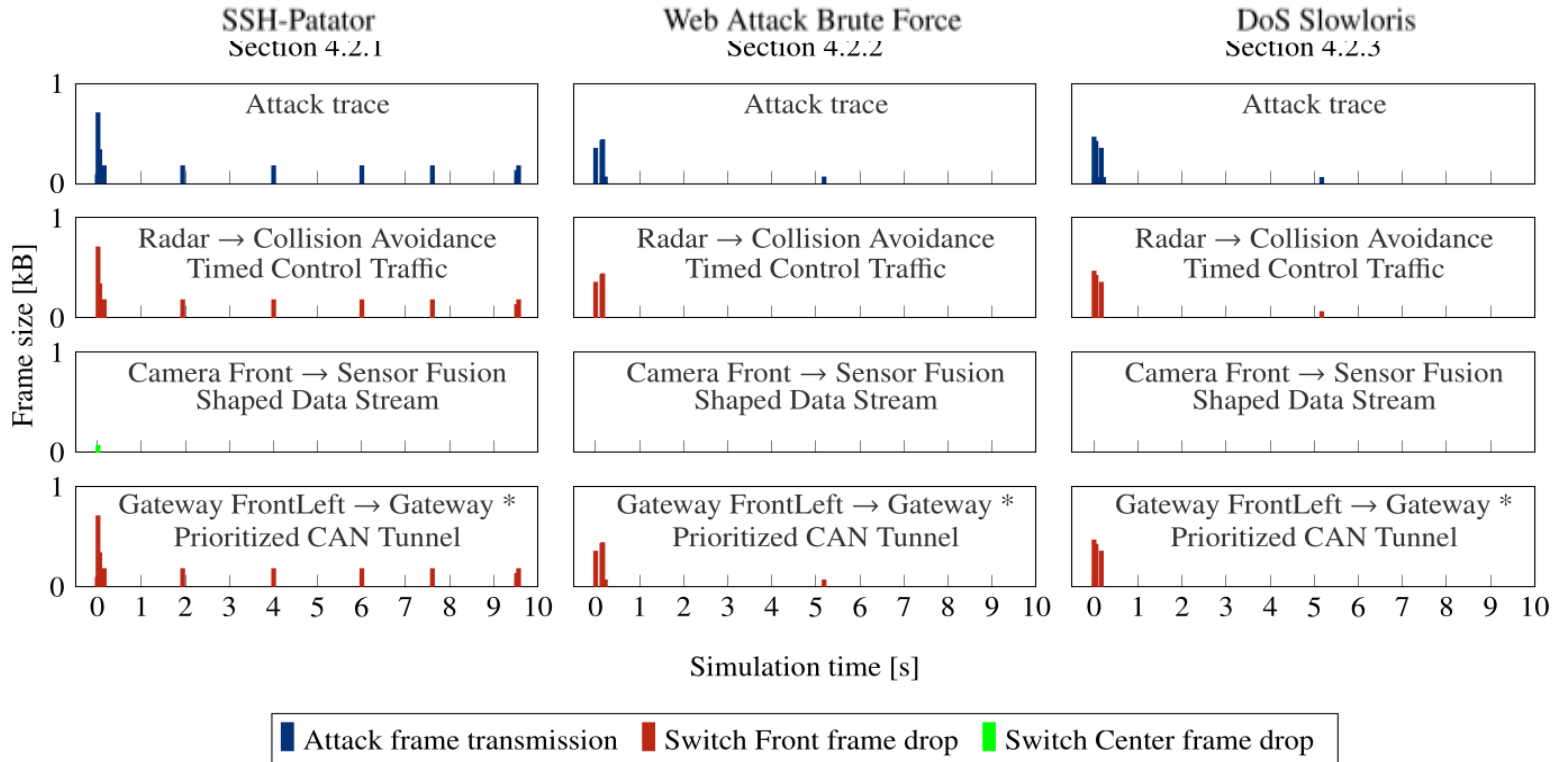
IVN Case Studies (1st Gen.)

- 207 streams
- 6 traffic classes
- 3 switches with 20 interfaces
- PSFP deployed on all interfaces
- Zero FPs during benign operation



IVN Case Studies

PSFP Frame Drops with Attacks



Summary

3. Can integrated indicators of TSN be exploited for anomaly detection?

- Zero false positives maximize report quality
- No link monitoring or classification algorithm
- Tendency to anomalies with resource overuse
- Combines TSN design with security requirements

[11] T. Häckel, P. Meyer, F. Korf, and T. C. Schmidt, “Securing Future In-Vehicle Networks: Monitoring and Control for Ethernet Backbones,” in Engineering Safe and Trustworthy Cyber Physical Systems: Essays Dedicated to Werner Damm on the Occasion of His 71st Birthday, M. Fränzle, J. Niehaus, and B. Westphal, Eds., Cham: Springer Nature Switzerland, 2026, pp. 163–182.

