Chapter 11
Safe Data-Driven Control in Autonomous Vehicles and Transportation Systems

P. William
https://orcid.org/0000-0002-0610-0390
Sanjivani College of Engineering, Kopargaon, India

Sachin Vasant Chaudhari
https://orcid.org/0009-0005-8856-8905
Sanjivani College of Engineering, Kopargaon, India

Ved Prakash Mishra
Amity University, Dubai, UAE

Monika Agrawal
Sanjivani College of Engineering, Kopargaon, India

Ritesh Agwan
Sanjivani College of Engineering, Kopargaon, India

Gurpreet Singh Chhabra
GITAM School of Technology, GITAM University, India

ABSTRACT

Safe data-driven control systems are necessary for large-scale automation in contemporary transport networks, including networked autonomous cars. In this research, methods, issues, and possible developments in autonomous vehicle system safety are examined. The chapter discusses important subjects including real-time data processing, cybersecurity, sensor fusion, and AI-enabled predictive modelling. evaluating Examine how VANETs may enhance communication between infrastructure, ad hoc networks, and automobiles. In addition, learn how crucial expert diagnostic systems are for prompt problem identification and fixing. The focus of the article is on encryption, authentication, and anomaly detection as it

DOI: 10.4018/979-8-3373-1832-5.ch011

examines cybersecurity threats and countermeasures. Studies contrasting regional adoption and accident rates demonstrate the benefits of autonomous vehicles for both transport efficiency and traffic safety. The highlights underscore the need of strict safety equipment and multi-tiered security to increase closure and confidence in autonomous transportation systems.

1. INTRODUCTION

Mobility is undergoing significant change as intelligent transportation systems (ITS) and autonomous vehicles (AVs) develop. The majority of these systems use data-driven control methods to ensure dependability, efficacy, and safety. AI, machine learning, and real-time data analytics enable autonomous vehicles (AVs) to make more complex decisions (Cavanini, Ferracuti, Longhi, & Monteriu, 2020). AVs are capable of this. It is challenging to meet security needs in data-driven control systems, nevertheless. Therefore, thorough frameworks that take potential risks and weaknesses into consideration are required. Using vast amounts of sensor data, V2X connections, and predictive analytics, safe data-driven control improves autonomous mobility decision-making. Cyberattacks, complex urban environments, and erratic traffic need a multifaceted approach that combines redundancy, fail-safe procedures, and adaptive learning models. The public's acceptance and use of autonomous technology are also influenced by international ethical and regulatory frameworks. These frameworks place a strong emphasis on transparency, accountability, and technical functioning monitoring. Technology and politics must strive to restrict dangers and guarantee that artificial intelligence findings match real-world safety and social norms (Jiang, Hu, Jia, Wang, & Wu, 2007).

The techniques, challenges, and prospects for safe data-driven control in autonomous vehicles and transportation networks are covered in this article. Real-time data processing, computer security, sensor fusion, and AI-driven predictive modeling are all covered in this article. Sensor fusion is used to combine data from LiDAR, radar, and cameras. With a comprehensive view of the environment provided by this integration, precise navigation and obstacle avoidance are made possible. AI-powered predictive modeling increases a vehicle's adaptability. Cybersecurity safeguards shield antiviral systems from damaging attacks by guaranteeing data confidentiality and integrity and preventing unauthorized access. This modeling analyzes historical and real-time data to identify risks and enhance solutions. The VANET has three communication domains (Lin & Maxemchuk, 2016). Initially, the "In-vehicle domain," was dependent on the On-board Unit. Depending on the VANET area, the On-board Unit (OBU) may contain one or more Application Units (AUs), as shown in Figure 1. This makes it possible for AUs to exchange data for safety,