On-board computers and sensors could stop the next car-based attack

November 3 2017, by Jeremy Straub

Credit: Yusuf Çelik from Pexels

In the wake of car- and truck-based attacks around the world, most recently in New York City, cities are scrambling to protect busy pedestrian areas and popular events. It's extremely difficult to prevent

vehicles from being used as weapons, but technology can help.

Right now, cities are trying to determine where and how to place statues, spike strip nets and other barriers to protect crowds. Police departments are trying to gather better advance intelligence about potential threats, and training officers to respond – while regular people are seeking advice for surviving vehicle attacks.

These solutions aren't enough: It's impractical to put up physical barriers everywhere, and all but impossible to prevent would-be attackers from getting a vehicle. As a researcher of technologies for self-driving vehicles, I see that potential solutions already exist, and are built into many vehicles on the road today. There are, however, ethical questions to weigh about who should control the vehicle – the driver behind the wheel or the computer system that perceives potential danger in the human's actions.

A computerized solution

Approximately three-fourths of cars and trucks surveyed by Consumer Reports in 2017 have forward-collision detection as either a standard or an optional feature. These vehicles can detect obstacles – including pedestrians – and stop or avoid hitting them. By 2022, emergency braking will be required in all vehicles sold in the U.S.

Safety features in today's cars include lane-departure warnings, adaptive cruise control and various types of collision avoidance. All of these systems involve multiple sensors, such as radars and cameras, tracking what's going on around the car. Most of the time, they run passively, not communicating with the driver nor taking control of the car. But when certain events occur – such as approaching a pedestrian or an obstacle – these systems spring to life.

Warning systems can make a sound, alerting a driver that the car is straying out of its lane, either into oncoming traffic or perhaps off the road itself. They can even control the car, adjusting speed to maintain a safe distance from the car ahead. And collision avoidance systems have a variety of capabilities, including audible alerts that require driver response, automatic emergency braking and even steering the car out of harm's way.

Existing systems can identify the danger and whether it's headed toward the car (or if the car's headed toward it). Enhancing these systems could help prevent various driving behaviors that are commonly used during attacks, but not in safe operations of a vehicle.

Preventing collisions

A typical driver seeks to avoid obstacles and particularly pedestrians. A driver using a car as a weapon does the opposite, aiming for people. Typical automobile collision-avoidance systems tend to handle this by alerting the driver and then, only at the last minute, taking control and applying the brakes.

Someone planning a vehicle attack may try to disable the electronics associated with those systems. It's hard to defend against physical alteration of a car's safety equipment, but manufacturers could prevent cars from starting or limit the speed and distance they can travel, if the vehicle detects tampering.

However, right now it's relatively easy for a malicious driver to override safety features: Many vehicles assume that if the driver is actively steering the car or using the brake and accelerator pedals, the car is being controlled properly. In those situations, the safety systems don't step in to slam on the brakes at all.

These sensors and systems can identify what's in front of them, which would help inform better decisions. To protect pedestrians from vehicle attacks, the system could be programmed to override the driver when humans are in the way. The existing technology could do this, but isn't currently used that way.

It's still possible to imagine a situation where the car would struggle to impose safety rules. For instance, a malicious driver could accelerate toward a crowd or an individual person so fast that the car's brakes couldn't stop it in time. A system that is specifically designed to stop driver attacks could be programmed to restrict vehicle speed below its ability to brake and steer, particularly on regular city streets and when pedestrians are nearby.

A question of control

This poses a difficult question: When the car and the driver have different intentions, which should ultimately be in control? A system designed to prevent vehicle attacks on crowds could cause problems for drivers in parades, if it mistook bystanders or other marchers as in danger. It could also prevent a car being surrounded by protesters or attackers from escaping. And military, police and emergency-response vehicles often need to be able to operate in or near crowds.

Striking the balance between machine and human control includes more than public policy and corporate planning. Individual car buyers may choose not to purchase vehicles that can override their decisions. Many developers of artificial intelligence also worry about malfunctions, particularly in systems that operate in the real physical world and can override human instructions.

Putting any type of computer system in charge of human safety raises fears of putting humans under the control of so-called "machine

overlords." Different scenarios – particularly those beyond the limited case of a system that can stop vehicle attacks – may have different benefits and detriments in the long term.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: On-board computers and sensors could stop the next car-based attack (2017, November 3) retrieved 23 April 2024 from https://phys.org/news/2017-11-on-board-sensors-car-based.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.