Lane Gramling
EECS 700
Reading 14

Summary - Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR

This paper focuses on studying the operation of sensors controlling automated vehicles and how they can be exploited using cheap hardware available to consumers. Among the attacks discussed are blinding, jamming, replay, relay, and spoofing attacks. Additionally, the paper proposes defense mechanisms to hedge against the effectiveness of these attacks.

Contributions

Before diving into the details of their major points, the authors first specify the type of AV sensor hardware they are working with, including their camera and LiDAR sensor, and explain the technical specifications that enable their attacks. Afterwards, an attack model is outlined, which outlines three types of attacks: a front/rear/side attack, a roadside attack, and an 'evil mechanic' attack.

Their attack model and sensor specifications lead the paper to its first major contribution, which is an outline of attacks that are possible on the sensor hardware they are testing. The authors first explain a number of possible attacks on an AV's camera. The first of these is a blinding attack, which works by emitting light into the camera to obfuscate the objects usually detected by it. Data expressing the effectiveness of this attack (and all demonstrated attacks) is available in the paper. The second camera attack works by bursting light at the camera in a manner that fools around with the camera's auto-balancing sensor controls, which is harder to detect than the first. The second string of attacks that the authors contribute focus on the LiDAR system. These attacks operate by fooling the LiDAR sensor's standard function by creating false echoes through relaying the LiDAR signal or spoofing its return signal.

The next major contribution of the paper is a number of countermeasures suggested by the authors to mitigate the efficacy of their demonstrated attacks. For example, redundancy was suggested as a means of reducing the likelihood that a sensor controlling an AV (or a multitude of AVs controlled by sensors) vulnerable to attack would succeed as an attacker would need to spoof multiple combined wavelengths. Other examples include randomizing the period of LiDAR probe waves, shortening the period to reduce the attack window, and sending out multiple probes. In summation, the authors draw the conclusion that the easiest and most effective countermeasures to their demonstrated LiDAR attacks would consist of adding complexity to the waves to make them harder for a malicious actor to affect.

Limitations

As noted by the authors, a number of limitations exist in their attacks, primarily relating to the spatial environment that the attacks are able to work with, and the space their testing was taking up. For example, the authors point out that their attack range is limited to about 100m for their LiDAR tests, which becomes a small window for attack when acting as a stationary adversary against a vehicle moving at potentially high speeds. Additionally, their testing was all performed in laboratory conditions rather than in a more true-to-life environment such as outdoors with a real moving vehicle or AV. One limitation not acknowledged by the paper is that many of their attacks on the camera sensor could be done on a human as well, including both their blinding attacks and their attacks to confuse the camera's auto-balancing sensors, albeit of course a necessary need to adjust the types and brightnesses of lights used in the experiments. And despite this, it seems uncommon that adversaries sit on the side of the road shining lasers into motorists' eyes.

Future Work

Given the ideas the papers gave, there seems to be quite a bit more exploration that can be done into working with LiDAR systems to obfuscate and secure AV LiDAR signatures from spoofing, relaying, or other attacks. This realm of study also seems useful when considering that in the future, the anticipated goal is for each car on a busy freeway to be an AV, likely bouncing LiDAR signals off every other car doing the same thing. It seems clear that whether or not interference to an AV's LiDAR system is intentional, it is worth exploring how signal collision avoidance and cooperation may be implemented.