[?] P.Meyer et al, “One Model, Many Streams: Clustering-Based Anomaly Detection for Time-Sensitive In-Vehicle Networks”, in preparation for submission

A Dedicated Monitoring Approach via Clustering of TSN Stream Behaviors

Will behavioral metrics form clusters of benign TSN stream patterns for dedicated anomaly detection?



Idea

Record per-Stream Behavior

- Learn complete IVN behavior without configuration
- Record statistics that describe per-stream pattern
- Clusters streams by behavior
- Detect misbehavior of individual streams

Open Source Building Blocks

Network Anomaly Detection System

new

PyNADS

Inputs (raw socket, scapy, pcapng, ...) / Filtering / Metrics (bandwidth, jitter, ...) /
Algorithms (isolation forrest, auto encoder, mean shift, ...) / Reporting

In-Vehicular Network Simulation

FiCo4OMNeT
CAN /
Flexray

extended

CoRE4INET
TTE / AVB / TSN / Anomalies

new

NIDSDatasetCreation
Anomalies / Labeling

INET 3.x
Ethernet / IP / TCP

INET 4.x
Ethernet / TSN / IP / TCP

OMNeT++

All Frameworks
available Open Source at

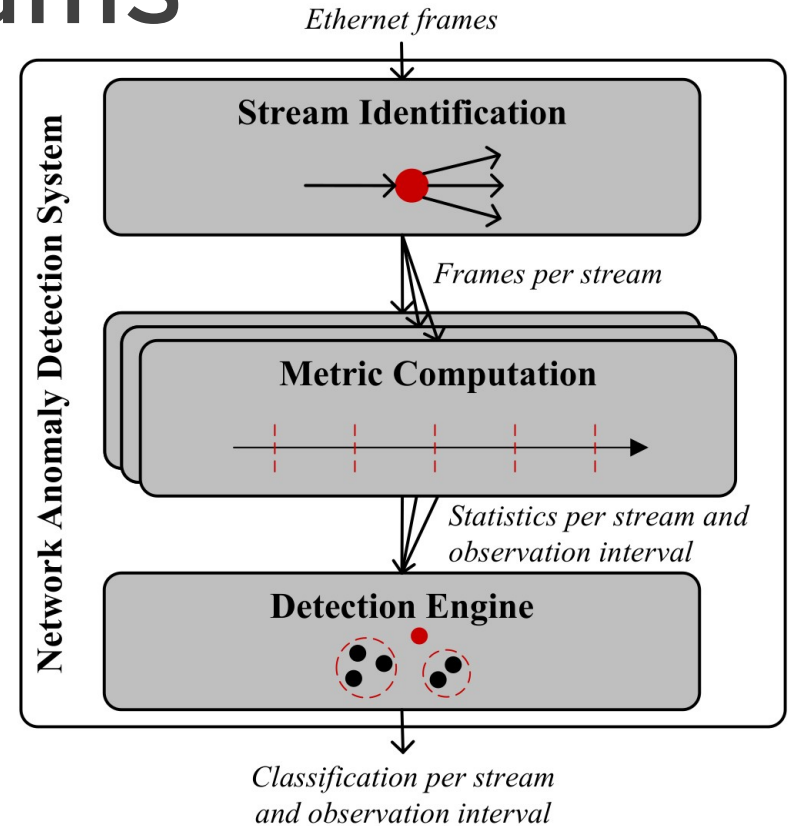


<https://github.com/CoRE-RG>

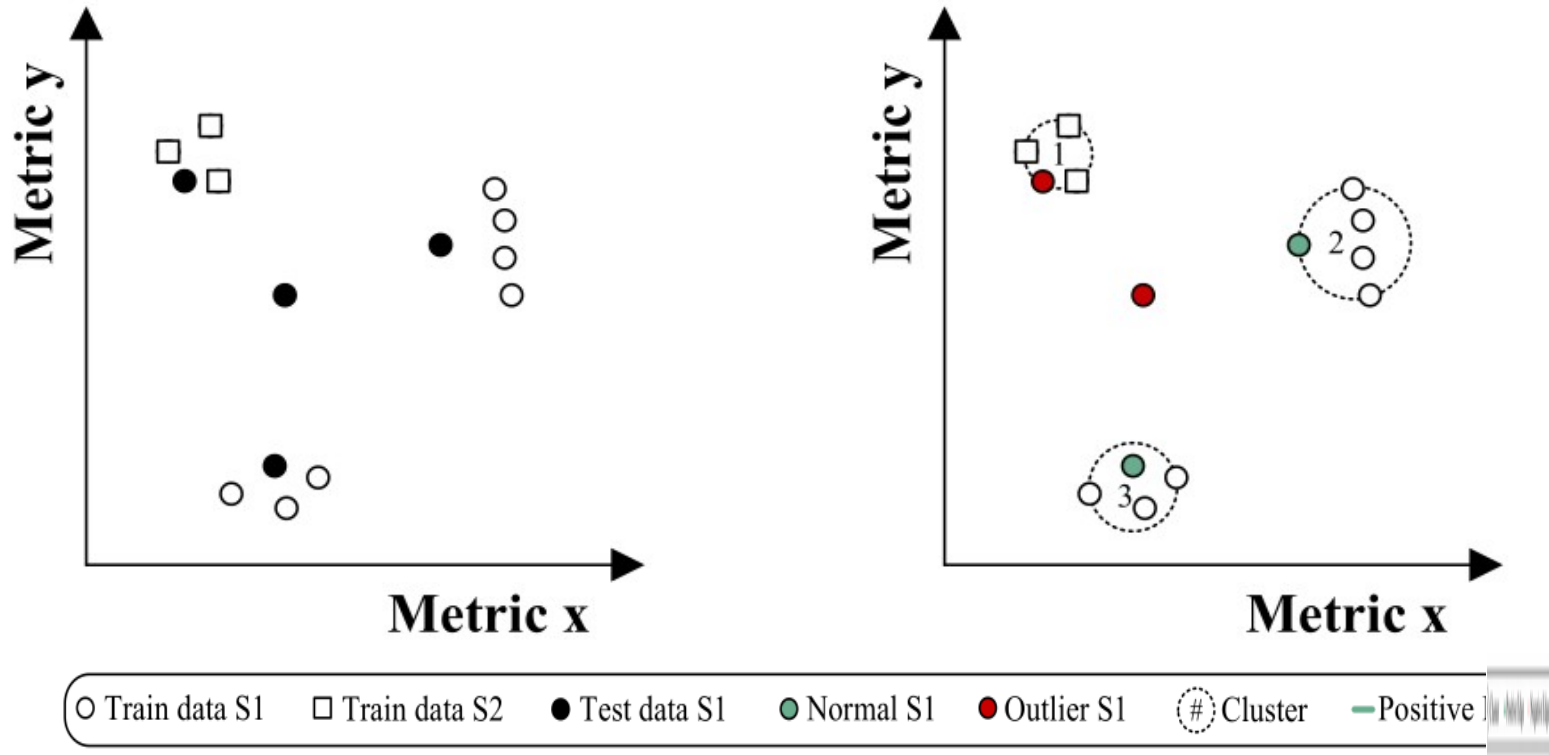
Concept

One Model, Many Streams

- Per-stream recording
- Uniform recording intervals
 - Min. Max. Avg. Dev. Burst Count
 - Min. Max. Avg. Dev. Frame Size
 - Min. Max. Avg. Dev. Inter Arrival Time
- Unified detection engine



Clustering of Behavioral Metrics Detection Engine

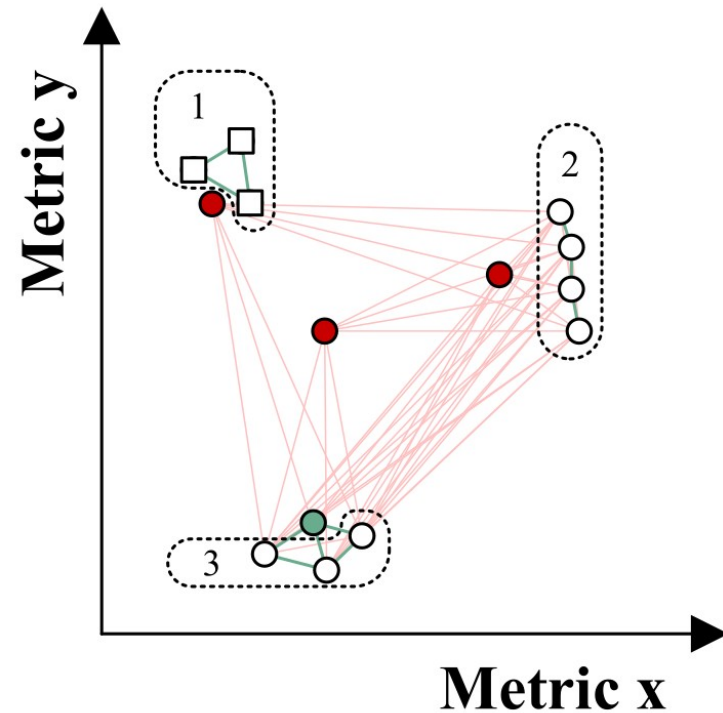
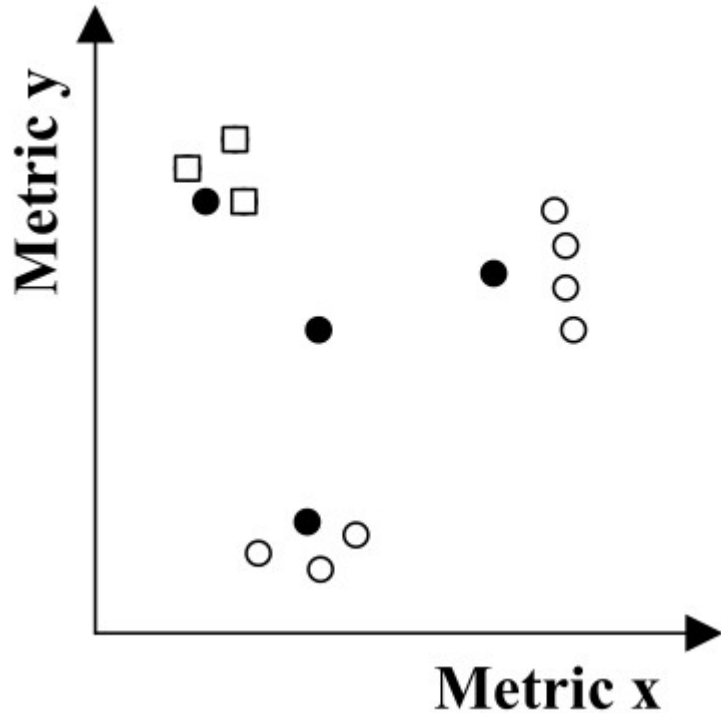


