Chapter 3
Comprehensive Overview of Autonomous Vehicles and Their Security Against DDoS Attacks

Swati Jaiswal
https://orcid.org/0000-0001-9671-534X
Pimpri Chinchwad College of Engineering, Pune, India

Pallavi S. Yevale
https://orcid.org/0000-0001-9366-6810
Dr. D. Y. Patil Institute of Engineering, Management, and Research, Pune, India

Anuja R. Jadhav
Pimpri Chinchwad College of Engineering, Pune, India

ABSTRACT

The automotive industry is developing trends in autonomous driving and connected vehicular systems. These vehicles can access and send the data, download the software updates, connect with other vehicles or other IoT devices via the internet or wireless communication. Autonomous vehicle control urges very strict requirements about the security of the communication channels used by the vehicle to exchange information and the control logic that performs complex driving tasks. So, the increased connectivity results in a heightened risk of a cyber-security attack. For maintaining the advances in safe communication, it is important to establish strong security for connected vehicular systems. For this, existing cybersecurity attacks must be considered to minimize future cybersecurity risks in the connected and autonomous vehicle systems. In this chapter, the authors will emphasize recent works on how autonomous vehicles can ensure strong operation under ongoing cyber security attacks and their possible solutions.

DOI: 10.4018/978-1-7998-9430-8.ch003

INTRODUCTION

In recent years, traffic security has attracted extending thought among trained professionals, organizations, and government affiliations. As demonstrated by a report from the U.S. Division of Transportation, there were 36,560 people were killed due to the car crashes in the U.S. in 2018 (NCSA, 2019) and that suggests there were around 100 deaths reliably. Human mishaps are related with 94 to 96 percent of all motor vehicle crashes. Consequently, the free driving development has been attracting light of an authentic worry for the researchers for quite a while. Beginning from this prolonged stretch of time, further created driver help developments, as electronic constancy control moreover, way departure alerted, were being made to further work on the security and diminish the driver load, which as well prepare to autonomous driving headways. The Society of Automotive Engineers (SAE) has described six particular levels of driver help development types of progress.

The type of technology is explained by established criteria. The automation standard ranges between level 0 and level 5. Level 0 includes all of Porsche's vehicles through 1967 to the new car, completely managed in 2018. The Level 1 automatic control allows the vehicle to decide about how to guide or stop or speed the autonomous driving support system (ADAS) mounted in the car. The functionality of Level 2 comprises of the driving and acceleration ADAS power. The human operator should, nevertheless, remain attentive. Level 2 instances are Audi Traffic Jam Assist, Cadillac Super Cruise, Autopilot, etc. Instances include Both facets of a driving automobile are carried out by level 3 robotics, however the human operator has to assume around when ADAS requires. The human operator must also be careful. In "Audi Traffic Jam Pilot" level 3 of optimization can be obtained. The second stage of autonomy allows the vehicles to execute all the functions as well as to control the world. Although ADAS performs all the tasks during the last stage of automation, people only are the travellers. In Stage 5, the system validates the location in GPS as well as the driver drove the passenger to that same endpoint directly regardless finding the help or knowledge from the person. Automotive industries are now looking for level 3. Tesla argues we are level 3, but Tesla's feedback is automatic level 2. Figure 1. Intelligent vehicle cyber-attack gateways Shows some of the potential cyber-attack gateways mostly on driverless vehicles. The machine is far more susceptible to theft by hackers as the amount of automation rises.

Any network-connected system will perform denial-of-service attack (Jaiswal & Chandra, 2017). IoT that we are using in the everyday lives transmits data on the web, transmits information and is processed in live time but is susceptible to hacking. The intelligent transportation system also communicates in full detail only with networks. The cyberwarfare trend reveals that under this risk the auto sector suffers. In addition, it could influence the rail. The recently installed rail service is

Modern Statistical Modeling in Machine Learning and Big Data Analytics: Statistical Models for Continuous and Categorical Variables

Niloofar Ramezani (2020). *Handbook of Research on Big Data Clustering and Machine Learning (pp. 135-151).*
www.irma-international.org/chapter/modern-statistical-modeling-in-machine-learning-and-big-data-analytics/241373