Vehicle individual CAN-profile for secure communication between control units

Reference No: B78004

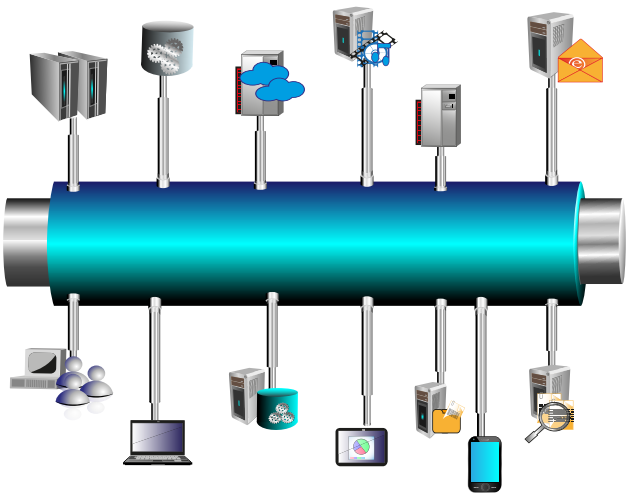
CHALLENGE

The control area network bus (CAN-bus) is the most commonly used bus system for electronic control units (ECU) communication. The communication via CAN-buses is realized by the transmission of frames. These frames comprise primarily an identifier, characterizing among other the priority of the frame, and a telegram. A **CAN-profile defines the format of the telegram and the identifiers.** For safety reasons, this CAN-profile is not freely available. An **attack to the communication system would require first obtaining the CAN-profile.** Since a CAN-profile is typically shared by different vehicles of a given manufacturer or model series, an unauthorized access to the CAN-profile of one of the vehicles may open the door to subsequent unauthorized accesses to the communication systems of all vehicles sharing the same CAN-profile.

A **known technique for providing communication security relies on encrypting the frames** so that the content thereof can only be accessed by authorized components having knowledge of the corresponding encryption keys. This **encryption method requires among other a large amount of computational power and processing time**.

INNOVATION

The here presented innovation describes a method of **obfuscated communication through the CAN-bus**. The method comprises **a one-time generation of a random value corresponding to a sequence of bits (seed).** The generation of the seed could be realized during the production process of the vehicle, per example. Based on the seed and the list of possible identifiers, a permutated identifier and a permutated telegram is obtained via two transformation functions. The seed is not stored after the generation of the permutated identifier and permutated telegram. The permutations based on the randomly chosen seed lead to a vehicle individual format of the telegram and the identifiers and thereby to a new vehicle individual CAN-profile. This prevents unauthorized accesses to the CAN-bus system, even if the CAN-profile of a comparable vehicle is known.



COMMERCIAL OPPORTUNITIES

This invention allows a secure and fast communication via CAN-buses. The integration of the invention in the consisting vehicle production process is easy and cost-efficient realizable.

The invention produces clear benefits:

- **No encryption** is necessary, leading to **fast data transfer;**
- **The individual CAN-profile per vehicle** ensures **Security against Aggressors.**

BayPAT

Technische Hochschule Ingolstadt

Technology from
TECHNISCHE
HOCHSCHULE
INGOLSTADT

IP rights:
Filed in 2018 (pending)

Contact:
Cornelia Sattler
+49 (0) 89 5480177 - 37
csattler@baypat.de

Bayerische
Patentallianz GmbH
Prinzregentenstr. 52
80538 München
www.baypat.de