cosmosmagazine.com

Driverless cars can be tricked, new strategy fools sensors

16 March 2022 / Imma Perfetto

5-6 minutos

Like something out of a spy movie, researchers have demonstrated the first attack strategy that can fool industry-standard autonomous vehicle sensors into believing nearby objects are closer or more distant than they appear – without being detected.

The research suggests that in order to fully protect driverless cars from attacks, it may be necessary to add 3D camera capabilities or the ability to share data with nearby cars. The findings will be presented at the 2022 USENIX Security Symposium in August in the US.

One of the biggest development challenges for autonomous driving systems is protecting against attacks, and a common way to do this is for separate instruments to check data against each other to confirm their measurements make sense.

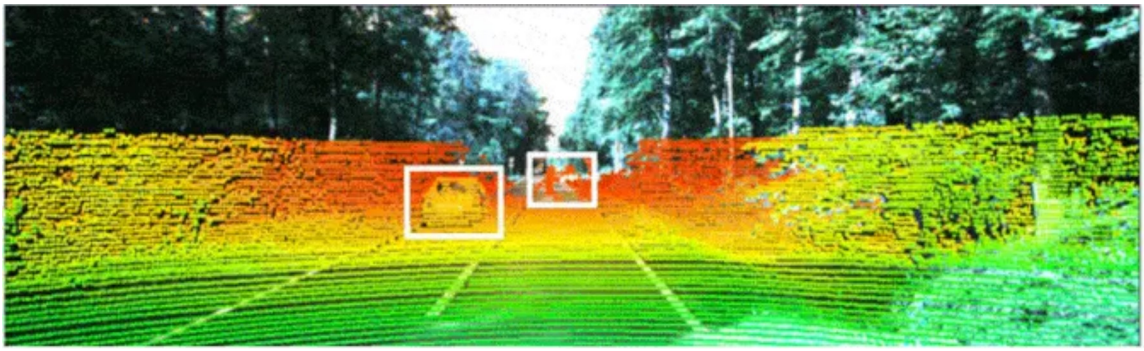
The most common technology currently used to do this by autonomous car companies is the industry-standard dual-camera LIDAR sensors, which combines 2D data from

cameras and 3D data from LIDAR.

LIDAR (Light Detection and Ranging) is a remote sensing method that uses pulses of laser light to measure distance ranges. The distance to an object is calculated by targeting it with the laser and measuring the time taken for the reflected light to return to the sensor.

So far, this combination has been very successful against attempts to trick it. At least, until now.

The attack strategy works by shooting a laser gun into a driverless car's LIDAR sensor to add false data points. Previous research has shown that a driverless car can recognise an attack if these data points are wildly at odds with what its camera is seeing. But 3D LIDAR data points carefully placed by a laser within a certain area of the camera's 2D field of view *can* fool the system, according to this new research.



Researchers have shown that a popular method to secure LIDAR sensors against "naive attacks" is still vulnerable at longer distances and only works at short distances. Here, a LIDAR system is fooled into thinking a car is somewhere

else until it becomes too late to avoid a sudden and drastic course correction. Credit: Spencer Hallyburton/Duke University

“This research shows how adding just a few data points in the 3D point cloud ahead or behind of where an object actually is, can confuse these systems into making dangerous decisions,” says co-author Miroslav Pajic, professor of Electrical and Computer Engineering at Duke University, USA.

This vulnerable area stretches out in front of a camera lens in the shape of a frustum – a 3D pyramid without its tip. If the attack laser places a few data points in front of or behind another nearby car, the ‘frustrum car’ system’s perception of that car can shift by several metres.

“This so-called frustum attack can fool adaptive cruise control into thinking a vehicle is slowing down or speeding up,” says Pajic. “And by the time the system can figure out there’s an issue, there will be no way to avoid hitting the car without aggressive manoeuvres that could create even more problems.”

This isn’t much of a problem for everyday driverless cars, as there isn’t much risk of someone taking the time to set up lasers on a car or roadside object. But the risk increases in military situations where single vehicles can be high-value targets.

So how do we protect against this? According to Pajic, it’s all about added redundancy.

For example, if cars had “stereo cameras” – a type of camera with two or more lenses that can capture 3D images – with overlapping fields of view, they could better estimate distances and assess LIDAR data that does not match their perception. Another option is to develop systems that enable cars in close proximity to one another to share some of their data.

“With all of the work that is going on in this field, we will be able to build systems that you can trust your life with,” says Pajic. “It might take 10+ years, but I’m confident that we will get there.”