The Autonomous Vehicle and Its Temptations

Vinton G. Cerf
Google

Self-driving vehicles must contend with many possibilities, including the behavior of bad actors.

I drive a Tesla. I work for Google, an Alphabet company. A sister company is Waymo, which is highly advanced in autonomous vehicle technology. What worries me has a lot to do with both the challenges of potentially buggy software but, much more serious, are the temptations to which our fellow human beings may give in. Bugs in software, including machine learning neural networks, can result in unexpected and unpredictable behaviors. Image recognition and classification is a key part of autonomous vehicle navigation. It must classify the images of vehicles and other objects in its surrounding area and make predictions of their immediate future behavior including provisions for the unexpected. A person on a bicycle may swerve into traffic. An incoming vehicle may try to make a turn before your vehicle enters an intersection. A blockage in the lane that the car is in should trigger either a slow down or an attempt to move out of the lane. All of these potential behaviors have to be accounted for in some measure if an autonomous vehicle is to successfully navigate a public street filled with a combination of traffic, vehicles of various kinds, pedestrians, bicycle or motorcycle riders, Segway riders, scooters and a mix of other objects—some stationery and some in motion.

The makers of autonomous vehicles must consider safety to be a highest priority—for passengers and for surrounding vehicles, people and objects in view. The ability to test the ensemble of algorithms used to animate self-driving vehicles is paramount—especially to validate behavior for low probability but potentially catastrophic situations like a small child chasing an errant ball into the street or an animal dashing across the road without warning. One important possibility is that fictitious but realistic inputs can be presented to the sensor systems or to the software receiving sensory signals to test whether the software does the "right" thing under all conditions.

In addition to my concerns about the functionality and reliability of the software used in autonomous vehicles, I worry about the misbehavior of humans who use these vehicles or, worse, choose to abuse them. It isn't hard to imagine that some people will find it attractive to vandalize autonomous vehicles because there is no human in the vehicle to observe or defend the vehicle from abuse. I have heard stories about robots that have been abused by humans who seem to enjoy interfering or even damaging them just because they can. The headlines about human drivers who ignore warnings that they need to take control of a supposedly "autonomous" vehicle are examples of deliberate human negligence. We are indeed a strange species!

One can also imagine hackers hoping to disrupt the operation of autonomous, communicating vehicles by launching denial of service attacks or sending malware or attempting to penetrate operating systems with the intent of disabling or otherwise confusing a self-driving vehicle.

Published by the IEEE Computer Society
1089-7801/18/$33.00 ©2018 IEEE

Moreover, since many autonomous vehicles carry a large complement of software, it is common for the makers to want to upgrade or repair errors in the code. By implication, it is vital that the vehicles be able to correctly reject any new software that cannot be confirmed as to origin or integrity. Digital signatures and signed hash codes over the new software can be used to increase the probability that the download is appropriate and valid. It is not hard to conclude that in addition to correct operation, the makers of self-driving vehicles will need to take into account a variety of challenges, not the least of which are brought about by people who don't have the best interests of the vehicles or their occupants in mind!

BIO

Vinton G. Cerf is vice president and chief Internet evangelist at Google, and past president of ACM. He's widely known as one of the "fathers of the Internet." He's a Fellow of IEEE and ACM. Contact him at vgcerf@gmail.com.