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

Sahar Amin
Tyler Clark
Rennix Offutt
Kate Serenko
Agenda

- Context Analysis
  - Stakeholder Analysis
  - Problem Statement & Needs Statement
  - Mission Requirements
  - Design Alternatives
  - Design of Experiment
  - Results and Recommendations
Currently, there are over 150 million passengers flying through the United States airspace.*

9.8 million flights fly domestic and internationally from the US each year (About 27,000 each day).*

By 2032, there will be over 250 million passengers flying.*

* Bureau of Transportation Statistics

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
Airspace Surveillance

- Surveillance in air transportation is needed to track and monitor flights.
- Current $\rightarrow$ Ground-based Primary and Secondary Radars
- Future $\rightarrow$ Next Generation (Next Gen)
  - New airspace for US to be implemented between 2012-2025
  - New framework for flight tracking and monitoring
  - Ground/radar-based tracking system $\rightarrow$ satellite-based tracking system
  - Major Component of NextGen: Automatic Dependent Surveillance-Broadcast (ADS-B)
How ADS-B Works

First, aircraft obtain their position information from the GPS satellites. Then, the ADS-B system simultaneously broadcasts the aircraft’s position to other aircraft, and to ground stations.

Figure 1: Data Block of an ADS-B message
- **DF**: Downlink Format
- **CA**: Capability
- **AA**: Individual Aircraft Address
- **ADS-B Data**: Aircraft type, Altitude, Latitude, Longitude, Airborne Velocity
- **PI**: Parity Information (Error Detection Code)
Automatic Dependent Surveillance-Broadcast (ADS-B)

**Advantages:**
- Increased situational awareness
- Coverage in areas without radar
- Less Expensive
- Can decrease separation distance
- Real time information

**Disadvantages:**
- Not secured
- Easily accessible
Decreased Separation Distance

Without ADS-B Coverage

One In, One Out

20 NM

With ADS-B Coverage

Separation distance decreased to 5 NM

5 NM 5 NM 5 NM 5 NM 5 NM
Threats

◆ **Spoofing** – falsification of transmitted information
  ◆ False Source – creates signal that is seen as coming from an incorrect location
  ◆ False Content – content within messages are altered

◆ **Jamming** – forceful disruption of signal
  ◆ Ghost Plane Flooding – floods ARTCC radar screen with ghost airplanes
  ◆ Ground Station Flooding - removes all aircraft from ARTCC radar screen
Project Scope

- Oceanic area between two land masses covered by ARTCC
- No radar coverage – Only ADS-B surveillance
- Commercial aviation – en route flights
- Spoofing attacks only - concentrating on prevention of attacks
  - Any further mention of “an attack” refers to spoofing attacks
  - Jamming is out of our scope
Surveillance Coverage

Radar and ADS-B coverage

Only ADS-B coverage
Agenda

- Context Analysis

- **Stakeholder Analysis**

- Problem Statement & Needs Statement

- Mission Requirements

- Design Alternatives

- Design of Experiment

- Results and Recommendations
Stakeholder Analysis

Primary Stakeholders
- Aircraft Companies
- Customers
- ADS-B Manufacturers

Secondary Stakeholders
- Congress
- Federal Aviation Administration (FAA)
- Air Route Traffic Control Center (ARTCC)
- Crew/Pilots
- Labor Unions

Interactions
- Installation Cost
- Reasonable Cost
- Reliable System
- Set Regulations
- Increased workload
- Flight Plan
- Budget Proposal
- Laws
- Salary

Tensions
- Congress
- Federal Aviation Administration (FAA)
- Air Route Traffic Control Center (ARTCC)
- Crew/Pilots
- Labor Unions
Agenda

- Context Analysis
- Stakeholder Analysis
- **Problem Statement & Needs Statement**
- Mission Requirements
- Design Alternatives
- Design of Experiment
- Results and Recommendations
Problem Statement

Unencrypted communication between aircraft and ARTCC

ADS-B signals vulnerable to cyber attacks → Unreliable transmissions

Reduced situational awareness

Decreased airspace throughput
Gap Analysis

Estimated Number of Aircraft Over the Gulf Handled by En Route Traffic Control Centers

Year


* Source: FAA Aerospace Forecast

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
The system needs to prevent spoofing attacks on ADS-B signals.
Agenda

- Context Analysis
- Stakeholder Analysis
- Problem Statement & Needs Statement
- **Mission Requirements**
- Design Alternatives
- Design of Experiment
- Results and Recommendations
Mission Requirements

1.0 The system shall enable the decrease of separation distance to 5 nm.
   1.1 The system shall not increase the time spent in flight by 1 minute.
   1.2 ADS-B messages shall be resistant to spoofing attacks 75% of the time.
   1.3 The system shall maintain collision rate of 22.5 per 1,000,000 flights.*

2.0 The system shall be ready to be implemented by 2020.

*Source: Collision Simulation
Agenda

- Context Analysis
- Stakeholder Analysis
- Problem Statement & Needs Statement
- Mission Requirements
- Design Alternatives
- Design of Experiment
- Results and Recommendations
Design Alternatives

1. Hashing
2. Symmetric Encryption
3. Asymmetric Encryption
4. Maintain Status Quo
1. Hashing

What Is It?

