Cybersecurity Defense of Aircraft Automatic Dependent Surveillance-Broadcasts (ADS-B) Using the ADS-B Cybersecurity Environment (ACE) for Public Safety

Lewis, Steven (School: Pine Creek High School)

All aircraft are reliant on situational awareness data contained in automatic dependent surveillance-broadcasts (ADS-B) to stay efficient and safe. Currently, ADS-B is broadcast on 1090 MHz in the clear with no security measures, and with the new ADS-B mandate that was effective January 1, 2020, ADS-B spoofing attacks on aircraft are going to be a likely and dangerous occurrence. As a solution to this blatant, severe vulnerability, I conducted research and analysis to develop the ADS-B Cybersecurity Environment (ACE) system in three phases. The preliminary experiments consisted of collecting ADS-B data from hundreds of planes and parsing and wrangling the data sets into a useful format. In the second phase of the ACE project, simple detection was explored with algorithms to detect abnormalities in ADS-B telemetry with an automated spoofing testbed that generates test data. The final phase of ACE was developing the supervised machine learning system that detects anomalous patterns of life of aircraft. After training the linear estimation machine learning algorithm on observations from several hundred planes, the evaluated patterns of life of real planes were shown to be accurate 99.95 % of the time. ACE, composed of a system pairing Software Defined Radios (SDRs) and machine learning capabilities, was shown to be a cost-efficient solution to make worldwide ADS-B broadcasts secure. By leveraging existing ground terminals and expanding the current ADS-B detection system with new, low-cost terminals, ACE can protect airspace, preserve the safety of life, and with future enhancements, prevent tragedies such as 9/11.