Air Traffic Management Security: ADS-B as an Example

Dr. Thabet Kacem

Email: thabet.kacem@udc.edu
Dr. Thabet Kacem

Education:
- January 2010: Master in Computer Science, University of the District of Columbia
- May 2016: PhD in Information Technology, George Mason University

Appointments:
- 2016–2022: Tenure-track assistant professor of Computer Science at the University of the District of Columbia
- 2022–Present: Tenured associate professor of Computer Science at University of the District of Columbia
- 2022–Present: Affiliate Faculty at the C4I Center at George Mason University
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS-B Security Problem
• Related Work
• ADS-Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS-B Security Problem
• Related Work
• ADS-Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Research Interests & Vision

Intelligent Transportation Systems

Cyber Security

CPS & Critical Infrastructure

Smart Cities

Blockchains
Research Vision

FROM RIVER RAFT TO AUTONOMOUS RAIL
Selection of innovative means of transport and events for traffic

- waterborne
- onshore
- in mid-air

- 20,000 BCE: Rafts used on rivers
- 3,500 BCE: Invention of the wheel
- 10th Century: Sea-going ship
- Late 16th century: Sailings ships cross oceans
- 1662: Horse-drawn public bus
- 1822: Engine-powered railway
- 1816: Bicycle
- 1807: Horsecar tram
- 1803: Steamboat
- 1783: Hot air balloons
- 1868: Common bicycle
- 1881: Electric tram
- 1844: Electric car
- 1885: Fuel engine powered car
- 1890: Underground
- 1893: Motor-driven airplane
- 1899: Airship
- 1897: Electric bicycle
- 1895: Motorbus
- 1894: Motorcycle
- 1904: Trolleybus
- 1907: Battery-electric bus
- 1908: Ford Model T
- 1910: Escalator
- 1911: Diesel engine-driven ship
- 1923: Nuclear-powered submarine
- 1947: Supersonic human flight
- 1939: Jet engine powered aircraft
- 1955: Hovercraft
- 1912: Diesel locomotive
- 1964: Commercial widebody airliner
- 2009: Autonomous Rail Rapid Transit
- 2018: Hydrogen-powered train
- 2019: Commercial passenger-carrying supersonic flight
"Intelligent Transportation Systems (ITS) apply a variety of technologies to monitor, evaluate, and manage transportation systems to enhance efficiency and safety", US DOT

Main Benefits of ITS:
- Safety
- Better Management
- Efficiency
- Cost Effectiveness
• **Concerns:**

  - Cyber Security
  - Environmental Risks
  - Supply Chain Resiliency

• **Research Vision:** How can we address the security concerns of ITSs so that they live up to their full potential of revolutionizing the human life quality?
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS-B Security Problem
• Related Work
• ADS-Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Air Traffic Management Overview
Cont’d – NextGen Project
Outline

- Research Interests & Vision
- Air Traffic Management Overview
- ADS-B Security Problem
- Related Work
- ADS-Bsec Framework
- Evaluation Results
- Conclusion and Future Challenges
### ADS-B Security Problem

<table>
<thead>
<tr>
<th>Traditional Surveillance Technologies</th>
<th>ADS-B advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Primary Surveillance Radar (PSR)</td>
<td>• Better Accuracy</td>
</tr>
<tr>
<td>• Secondary Surveillance Radar (SSR)</td>
<td>• Capability to be deployed in remote areas</td>
</tr>
<tr>
<td></td>
<td>• Less operational &amp; maintenance Costs</td>
</tr>
</tbody>
</table>
Cont'd – How ADS-B Works
Cont’d – ADS-B Message Format
Cont’d – ADS-B Threat Model

- Types of Attacks:
  - Eavesdropping
  - GPS Spoofing
  - Jamming
  - Replay Attacks
  - Ghost Aircraft Injection
  - Multiple Ghost Aircraft Injection
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS–B Security Problem
• Related Work
• ADS–Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Related Work