- Goal – Confirming the source of a message
- Digital Signature/Hash created by sender – aircraft
- Attached at the end of the message
- Verified by receiver - ARTCC Fusion System
2. Symmetric Encryption

- What Is It?
  - Encryption – converting data into code
  - Symmetric – each entity has one private key
  - Message encrypted with key has to be decrypted with the same key
3. Asymmetric Encryption

- **What Is It?**
  - Two keys – Public and Private
  - Longer keys – stronger security

![Diagram showing the process of asymmetric encryption]
Agenda

- Context Analysis
- Stakeholder Analysis
- Problem Statement & Needs Statement
- Mission Requirements
- Design Alternatives

- Design of Experiment

- Results and Recommendations
Goal – show how securing ADS-B signals can increase airspace throughput and maintain current safety level under diverse or dangerous conditions.

Value Hierarchy

- Signal Security: $W_S = 0.1266$
- Feasibility: $W_F = 0.1899$
- Additional Time in Flight: $W_E = 0.3038$
- Collision Risk: $W_C = 0.3797$
Goal – show how securing ADS-B signals can increase airspace throughput and maintain current safety level under diverse or dangerous conditions.

Value Hierarchy

- Signal Security
  \[ W_S = 0.1266 \]

- Feasibility
  \[ W_F = 0.1899 \]

- Additional Time in Flight
  \[ W_E = 0.3038 \]

- Collision Risk
  \[ W_C = 0.3797 \]
Signal Security

- Determined from Research
- Reliability of Alternatives
  - Hash: 50%*
  - Symmetric: 85%
  - Asymmetric: 99%

*Chen, et. Microsoft. Oblivious Hashing: A Stealthy Software Integrity Verification Primitive
Feasibility Analysis

- Determines the feasibility of alternatives based on:
  - Execution Time
  - Availability of Technologies
  - Additional Requirements

Value Hierarchy

- Signal Security: $W_S = 0.1266$
- Feasibility: $W_F = 0.1899$
- Additional Time in Flight: $W_E = 0.3038$
- Collision Risk: $W_C = 0.3797$

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
## Feasibility Analysis

<table>
<thead>
<tr>
<th>Design Alternative</th>
<th>Execution Time</th>
<th>Availability of technology</th>
<th>Additional Requirements</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing</td>
<td>Negligible</td>
<td>Available</td>
<td>Free Additional Bits</td>
<td>1</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>Negligible</td>
<td>Available</td>
<td>Secure Key Management System</td>
<td>1</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>Negligible</td>
<td>Available</td>
<td>Encryption Software</td>
<td>1</td>
</tr>
<tr>
<td>Maintain Status Quo</td>
<td>None</td>
<td>N/A</td>
<td>None</td>
<td>1</td>
</tr>
</tbody>
</table>
Derived average time in flight from Airspace Throughput Simulation

Purpose: Calculate the difference in flight times for each alternative

Value Hierarchy

- Signal Security
  \[ W_S = 0.1266 \]
- Feasibility
  \[ W_F = 0.1899 \]
- Additional Time in Flight
  \[ W_E = 0.3038 \]
- Collision Risk
  \[ W_C = 0.3797 \]
Airspace Throughput Simulation

**Inputs**
- Aircraft departure distributions \(\rightarrow\) derived from real world data for 5 days
- Velocities
- Attack locations
- Mitigation techniques
- Separation Distances

**Outputs**
- Number of violations \(\rightarrow\) cells going over capacity
- Time spent in flight for each route
- Excess fuel burn
- Number of aircraft flying per day
- Number of aircraft in cell at any time t
Conceptual Model
Model Assumptions

- The altitudes of aircraft are constant and are regulated by ARTCC outside the scope of the simulation.

- The capacity of a cell accounts for 12 flight levels with 1000 ft vertical separation.

- Alternatives are evaluated as follows:
  - Hashing – attack location is determined and aircraft avoids attacked areas.
  - Symmetric & Asymmetric Encryption – attacks are prevented → attacks are always mitigated.
**Formulas:**

*Dot Product:*

\[ \text{Dot}_{\text{prod}} = \overrightarrow{V_{c \to t}} \cdot \overrightarrow{V_{p \to t}} \]

*Time to Cross One Cell:*

\[ T = \frac{D_{\text{cell}}}{V} \]
Airspace Capacity in Adverse Conditions

Throughput with Encryption

Throughput with Hashing

Legend:
- Blue: =0
- Green: <100
- Yellow: <300
- Red: >300

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
# Flight Times for Encryption vs Hashing