Graph-based Correlation Clustering

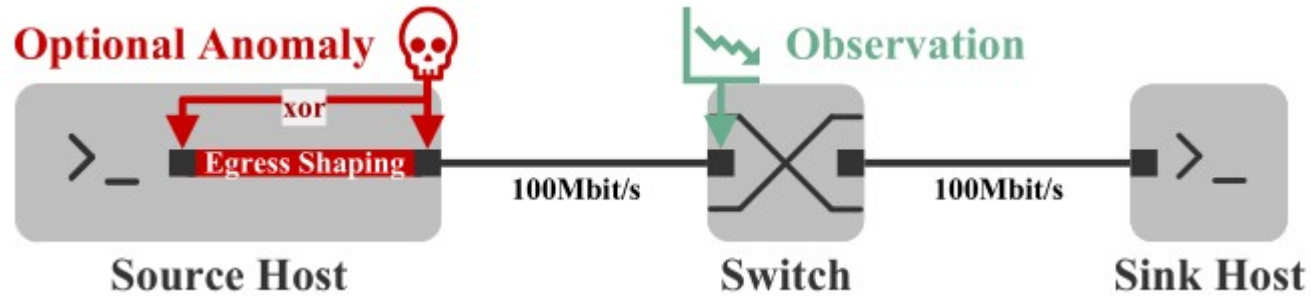
- 1) Record 12-dimensional behavior per stream and interval
- 2) Edges between data points of the same streams
- 3) Distance as similarity measure
- 4) Convert distances to signed weights
- 5) Multicut separates behavior into clusters
- 6) If sum of weights to nodes for each stream cluster < 0
→ Anomaly