**Cryptographic Approaches**
- **Rationale:** Add digital signature data in extra ADS-B messages
  - Pan et al
  - Yang et al
- **Weakness:** not scalable and may increase error rate, and may require changing the message format

**Artificial Intelligence Approaches**
- **Rationale:** Use machine learning and/or deep learning classifiers
  - Ying et al
  - Habler and Shabtai
- **Weakness:** these approaches are not preventive, not much insight on the type of the attacks

**Location Verification Approaches**
- **Rationale:** Use the time difference of arrivals from nearby aircraft
  - Strohmeier et al
  - Kaune et al
- **Weakness:** requires several multilateration stations, no message attribution
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS-B Security Problem
• Related Work
• ADS-Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
ADS-Bsec Framework - Overview

**Sender**
- Flight Path
  - Aircraft Prediction Module
    - Security Analysis Module
      - Key Management Module
        - Secure Message Generator
          - Secure ADS-B Sender
            - BADA

**Receiver**
- ML Classifier Module
  - Secure ADS-B Receiver
    - Security Analysis Module
      - Key Management Module
        - BADA
          - Aircraft Prediction Module
            - Flight Path
Rationale: Replace the Cycle Redundancy Check (CRC) field with a security metadata based on Keyed Hash Message Authenticated Code (HMAC)

- This is a software change that does not require any hardware change
- There is no need for an ADS-B message format modification
- The power of the HMAC lies mainly in the length of the key
- No need for sending extra data that harm the scalability of the approach

Two variants of the secure message generator:

- **Version 1**: ADS-B Out only
- **Version 2**: Both ADS-B Out and ADS-B In
Cont’d – Version 1

Insecure Even ADS-B Message
Message Even Payload CRC
Message Odd Payload CRC
Insecure Odd ADS-B Message

Message Even Payload Message Odd Payload

H1 H2 H3 H4 H5 H6 H7 H8
HMAC Digest

Secure Even ADS-B Message
Message Even Payload \( H_{\text{even}} \)
Message Odd Payload \( H_{\text{odd}} \)
Secure Odd ADS-B Message

XOR
Binary Vector Multiplication
Bit Manipulation Algorithms

8 bits 16 bits

HMAC-based Metadata
Sequence Number HMAC Portion
Cont’d – Version 2
ADS-Bsec – Security Analysis Module

Aircraft AB76N8

ADS-B Even

ADS-B Odd

ATC Center

12DF8Y

34DF9X

AB76N8

KL39V3

Seq# i

Seq# 1

Seq# 2

Seq# 255

ADS-B Even

ADS-B Odd

Extract & Generate HMAC

HMAC match?

Yes

No

ML Classifier
ADS-Bsec – Key Management Module

Rationale:

- PKI schemes are difficult to deploy to share ADS-B keys mainly due to trust issues
- Symmetric keys are more adequate
- Delegate the initial key distribution to the ATC Center of departure

Key Exchange Constraints:

- Ideal flight conditions
- Unforeseen flight changes
- ADS-B Out vs ADS-B In and ADS-B Out
Cont’d – Ideal Flight Conditions
Cont’d – Unforeseen Flight Changes
Cont’d – Key Exchange for ADS-B In and ADS-B Out

• Rationale:
  • Nearby aircraft, equipped with ADS-B In, receive ADS-B messages from each other
  • All aircraft in a given zone generate their security metadata using a group key that is generated from seed keys
  • The granularity of the groups are inspired from the airspace subdivision by the authorities (e.g. Flight Information Regions)
  • Group keys need to be updated every time a member joins or leaves the group
  • Each day is subdivided into time intervals depending on the frequency of aircraft in that zone
    • Seeds are generated in μTesla-like fashion
Cont’d

