Department of Computer Science

UNIVERSITY OF OXFORD

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

OPENSKY
NETWORK

http://www.opensky-network.org

- 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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
armasuisse

FH
Bern University
of Applied Sciences

CWI
Centrum Wiskunde & Informatica

disco
DISTRIBUTED COMPUTER SYSTEMS

EURECOM
Sophia Antipolis

USI/SUPSI
Istituto
Dalle Molle
di studi
sull'intelligenza
artificiale
IDSIA

institute
iMdea
networks

SeRo
Systems

Transkom
Kommunikationsnetzwerke GmbH
Powered By IP

trivadis
makes IT easier.

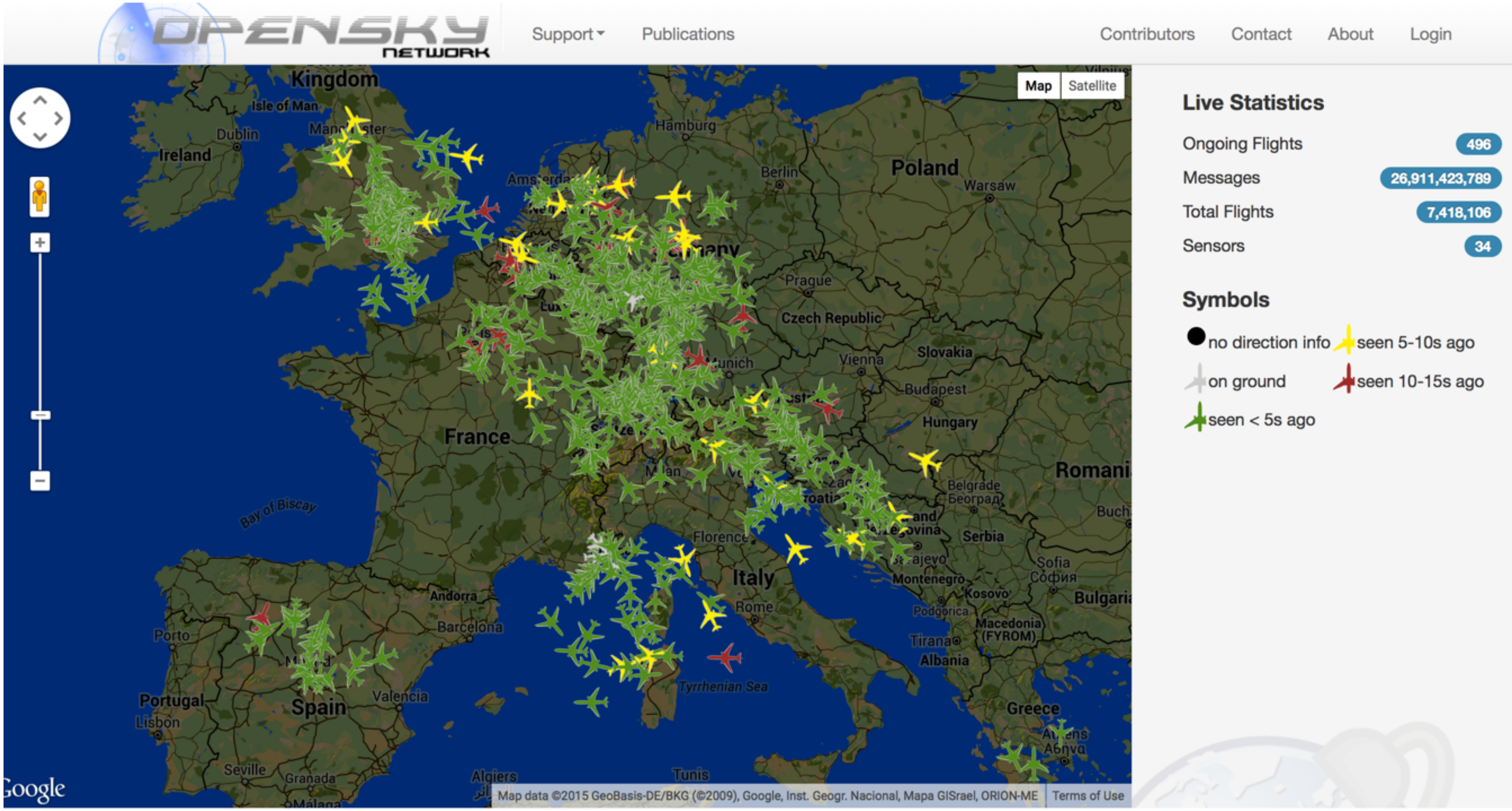
UNIVERSITY OF
OXFORD