Clustering of Behavioral Metrics

Correlation Clustering



Microbenchmarks



Microbenchmarks

Result Matrices

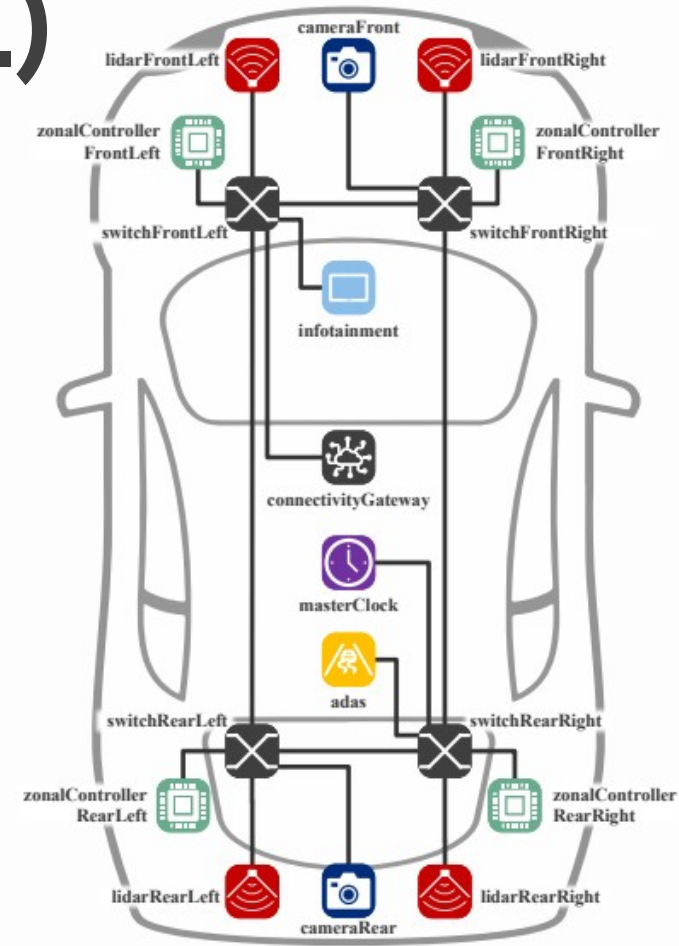
Stream	Layer	Detection Engine	Elimination		Injection		Manipulation		Reordering		Rescheduling	
			Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall	Precision	Recall
Synchronous data	App.	Mean shift	0.99	1.00	1.00	1.00	0.98	1.00	0.00	0.00	0.00	0.00
		DBSCAN	0.99	1.00	1.00	1.00	0.98	1.00	0.00	0.00	0.00	0.00
		Multicut	0.92	1.00	0.98	1.00	0.92	1.00	0.00	0.00	0.00	0.00
		GASP	0.92	1.00	0.98	1.00	0.92	1.00	0.00	0.00	0.00	0.00
		PSFP [34]	1.00	0.00	1.00	0.72	1.00	0.81	1.00	0.00	1.00	0.00
	Link	Mean shift	1.00	1.00	0.33	1.00*	1.00	0.98	1.00	0.33	1.00*	1.00
		DBSCAN	1.00	1.00	0.33	1.00*	1.00	0.98	1.00	0.33	1.00*	1.00
		Multicut	0.96	1.00	0.33	1.00*	1.00	0.92	1.00	0.33	1.00*	1.00
		GASP	0.96	1.00	0.33	1.00*	1.00	0.92	1.00	0.33	1.00*	1.00
		PSFP [34]	1.00	0.00	1.00	0.92	1.00	0.81	1.00	1.00	1.00	0.78
Asynchronous data	App.	Mean shift	1.00	0.65	0.50	1.00*	1.00	0.50	1.00*	1.00	0.01	0.01
		DBSCAN	1.00	0.65	0.50	1.00*	1.00	0.50	1.00*	1.00	0.01	0.01
		Multicut	0.94	1.00	0.50	1.00*	1.00	0.50	1.00*	1.00	0.13	0.88
		GASP	0.94	1.00	0.50	1.00*	1.00	0.50	1.00*	1.00	0.13	0.88
		PSFP [34]	1.00	0.00	1.00	0.00	1.00	0.00	1.00	0.00	1.00	0.00
	Link	Mean shift	1.00	0.31	0.33	1.00*	1.00	0.55	1.00*	1.00	0.98	0.46
		DBSCAN	1.00	0.31	0.33	1.00*	1.00	0.55	1.00*	1.00	0.98	0.46
		Multicut	0.96	1.00	0.33	1.00*	1.00	0.51	1.00*	1.00	0.75	1.00
		GASP	0.96	1.00	0.33	1.00*	1.00	0.51	1.00*	1.00	0.75	1.00
		PSFP [34]	1.00	0.00	1.00	0.95	1.00	0.70	1.00	0.00	1.00	0.00
Cyclic control	App.	Mean shift	1.00	1.00	0.95	1.00	0.98	1.00	1.00	1.00	0.00	0.00
		DBSCAN	1.00	1.00	0.95	1.00	0.98	1.00	1.00	1.00	0.00	0.00
		Multicut	0.99	1.00	0.91	1.00	0.93	1.00	0.99	1.00	0.50	0.03
		GASP	0.99	1.00	0.91	1.00	0.93	1.00	0.99	1.00	0.50	0.03
		PSFP [34]	1.00	0.00	1.00	0.97	1.00	0.97	1.00	0.00	1.00	0.00
	Link	Mean shift	1.00	1.00	0.33	1.00*	1.00	0.97	1.00	0.99	1.00	1.00
		DBSCAN	1.00	1.00	0.33	1.00*	1.00	0.97	1.00	0.99	1.00	1.00
		Multicut	0.97	1.00	0.33	1.00*	1.00	0.96	1.00	0.91	1.00	1.00
		GASP	0.97	1.00	0.33	1.00*	1.00	0.96	1.00	0.91	1.00	1.00
		PSFP [34]	1.00	0.00	1.00	0.98	1.00	0.97	1.00	0.00	1.00	0.00

Microbenchmarks Results

- Up to 0.02% FP rate during benign operation
- Egress shaping masks reordering and rescheduling
- Reliable detection of elimination
- All link-layer infused anomaly classes detectable
- Correlation clustering outperformed other engines

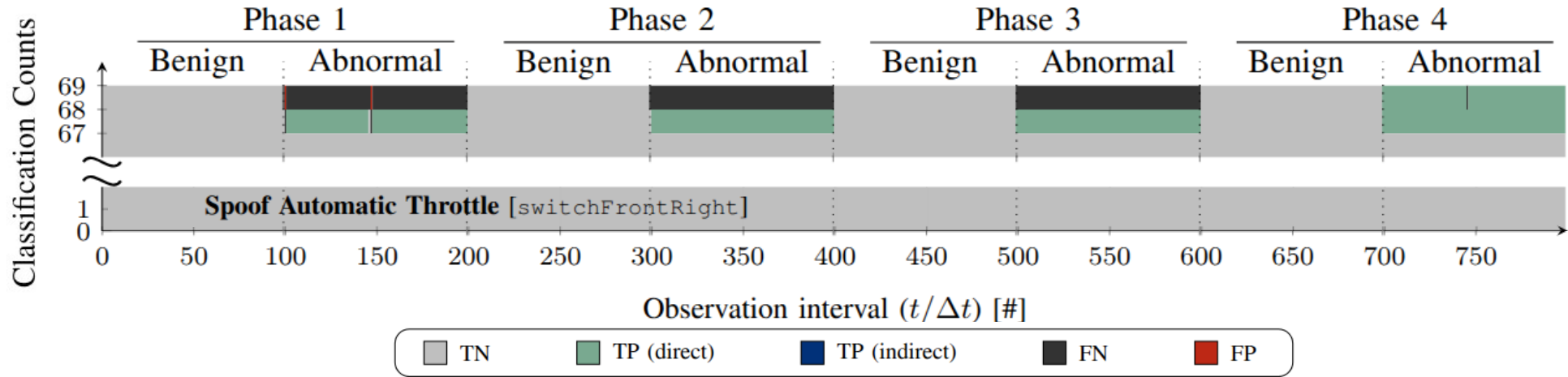
IVN Case Studies (2nd Gen.)

