Rajat Sethi

CPSC 8580

**Paper Summary 9 - Towards Robust LiDAR-based Perception in Autonomous Driving: General Black-box Adversarial Sensor Attack and Countermeasures**

Autonomous Vehicles are one of the newest and most dangerous technologies in development right now. As such, it is quite imperative that security measures are implemented into their systems. According to the paper, LiDAR – the sensor that uses light signals to determine the car’s surroundings, may have a spoofing vulnerability if a crafted light signal is sent to the device. While this type of attack is difficult to accomplish in a black-box model, it is still possible. To prevent these attacks, the researchers invented CARLO, a detection system that locates and filters out spoofed data.

The paper looks at CARLO: The oCclusion-Aware hieRarchy anomaLy detectiOn system. CARLO looks for the number and location of spoofed points in LiDAR’s data. If it detects a large number of spoofed points in the same location, then it determines those points as an attack and responds accordingly.

One of the main weaknesses of the paper is the reliance on black-box testing. Since the researchers could not use the car’s source code, they were limited on what attacks they could try. While CARLO worked well on the attacks they could test, there may be several unknown attacks that CARLO could not notice.

As discussed in the paper, one of the main aspects of future improvement is the use of CARLO in a practical scenario. The paper was written at the University of Michigan, likely in their controlled MCity environment. A more robust and practical test would have to occur on a real road with many more obstacles, cars, and perhaps even false positives. This also applies to the attacks as well, since it may be quite difficult to send a spoofed signal to a moving vehicle with a dynamic environment.