Design of Cyber Security Framework for ADS-B Based Surveillance Systems

Sahar Amin, Tyler Clark, Rennix Offutt, Kate Serenko
System Engineering & Operations Research, George Mason University

Context
Currently, there are over 150 million passengers flying through the United States airspace. By 2032, there will be over 250 million passengers flying.*

Problem & Need Statement
Problem Statement
Unencrypted communication between aircraft and ARTCC
ADS-B signals vulnerable to cyber attacks → Unreliable transmissions

Need Statement:
The system needs to prevent spoofing attacks on ADS-B signals.

Method of Analysis

Asymmetric Encryption
Symmetric Encryption
Hashing
Maintain Status Quo

Alternatives

Strength Security
Asymmetric Encryption
Symmetric Encryption
Hashing
Maintain Status Quo

Feasibility Analysis

Collision Simulation
Random flights with no situational awareness → cells under attack evaluating locations at time \(t\)
If distance between two flights is significantly small (\(<1024\)), records collision between two aircrafts

Results

Estimates of aircraft throughput for each alternative:

- Symmetric Encryption: 1.720
- Hashing: 0.395

Conclusion & Future Research

- Asymmetric Encryption maintains higher security.
- Signal quality degradation may become an issue.
- Preparing through separation and improving accuracy of the system.