- 216 streams
- 5 traffic classes
- Time sync and redundant paths
- Each switch is monitored
- 0 – 0.06% FP rate in benign operation
- 0 FPs for timed control traffic



IVN Case Studies

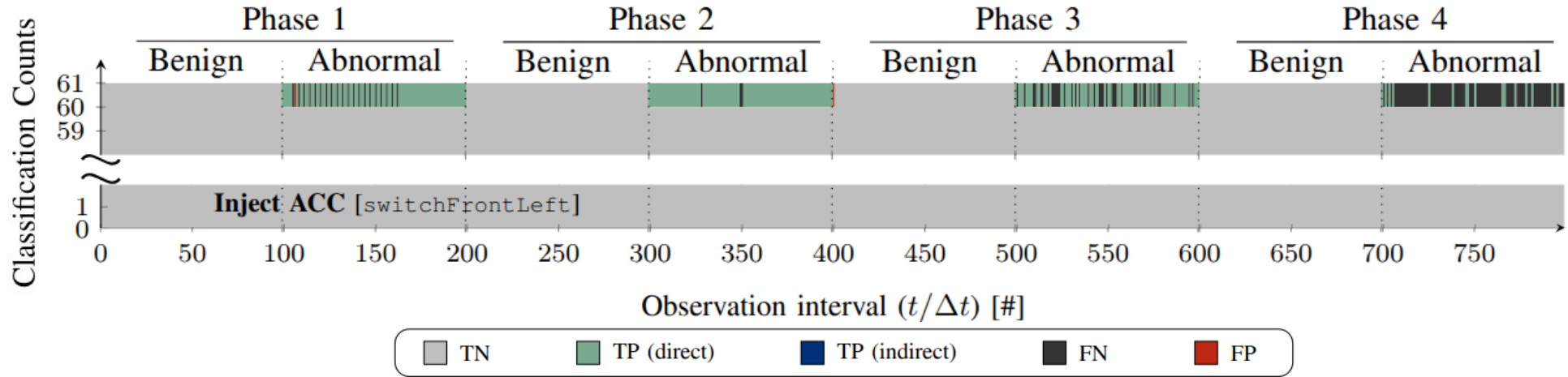
Spoof Automatic Throttle



- Manipulation seen as elimination and injection

IVN Case Studies

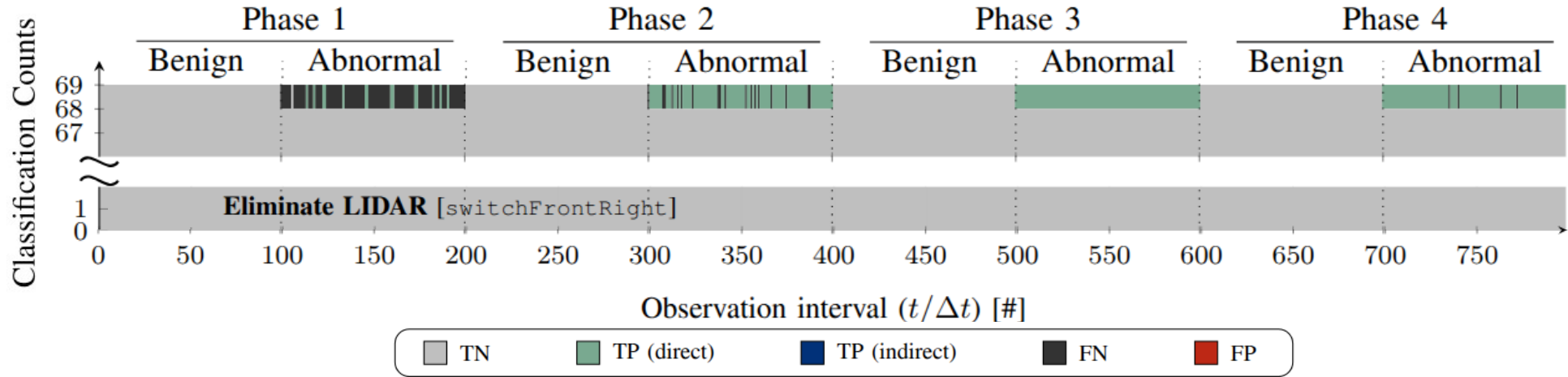
Inject ACC



- Detection not bound to increased resource usage

IVN Case Studies

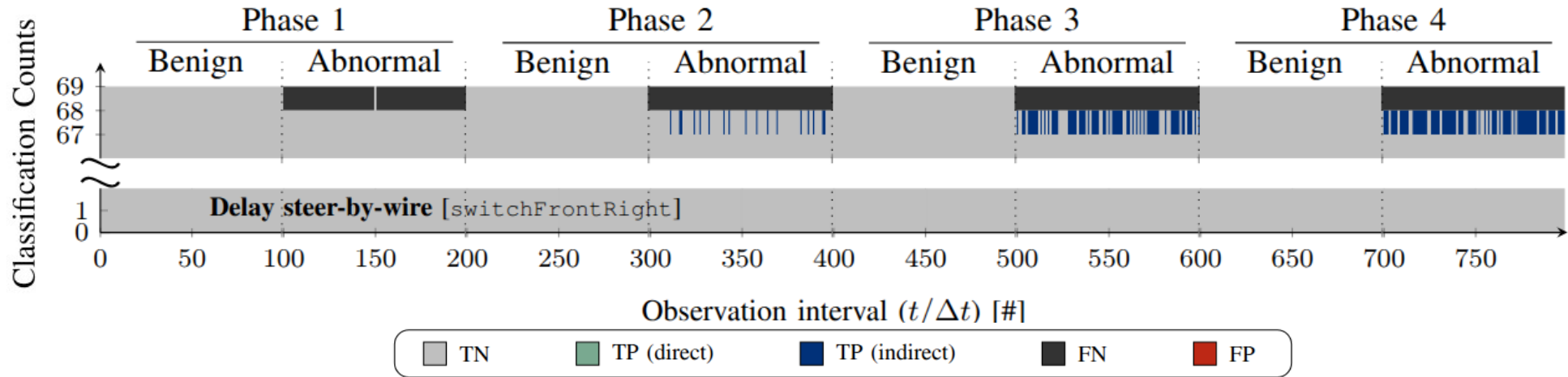
Eliminate LIDAR



- Elimination is detected in shaped data stream

IVN Case Studies

Delay steer-by-wire



- Cascading effects can enable detection

Summary

4. Will behavioral metrics form clusters of benign TSN stream patterns for dedicated anomaly detection?

- Low false positive rates
- Downstream report fusion and filtering needed
- Unsupervised learning of complete IVN behavior
- Detects all anomaly classes infused on link-layer

Conclusion and Outlook



Conclusion

- Anomaly detection and countermeasures are crucial for IVNs
- Domain specific data and knowledge is essential
- Open source assessment framework enables deep evaluation
- Integrated TSN-based approach maximizes report quality
- Dedicated clustering-based approach maximizes detection performance

Outlook

- Test in a real vehicle
- Employ open source assessment framework
- Transfer to other TSN domains
- Evaluate hybrid and online approaches

Questions



Publications

- [1] P. Meyer, F. Korf, T. Steinbach, and T. C. Schmidt, "Simulation of Mixed Critical In-vehicular Networks," in Recent Advances in Network Simulation, A. Virdis and M. Kirsche, Eds., in EAI/Springer Innovations in Communication and Computing, Springer International Publishing, 2019.
