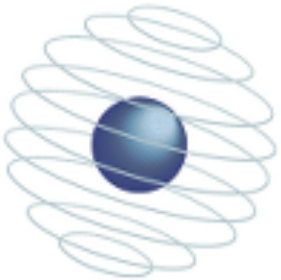


CYBER SECURITY OXFORD

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY

Security & Privacy in a World of Safety: Analysing Avionic Data Links and NextGen ATC Networks

Prof Ivan Martinovic
Computer Science Department
University of Oxford, UK
(ivan.martinovic@cs.ox.ac.uk)

Systems Security Lab

Department of Computer Science

UNIVERSITY OF OXFORD

Members

Prof Ivan Martinovic

Dr Martin Strohmeier

Dr Riccardo Spolaor

Dr Vincent Taylor

Bushra AlAhmadi

Richard Baker

Simon Eberz

Giulio Lovisotto

Ivo Sluganovic

Matt Smith

Michal Piskozub

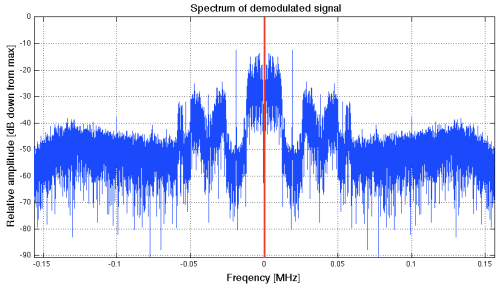
Vincent Taylor

Chris Vaas

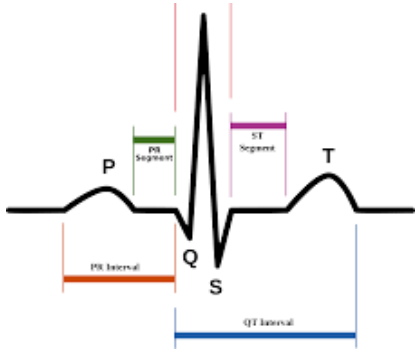
Systems Security Lab

UNIVERSITY OF OXFORD

Research Areas



Technology



Adversary

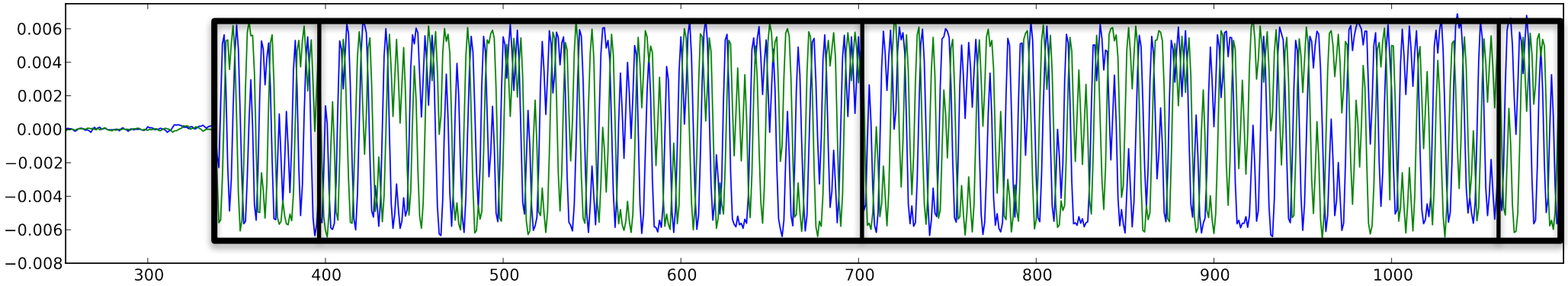
Cyber-physical System Security

Digital (Cyber) View

Cryptography (secrets)

Secret Key Exchange
Content Authentication
Content Confidentiality
Content Integrity
…

DIGITAL DATA



Physical signal (frequency-, time-, and position-dependent)

