CAN Message Collision Avoidance Filter for In-Vehicle Networks

Uma Kulkarni
Institute for Secure Cyber-Physical Systems
Hamburg University of Technology
Hamburg, Germany
email: uma.kulkarni@tuhh.de

Sibylle Fröschle
Institute for Secure Cyber-Physical Systems
Hamburg University of Technology
Hamburg, Germany
email: sibylle.froeschle@tuhh.de

***Abstract*—Modern Vehicles are architecturally very complex with a large number of Electronic Control Units (ECUs) connected to each other by network buses such as Controller Area Network (CAN). When two messages with the same ID but different contents appear on the bus simultaneously, it results in a message collision. This can result in loss or delay of critical information. If done deliberately by malicious actors, it can lead to unsafe conditions. In this paper, the goal is to motivate the need for a solution against message collisions and propose a concept of a one time programmable CAN message collision avoidance filter that needs no updates or secure storage.**

***Keywords*-Controller Area Network(CAN); In-Vehicle Networks; Message Collisions; Filter.**

I. Introduction and Related Work

Vehicles today have a large number of Electronic Control Units (ECUs) connected to each other by network buses such as Controller Area Network (CAN). CAN is one of the most widely employed network bus systems in the automotive domain due to its simplicity of implementation and low computational resource requirement. Since CAN's introduction, the vehicle has changed a lot: with more functions and more connectivity. But CAN still remains one of the preferred options. As a result, a need for add-on measures for filling in the gaps for which CAN was not designed (such as security) arises.

The in-vehicle network is commonly functionally divided into domains of grouped ECUs or nodes with gateways between the domains. Certain domains such as the powertrain CAN can be categorised as safety-critical. The nodes on a safety-critical section of CAN exchange important information that is crucial for a vehicle's seamless functioning and safety. Any missing information is undesirable and in certain cases, dangerous as e.g. pointed out in [1]. The present work summarises the problem of CAN message collisions and proposes a solution for the same. The main contributions are: (1) we present the need for a filter to avoid CAN message collisions. (2) we present a concept for one such filter with its operation and advantages.

The CAN specification [2] shows that when a transmitting node monitors a different bit value on the bus from the one it has sent, it interprets this as a bit error and the transmission is unsuccessful. It is clear that an error that is not due to a fault in the sender itself or in the bus will unfairly stop a transmission that would otherwise be successful. Furthermore, the security concerns arising from message collisions are shown in [3] and [1]. In [1], it has been shown how, based on collisions, an attacker can silence a target node. To carry out such attacks remotely, the attacker first has to pass through a gateway to disrupt a target safety-critical CAN. The idea being proposed in the present work is primarily motivated by [4] where a firewall is presented for blocking all unauthorised CAN frames from nodes categorised as high-risk. The firewall goes between every high-risk node and the internal CAN bus. It decides its actions based on a programmed pass list of acceptable message IDs. Our work aims at eliminating this list of IDs altogether and is in contrast only targeted at collision causing frames. As a result, our proposed solution does not need any updates after architectural changes. A statefull firewall is presented in [5] which also operates based on pass and block lists of frames and sequences of frames. Another closely related idea is implementing a filter in a secure CAN transceiver by NXP [6]. Its adoption would require all nodes, or at least all critical nodes, to include this secure transceiver. As opposed to this, as already stated, our approach eliminates the pass and block lists and can be a stand-alone addition to a complete critical section of CAN. In particular, in view of remote attacks, our approach exploits the directionality of attacks from gateway to the safety-critical CAN, enabling an overall security concept. The existing studies have elaborate solutions to broad frame filtering needs, but we believe that, for message collisions, our light solution will be sufficient and more efficient.

The rest of the paper is structured as follows. In Section II, we present the necessary preliminaries and our motivation for this work. In Section III, we present the filter concept and operation. Finally, we conclude and state future work directions in Section IV.

II. Preliminaries and Motivation

Some of the fields in a CAN frame that are relevant to the concept are described here: The Start Of Frame (SOF), a single dominant bit, is an indication of a node's wish to start transmission. The Identifier (ID) serves two purposes: identifying the information as well as the priority of the frame in case of simultaneous transmission attempts. The priority is decided by bitwise arbitration of the ID. Data Length Code (DLC) denotes the length of data in Data Field. CAN also offers fault confinement features. The errors that could possibly occur during a frame transmission are classified into five types: Bit, Stuff, Form, ACK and CRC of which bit error is relevant here. Every occurrence of an error results in the

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

observing node notifying this on the bus by sending error frames and adding to its Transmit Error Counter (TEC) or Receive Error Counter (REC) by following the rules of fault confinement. Successful transmissions and receptions result in the reduction of the count. The CAN nodes can be in one of the following states: (1) Error Active: TEC<127 and REC<127. The node can participate normally in communication on the bus and is capable of sending an Active Error Flag of 6 dominant bits. (2) Error Passive: 127 $<$ TEC $<$ 256 and 127 $<$ REC. The node can only send a Passive Error Flag of 6 recessive bits. (3) Bus-off: TEC $\geq$ 256. A node no longer participates on the bus unless it gets out of bus-off state or is reset [2].

When two messages with the same ID appear on the bus simultaneously, it is non-consequential if the message contents are identical. But if the message contents differ, i.e., a message collision occurs, the first different bit results in a bit error. An error frame is sent and the sender's TEC increases. If this happens repeatedly, the sender acts according to the fault confinement rules of CAN and goes into error passive and eventually bus-off state. Such message collisions are undesired for multiple reasons, the most critical being: it results in unavailability of information that is critical for safety relevant functions. Also, it may be exploited by malicious actors intentionally causing denial of service by forcing a critical node into bus-off state.

