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

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

Sensors are important part of the automated vehicles as these vehicles highly rely on the input from the sensor data. Hence, security of these sensors is very important, as these sensors are highly available and thus highly risky. Successful autonomous vehicles such as Stanford Shelley, AnnieWAY or Google driverless car use LiDAR (Light Imaging Detection and Ranging), to detect objects (acquisition of geometry) and camera to for traffic light signal detection and delineation (hence the paper considers attacks on these two sensors). An attacker attacks in a way that he tries to degrade the sensor data, and such attacks are dangerous as can lead to fatalities. The paper discusses attacks on camera and LiDAR (the authors used MobilEye C2-270 camera and LiDAR ibeo LUX 3 in their system model). Authors considered three attack scenarios, viz. Front/rear/side attack, Roadside attack and Evil mechanic attack, in their attacker model. The camera can be attacked by blinding it or confusing the auto controllers. The LiDAR can be attacked by relaying or spoofing the signal. Paper also proposes countermeasures against these attacks. To prevent the attacks on the camera, multiple cameras can be used (redundancy) or the existing cameras can be modified (optics and materials). The attacks on the LiDAR can be stopped by combining multiple wavelength LiDAR (redundancy), by probing multiple times and by shortening the pulse period.

2 Contribution

The paper presents the attacks (by considering different types and conditions) on the Camera and LiDAR sensors and proposes countermeasures for those attacks. Paper also discusses the limitations of their attacks. Most importantly pointing out these kind of attacks is their biggest contribution.

3 Strengths

I liked that they pointed out the limitations of their own proposed attacks. They not only proposes the attacks (and successfully constructs them), but also gave the countermeasures.

4 Limitations

I think the authors discusses the limitations of their attacks in detail. In addition to that, I think there are limitations in their suggested countermeasures. More importantly using more cameras or modifying the existing once, would increase the cost a lot. Also, I think that they should have tested these attacks on real vehicles.

5 Future Work

Paper considered three attack scenarios, but other (more) attack scenarios can also be considered. These kinds of attacks can be tested on real (successful) vehicles, which are being tested and used on road.

References

[1] Jonathan Petit and Bas Stottelaar and Michael Feiri *Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR* (2015)