CAN Message Collision Avoidance Filter For In-Vehicle Networks

29 Sept 2024

Uma Kulkarni, Prof. Dr. Sibylle Fröschle

Email: uma.kulkarni@tuhh.de, sibylle.froeschle@tuhh.de

Institute for Secure Cyber-Physical Systems

Hamburg University of Technology (TUHH)

TUHH

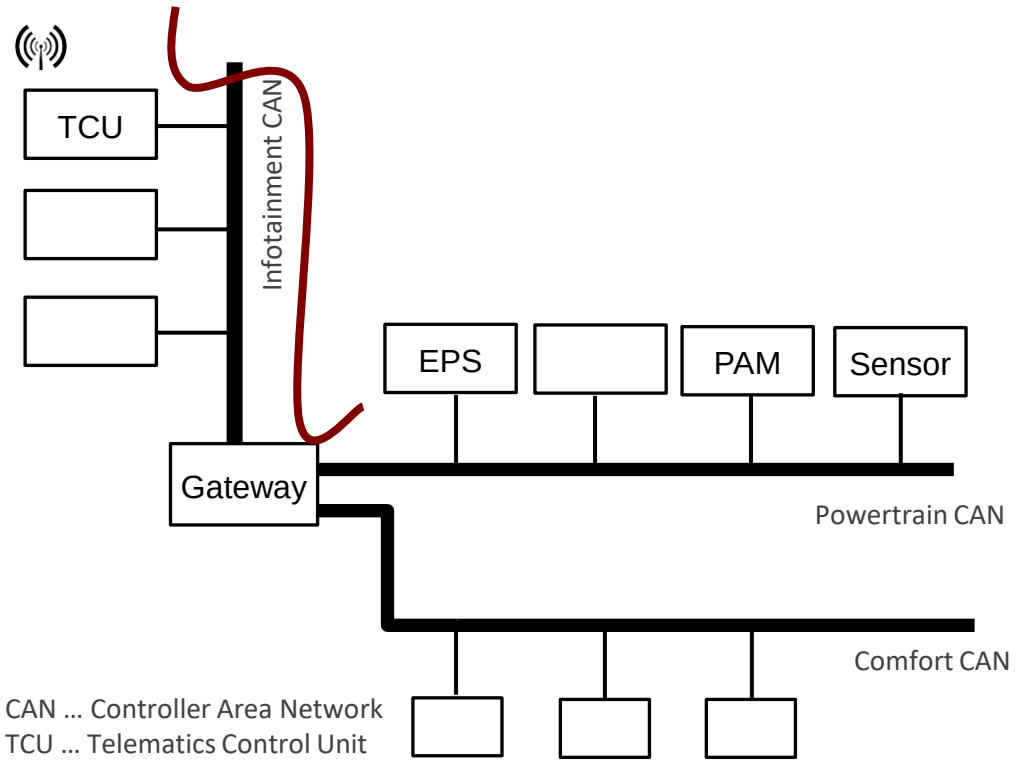
SCPS

IARIA

Outline

- Introduction and Motivation
- Related Work
- CAN Preliminaries
- Concept
- Conclusion and Future Work

Motivation



CAN … Controller Area Network
TCU … Telematics Control Unit
EPS … Electric Power Steering
PAM … Park Assist Module

In-Vehicle Attacker:

1. Obtains remote code execution on TCU via software exploit.
2. Compromises Gateway ECU, e.g. by reprogramming
3. Silences one of the critical nodes and injects malicious messages on to the bus, e.g. messages that control the steering angle. (Part of Park Assist Functionality: from PAM to EPS.)

Assuming that the attacker is successful in achieving steps 1 and 2, how to prevent the last stage?

❑ Overall security concept. The problem can be reduced to stopping message collisions.

