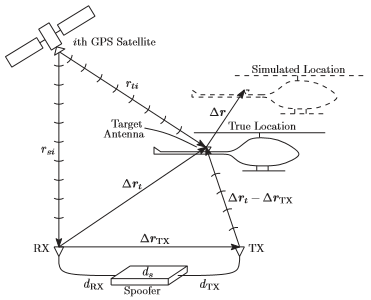
[ATT-SPOOF]kerns2014

The theory and practice of unmanned aerial vehicle (UAV) capture and control via Global Positioning System (GPS) signal spooﬁng are analyzed and demonstrated. The goal of this work is to explore UAV vulnerability to deceptive GPS signals.. During post-capture control, the spoofer manipulates the true state of the UAV, potentially resulting in the UAV ﬂying far from its ﬂight plan without raising alarms. Both overt and covert spooﬁng strategies are considered, as distinguished by the spoofer’s attempts to evade detection by the target GPS receiver and by the target navigation system’s state estimator, which is presumed to have access to non-GPS navigation sensor data GPS receiver tracking loops are analyzed and tested to assess the spoofer’s capability for covert capture of a mobile target.

[ATT-SPOOF]mobicom2016