Outline:

1.Which 2 sensors are used most often?

LiDAR (Light Detection And Ranging) and camaera.

2.How an attacker can do to these sensors?

an attacker can perturb sensor data to change object classification (misclassification) [9], introduce fake objects (false positives) [10, 11], and remove existing objects (false negative) [12,13], each with devastating consequences at the driving decision and control levels.

3.What does this paper do?

Black-box attack to the camera-LiDAR fusion. (frustum attack)

4.What kind of attacks are for cameras?

object detection and classification are vulnerable when using only camera data

5.LiDAR-sproofing defences:

independent of the perception model: CARLO (if there are many LiDAR points appearing to pass through a detected object, the object is likely a false positive (FP)), Shadow-catcher

model-based defenses: SVF, LIFE

6.Why frustum?

2D detections of a target vehicle from the victim camera’s front-view cannot resolve range, and thus the 3D uncertainty of a 2D (camera) detection defines a frustum from the camera image plane in the direction of the target vehicle.

7. Frustum:

For the frustum attacks, we assume the attacker knows the approximate position of the target object so as to obtain a frustum region for spoof point placement.

🡺 Points are placed behind or in front of existing objects so that they have front-view consistency.

S1: Spoofer on target. A spoofer is placed on a target car and aimed at victim (the target AV owner/passengers may or may not be aware of this). The target car does not have to be endangered for this to have impact because the attacker creates FPs that cause the victim to perform evasive maneuvers. The target car is by definition in line with its own frustum. Any spoofed points along the line-of-sight (LOS) between the target and the victim will remain in the frustum.

S2: Spoofer on other vehicle in line. Spoofer is placed on a non-target car on the line defined by the victim AV and target vehicle. This scenario arises often in natural driving, as a lane, which is usually locally straight, helps cars stay in line

with each other, and thus in each others frustums.

🡺 In fact, a frustum attack only requires LOS between the spoofing device and the victim AV with at least one object in the scene

8. Weakness:

CARLO FP: naive spoofing is stealthy to CARLO when placed outside of front near.

🡺 an increase in range leads to spoofed instances that appear more similar to normal instances under the CARLO hypothesis.

CARLO FN: Specifically, an adversary can spoof points behind valid objects (in no particular spoofing pattern, unlike the attacks required by [10,11]) which will trigger CARLO into believing the detected object is invalid.

9. Experiment:

15-40 m:nearly 100% of instances using any of the perception algorithms are attackable.

🡺 even spoofing just 2 points may be enough to obtain FP outcomes at the site of spoofed point.

(more successful as the range to target vehicles increases.)

Ideas:

This paper proposed a new method of attack: frustum. Given that the attack for only one sensor might be defenced if there are the help of other sensors, the attackers should also consider the consistency between the data of sensors. In this paper, the author considers the consistency of cameras and LiDAR, so the spoofing points are around the target vehicles. I think, what is interesting is that in the papaer, it said that the state-of-art technology cannot defend this kind of attack because only 2 spoofing points could be enough to induce a false positive. However, the experiments of this paper didn’t run the real experiment but only the simulation. According to the last paper of LiDAR-spoofing, this success rate of attack should be taken with a pinch of salt.