Lane Gramling
EECS 700
Reading 13

Summary - Controlling UAVs with Sensor Input Spoofing Attacks

This paper focuses on an attack method for taking control of UAVs. Specifically, the authors show that with knowledge of the Lucas-Kanade optical flow method, an adversary can craft particular patterns with lasers or projectors to project an image onto the ground plane, which are designed to fool the UAV's software by feigning and manipulating features that are detected by the UAV's input sensors. The paper dubs this attack a sensor input spoofing attack.

Contributions

To preface their key point, the authors first give an outline for what types of sensors UAVs typically use, and the role the respective sensor data plays in the overall navigation system. As noted by the authors, sensor input spoofing can potentially prove a difficult attack vector to solve, because UAVs are dependent on their sensor input data to properly navigate and maintain stability. Additionally, a brief rundown of the Lucas-Kanade method for optical flow is given, which leads the paper to its major contribution.

The major contribution of the paper is an explanation of how an understanding of the Lucas-Kanade optical flow method can be used to specifically construct an adversarial pattern to project onto the ground plane beneath the UAV, such that the UAV's input sensors are fooled into detecting the malicious pattern's features as the natural ground features that the algorithm was designed to reference. Since these features are under control of the adversary, the adversary can manipulate the pattern to exert control over the UAV. Given this realization, the authors also contribute information regarding a series of tests under different environmental variables such as surface type, in addition to using both lasers and projectors for creating the malicious patterns. The authors follow up these tests with data and surrounding discussion in regards to the efficacy of the attacks under the various conditions. The authors then use this information to outline how sensor input spoofing attacks can be simulated, allowing for deeper insight into the foundations of what is going on with how the optical flow method and corner detector interprets the spoofed sensor input.

Complimenting the contributions to the offensive side of this study, the paper postulates a defense mechanism, proposing a modification to the Lucas-Kanade optical flow algorithm which filters out outliers and reduces the efficacy of their previously described attack. Their proposal implemented a weighted RANSAC algorithm into the optical flow method, which also carried context from previous frames. Altogether, this modification reduced the efficacy of the best adversary tested by the authors from 45% to 29% under optimal conditions for the adversary.

Limitations

The paper gave a complete evaluation on the case study in focus, including a balanced emphasis on offensive techniques, defensive mitigations, and supporting data on the effectiveness of each. In terms of limitations, most of the research was done on smaller UAVs given assumptions of lower altitudes, and only one kind of sensor input spoofing attack was explored. It would be interesting to see what potential there is for these attacks on UAVs operating at higher altitudes, or other attack vectors for sensor input.

Future Work

As noted in the paper, there is a number of potential directions for exploring future work in the realm of sensor input spoofing attacks. Examples listed in the paper include an expansion to the repertoire of potential sensor attacks, improving robustness on the hardware level, or combining data from multiple sensors for optical flow computations. Additionally, further exploration could be done into how adversarial machine learning could accelerate and optimize the efficiency of sensor attacks in the future.