Sensors, vol.25, no.8, pp.2605-1-2605-15, April, 2025.

Revisiting Wireless Cyberattacks on Vehicles

G. López López; R. Gesteira Miñarro; R. Palacios Hielscher

Abstract-

The automotive industry has been a prime target for cybercriminals for decades, with attacks becoming more sophisticated as vehicles integrate advanced digital technologies. In response, new standards and regulations have been introduced, requiring manufacturers to implement robust cybersecurity measures to obtain necessary certifications. Modern vehicles have an extensive attack surface due to the increasing number of interconnected electronic components and wireless communication features. While new technologies improve connectivity, automation, and comfort, they also introduce new vulnerabilities that can be exploited by attackers. This paper presents a comprehensive analysis of the attack surface of modern vehicles, focusing on the security risks associated with wireless communication technologies. Each technology is examined in detail, highlighting existing research, known vulnerabilities, and potential countermeasures. Furthermore, this study identifies key research gaps in the field, providing insights into critical areas that require further investigation. This work aims to guide future research efforts in order to enhance vehicle cybersecurity in the evolving landscape of smart, autonomous, and connected vehicles.

Index Terms- cyberattacks; radio frequency; vehicles; wireless

Citation:
Gesteira-Miñarro, R.; López, G.; Palacios, R. "Revisiting Wireless Cyberattacks on Vehicles", Sensors, vol.25, no.8, pp.2605-1-2605-15, April, 2025.