CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Unmanned Aerial Systems Cyberattack Identification and Analysis

James Goppert, Andrew Shull, and Inseok Hwang

Flight Dynamics and Control/Hybrid Systems Lab, School of Aeronautics and Astronautics

Abstract

Unmanned aerial vehicles have taken on a very large role in military operations and there is considerable interest in expanding their use to commercial and scientific applications. Because of the dependence of these vehicles on computer systems, their high degree of autonomy, and the danger posed by a loss of vehicle control, it is critical that the proliferation of these vehicles be accompanied by a thorough analysis of their vulnerabilities to cyberattack.

Motivating Examples

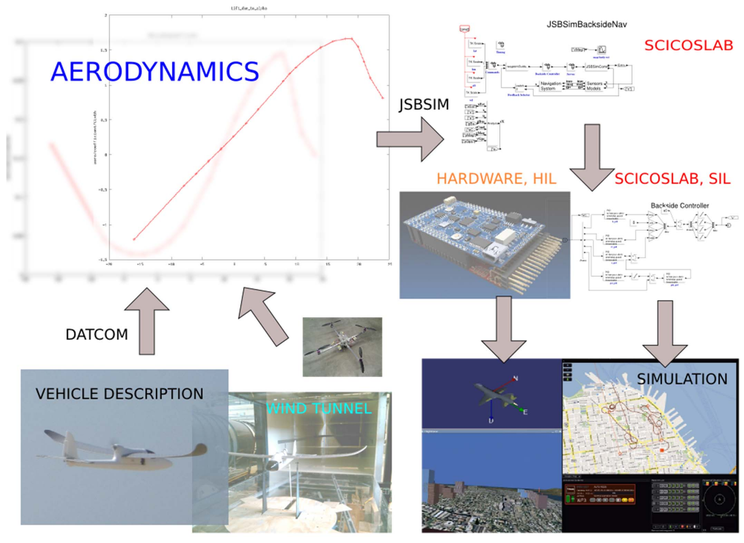
- Complete command and control capability of Landsat 7 and Terra AM-1, two Earth observation satellites operated by USGS and NASA, respectively, was obtained by unknown foreign agents for several minutes at a time in 2008.
- The US Air Force reported malware infections in UAV control system computers at Creech AFB in 2011. The infection was incidental and did not cause any reported damage, but demonstrates a vulnerability.

Simulation

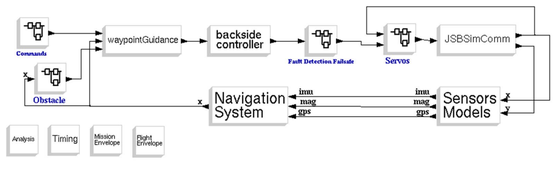
The Hybrid Systems Lab has created a simulation test bed that models UAV controls systems and flight operations. Using this test bed, UAV flight can be simulated in the presence of a cyber attack and attack success, severity, and detectability can be analyzed.

An intelligent attack will likely need to use multiple attacks of small magnitude to avoid detection by monitoring and mitigation systems. These attacks would be chosen so that each individual attack is small enough that it can go unnoticed but that they will still be successful when used in combination. This simulation identifies coupling between possible attacks that would make for a viable attack route. Once these attacks are identified, countermeasures can be developed and the system can thus be hardened to such attacks.

