Controlling UAVs with Sensor Input Spoofing Attacks

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

Autonomous vehicles rely on sensors for their operation. The paper introduces an idea of an attack, in which the attacker can take a direct control over the autonomous vehicle, with the knowledge of the optical flow sensor algorithms. They called this a 'sensor network spoofing attack'. In order the attack to work, the attacker must meet the following requirements, viz. environment influence requirement, plausible input requirement and the meaningful response requirement. Paper shows that the algorithms (eg. Shi-Tomasi) employed by optical flow sensors are vulnerable to spoofing attacks. Paper demonstrates a spoofing attack aginst the Lucas-kanade method of optical flow estimation. The authors used two consumer-grade UAVs, the AR.Drone 2.0 and the APM 2.5 ArduCopter for experimentation, as UAVs are highly available, as well as safety critical. Lastly, paper proposes RANSAC and weighted RANSAC algorithms for defending against 'sensor network spoofing attacks'. Weighted RANSAC outperforms Lucas-kanade. "The best adversary for Lucas-Kanade picks up about 45% of the adversary movement, while under the same adversary weighted RANSAC is affected by 29% only".

2 Contribution

Paper introduces a new attack called 'sensor network spoofing attack' and shows that existing algorithms employed by optical flow sensors are vulnerable to this type of attacks. Paper shows that these attacks (on UAVs) are possible in indoor, as well as outdoor settings. Paper proposes RANSAC and weighted RANSAC and shows that weighted RANSAC outperforms Lucas-kanade by a wide margin.

3 Strengths

First, the paper is very well written (It was really difficult for me to find limitations, most of them can be considered as a future work), it explains the problem (Spoofing attack) and gives the effective solution (RANSAC). Second, in all of the cases (experimental), weighted RANSAC outperforms Lucas-Kanade, hence it is certainly better. Third, I liked that the authors considered different scenes like tile, carpet, concrete, grass while experimentation.

4 Limitations

RANSAC will fail in the attacks in which an adversary can control a large number of features (number of adversarial features dominate the background features). Weighted RANSAC outperforms Lucas-Kanade, but it is still vulnerable.

5 Future Work

As authors suggested, it is important to consider the spoofing attacks on LIDAR and sonar, as both of these are used to detect the proximity to the obstacles (i.e. safety critical). The hardware robustness of the system must be increased (eg. using high resolution camera). Also, it may be possible to bound the displacement of the optical flow system in a number of ways such as maximum speed, perceived light gradient, etc". Sensor fusion must be used to increase the difficulty of spoofing attacks.