University of Ljubljana
Faculty of Computer and
Information Science

OpenSky Basis

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

OpenSky Frontend



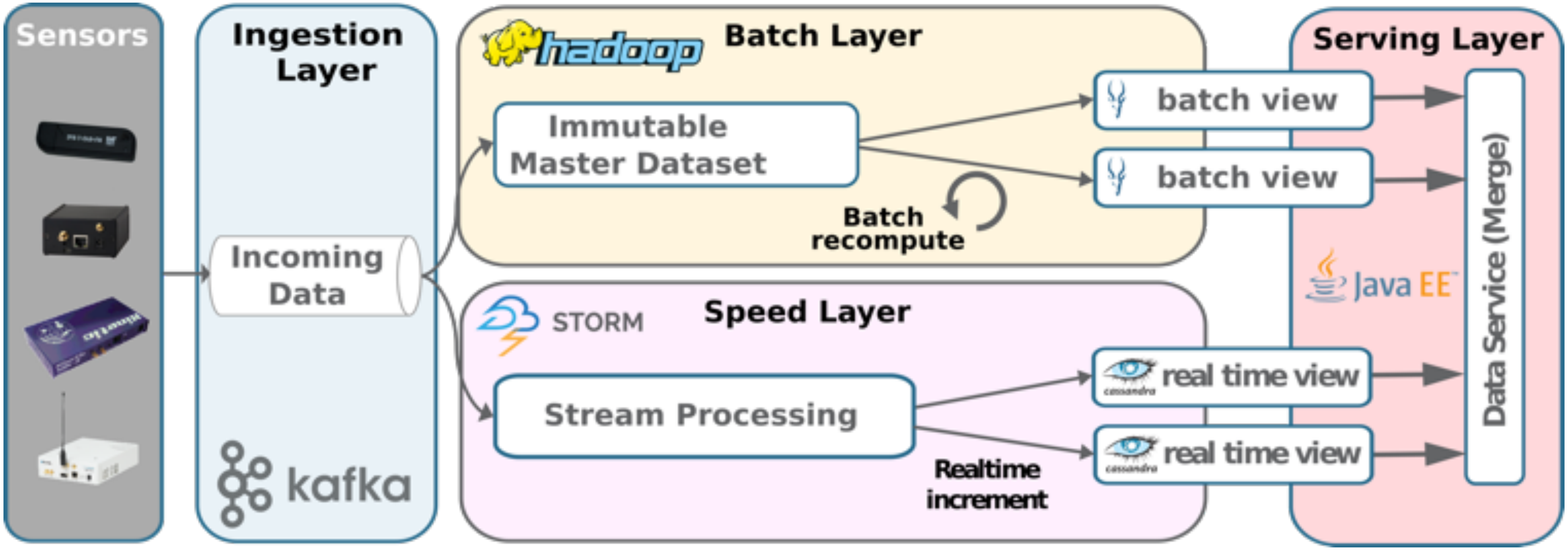
Live Statistics

Ongoing Flights	496
Messages	26,911,423,789
Total Flights	7,418,106
Sensors	34

Symbols

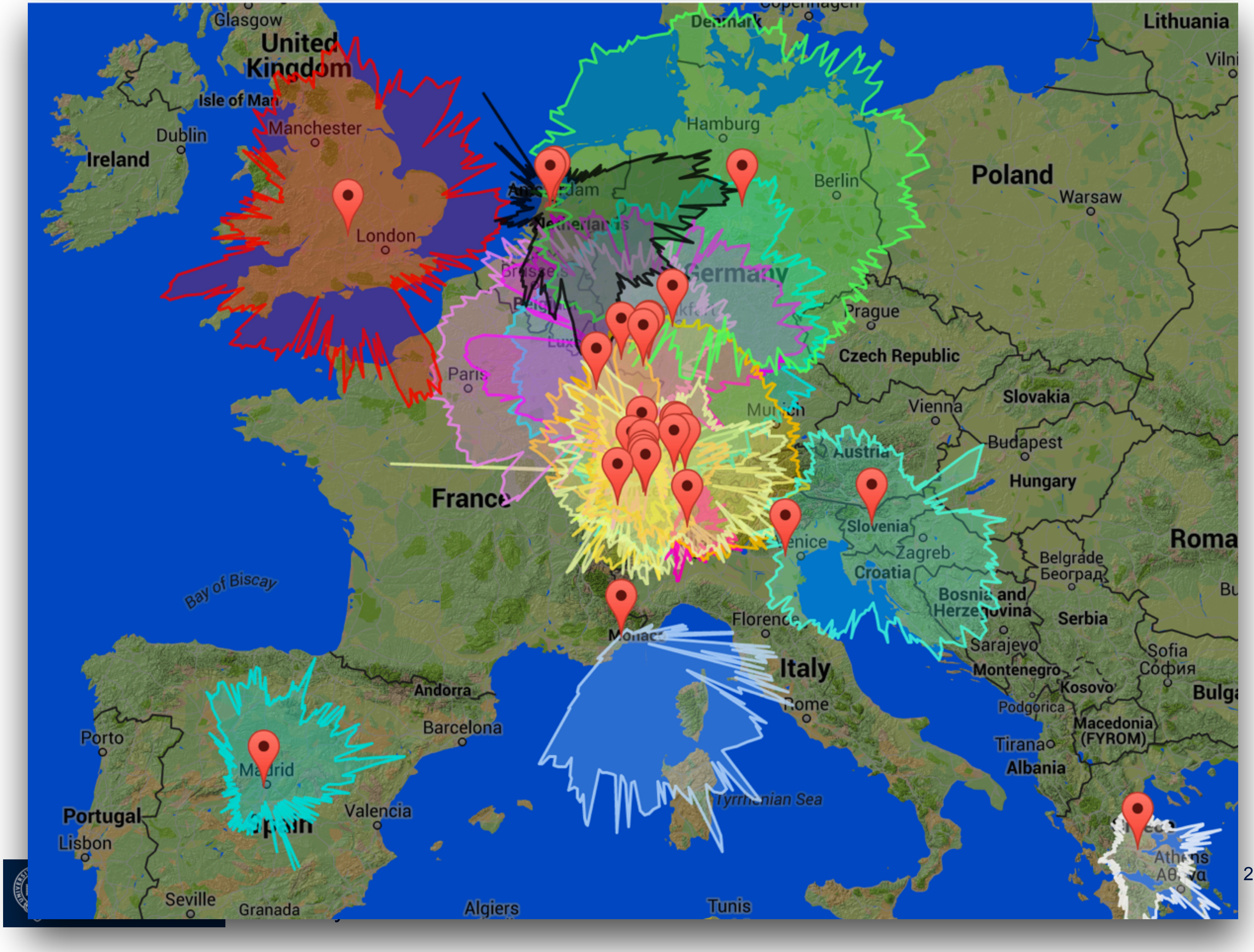
● no direction info	✈ seen 5-10s ago
✈ on ground	✈ seen 10-15s ago
✈ seen < 5s ago	

OpenSky Backend



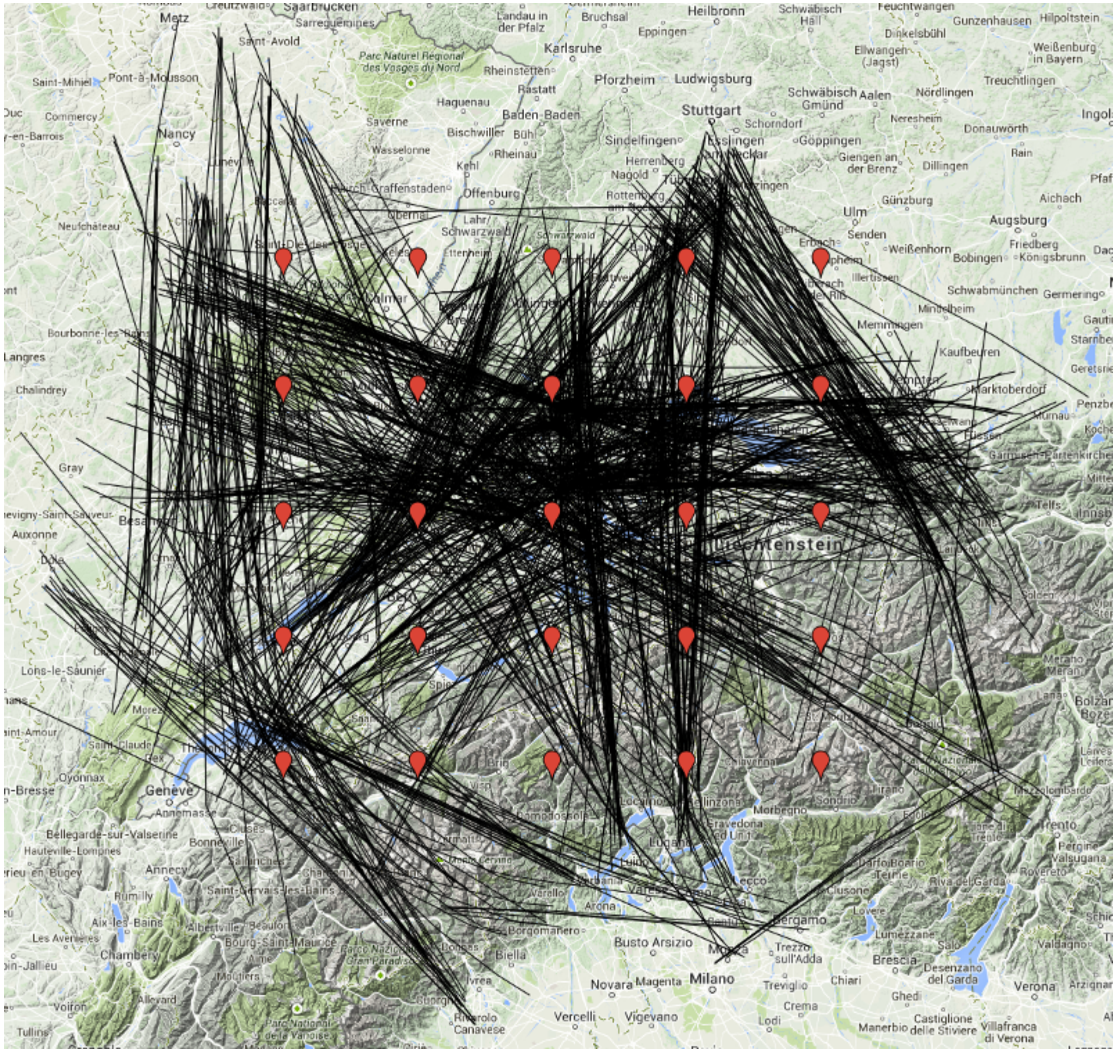
- Move from RDMS architecture to big data system
- Four horizontally scalable layers
- Enables real-time processing of all received messages in <20ms, and fast large-scale analysis over all data

