Paper: An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs

Summary:

The paper acknowledges limitations in the field on the behavior of UAVs under GPS spoofing attacks in real-time and hence goes on to understand the feasibility and requirement for demonstrating this attack relying solely on spoofing GPS to take complete takeover without crashing. It also highlights the importance of careful manipulation of spoofing signals required in realtime for successfully exploiting the vulnerability shown by COTS UAVs. Since UAVs rely heavily on GPS for positioning and navigation for autonomous operation in a pre-programmed manner it proves to be the single-point failure of UAVs. Since spoofing GPS can be done using an RF transmitter it would give the attacker an edge without compromising flight control software or command and control radio link, with the only limitation to work around being the amplification of RF signal.

The previous works have mainly focused on changing or hindering the motion of UAVs in random directions or analyzed standalone GPS receivers which resulted in results like uncontrolled acceleration in simulations or just diversion of UAVs without maneuvering ability. This paper performs real-time experiments on a variety of drones and uses it’s over GPS signal generator to give strategies for velocity control, direction control, human handling of drones via GPS spoofing, and triggering fail safes for a safe landing.

Strengths:

1. This paper shows that the proposed implementations have been tested on commercially available UAVs, it has addressed the possibility of precise control and actual responses using different spoofing attacks on UAVs like DJI, Autel and arducopter for longer distances.
2. It works around the problem of introducing predefined static location by designing and implementing a real time GPS signal generation for configuring arbitrary trajectory to better handle changes to GPS signals in real time.
3. The paper explains all the experiments, assumptions and observations like directionality of UAV, failsafes triggers, rapid acceleration causes, to name a few that are required for developing a realtime GPS system controlled by user input.

Weakness:

1. Since the analysis is done in a controlled environment, as the paper highlights, this results in accounting for the best case scenario where only the attacker’s gps spoofing to takeover GPS is considered. In reality, environmental factors like wind and temperature would definitely affect UAVs performance and make a difference when analysing the success and robustness of this technique.
2. Synchronizing the spoofed GPS signal with the target device's internal clock is also a considerable challenge since it is used to time-stamp the received GPS signals. This requires a high-precision clock synchronised with the GPS time reference and capable of generating a signal that’s precisely aligned with the genuine GPS signal.
3. Spoofing in the correct direction indirectly has an inherent challenge of understanding that the direction of spoofing signals results in the UAV shifting in the opposite direction, which makes it crucial for the attacker to manuevering correctly, especially making It harder when UAV isn’t in visible sight.