

# Critical review on communication security between autonomous driver-less vehicles

Chang Yang

May 1, 2018

## 1 Introduction

For a long time the concept of car safety was synonymous with seatbelts, an adequately sized crumple zone, and air bags. Devices such as these protect drivers and passengers from physical dangers caused by accidents. But in the age of the connected car, safety functionality may also be impacted negatively by humans deliberately deploying cyber-attacks on the car similar to those seen on the internet for some time. Therefore cyber-security in the car becomes a priority.

## 2 Reviews

With the popularization and application of new communication technologies, the CAN bus, as an ancient communication technology, has not kept pace with the development of smart driving technology. Nowadays, the common communication methods of the Internet, such as Ethernet, 4G, and WiFi, are gradually applied to automobiles. The hackers' familiar network communication method makes new-generation cars more vulnerable.

In a typical V2X (Vehicle-to-everything) system, cellular networks and 802.1p protocols are used in the exchange of information between vehicles and the outside world.

## 3 Summary