Current OpenSky Coverage



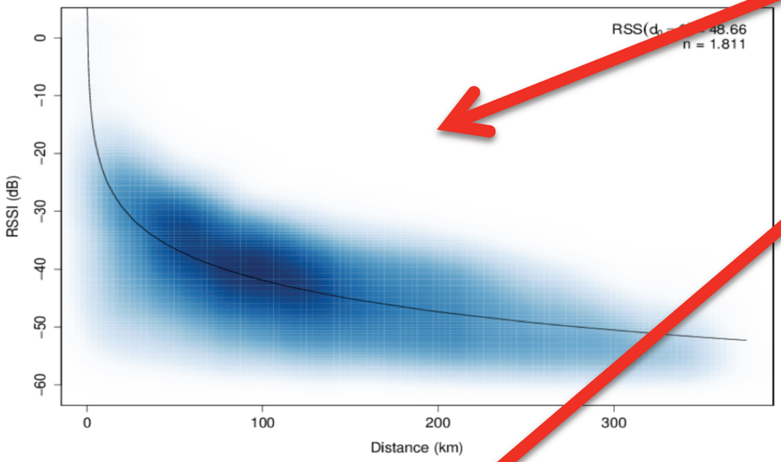
Example of an OpenSky Dataset

- Contents
  - ID
  - Velocity
  - Position
  - …
- Meta Data
  - Physical layer data
    - RSS
    - Loss
    - SNR
  - Timestamps
  - Sensor ID



ADS-B Channel Analysis with OpenSky

Propagation Model



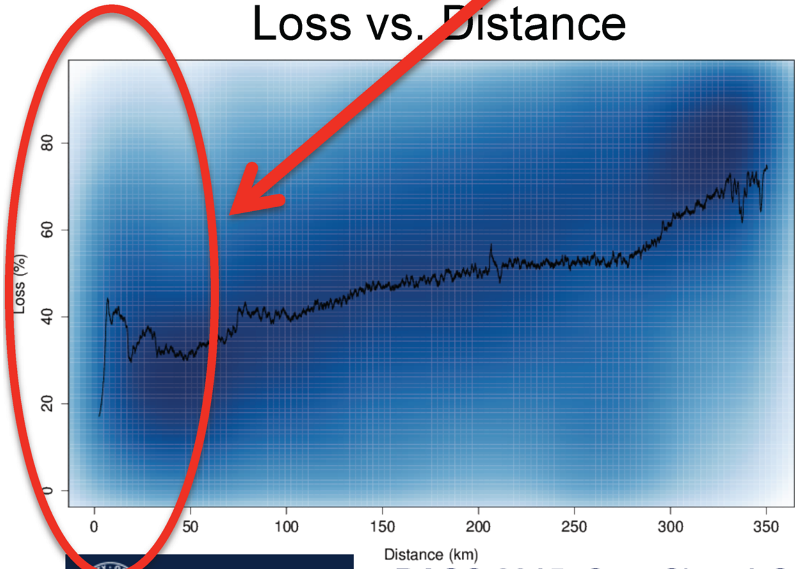
Log-distance Path Loss Model (LDPL)

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

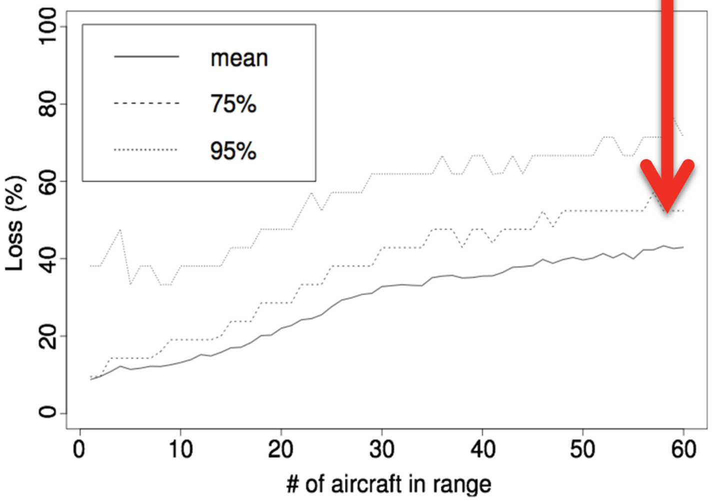
1090 MHz channel utilization is very high

