Increasing the Resilience of ATC Systems against False Data Injection Attacks using DSL-based Testing

8th International Conference on Research in Air Transportation Doctoral Symposium

Aymeric Cretin, Bruno Legeard
Fabien Peureux, Alexandre Vernotte
Summary

- Context: ADS-B Protocol and FDIAs
- Objectives of research
- Proposed approach: T-FDIA Framework
- Conclusion and Future Work
Automatic Dependent Surveillance-Broadcast (ADS-B)

**ADS-B goal:**
- Reduce the surveillance cost
- Improve the aircraft position accuracy

**ADS-B characteristics:**
- Deployed in most aircraft
- 1090 MHz frequency
- Periodically broadcast positioning
- Unencrypted and unauthenticated

---

<table>
<thead>
<tr>
<th>MSG 1</th>
<th>MSG 2</th>
<th>MSG 3</th>
<th>MSG 4</th>
<th>MSG 5</th>
<th>MSG 6</th>
<th>MSG 7</th>
<th>MSG 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>VT</td>
<td>TT</td>
<td>SD</td>
<td>Aid</td>
<td>Hex</td>
<td>RID</td>
<td>DMG</td>
<td>TMC</td>
</tr>
<tr>
<td>Alt</td>
<td>GS</td>
<td>Trk</td>
<td>Lat</td>
<td>Lng</td>
<td>Gnd</td>
<td>Alt</td>
<td>GS</td>
</tr>
<tr>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
<td>Alt</td>
</tr>
<tr>
<td>STA</td>
<td>CLK</td>
<td>STA</td>
<td>CLK</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MSG: 4,5,211,4CA2E6,10057,2008/11/28,14:53:49.986,2008/11/28,14:58:51.153,408.3,146.4,64,64
MSG: 8,5,211,4CA2E6,10057,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,408.3,146.4,64,64
MSG: 4,5,211,4CA2E6,10057,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,408.3,146.4,64,64
MSG: 3,5,211,4CA2E6,10057,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,37000,51.54735,-1.02826,0,0,0,0
MSG: 8,5,812,ABBEE3,10095,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,0,0,0,0
MSG: 3,5,276,4010E9,10088,2008/11/28,14:53:49.986,2008/11/28,14:58:51.153,28000,53.02551,-2.91389,0,0,0,0
MSG: 8,5,276,4010E9,10088,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,0,0,0,0
MSG: 3,5,276,4010E9,10088,2008/11/28,14:53:50.594,2008/11/28,14:58:51.153,28000,53.02677,-2.91310,0,0,0,0
MSG: 4,5,769,4CA2CB,10061,2008/11/28,14:53:50.188,2008/11/28,14:58:51.153,367.7,138.6,-2432,0,0,0
MSG: 8,5,769,4CA2CB,10061,2008/11/28,14:53:50.391,2008/11/28,14:58:51.153,0,0,0,0
ADS-B: How it works?

- Not secure by design
- Vulnerable to cyber attacks
- Especially False Data Injection Attacks

What is an FDIA?
FDIAs Example (1): Smart Grid

Smart Grids characteristics
- A power grid
- Promotes the use of digital information and controls technology
- Adjusts the production and distribution of electricity
- Works in real time

FDIAs comes from Smart Grids
« a cyber-attack in which power system state estimation outputs are corrupted by injecting false data into meter measurements in a carefully coordinated fashion » [1]

Possible impacts of FDIAs
- Implications in 2015 Ukraine Blackout

FDIAs Example (2): Vehicular Ad-hoc Networks (VANETs)

VANETs definition
« A network through which vehicles participate in information sharing and cooperative driving to improve the safety and performance of autonomous driving. » [1]

Possible impacts of FDIAs
For impacted vehicles the consensus of the traffic state is altered.

False Data Injection Attacks (FDIAs) definition

Analogy between those domains permits to consider a general definition of FDIAs:

« A combination of basic, illegal operations (listening, blocking, modifying and creating messages) to alter the consensus reached by the nodes of a network, while preserving the logic of the communication flow »

<table>
<thead>
<tr>
<th></th>
<th>Smart Grid</th>
<th>VANETs</th>
<th>ADS-B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
<td>Sensors</td>
<td>Vehicles/Road Infrastructures</td>
<td>Transponders/Ground Stations</td>
</tr>
<tr>
<td>Consensus</td>
<td>Power system state estimation</td>
<td>Traffic state</td>
<td>Recognized Air Picture</td>
</tr>
</tbody>
</table>
False Data Injection Attacks on ADS-B

Different scenarios of FDIA:
- Ghost Aircraft Injection
- Ghost Aircraft Flooding
- Virtual Trajectory Modification
- False Alarm Attack
- Aircraft Disappearance
- Aircraft Spoofing
- Potentially any combination of basic operations (modification, creation, deletion)

Examples of possible impacts:
- Controller distraction with false events
- Loss of an aircraft position
- Crash of the ATC system
Summary

• Context: ADS-B Protocol and FDIAs

• Objectives of research

• Proposed approach: T-FDIA Framework

• Conclusion and Future Work
Main Objectives of Research (RO)

How to automate resilience testing of ADS-B based ATC systems against False Data Injection Attacks?