- [2] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "DoS Protection through Credit Based Metering - Simulation Based Evaluation for Time-Sensitive Networking in Cars," in Proceedings of the 6th International OMNeT++ Community Summit, M. Zongo, A. Virdis, V. Vesely, Z. Vatasdas, A. Udugama, K. Kuladinithi, M. Kirsche, and A. Förster, Eds., in EPIC Series in Computing, vol. 66, EasyChair, Sep. 2019, pp. 52–59.
- [3] P. Meyer, T. Häckel et al., "Demo: A Security Infrastructure for Vehicular Information Using SDN, Intrusion Detection, and a Defense Center in the Cloud," in 2020 IEEE Vehicular Networking Conference (VNC) (IEEE VNC 2020), virtual, Dec. 2020, pp. 1–2.
- [4] P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "Network Anomaly Detection in Cars based on Time-Sensitive Ingress Control," in Proc. of the IEEE Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada: IEEE Press, Oct. 2020.
- [5] P. Meyer, T. Häckel, S. Reider, F. Korf, and T. C. Schmidt, "Network Anomaly Detection in Cars: A Case for Time-Sensitive Stream Filtering and Policing," Computer Networks, vol. 255, no. 110855, pp. 1–13, Dec. 2024.
- [6] P. Meyer, T. Häckel, T. Lübeck, F. Korf, and T. C. Schmidt, "A Framework for the Systematic Assessment of Anomaly Detectors in Time-Sensitive Automotive Networks," in Proc. of the IEEE Vehicular Networking Conference (VNC), Kobe, Japan: IEEE, May 2024, pp. 57–64.
- [7] P. Meyer, T. Lübeck, T. Häckel, F. Korf, and T. C. Schmidt, "Anomaly Detection in Real-Time Networks Using Asynchronous Traffic Shaping," in Proc. of the IEEE Vehicular Technology Conference (VTC2025-Fall), Chengdu, China: IEEE, Oct. 2025, pp. 1–7.