60 aircraft → 40% message loss

Loss vs. Distance



Loss vs. Traffic

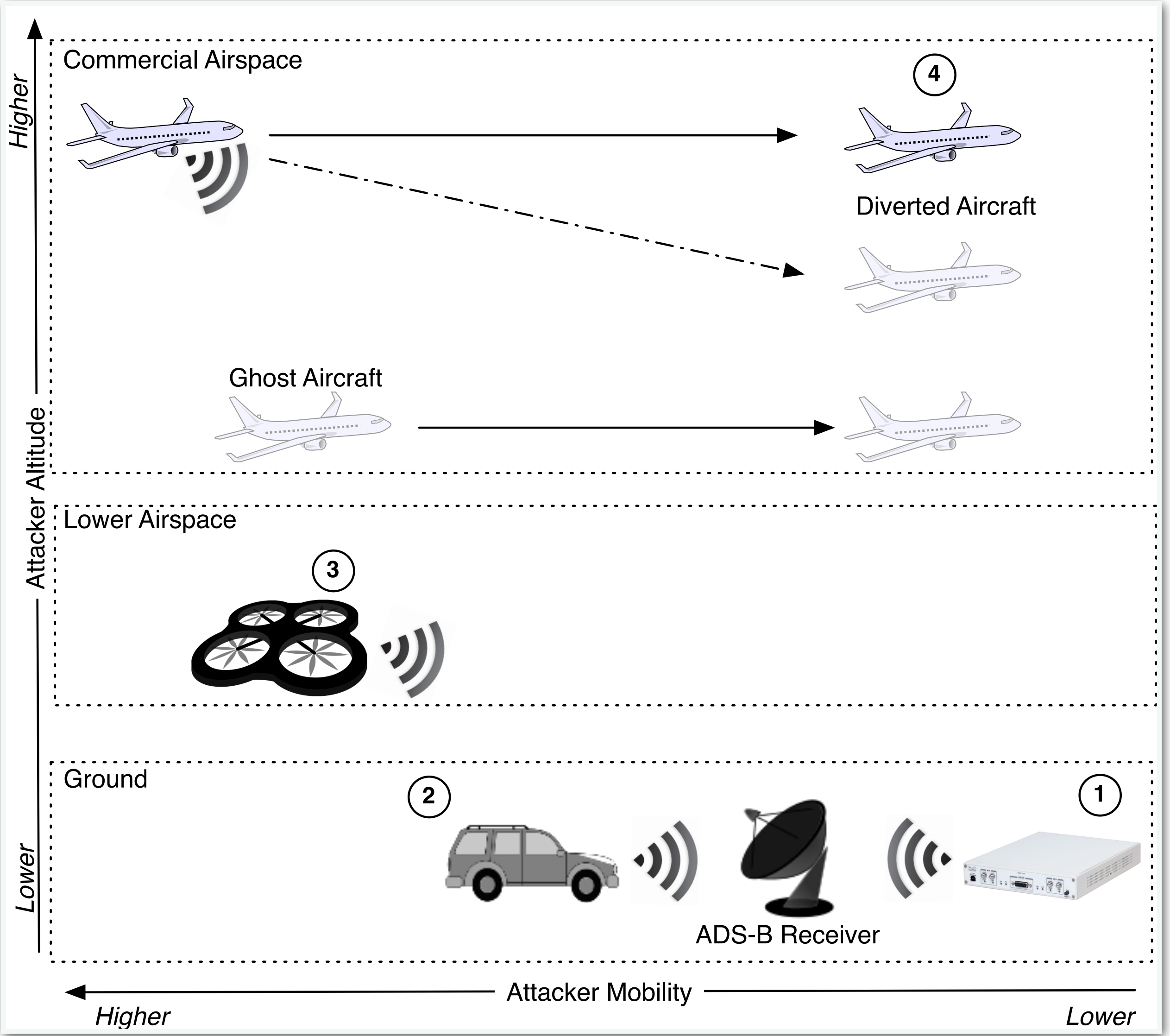


Exemplary Security Research with OpenSky

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

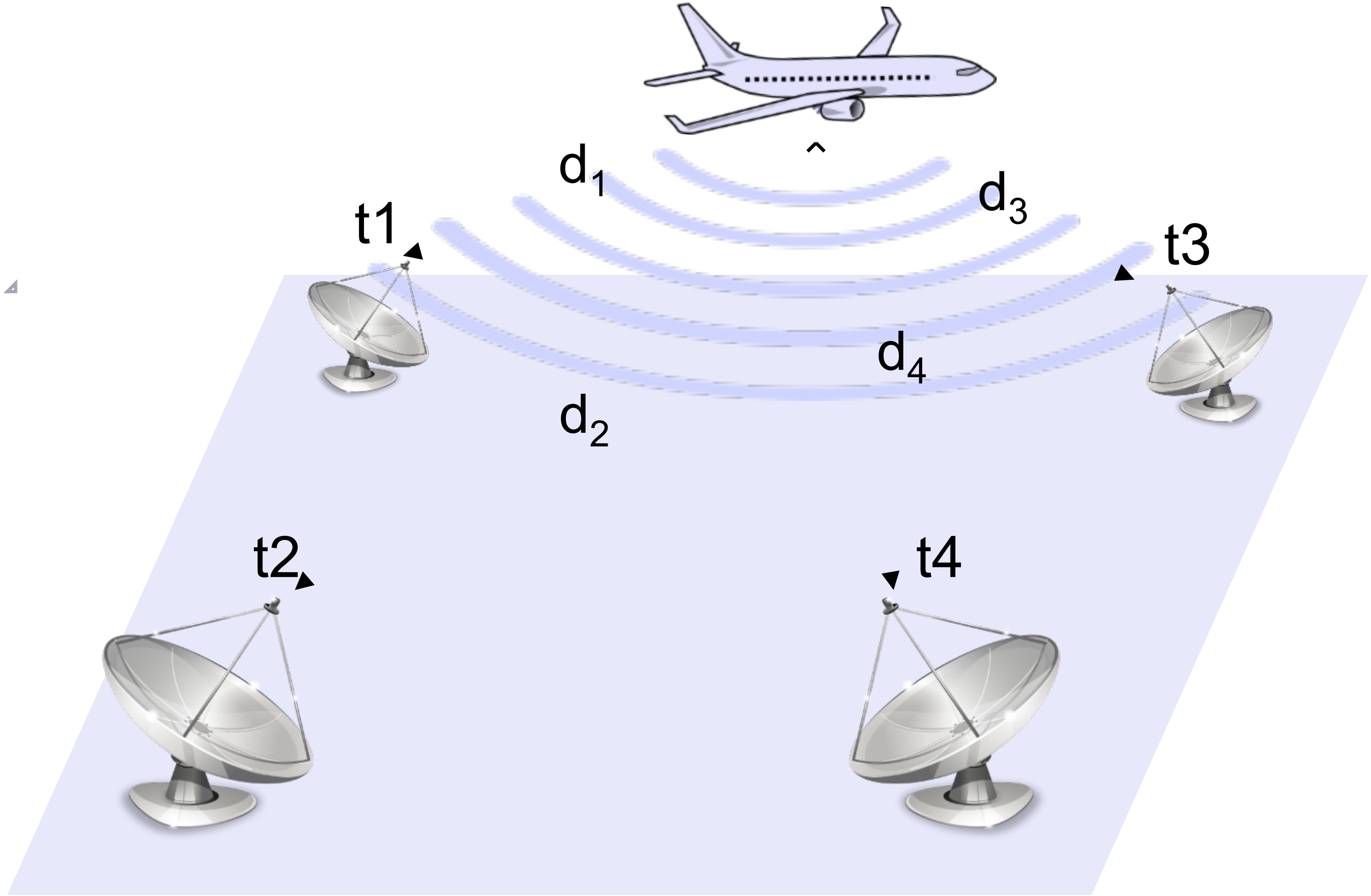
- **For all the details, read the papers on the OpenSky website!**