## Differences in Flight Times of Encryption and Hashing for 2014, at 20 NM Separation Distance

<table>
<thead>
<tr>
<th>Design Alternative</th>
<th>Average Time in Flight, 2014</th>
<th>Average Time in Flight, 2032</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing</td>
<td>58.891±3.988</td>
<td>56.844±3.824</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
<tr>
<td>Maintain Status Quo</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
</tbody>
</table>

## Differences in Flight Times for Encryption and Hashing for 2032, at 5 NM Separation Distance

<table>
<thead>
<tr>
<th>Design Alternative</th>
<th>Average Time in Flight, 2014</th>
<th>Average Time in Flight, 2032</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing</td>
<td>58.891±3.988</td>
<td>56.844±3.824</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
<tr>
<td>Maintain Status Quo</td>
<td>52.683±3.668</td>
<td>52.161±3.547</td>
</tr>
</tbody>
</table>
Collision Simulation

- Random flights with no situational awareness → cells under attack
- Evaluating locations at time t
  - If distance between two flights is significantly small (~<102ft), record collision between two aircrafts

Value Hierarchy

- Signal Security: $W_S = 0.1266$
- Feasibility: $W_F = 0.1899$
- Additional Time in Flight: $W_E = 0.3038$
- Collision Risk: $W_C = 0.3797$
12 levels
Each level – 20NM by 20 NM, with 1000 ft. depth

Collision

*Not to scale
Collision Simulation

Inputs

• Number of Aircraft in Cell at Each Time $t$
• Aircraft Altitude
• Aircraft Speed

Outputs

• Number of iterations with collision per 1,000,000 iterations
Collision Simulation Diagram

Formulas:

Distance at time $t$:
$$x_{current} = \frac{v}{\sqrt{1+m^2}} + x_{previous}$$

Current Y Coordinate:
$$y_{cur} = m(x_{cur} - x_{prev}) + y_{prev}$$

Distance Between Two Points:
$$D = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

Collision Risk:
$$CR = \Sigma(P(collision) \times N_{cell})$$
Collision Simulation Results

Number of Collisions in 1,000,000 iterations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing</td>
<td>0.000677</td>
<td>0.000707</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Asymmetric Encryption</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Maintain Status Quo</td>
<td>0.00511</td>
<td>0.0082663</td>
</tr>
</tbody>
</table>

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
Agenda

- Context Analysis
- Stakeholder Analysis
- Problem Statement & Needs Statement
- Mission Requirements
- Design Alternatives
- Design of Experiment

Results and Recommendations

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
Utility vs Cost

<table>
<thead>
<tr>
<th>Alternative</th>
<th>Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asymmetric Encryption</td>
<td>0.832</td>
</tr>
<tr>
<td>Symmetric Encryption</td>
<td>0.814</td>
</tr>
<tr>
<td>Hashing</td>
<td>0.744</td>
</tr>
<tr>
<td>Status Quo</td>
<td>0.327</td>
</tr>
</tbody>
</table>

Utility vs Cost

- **Collision risk**
- **Time in Flight**
- **Security Strength**
- **Feasibility**

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
<table>
<thead>
<tr>
<th></th>
<th>Calendar Year 2012</th>
<th>Direct Aircraft Operating Cost per Block Minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Quo – Fuel Spent per Year</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>$1,409,950,237</td>
<td></td>
</tr>
<tr>
<td>Encryption (Symmetric &amp; Asymmetric) - Additional Fuel Spending</td>
<td>+0</td>
<td>+$44,834,140-287,488,121</td>
</tr>
<tr>
<td>2032</td>
<td>$1,982,344,674</td>
<td>+$12,124,185-343,841,991</td>
</tr>
<tr>
<td>Hashing - Additional Fuel Spending</td>
<td>55.05</td>
<td>+$343,841,991</td>
</tr>
<tr>
<td>Fuel</td>
<td>$39.26</td>
<td></td>
</tr>
<tr>
<td>Crew - Pilots/Flight Attendants</td>
<td>16.26</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>12.02</td>
<td></td>
</tr>
<tr>
<td>Aircraft Ownership</td>
<td>7.92</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>2.71</td>
<td></td>
</tr>
<tr>
<td>Total DOCs</td>
<td>$78.17</td>
<td></td>
</tr>
</tbody>
</table>

Source: Airlines for America
Recommendations

- Asymmetric encryption is preferred method of signal security
  - Signal security will allow for better situational awareness
  - Prepares airspace for any increases in throughput by allowing decreased separation distances (20 NM $\rightarrow$ 5 NM)
Gap Analysis Revisited

Gap Analysis

Estimated Number of Aircraft Over the Gulf Handled by En Route Traffic Control Centers

* Source: FAA Aerospace Forecast

Department of Systems Engineering and Operations Research
Design of A Cyber Security Framework for ADS-B Based Surveillance Systems
SYST 495 - 2014
Future Research

Security Strength

• Improvement in analysis on security strength of alternatives

Implementation

• Further research required on available algorithms
• Secure ADS-B Authentication System and Method was developed and patented in 2010

Cost

• Cost of securing signals needs in-depth research
Questions?