Chapter 7
Ensuring Security in Vehicular Cyber Physical Using Flexray Protocol

Neha Bagga
Guru Nanak Dev University, India & Lovely Professional University, India

Sheetal Kalra
https://orcid.org/0000-0003-0694-7468
Guru Nanak Dev University, India

Parminder Kaur
https://orcid.org/0000-0003-1954-3390
Guru Nanak Dev University, India

ABSTRACT

With evolving automotive technology V2V communication will follow an evolutionary path as well alerts are provided to driver to maintain safety on road and take timely decision for received warnings. V2I helps vehicle to share information with roadside components of Intelligent Transportation Systems. All the communication above is susceptible to be intercepted and wrong messages can be communicated by exploiting the integrity, or act of cyber terrorism can be performed. Erroneous communication done by attackers can lead to opening of airbags while driving, giving wrong indication of turning of vehicle, which in turn can cause loss of human life, damage to vehicles. ECU's are the easiest target for the attackers to gain access into the vehicle as communication protocols like CAN, LIN, FlexRay, MOST and Ethernet are connected to the ECU's. In this chapter authors would be discussing the Flexray protocol specifications which can be exploited to perform attacks and the corresponding potential security and safety effects of these attacks and propose

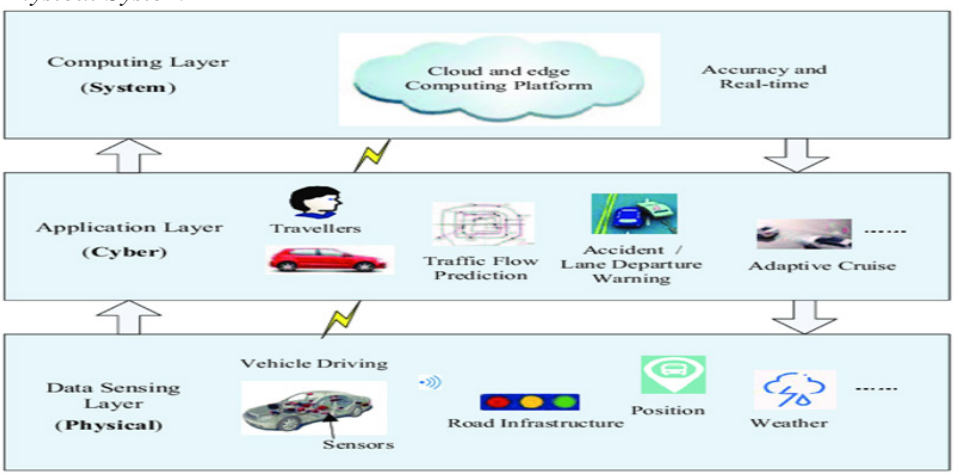
DOI: 10.4018/979-8-3693-5728-6.ch007

some futuristic security protections.

1. INTRODUCTION

1. Vehicular cyber-physical systems (VCPS) are arrangements of vehicles equipped with integrated computational, sorting, and real capabilities, allowing them to interact with their internal and external environments. Contemporary vehicles contain more than 100 electronic control units (ECUs) and numerous sensors and actuators, which are connected through various communication networks such as CAN, LIN and FlexRay. These integrated components consistently provide continuous control, status monitoring, and safety systems in vehicles. As vehicles continue to advance towards greater levels of automation and connectivity, they are becoming increasingly complex digital real-world structures (FlexRay Consortium, 2005) (Mateus & Königseder, 2014).

Figure 1. Bridging gap between Physical and Cyber World using Vehicular Cyber Physical System



VCPS are safety-critical systems, as any security breaches can directly endanger human lives. At the same time, increased connectivity also exposes them to cyber attacks aiming to take control or manipulate the system. Research shows that currently prevalent bus protocols like CAN are vulnerable, allowing attackers to inject malicious messages or take over ECUs once they gain internal access. Hence security in VCPS is an immensely critical issue that needs to be handled at multiple layers across hardware, networking and software.