Some Attacker Models

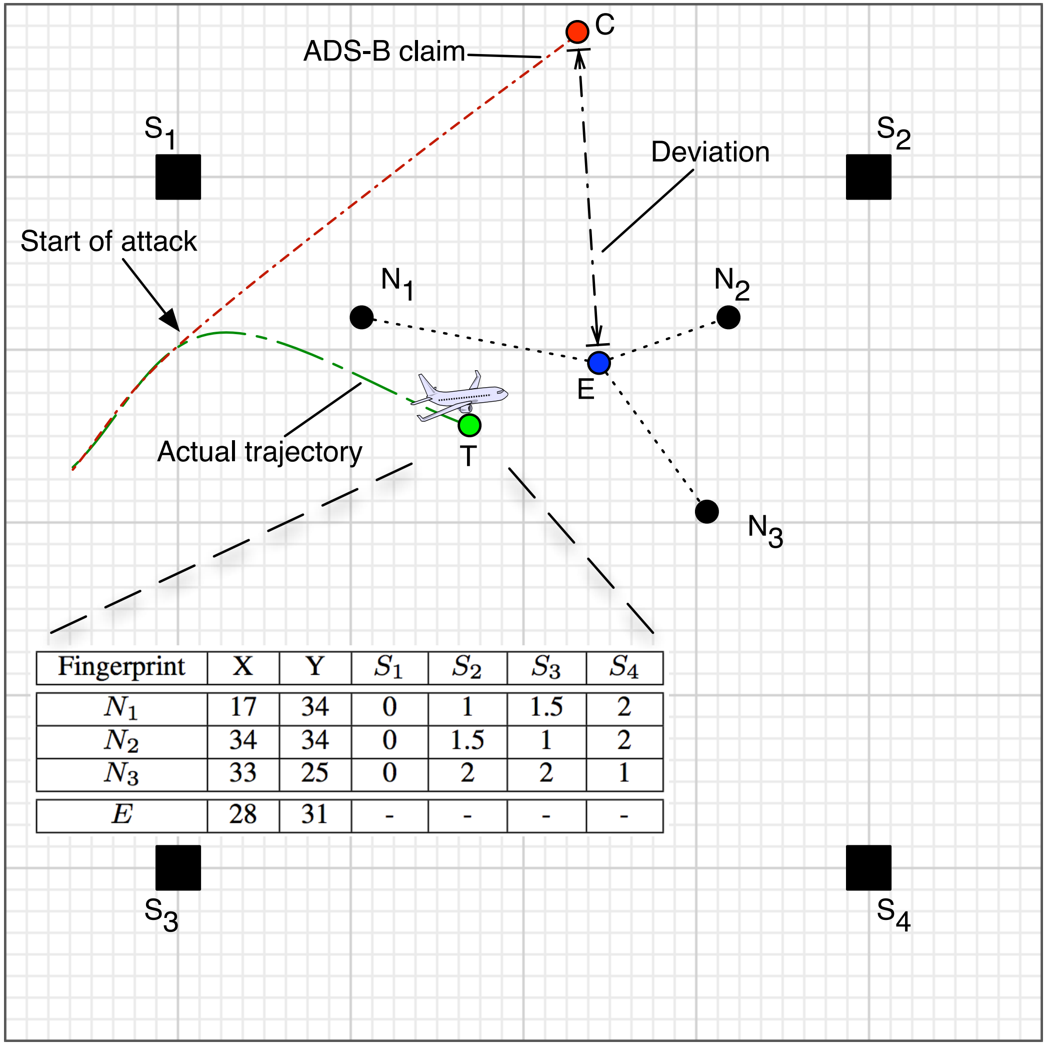


Aircraft Location Verification

Aircraft Location Verification: Multilateration



Aircraft Location V



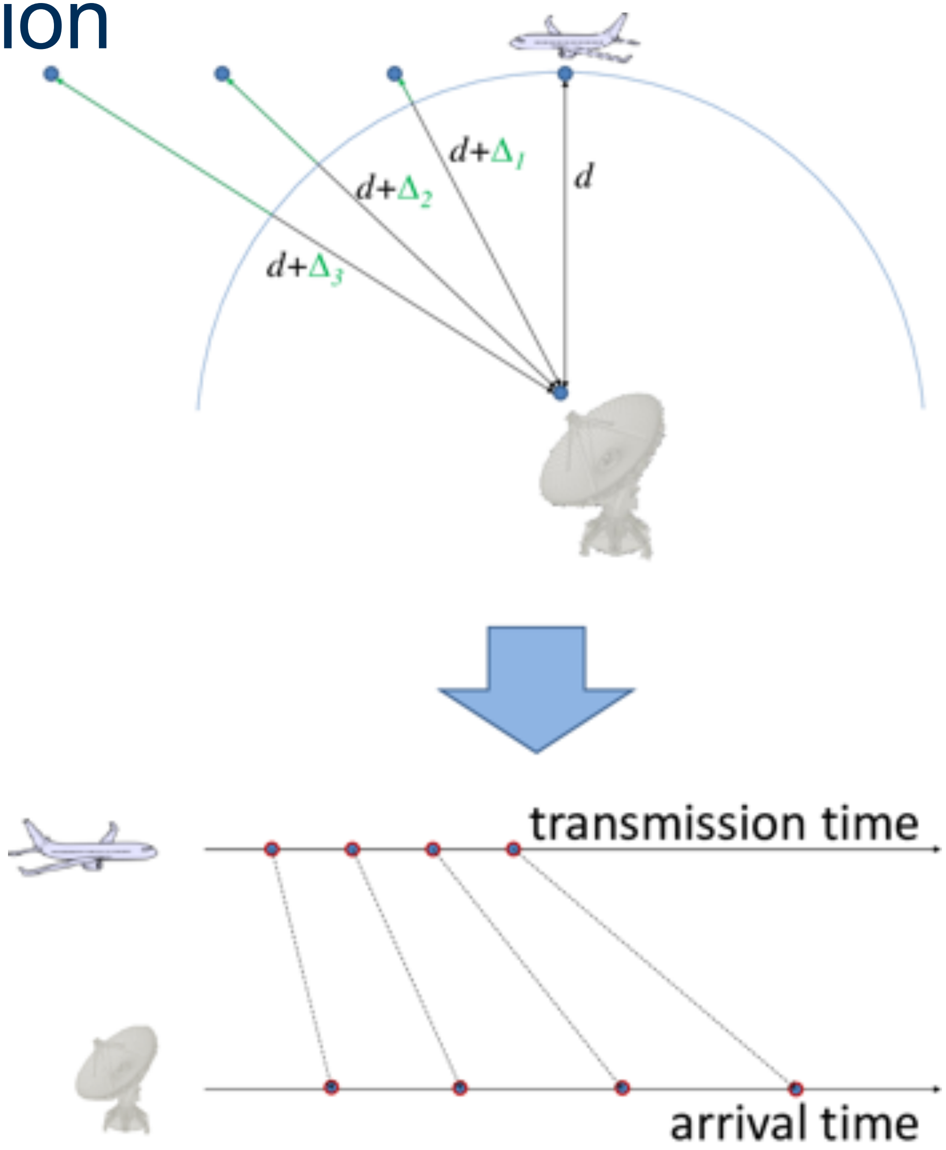
Fingerprint	X	Y	S_1	S_2	S_3	S_4
N_1	17	34	0	1	1.5	2
N_2	34	34	0	1.5	1	2
N_3	33	25	0	2	2	1
E	28	31	-	-	-	-

[1] “Lightweight Location Verification in Air Traffic Surveillance Networks.” Martin Strohmeier, Vincent Lenders and Ivan Martinovic. In Proceedings of the 1st ACM Workshop on Cyber−Physical System Security (CPSS '15). April, 2015.

