

Understanding threats to electric vehicles and effective countermeasures

3

Pimal Khanpara and Kruti Lavingia

Department of Computer Science and Engineering, School of Technology,
Nirma University, Ahmedabad, Gujarat, India

1 Introduction

The changes in the present climate conditions necessitate the replacement of conventional technologies with improved environment-friendly solutions. One of the main contributors to greenhouse gas emissions, among others, is transportation powered by fossil fuels. As an environment-friendly solution, electric batteries are used as the energy source in electric vehicles (EVs). More people have chosen the EV option, and the sales have exceeded almost half of the total sales in many nations [1]. In the upcoming years, it is anticipated that EV usage will continue to rise. In reality, governments are encouraging the use of EVs by deploying a significant number of charging stations in public charging facilities and preparing to outlaw the sale of conventional vehicles [2,3].

In addition, technological developments provide improved driving range and hassle-free charging, eliminating the existing barriers to consumers adopting EVs. The growing use of EVs necessitates a careful examination of infrastructure security and vehicle security [4]. Like conventional cars, EVs come with various functional units such as different sensors, controllers, and actuators to measure, process, and regulate multiple parameters inside and outside the car. Although EVs come with extra parts compared to conventional vehicles [5,6], an EV consists of parts to control both the hardware and software responsible for effectively utilizing electric power. Examples of such parts include the charging system and the battery system. Numerous research studies have already established the effects of prospective cybersecurity attacks on automotive systems. In addition, most available automobiles use the insecure controller area network as their internal network architecture, making them susceptible to hacker attacks [7].

Last but not least, privacy must be ensured to stop malevolent users from discovering private information about the driver, such as their whereabouts or routines. To stop these and other assaults, it is crucial to incorporate security and privacy measures into the design process. Focusing on the various facets of in-car communications, researchers looked at vehicle security [8]. But EVs come with particular parts that essentially offer various attack surfaces and exploitation spots. As depicted in EVs,