The idea proposed in this work aims at preventing such collisions while causing negligible interruption to the CAN functioning. The advantages of the concept are: No changes to the existing CAN protocol. No pass list of permissible messages. So, there is also no need of storing such a list securely. It does not depend on the database of message IDs. So, there is no need for an update to the filter with every change in the architecture or message matrix. It can be implemented on a one time programmable chip making it tamper-proof and low-maintenance. It is stand-alone and does not need to be integrated with every ECU. This is favourable as the ECUs in a vehicle come from multiple manufacturers. Due to its characteristics: stand-alone, one time programmable and no-update, it will be an economic solution.

III. Filter Concept and Operation

The filter contains two transceivers, let us say transceiver-left and transceiver-right, with a microcontroller in between. As depicted in Fig. 1, on the left of transceiver-left is the gateway to the domain in question and beyond transceiver-right on the right is the CAN with critical and honest nodes (such as Powertrain CAN). The microcontroller is extremely lean with limited functions in order to keep the overhead of the filter to a minimum.

The operation of the filter can be explained with the help of four scenarios (see Fig. 2 for a part of the operation with standard CAN). Scenario 1: Bus is idle on both sides. In this case, the filter continues to monitor the bus on both sides. Scenario 2: An SOF bit is encountered by only one of the transceivers. The filter acts as a simple forwarding block. It

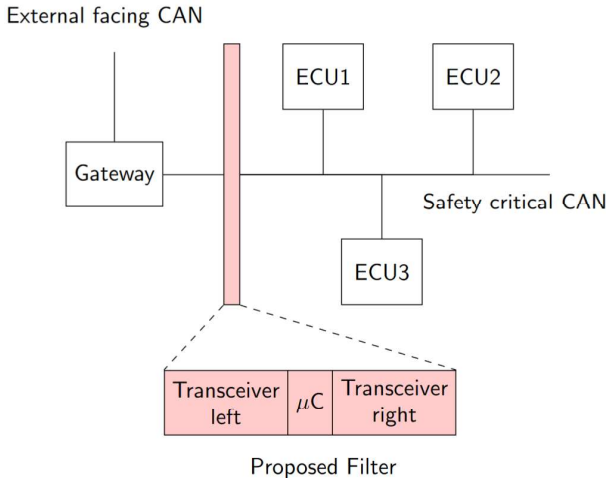

Figure 1. Example architecture of an in-vehicle CAN network with the proposed filter.

replicates every bit as it is from the side it is received, say transceiver-right, to the other side, say left side. Dominant bits on the left side while the frame is being transmitted are forwarded to the right as they might be a part of an error flag. Scenario 3: An SOF bit is encountered on both sides of the filter simultaneously and the IDs are different. The filter does not interfere with the bitwise arbitration process. The filter compares the bits on both sides until the last but one bit of the ID. Temporary counter C counts the bits. As soon as different bits are monitored, the bit monitored by transceiver-left is forwarded on the right bus and the bit monitored by transceiver-right is forwarded on the left bus. After the arbitration phase, in normal conditions, the behaviour is the same as in Scenario 2, as shown in Step (3) in the figure. Scenario 4: An SOF bit is encountered on both sides of the filter simultaneously and the IDs are the same. The initial steps

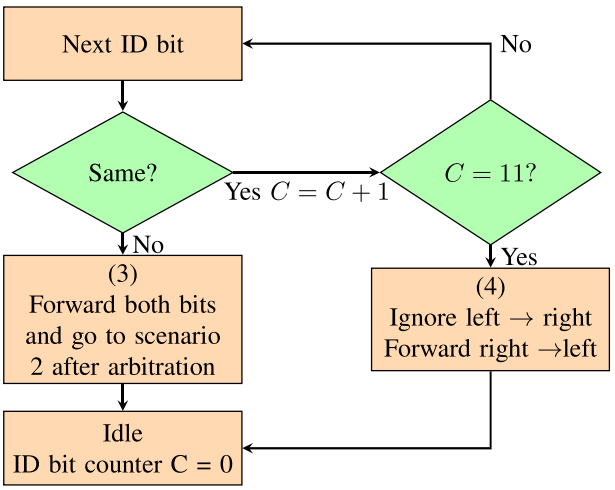

Figure 2. Operation after SOF received on both sides for a message with 11 bit ID

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

are the same as in Scenario 3. As soon as the last bit of the ID field is compared and it is observed that the entire ID was the same on both sides, the filter blocks the rest of the frame received by transceiver-left (non-critical side) and only forwards the remaining frame received by transceiver-right (critical side) to the other side, as shown in Step (4) in the figure. In normal cases, the filter will be faced with one of the Scenarios 1-3. In case of an impending collision, the filter behaves according to Scenario 4.

IV. Conclusion and Future work

We have proposed a lightweight filter for preventing CAN message collisions that comes with the following advantages: (1) It requires no change to the existing protocol. (2) It does not require secure storage for pass and block lists. (3) It is one-time programmable, and hence, it is tamper-proof. (4) It is stand-alone and does not need to be integrated into every ECU. These advantages make our solution economical and it will be sufficient and efficient for preventing CAN message collisions.

Future work includes implementing the filter and demonstrating its operation on a simulation platform and experimental work to analyse the delay introduced by the filter. We will also show how the filter provides a crucial component within an overall CAN 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*, 2019. [Online]. Available: https://www.nxp.com/docs/en/fact-sheet/SECURCANTRLFUS.pdf [last accessed 24 Sept 2024]

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org