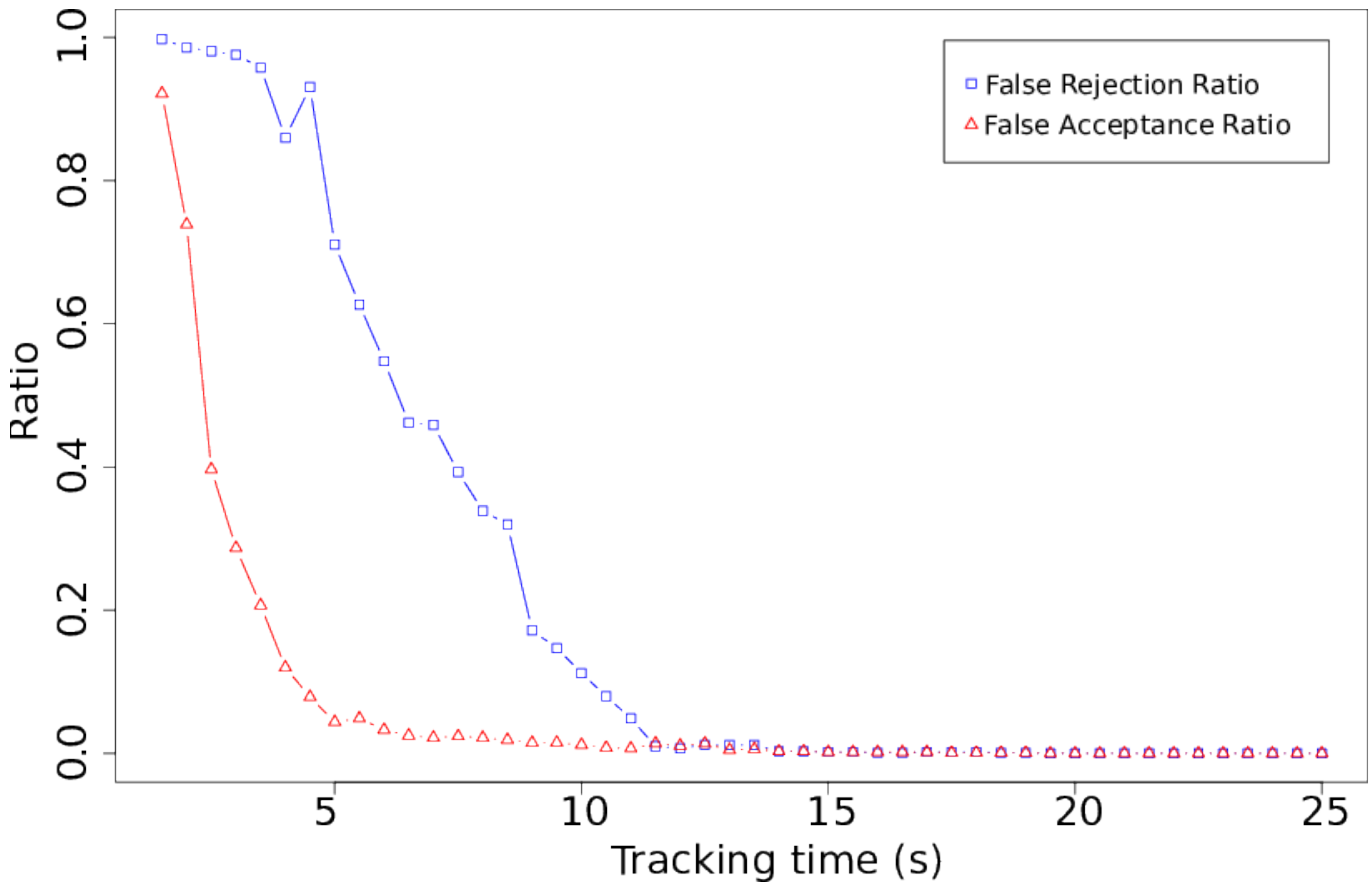
Secure Track Verification

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

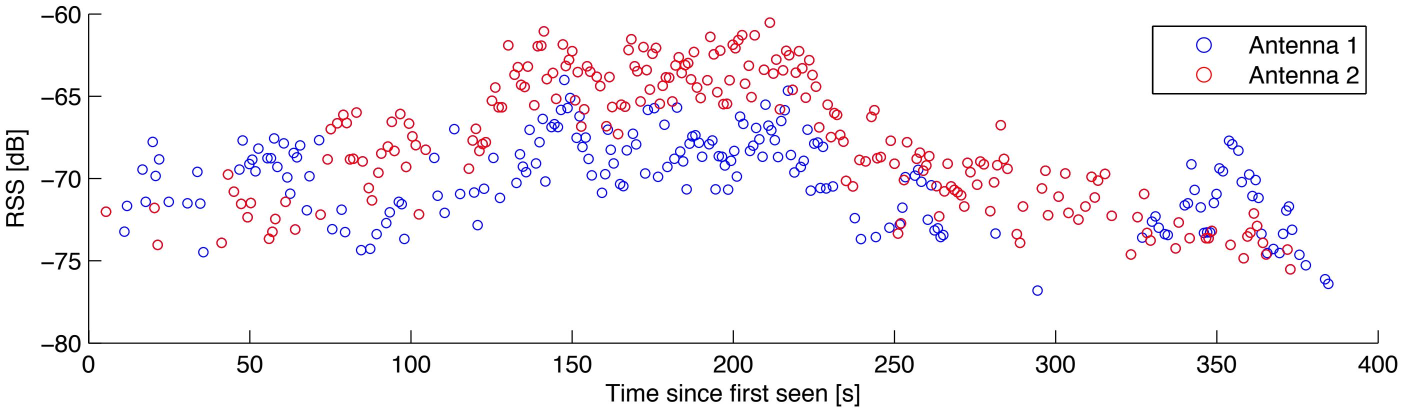


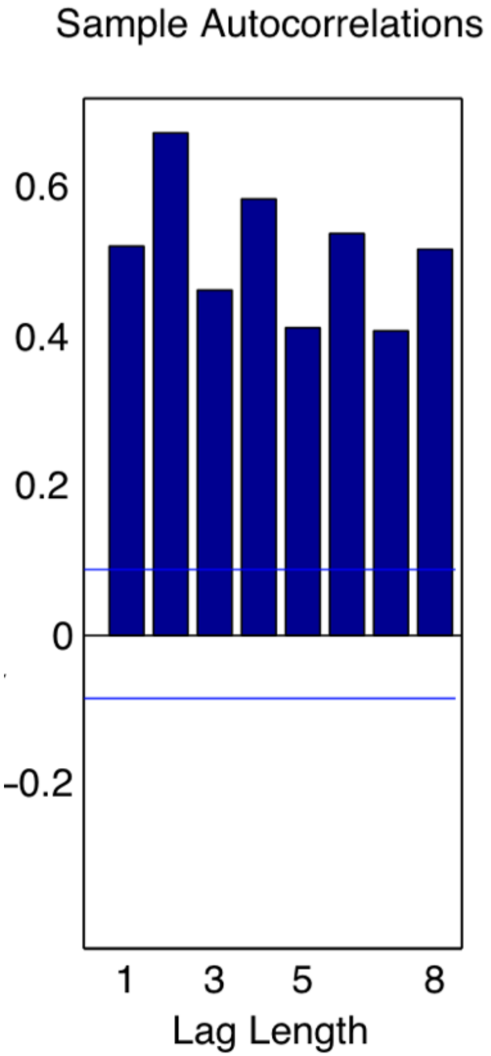
[2] “Secure Track Verification.” Matthias Schäfer, Vincent Lenders and Jens B Schmitt. In IEEE Symposium on Security and Privacy (S&P) May 2015.

PHY-Layer Intrusion Detection

PHY-Layer Features

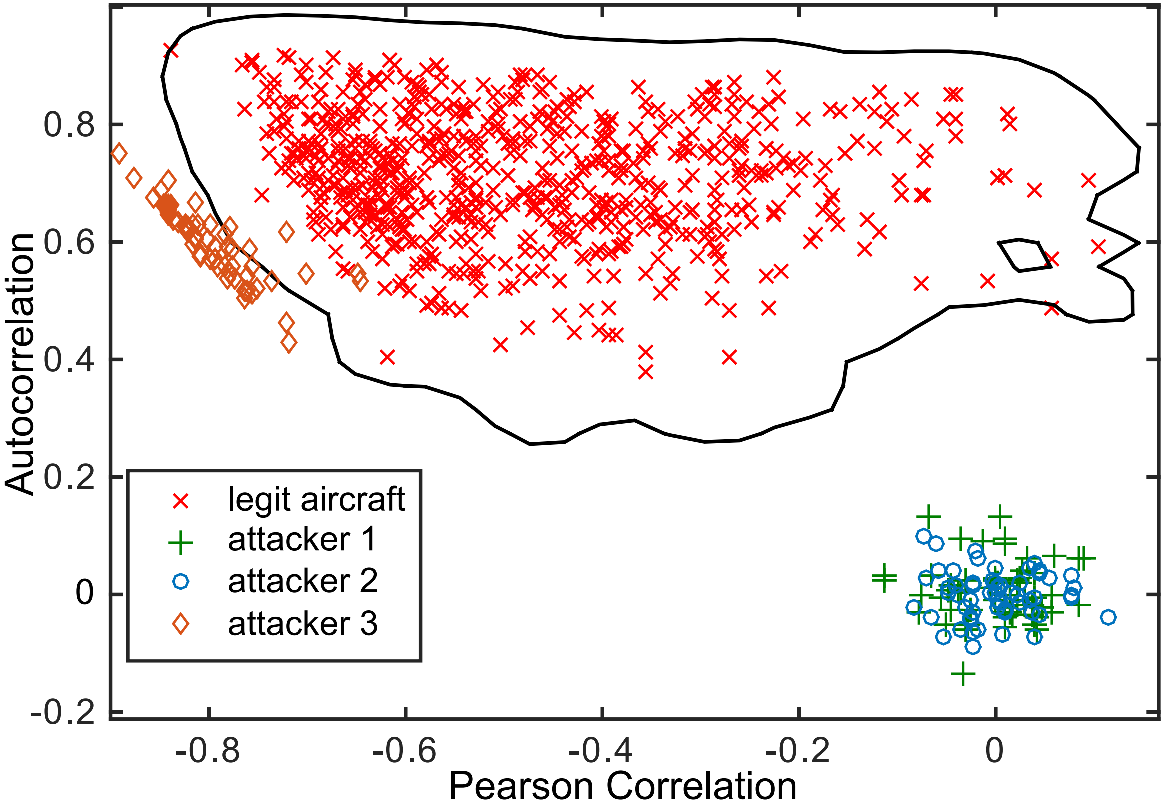
- Commercial ADS-B transponders use two antennas
- Possible to detect single-antenna attackers with high certainty by exploiting distinct autocorrelation features





