Abstract

Depth estimation-based obstacle avoidance has been widely adopted by autonomous systems (drones and vehicles) for safety purpose. It normally relies on a stereo camera to automatically detect obstacles and make flying/driving decisions, e.g., stopping several meters ahead of the obstacle in the path or moving away from the detected obstacle. In this poster, we explore new security risks associated with the stereo vision-based depth estimation algorithms used for obstacle avoidance. By exploiting the weaknesses of the stereo matching in depth estimation algorithms and the lens flare effect in optical imaging, we propose DoubleStar, a long-range attack that injects fake obstacle depth by projecting pure light from two complementary light sources.

DoubleStar includes two distinctive attack formats: beams attack and orbs attack, which leverage projected light beams and lens flare orbs respectively to cause false depth perception. We successfully attack two commercial stereo cameras designed for autonomous systems (ZED and Intel RealSense). The visualization of fake depth perceived by the stereo cameras illustrates the false stereo matching induced by DoubleStar. We further use Ardupilot to simulate the attack and demonstrate its impact on drones. To validate the attack on real systems, we perform a real-world attack towards a commercial drone equipped with state-of-the-art obstacle avoidance algorithms. Our attack can continuously bring a flying drone to a sudden stop or drift it away across a long distance under various lighting conditions, even bypassing sensor fusion mechanisms. Specifically, our experimental results show that DoubleStar creates fake depth up to 15 meters in distance at night and up to 8 meters during the daytime. To mitigate this newly discovered threat, we provide discussions on potential countermeasures to defend against DoubleStar.