[1] S. Fröschle and A. Stühring, “Analyzing the capabilities of the can attacker,” in Computer Security–ESORICS 2017

Related Work

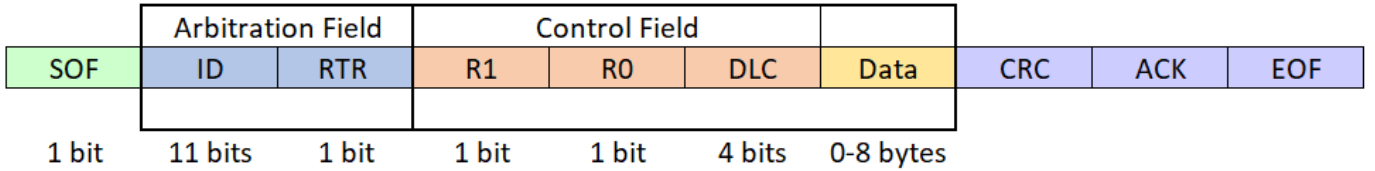
Many specific solutions exist. An overall security concept is required.

Solutions capable of handling CAN message collision: Firewalls/ Filters

- Humayed, Li, Lin and Luo presented a firewall at ESORICS 2020 and Lenard and Bolboaca presented a firewall concept at European Interdisciplinary Cybersecurity Conference, 2021
  - Solutions with Pass and Block Lists.
    - Need secure storage
  - Solutions that depend on architecture.
    - Need updates and reprogramming
- NXP has developed a secure CAN transceiver. These transceivers need to be integrated into every ECU.
  - All ECUs in a vehicle come from multiple suppliers

CAN Preliminaries

- CAN data frame

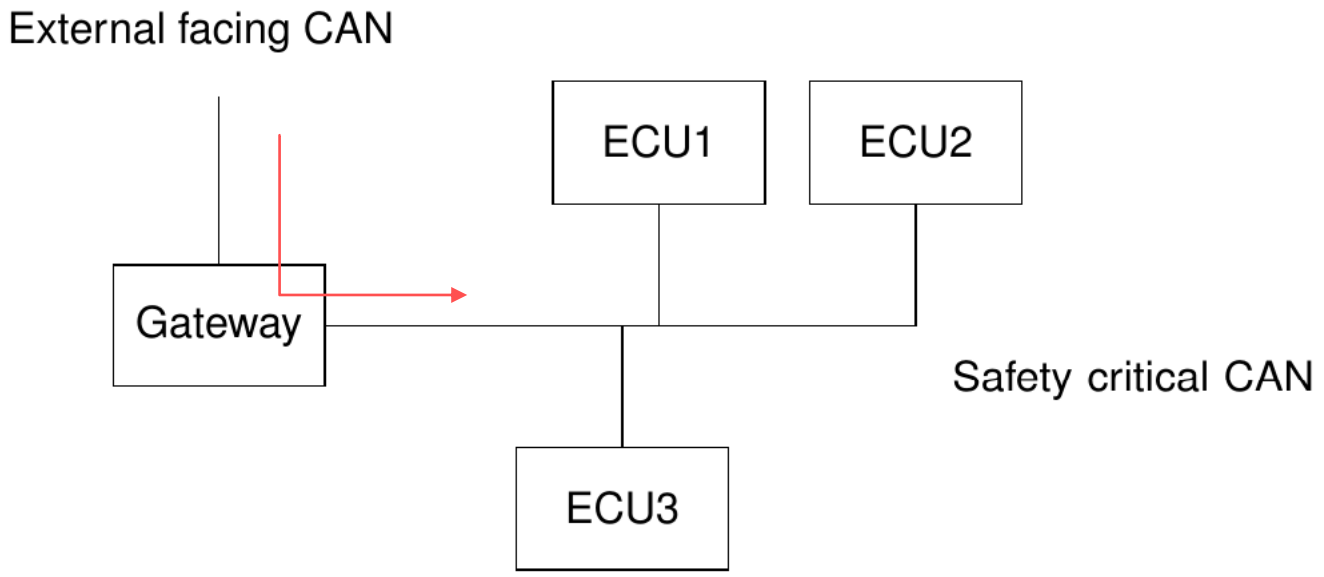


- Errors
  - Bit, Stuff, Form, ACK, CRC
  - Error Frame

- Fault confinement rules
  - Error Counters – TEC and REC
  - ECU states
    - Error Active
    - Error Passive
    - Bus-off

