I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights

Rahavee Prabakaran

The paper investigates the features of Infrared light and introduces a new security challenge called I-Can-See-the-Light-Attack that can alter environment perception results and introduces Simultaneous Localization and Mapping errors to the Autonomous vehicle. By leveraging these identified features, the paper explores to generate invisible traffic lights, create fake invisible objects, ruins the in-car user experience and introduces SLAM errors to the AV. The paper later implements the ICSL Attack by using off-the -shelf IR light sources and conducts an extensive evaluation on Tesla Model 3 and an enterprise-level autonomous driving platform under various environments and settings. There are three aspects that the paper accomplishes, one it analyzes the effect of invisible IR light on the autonomous vehicle, two conducts extensive real-world experiments by using a Tesla Model 3 and three, defends against the ICSL Attack. The paper describes the system architecture of the Autonomous vehicle, the spectral sensitivity of silicon photo detector and a human eye and also publishes a survey of the IR light visibility. The paper also describes the attack in which the attacker creates fake invisible traffic signal, then the attacker uses IR light to alter AV's environment perception results, then the attacker blinds the AV's camera to create frequent system alters and the attacker controls the IR sources on the road to alter AV's SLAM results. The attack goal is to alter the environment perception and SLAM results of an autonomous vehicle embedded with different sensors. The vulnerability of the AV to ICSL Attack is due to the fact that Humans cannot see IR lights, the enterprise-level autonomous vehicle has to trust the data gathered from cameras, the Invisible IR light is detected as the visible magenta color in the camera and during the SLAM process, it is possible for the invisible IR source to be selected as the key points. In the threat model it is assumed that the positions of the camera on the target autonomous vehicle. So in the experimental setup there is implementation of IR light LEDs in the traffic light LEDs in the traffic light to create fake invisible red signal. According to the paper the attacker can create following harmful results by performing the following attack, namely Alter Environment Perception Results, Ruin the In-car User Experience and introduces SLAM errors. The ICSL attacks on Tesla are explored where in the experimental setup IR light is used to blind the right main forward camera and narrow forward camera of Tesla. Then there is an experiment for Ruin In-Car User Experience includes Blind the triple forward cameras of Tesla and the system is triggered. For studying the ICSL Attacks on SLAM system, the experiment is carried out in an indoor parking lot. The paper also goes on to propose a light weight ICSL attack detection module to defend against ICSL Attack without requiring a hardware modification by utilizing a unique feature of IR light. The IR filter have some disadvantages such as high implementation cost and filtering out useful information. The proposed detection consists of two parts namely the Light source detector & filter module and the Reflection Detection module. Finally, the paper discusses the trade-offs between defense solutions. The proposed attack has some advantages which introduces severe security risks to the Avs.

Three strong points:

1. The system architecture of the autonomous vehicles are represented well.
2. The experimental setup for each of the harmful results of the attack is described well.
3. The mathematical equations for the SLAM attack model is described well.

Three weak points:

1. The paper did not mention on what basis the defense method against ICSL is proposed.
2. The paper did not mention why this specific attack is of more importance than other attacks on Avs.
3. The architecture of the defense detection is not described in terms of hardware.