R1 "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle"

Target System :

Sensors mounted in autonomous vehicles, particularly Ultrasonic sensors , Forward-looking cameras, a Medium Range Radar(MRR) which are used to detect obstacles

Vulnerability :

The data for sensing passes through unprotected channel.

An appropriate signal, which means that it has the similar frequency and data form compared to the original signal for sensors, can deceive the sensor.

Automotive cameras could be damaged by strong light.

Exploitation :

(1)Ultrasonic

- Jamming attack can make obstacles undetectable and force the car to stop during the self-parking.
- Spoofing attack can deceive the sensor into detecting pseudo-obstacles.

(2)MMW Radars

- Jamming attack can make detected objects disappear.
- Spoofing attack can alter the object distance.

(3) Automotive cameras

- The optical source force it not to work, causing the car to have trouble in camera-based functionalities.

Evaluation :

(1)Ultrasonic(frequency : 40~50Khz)

Setup : Arduino Un board used to generate controllable wave associated with a jamming signal, a spoofing signal. An obstacle is always located certain distance to sensors, all sensor could detect it.

Jamming attack :

- Tested on 8 ultrasonic sensors : Some of them thought that there was very close object under the jamming attack, others thought that an obstacle was far from them.
- Tested on 4 different models car : the obstacle was not detected by the car.
- On Tesla Model S with Automatic parking : It would be stop at once as soon as they launched jamming.

Jamming attack can disturb the sensor reading.

(2) MMR Radars(76~77 GHz, on Tesla Model S)

Signal analysis : To understand its characteristic, they analyzed the radar's signal thorough the signal analyzer and the software. They could figure out the center-frequency(76.65Hz), the bandwidth(450MHz), the type of modulation(FMCW).

Jamming : When turn on the jamming, the car disappears at once

Spoofing : fail.

(3) Automotive cameras

- They set up experiment with the calibrated board positioned 1m from the camera and the laser being pointed either at the camera and the board. They tested with 650nm red laser, 850nm infrared LED spot and LED spot of 800mW power. Aiming LED at both the board and the camera leads to blinding effect sufficiently and the laser pointing directly the camera leads to damage of the camera. The others didn't cause blinding enough.

Defense:

Alarm of malicious attack or system failure. If the car cannot interpreted the signal of the sensor, it notice the user which radar have some trouble.

Cover the Laser filter to camera.

F.W : It need to measure how fast the autonomous vehicle react when the obstacle suddenly appears. And analyze all sensor for this situation.