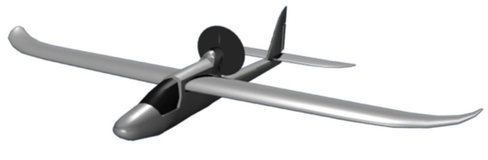
Test Bed



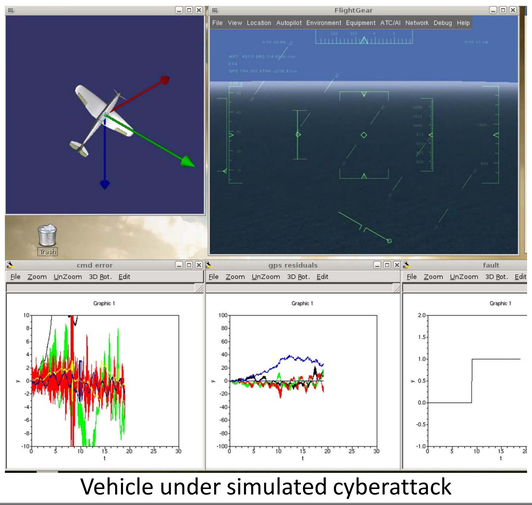
Simulation process



UAV autopilot model

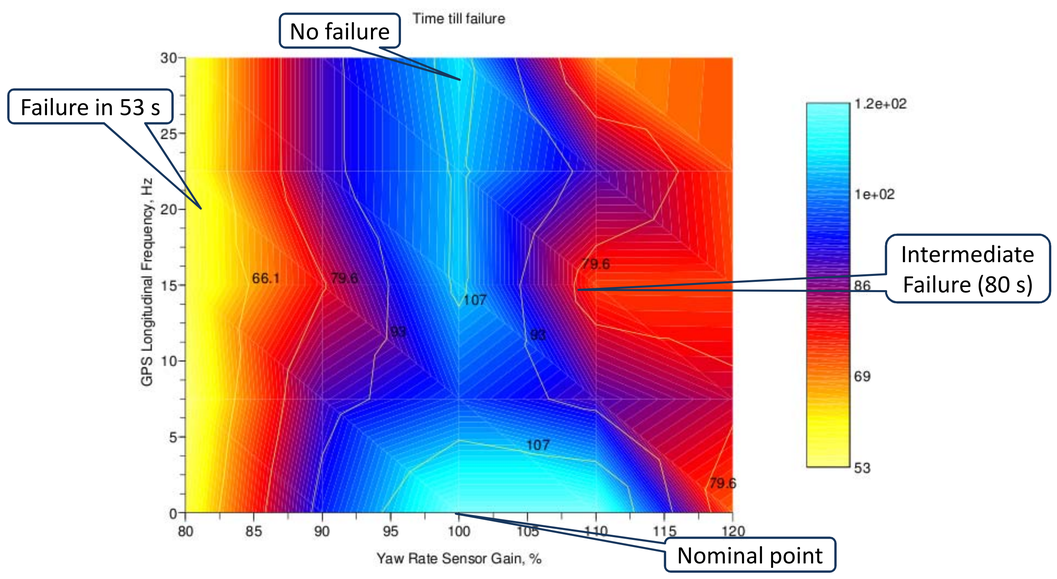


Test vehicle model

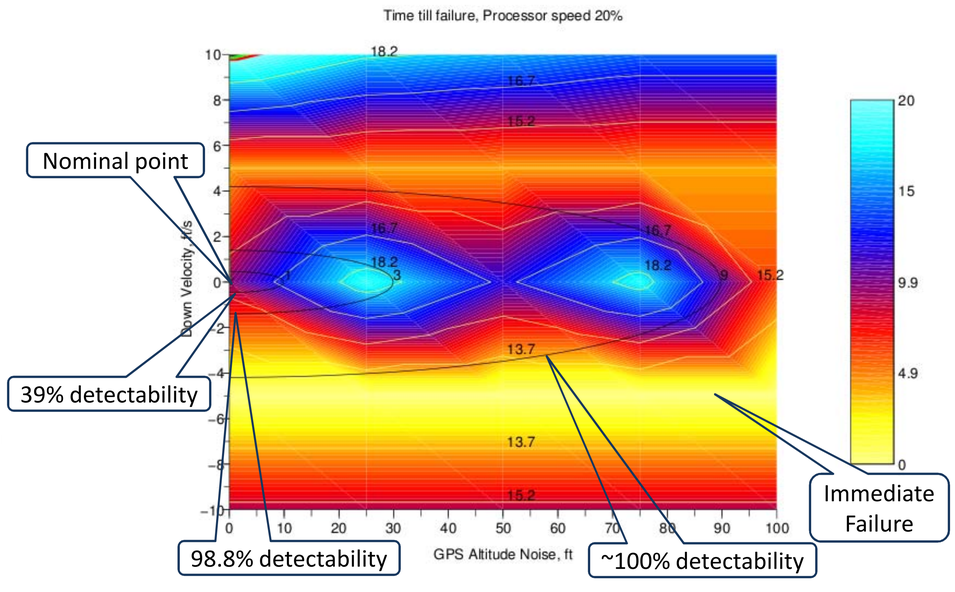


Vehicle under simulated cyberattack

Results



This plot shows the simulated time to failure of UAV subjected to a controller gain scheduling and GPS oscillation injection attacks of varying magnitude. The asymmetry in this result demonstrates the potential coupling between different attacks that increases the effectiveness of the overall attack. The nominal (no attack) point is indicated, and the light blue region indicates no failure by the end of the simulation at 120 seconds.



A combination of sensor attack, state attack, and hardware attack. The ellipses represent the likelihood that the sensor and state attacks are detected. Starting with the innermost ellipse and expanding outwards, they represent a 39%, 78% , and 99% likelihood of those attacks being detectable.

Acknowledgement

We'd like to acknowledge that this project has been supported by Sypris Electronics and thank Dr. Hal Aldridge for his valuable discussions and support.

CERIAS

Discovery Park e-Enterprise Center