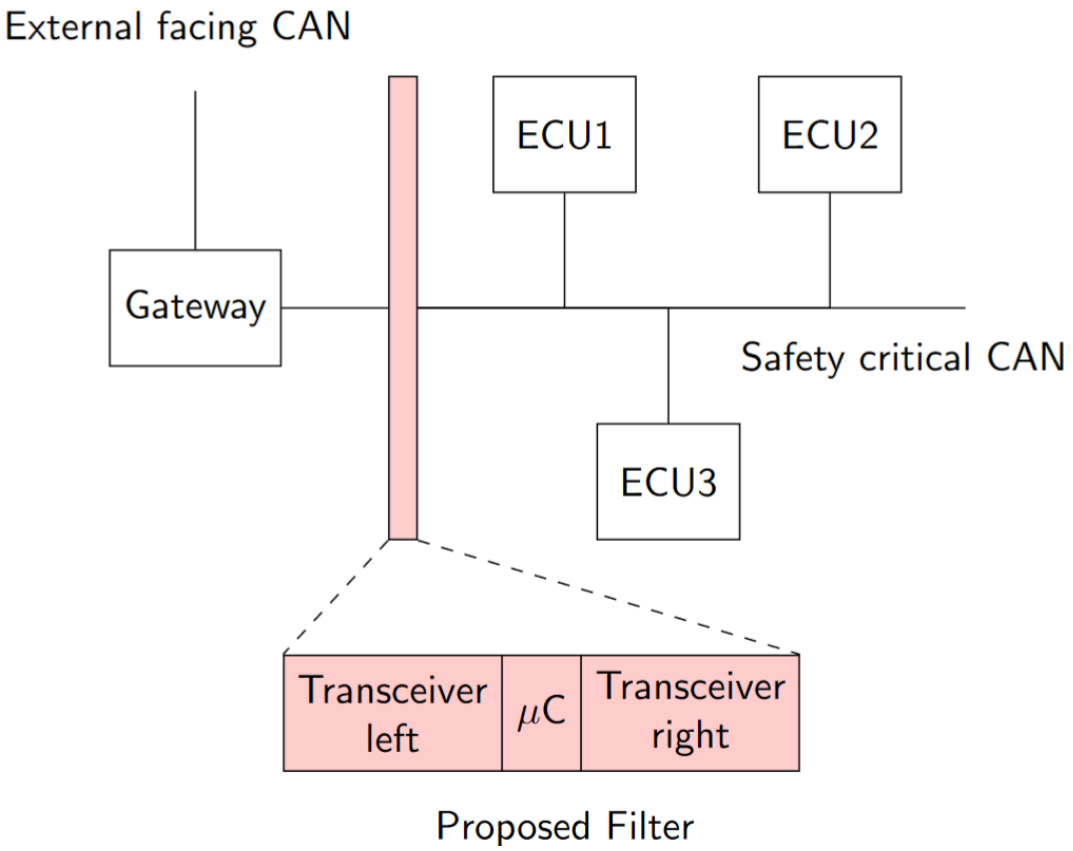
Error Active	**Error Passive**	**Bus-off**
TEC ≤ 127	127 < TEC ≤ 255	TEC > 255
REC ≤ 127	127 < REC	
Participation on bus – Yes Error Flag – Active (6 dominant bits)	Participation on bus – Yes Error Flag – Passive (6 recessive bits)	Participation on bus – No

