OpenSky: A Swiss Army Knife for Air Traffic Security Research

Martin Strohmeier 1
Matthias Schäfer 2
Markus Fuchs 4
Vincent Lenders 3
Ivan Martinovic 1

1 University of Oxford, UK
2 University of Kaiserslautern, Germany
3 armasuisse, Switzerland
4 SeRo Systems, Germany

September 15, 2015
Original motivation: Security research into ADS-B

Basic testing with single sensors in our lab

Collaboration across countries and labs, sharing of data

Development of the OpenSky idea: formalisation and development of adequate research and sharing infrastructure

Registered association since 2014

http://www.opensky-network.org
Who and What is OpenSky?

- A large-scale ADS-B sensor network (online Jan. 2013)
- Cheap ADS-B sensors distributed (mostly) in Europe
- Receivers are connected over the Internet
- Access to raw ADS-B data and PHY-layer information
OpenSky Basis

Various off-the-shelf sensors installed by motivated volunteers.
OpenSky Frontend

DASC 2015: OpenSky - A Swiss Army Knife for Air Traffic Security Research
OpenSky Backend

- Move from RDMS architecture to big data system
- Four horizontally scalable layers
- Enables real-time processing of all received messages in <20ms, and fast large-scale analysis over all data
Current OpenSky Coverage
Example of an OpenSky Dataset

- **Contents**
  - ID
  - Velocity
  - Position
  - ...

- **Meta Data**
  - Physical layer data
    - RSS
    - Loss
    - SNR
  - Timestamps
  - Sensor ID
ADS-B Channel Analysis with OpenSky

**Log-distance Path Loss Model (LDPL)**

*Doughnut effect*: noticeable drop in reception quality of messages sent in close proximity to a receiver.

**1090 MHz channel utilization is very high**

60 aircraft → 40% message loss

**Loss vs. Distance**

**Loss vs. Traffic**

---

*DASC 2015*: OpenSky - A Swiss Army Knife for Air Traffic Security Research

September 15, 2015
Page 9
Exemplary Security Research with OpenSky

- Aircraft Location Verification
- Secure Track Verification
- Physical Layer Intrusion Detection
- Transponder Fingerprinting
- Event Detection

- For all the details, read the papers on the OpenSky website!
Some Attacker Models

- **Attacker Altitude**
  - **Commercial Airspace**
  - **Ghost Aircraft**
  - **Diverted Aircraft**
  - **Ground**

- **Attacker Mobility**
  - **ADS-B Receiver**

**Commercial Airspace**: Aircraft that are flying at higher altitudes.

**Ghost Aircraft**: Aircraft that are not actually present, but their signals are transmitted by an attacker.

**Diverted Aircraft**: Aircraft that are flown to a specified destination by a hijacker or attacker.

**Ground**: Aircraft flown at lower altitudes, close to the ground.
Aircraft Location Verification
Aircraft Location Verification: Multilateration
Aircraft Location Verification

Secure Track Verification
Secure Track Verification

- New approach, exploiting the inherent mobility of aircraft
- Use sequences of location claims, measure differences in propagation delay to receivers
- Detect any deviation
- Not dependent on tight synchronisation and hardware
Secure Track Verification

PHY-Layer Intrusion Detection
PHY-Layer Features

- Commercial ADS-B transponders use two antennas.
- Possible to detect single-antenna attackers with high certainty by exploiting distinct autocorrelation features.
Anomaly Detection

- One-class classification
- Simulation of different attacker types
  - constant sending strength
  - random sending strength
  - adaptive sending strength

Transponder Fingerprinting
Transponder Fingerprinting

- Different ADS-B transponder types / implementations used in the commercial aviation market.

- Several features based on random message inter-arrival times.
Transponder Fingerprinting

- **6 main types.** With 100 samples, prediction accuracy of 99.91%

- Some special cases with unique feature combinations, making aircraft potentially identifiable, even when using pseudonyms / not broadcasting their ID.

<table>
<thead>
<tr>
<th>Feature</th>
<th># Slots</th>
<th>Slot width</th>
<th>Inter-slot width</th>
<th>Missing slots</th>
<th>No width slots</th>
<th>First slot</th>
<th>Last slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1a</td>
<td>39</td>
<td>±0.00025s</td>
<td>0.005s</td>
<td>No</td>
<td>No</td>
<td>0.405s</td>
<td>0.595s</td>
</tr>
<tr>
<td>Type 1b</td>
<td>41</td>
<td>±0.00025s</td>
<td>0.005s</td>
<td>No</td>
<td>Yes</td>
<td>0.40s</td>
<td>0.60s</td>
</tr>
<tr>
<td>Type 2</td>
<td>16</td>
<td>±0.001s</td>
<td>0.01s</td>
<td>Yes</td>
<td>No</td>
<td>0.40s</td>
<td>0.59s</td>
</tr>
<tr>
<td>Type 3</td>
<td>20</td>
<td>±0.0005s</td>
<td>0.01s</td>
<td>No</td>
<td>No</td>
<td>0.40s</td>
<td>0.59s</td>
</tr>
<tr>
<td>Type 4</td>
<td>16</td>
<td>±0.0015s</td>
<td>0.125s</td>
<td>No</td>
<td>Yes</td>
<td>0.40s</td>
<td>0.60s</td>
</tr>
<tr>
<td>Type 5</td>
<td>26</td>
<td>+0.00016s</td>
<td>0.008s</td>
<td>No</td>
<td>No</td>
<td>0.40s</td>
<td>0.61s</td>
</tr>
</tbody>
</table>

Event Detection
Event Detection

- Time series analysis to identify anomalies.
- Combine OpenSky ADS-B sensor data with publicly available databases about 24-bit ICAO identifiers, aircraft types and airline to track various types of activity.
- Data from 2 OpenSky sensors closest to Davos / Zurich:
Event Detection

- >70% increase from mean and 45% increase over previous peaks.

Pitfalls:

- Data quality / consistency.
- Need to take long-term trends into account / compare to recent data.
- Doesn’t tell us what is going on!

![Event Detection Graph](image-url)
Conclusion

- OpenSky provides a scalable, open, and collaborative architecture for air traffic research.

- Communications security is an important problem in modern aviation.

- Our research using OpenSky proposes and analyses attack detection using several different approaches.

- Security and privacy has been OpenSky’s main theme but the data is used for many other applications now.

- Check out http://opensky-network.org if you are interested further in air traffic communication research, security and non-security related.
References


Questions?