Anomaly Detection

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

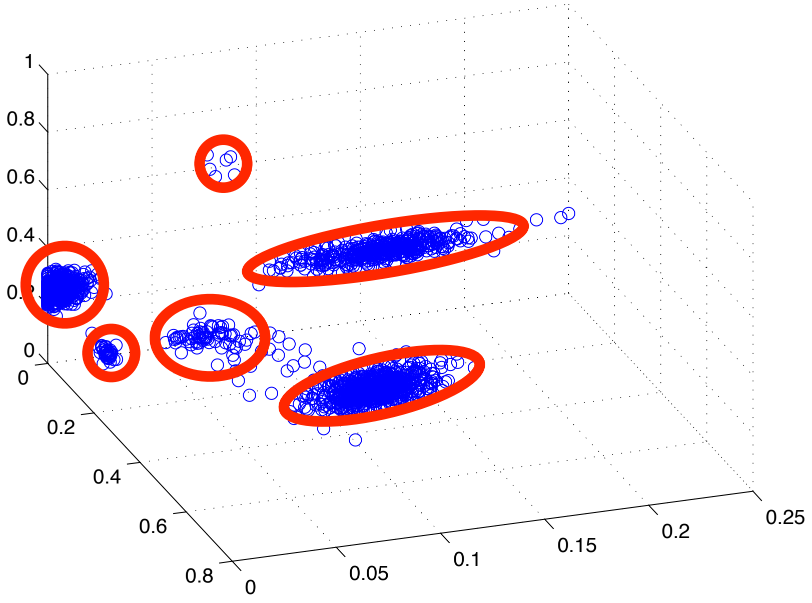


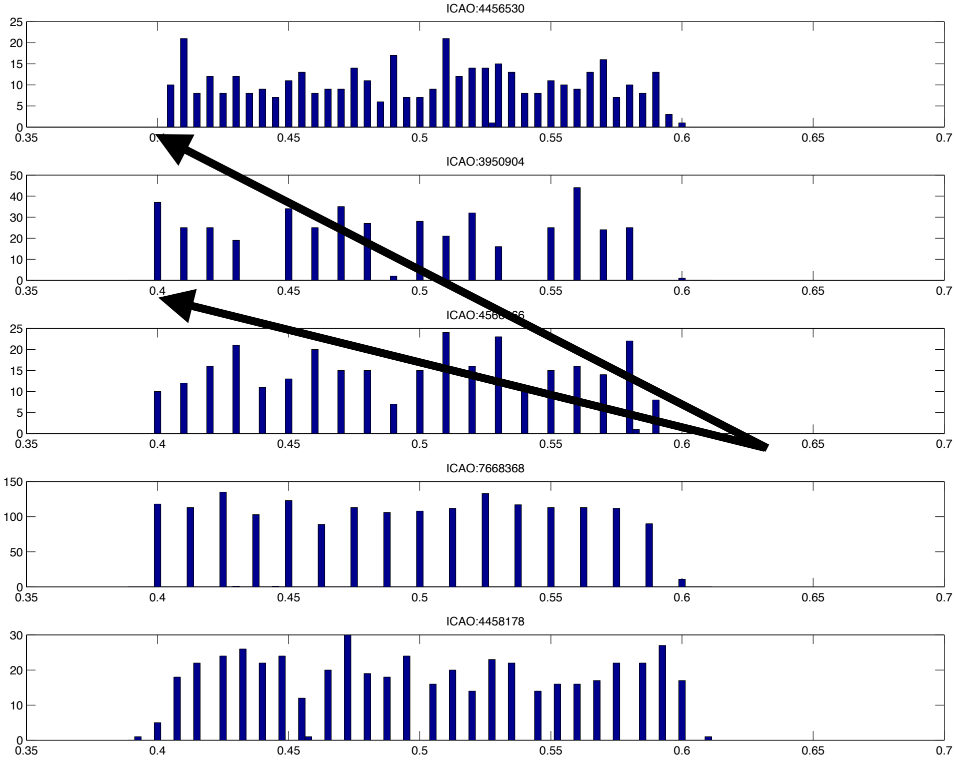
[3] “Intrusion Detection for Airborne Communication using PHY−Layer Information.” Martin Strohmeier, Vincent Lenders and Ivan Martinovic. In Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). July, 2015.

Transponder Fingerprinting

Transponder Fingerprinting

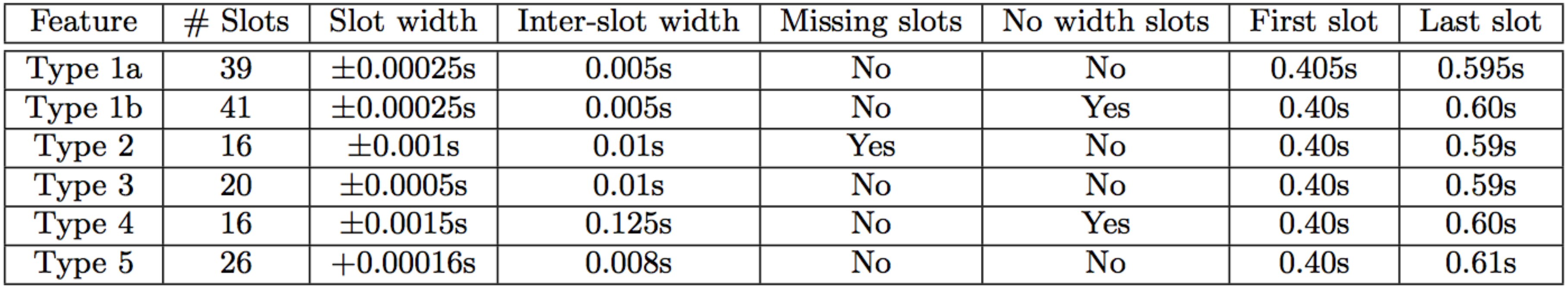
- Different ADS-B transponder types / implementations used in the commercial aviation market.
- Several features based on random message inter-arrival times.





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.