Architecture



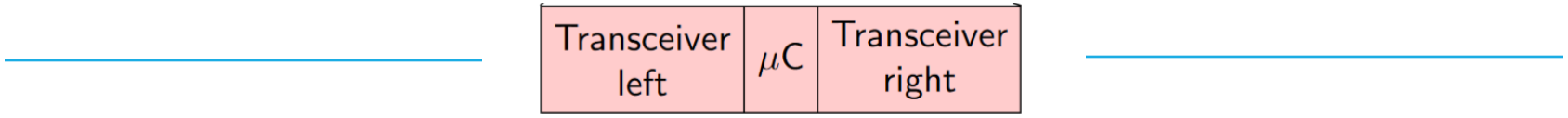
Typical direction of attack.

Concept - Structure



Concept - Operation

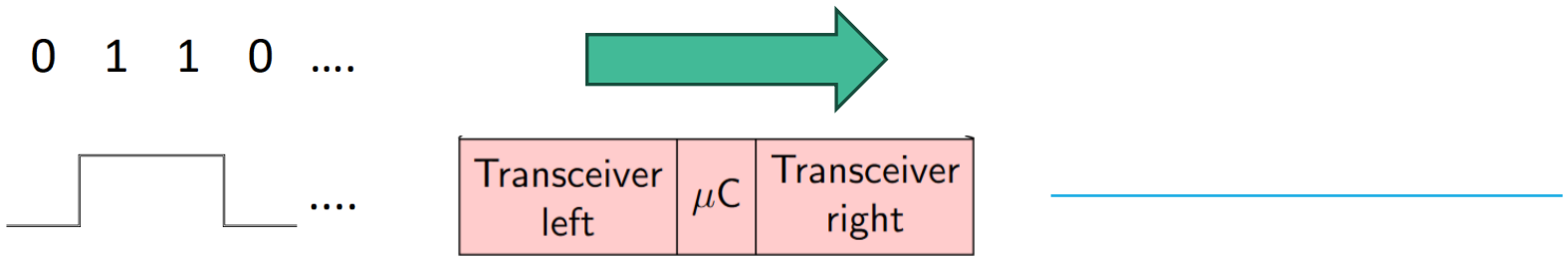
- Scenario 1 - Bus is idle on both sides.



The filter continues to monitor the bus on both sides.

Concept - Operation

- Scenario 2 - A SOF bit is encountered by only one of the transceivers.



Consider for example that the SOF arrives on the left side.

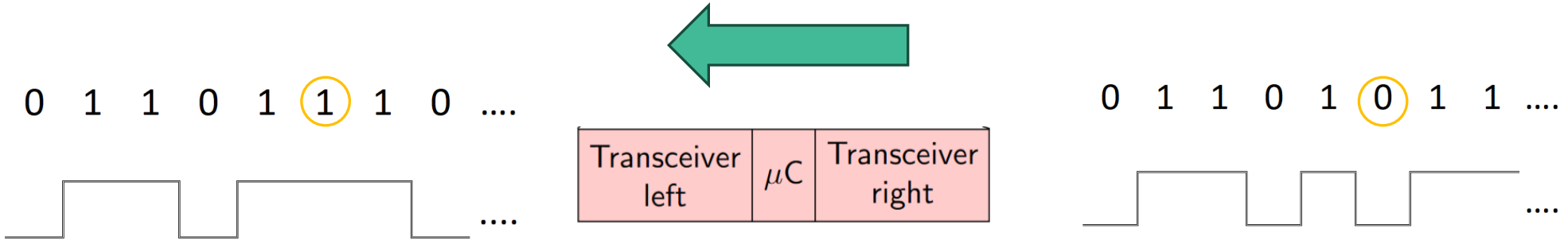
The filter simply forwards each bit as received from the left side to the right side.

Dominant bits from the right side are forwarded to the left as they might be a part of error flag.

Concept - Operation

- Scenario 3 - A SOF bit is encountered on both sides of the filter simultaneously.

  - IDs are different.



