SciencePG
Science Publishing Group

In-vehicle Network Security: Detecting Anomalies in CAN Bus Frames by Analyzing Data Field Sequences

Mohammed Karrouchi*, Mohammed Rhiat, Anas Hassari, Ilias Atmane, Hanae Azzaoui, Kamal Hirech

Higher School of Education and Training, Mohammed First University, Oujda, Morocco

Email address:

m.karrouchi@ump.ac.ma (Mohammed Karrouchi), mohammed.rhiat@ump.ac.ma (Mohammed Rhiat),
anas.hassari@ump.ac.ma (Anas Hassari), i.atmane@ump.ac.ma (Ilias Atmane),
hanae azzaoui.indus@gmail.com (Hanae Azzaoui), k.hirech@ump.ac.ma (Kamal Hirech)

*Corresponding Author

Abstract

Modern vehicles are equipped with many driver assistance mechanisms to make life easier for drivers. These features are made possible by the use of a range of technologies, first and foremost the CAN (Controller Area Network) bus, which is a means of communication between electronic control units (ECUs). Scientific research has revealed the weakness of this protocol and the availability of WIFI, Bluetooth, USB, OBD2 connection in the vehicle increases the possibility of attack from the outside. The risk of attack increases according to the vulnerability of the system under attack (engine ECU, anti-lock braking system ABS, gearbox, GPS...), that's why manufacturers and researchers are working to find solutions to this problem. In this paper, we have proposed an approach to deal with any attack on car security. It is presented by an algorithm that uses crypto-graphic bases that protects data, detects attack attempts and takes into account the real operating time of the automotive nodes. This approach is implemented on the Software level as how it can be applied on the Hardware side or both at same time, cheaper and more secure.

Keywords

Anomaly Detection, Intrusion Injection, CAN Bus Frames, OBD2