Table

<table>
<thead>
<tr>
<th>Zone 1</th>
<th>Zone 2</th>
<th>Zone 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>a₁₁</td>
<td>a₁₂</td>
<td>a₁₃</td>
</tr>
<tr>
<td>a₂₁</td>
<td>a₂₂</td>
<td>a₂₃</td>
</tr>
<tr>
<td>a₃₁</td>
<td>a₃₂</td>
<td>a₃₃</td>
</tr>
</tbody>
</table>

Equations:

\[ X_1 \rightarrow X_2 = H(X_2) \rightarrow \ldots \rightarrow X_n = H(X_{n-1}) \]

\[ Y_1 \rightarrow Y_2 = H(Y_2) \rightarrow \ldots \rightarrow Y_n = H(Y_{n-1}) \]

\[ G_{K_n} = H'(\text{bitManip}(X_1, Y_1)) \]

\[ G_{K_1} = H'(\text{bitManip}(X_n, Y_n)) \]
ADS-Bsec – ML Classifier

Original Dataset

Original Dataset with Attacks

Modified Dataset with Attacks

Machine Learning Classifiers

Performance Evaluation

ADS-B Attacks
ADS-Bsec - Radio-Location Module
Cont’d – Computing the TODT

\[ \tau_n = t_n + p_n \]

\[ t_n = \frac{\sqrt{(x_n - x_E)^2 + (y_n - y_E)^2 + (z_n - z_E)^2}}{C} \]

\[ \tau_i - \tau_j = (t_i - t_j) + (p_i - p_j) \]

\[ \tau_i - \tau_j = t_i - t_j + \mathcal{N}(0, 2\sigma^2) \]
### Algorithm: Detection of Bogus ADS-B Messages

1. Initialize arrays to store the Cartesian coordinates of both the MLAT sensors and the emitters;
2. **while** \( t < \text{endTime} \) **do**
   3. Store the coordinates of each emitter in its corresponding array;
   4. Run the multilateration algorithm to determine the location of the emitter based on the collected TDOT values;
   5. Apply Kalman Filter to improve the location estimation;
   6. Compute the horizontal difference \( h_{Diff} \) between the estimated and reported position;
   7. **if** \( h_{Diff} < \text{Threshold} \) **then**
      8. ADS-B message is valid
   **else**
      9. ADS-B message is malicious
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS-B Security Problem
• Related Work
• ADS-Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Evaluation Results

Crypto Module
- Measure the sending time and receiving time of secure ADS-B messages
- Compare the overhead of the added security vs the original protocol
- Study the effect of the implementation of the Key Management Module

AI Module
- Measure the classification accuracy, sensitivity and specificity of the ML classifier
- Compare the classification scores of the original vs modified datasets

Location Verification
- Comparing TDOT vs TDOA
- Location estimation using TDOT
- Detecting malicious ADS-B messages
Cont’d – Crypto-Module Evaluation

The ADS-Bsec Test Bed
Cont’d – Sending Time

Sending Time Plain ADS-B

Sending Time Secure ADS-B
Cont’d – Receiving Time
Cont’d – Key Management
Cont’d

Sending Time with SHA1 and 128-bit key

Receiving Time with SHA1 and 128-bit key
## Cont’d – AI Module Evaluation

### Classification Results with Original Dataset.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Classifier</th>
<th>CA</th>
<th>Sens</th>
<th>Spec</th>
</tr>
</thead>
<tbody>
<tr>
<td>95-05</td>
<td>Dtree</td>
<td>0.96</td>
<td>0.69</td>
<td>0.92</td>
</tr>
<tr>
<td>95-05</td>
<td>SVM</td>
<td>0.97</td>
<td>0.51</td>
<td>0.92</td>
</tr>
<tr>
<td>95-05</td>
<td>RF</td>
<td>0.97</td>
<td>0.71</td>
<td>0.92</td>
</tr>
<tr>
<td>90-10</td>
<td>Dtree</td>
<td>0.95</td>
<td>0.68</td>
<td>0.92</td>
</tr>
<tr>
<td>90-10</td>
<td>SVM</td>
<td>0.94</td>
<td>0.49</td>
<td>0.92</td>
</tr>
<tr>
<td>90-10</td>
<td>RF</td>
<td>0.94</td>
<td>0.70</td>
<td>0.92</td>
</tr>
<tr>
<td>85-15</td>
<td>Dtree</td>
<td>0.92</td>
<td>0.61</td>
<td>0.92</td>
</tr>
<tr>
<td>85-15</td>
<td>SVM</td>
<td>0.91</td>
<td>0.50</td>
<td>0.91</td>
</tr>
<tr>
<td>85-15</td>
<td>RF</td>
<td>0.90</td>
<td>0.69</td>
<td>0.91</td>
</tr>
</tbody>
</table>