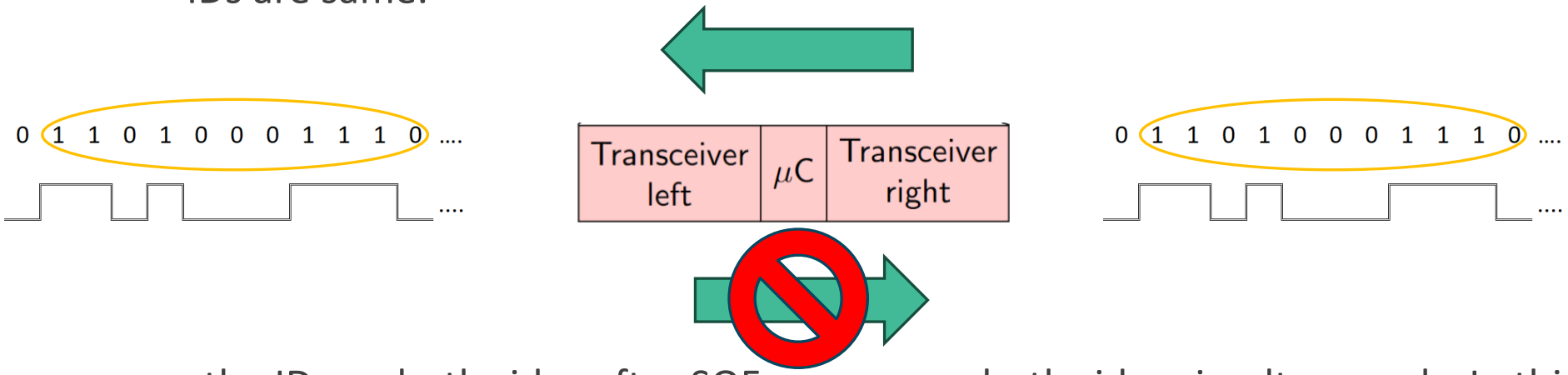
Filter observes as long as the ID bits on both sides are same. As soon as they are different, they are forwarded to the other side to facilitate the bitwise arbitration.

Once the arbitration is complete, same as Scenario 2.

Concept - Operation

- Scenario 4 - A SOF bit is encountered on both sides of the filter simultaneously.

  - IDs are same.



Filter compares the IDs on both sides after SOF appears on both sides simultaneously. In this case,all 11 bits will be same.

Filter blocks the rest of the frame from the left side. The transmission of the frame on the right side is successful.

Conclusion and Future Work

We have proposed a lightweight filter for preventing CAN message collisions

- Requires no change to the existing protocol
- Does not require secure storage for pass and block lists
- Is one-time programmable and hence, is tamper-proof
- Is stand-alone and does not need to be integrated into every ECU

This makes our solution economical and will be sufficient and efficient for preventing CAN message collisions.

Future work:

- Implement the proposed filter on a HIL set-up.
- Evaluate the performance of the filter.
- Integrate the filter as a part of an overall security concept.

References

[1] S. Fröschle and A. Stühring, “Analyzing the capabilities of the can attacker,” in Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I 22. Springer, 2017, pp. 464–482.

[2] CAN Specification, Robert Bosch GmbH, Postfach, vol. 50, p. 15, 1991.

[3] K.-T. Cho and K. G. Shin, “Error handling of in-vehicle networks makes them vulnerable,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1044–1055.

[4] A. Humayed, F. Li, J. Lin, and B. Luo, “Cansentry: Securing can-based cyber-physical systems against denial and spoofing attacks,” in Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25. Springer, 2020, pp. 153–173.

[5] T. Lenard and R. Bolboaca, “A statefull firewall and intrusion detection system enforced with secure logging for controller area network,” in Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference, 2021, pp. 39–45.

[6] NXP Semiconductors. NXP TJA115x Secure CAN Transceiver Family.

Thank You