Additional contributions:

- [8] S. Reider, P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "Integration realer Angriffe in simulierte Echtzeit- Ethernet-Netzwerke," in Echtzeit 2020, in Informatik aktuell, Wiesbaden: Springer Vieweg, Jan. 2021, pp. 51–60.
- [9] T. Häckel, P. Meyer et al., "A Multilayered Security Infrastructure for Connected Vehicles – First Lessons from the Field," Presented at IEEE Intelligent Vehicles Symposium Workshops (IV Workshops), May 2022.
- [10] T. Lübeck, P. Meyer, T. Häckel, F. Korf, and T. C. Schmidt, "Asynchronous Traffic Shaping and Redundancy: Avoiding Unbounded Latencies in in-Car Networks," in Proc. of the 16th IEEE Vehicular Networking Conference (VNC), Porto, Portugal: IEEE, Jun. 2025, pp. 1–8.
- [11] T. Häckel, P. Meyer, F. Korf, and T. C. Schmidt, "Securing Future In-Vehicle Networks: Monitoring and Control for Ethernet Backbones," in Engineering Safe and Trustworthy Cyber Physical Systems: Essays Dedicated to Werner Damm on the Occasion of His 71st Birthday, M. Fränzle, J. Niehaus, and B. Westphal, Eds., Cham: Springer Nature Switzerland, 2026, pp. 163–182.

References I

- [Checkoway11] S. Checkoway et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” USENIX Security, 2011.
- [Miller15] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” Black Hat USA, vol. 2015, p. 91, 2015
- [Steinbach18] T. Steinbach, Ethernet-basierte Fahrzeugnetzwerkarchitekturen für zukünftige Echtzeitsysteme im Automobil. Springer Fachmedien Wiesbaden, 2018.
- [Monteuuis18] J.-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, “SARA: Security Automotive Risk Analysis Method,” in Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, in CPSS’18. Incheon, Republic of Korea: Association for Computing Machinery, 2018, pp. 3–14.
- [Sharafaldin18] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in 4th International Conference on Information Systems Security and Privacy (ICISSP), SciTePress, Jan. 2018, pp. 108–116.
- [Langer19] F. Langer, F. Schüppel, and L. Stahlbock, “Establishing an Automotive Cyber Defense Center,” in 17th escar Europe : embedded security in cars, 2019
- [Walrand21] J. Walrand, M. Turner, and R. Myers, “An Architecture for In-Vehicle Networks,” IEEE Transactions on Vehicular Technology, vol. 70, no. 7, pp. 6335–6342, Jul. 2021.
- [8021Q22] IEEE, “IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks,” IEEE, IEEE Std 802.1Q-2022 Revision of IEEE Std 802.1Q-2018, Dec. 2022.

References II

[Lauinger22] J. Lauinger, A. Finkenzeller, H. Lautebach, M. Hamad, and S. Steinhorst, "Attack Data Generation Framework for Autonomous Vehicle Sensors," in 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE, Mar. 2022.

[Lee23] S. Lee, W. Choi, I. Kim, G. Lee, and D. H. Lee, "A Comprehensive Analysis of Datasets for Automotive Intrusion Detection Systems.," Computers, Materials & Continua, vol. 76, no. 3, 2023

[Flood24] R. Flood, G. Engelen, D. Aspinall, and L. Desmet, "Bad Design Smells in Benchmark NIDS Datasets," in 2024 9th IEEE European Symposium on Security and Privacy (EuroS&P), 2024, pp. 658–675.

[Andronovici24] D. Andronovici, I. Turcanu, J. Bigge, and C. Sommer, "Cross-Validating Open Source In-Vehicle TSN Simulation Models With a COTS Hardware Testbed," in 2024 IEEE Vehicular Networking Conference (VNC), 2024, pp. 172–179.

[Upstream26] Upstream, "2026 Automotive & Smart Mobility Global Cybersecurity Report," Upstream Security Ltd., 2026.

[Solaas25] J. R. V. Solaas, E. Mariconti, and N. Tuptuk, "Systematic Literature Review: Anomaly Detection in Connected and Autonomous Vehicles," IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 1, pp. 43–58, Jan. 2025.

[8021DG25] IEEE, "IEEE Standard for Local and Metropolitan Area Networks – Time-Sensitive Networking Profile for Automotive In-Vehicle Ethernet Communications," IEEE, IEEE Std 802.1DG-2025, Jun. 2025.

[OpenSim] OpenSim Ltd.: OMNeT++ Discrete Event Simulator and the INET Framework, <https://omnetpp.org/>

[AndresGraph] "Graphs and Graph Algorithms in C++," [Online]. Available: <https://github.com/bjoern-andres/graph>