### Classification Results with Modified Dataset.

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Classifier</th>
<th>CA</th>
<th>Sens</th>
<th>Spec</th>
</tr>
</thead>
<tbody>
<tr>
<td>95-05</td>
<td>Dtree</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
</tr>
<tr>
<td>95-05</td>
<td>SVM</td>
<td>0.94</td>
<td>0.69</td>
<td>0.97</td>
</tr>
<tr>
<td>95-05</td>
<td>RF</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
</tr>
<tr>
<td>90-10</td>
<td>Dtree</td>
<td>1.00</td>
<td>0.98</td>
<td>1.00</td>
</tr>
<tr>
<td>90-10</td>
<td>SVM</td>
<td>0.96</td>
<td>0.71</td>
<td>0.96</td>
</tr>
<tr>
<td>90-10</td>
<td>RF</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
</tr>
<tr>
<td>85-15</td>
<td>Dtree</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
</tr>
<tr>
<td>85-15</td>
<td>SVM</td>
<td>0.94</td>
<td>0.69</td>
<td>0.97</td>
</tr>
<tr>
<td>85-15</td>
<td>RF</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
</tr>
</tbody>
</table>
Cont’d

Average Classification Score: Original dataset vs Modified dataset

- Average of CA
- Average of Sens
- Average of Spec
Cont'd – Radio Location Module Evaluation

TDOA vs TDOT

Location Estimation using TDOT
Cont’d

Effect of Kalman Filter on Location Estimation

Detecting Malicious ADS-B Messages
Outline

• Research Interests & Vision
• Air Traffic Management Overview
• ADS–B Security Problem
• Related Work
• ADS–Bsec Framework
• Evaluation Results
• Conclusion and Future Challenges
Conclusion

ADS-Bsec framework addresses the security problems of ADS-B from a holistic approach without altering the packet format or requiring new equipment.

It combines novels cryptographic, artificial intelligence and location verification techniques to provide the integrity and authenticity of the ADS-B messages.

The findings are supported by a set of experiments that assess the performance of the key modules of ADS-Bsec.
Achievements

Patents


Selected Conference Publications


Selected Journal Publications


Future Challenges

1. Risk of adversarial attacks on ML and DL approaches to detect ADS-B Security Problems
2. Universal Access Transceiver (UAT) Security
3. ACAS-X Security
4. Unmanned Aircraft System Traffic Management Security
5. Security of other transportation protocols such as the AIS and IoV
Thank you very much
Backup Slides
Cont’d – Formal Key Exchange Protocol

Initial Key Exchange Protocol

Flight Change Key Exchange Protocol
Cont’d – Key Management Module Class Diagram
Create a new research lab focusing on Intelligent Transportation Systems Security

- Aligned with GMU participation in CyManII and VA Cyber Initiative
- Promotion of MS and PhD theses
- Foster research collaboration between faculty members at GMU and beyond

Support the research with a proper educational foundation

- Develop new courses on:
  - ITS Security
  - Critical Infrastructure Security
  - Smart Cities Security

Apply for research Grants. Some potential programs include:

- DOT: University Transportation Centers (UTC) Competition
- FAA: Aviation Research Grants Program
- NSF: SaTC, CPS, S&CC