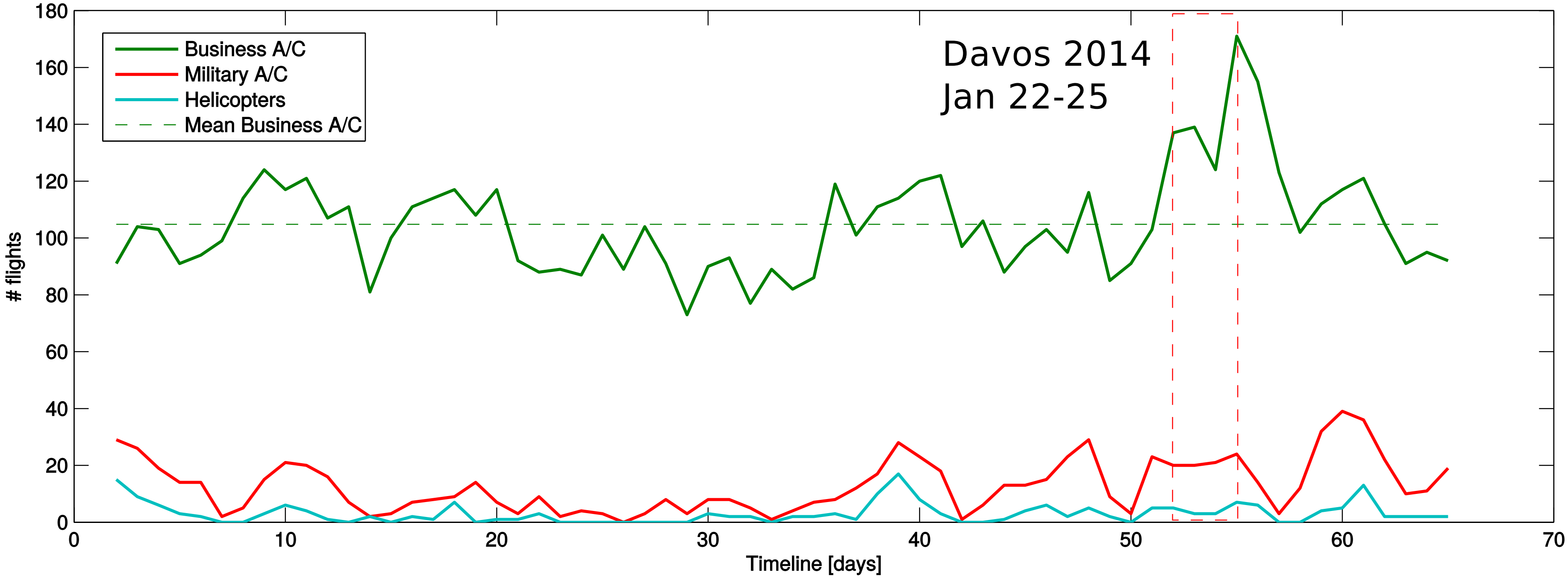
Feature	# Slots	Slot width	Inter-slot width	Missing slots	No width slots	First slot	Last slot
Type 1a	39	±0.00025s	0.005s	No	No	0.405s	0.595s
Type 1b	41	±0.00025s	0.005s	No	Yes	0.40s	0.60s
Type 2	16	±0.001s	0.01s	Yes	No	0.40s	0.59s
Type 3	20	±0.0005s	0.01s	No	No	0.40s	0.59s
Type 4	16	±0.0015s	0.125s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

[4] “On Passive Data Link Layer Fingerprinting of Aircraft Transponders.” Martin Strohmeier and Ivan Martinovic. In 1st ACM Workshop on Cyber−Physical Systems Security & Privacy (CPS−SPC). October, 2015.

Event Detection

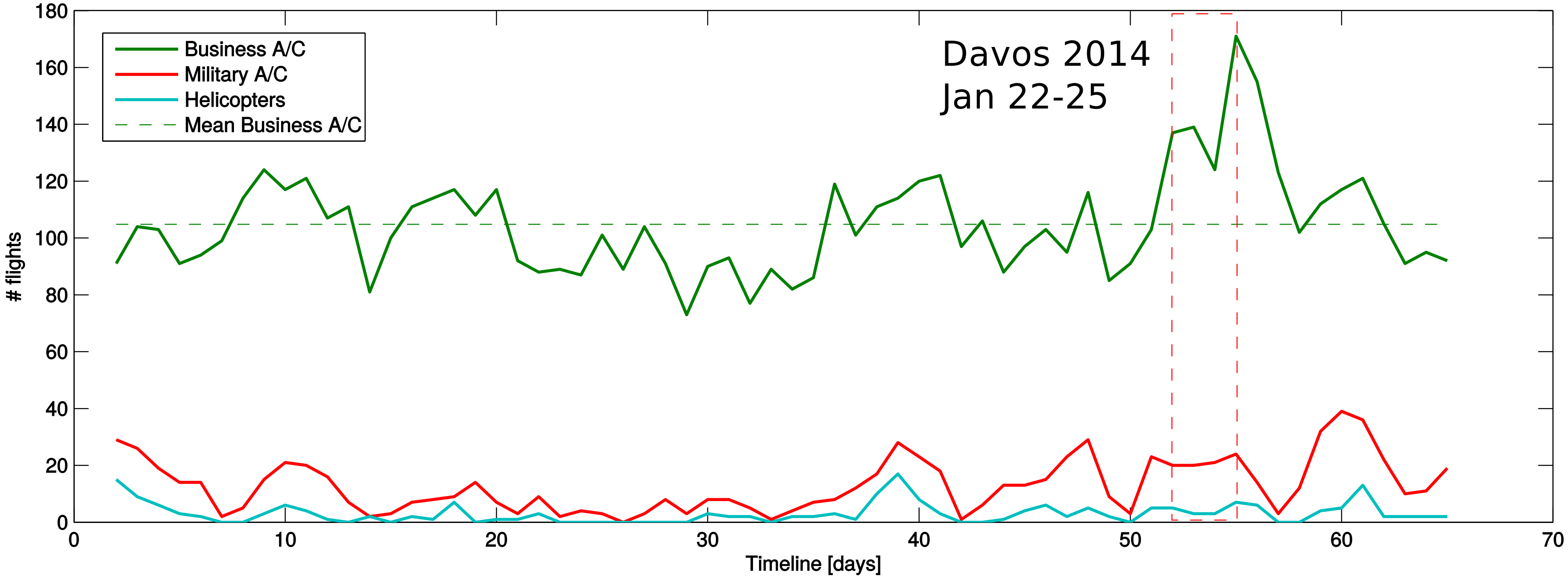
Event Detection

- 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!



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

[1] “Lightweight Location Verification in Air Traffic Surveillance Networks”, Martin Strohmeier, Vincent Lenders and Ivan Martinovic In Proceedings of the 1st ACM Workshop on Cyber−Physical System Security (CPSS '15). April, 2015.

[2] “Secure Track Verification”, Matthias Schäfer, Vincent Lenders and Jens B Schmitt. In IEEE Symposium on Security and Privacy (S&P). May 2015.

[3] “Intrusion Detection for Airborne Communication using PHY−Layer Information”, Martin Strohmeier, Vincent Lenders and Ivan Martinovic. In Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). July, 2015.

[4] “On Passive Data Link Layer Fingerprinting of Aircraft Transponders”, Martin Strohmeier and Ivan Martinovic. In 1st ACM Workshop on Cyber−Physical Systems Security & Privacy (CPS−SPC). October, 2015.

Questions?