Definition and development of a testing framework (T-FDIA):

- Able to formalize the design of FDIA for automation (RQ1)
- Able to generate accurate FDIA on ADS-B protocol (RQ2)
- Able to assess the resilience of ATC Systems against FDIAs (RQ3)
Research question (RQ1)

To what extent can test design be efficiently supported for FDIA?

In real situation, an FDIA is complex to design and achieve:

- **Complex attacks** based on simple operations
- Requires a deep understanding of the system *protocols and logic*
- The communication flow must be preserved
Research question (RQ2)

To what extent can an FDIA be accurately generated on ADS-B?

FDIAs can be designed and injected in an ATC System. However, this process could be improved by smart generation strategies.

A simple FDIA only covers few test cases.

FDIA scenarios could improve the detection of vulnerabilities.
Research question (RQ3)

To what extent can the resilience of a system be evaluated?

- **Detection of attacks** (security)
  - Can the system differentiate legitimate data from illegitimate data?
  - Are controllers prepared to recognize an attack?

- **Reaction of the system** (security)
  - Does the system yield the expected response in case of an attack?

- **Robustness of the system to uncommon data** (safety)
  - Is the system still reliable while receiving corrupted data?
T-FDIA: Positioning within resilience issues

Resilience Umbrella

Pre-incident
- Prevention
- Preparedness

Post-incident
- Response
- Recovery
- Operational Continuity

Incident

Time
Summary

- Context: ADS-B Protocol and FDIA

- Objective of research

- Proposed approach: T-FDIA Framework

- Conclusion and Future Work
T-FDIA: Architecture proposal

1) Collecting of legitimate ADS-B recordings from internet or using an antenna.

2) Graphical or textual design of a scenario of FDIA.

3) Production of a set of alteration to perform on an ADS-B recording according to the designed FDIA.

4-5) Generation of the altered ADS-B messages and injection in the ATC System

6) Assessment of the resilience of the ATC System by analyzing the output.
T-FDIA: Domain Specific Language (DSL)

• Using ATC specific terminology

• Defining scenario pattern:
  – A scenario is a combination of basic operations (modification, creation, deletion)
  – A pattern is applicable on any recording

• Example of a ghost aircraft flooding pattern:

  saturate plane with ICAO = "40688A"
  from 10 seconds until 30 seconds
  with_values ICAO = "RANDOM"
  and AIRCRAFT_NUMBER = 5
  global assert "Fake Aircraft detected"
T-FDIA: basic principles

- Concretize the scenario: create 5 fake aircrafts with random ICAO

Socket Data Format: [http://woodair.net/sbs/Article/Barebones42_Socket_Data.htm](http://woodair.net/sbs/Article/Barebones42_Socket_Data.htm)

- Record ADS-B messages in a file with an antenna

- Import the ADS-B recording in the Testing Framework

- Design False Data Injection Attack scenario to apply on the recording.

- Concretize the scenario: create 5 fake aircrafts with random ICAO

- Inject the altered ADS-B in the targeted system through Ethernet

- Saturate plane with ICAO = "40688A" from 10 seconds until 30 seconds

- with_values ICAO = "RANDOM" and AIRCRAF_NUMBER = 5

- Global assert "Fake Aircraft detected"
T-FDIA: Tool Support
T-FDIA: Scenario Designer GUI
Summary

• Context: ADS-B Protocol and FDIAAs

• Objective of research

• Proposed approach: T-FDIA Framework

• Conclusion and Future Work
Achievements of Research Objectives

How to automate resilience testing of ADS-B based ATC systems against False Data Injection Attacks?

Able to formalize the design of FDIA for automation (**RQ1**):
- Definition and implementation of a DSL to design complex FDIA

Able to generate accurate FDIA on ADS-B protocol (**RQ2**):
- Development of a first basic strategie based on FDIA parameters combination (Cartesian Product)

Able to assess the resilience of ATC Systems (**RQ3**):
- Definition of assertions, and basic report generation
Future Work: Use the test results to train an AI

- Test design and generation assisted by Artificial Intelligence
Future Work: Toward post-incident resilience

Resilience Umbrella

Pre-incident
- Preparedness
- Prevention

Post-incident
- Response
- Recovery
- Operational Continuity

Time

Incident
Thanks for your attention
Any questions?

Contact: aymeric.cretin@femto-st.fr