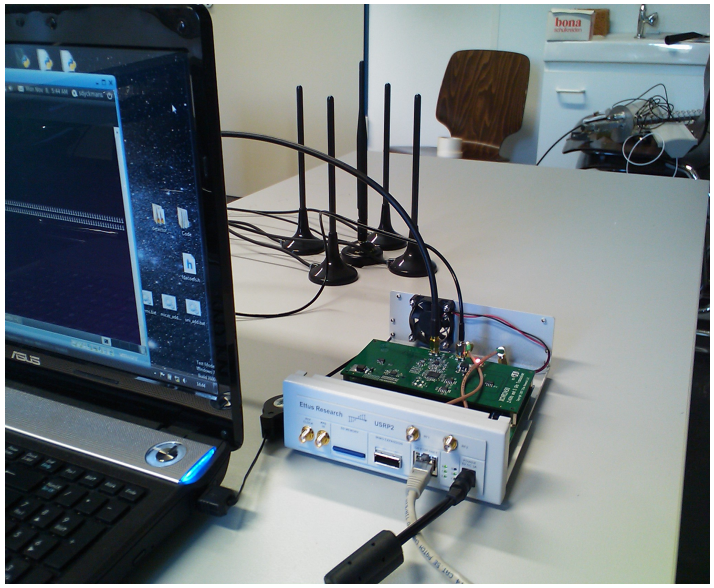
Physical View

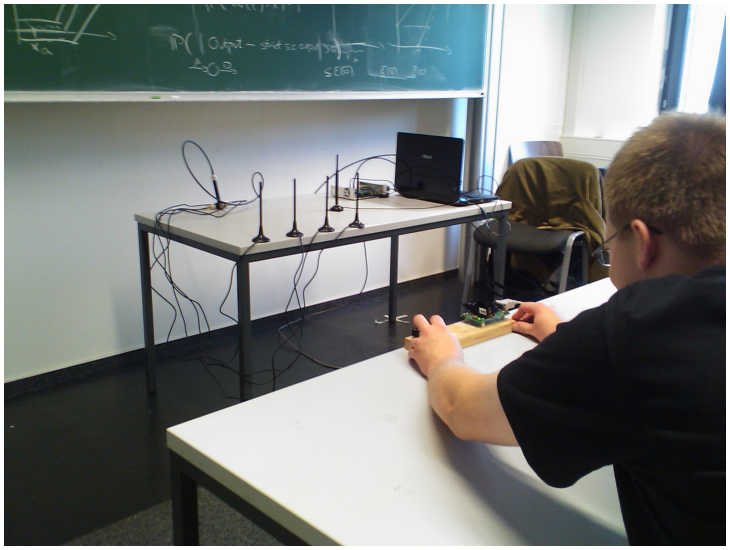
Nature (physical laws)

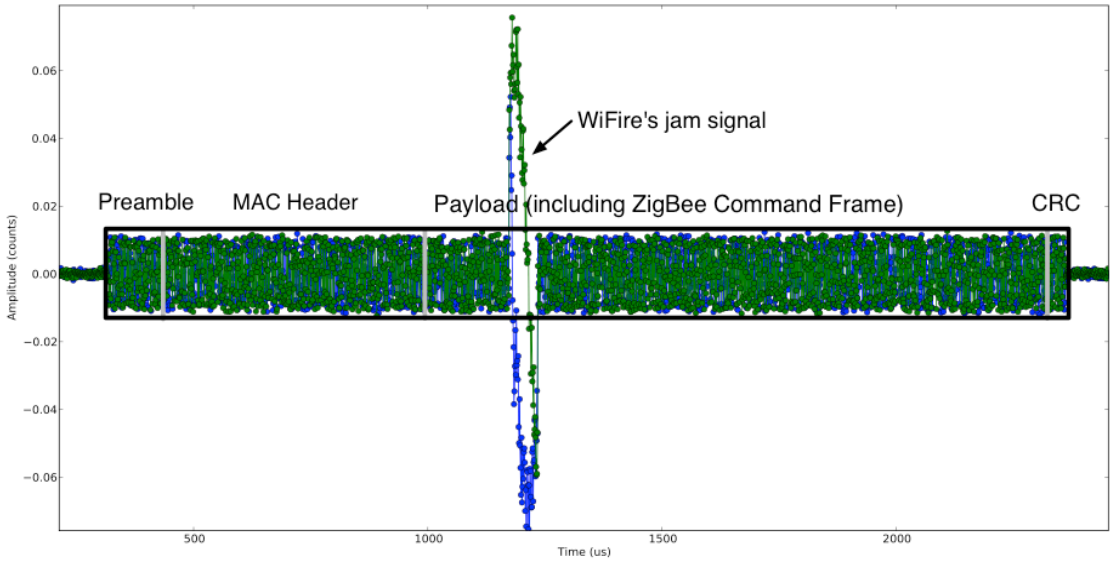
Location verification
PHY-Fingerprinting
Randomness for secrets
Behavioral authentication

Firewalling IoT Device

- Generating a precise jamming signal
- Firewalling IoT devices
  - Applying security policies in real-time
  - Policies: only indoor comms, dedicated channels, no unencrypted comm.
- USRP2 (Software-Defined Radio)
  - Prototype implementation using SDRs





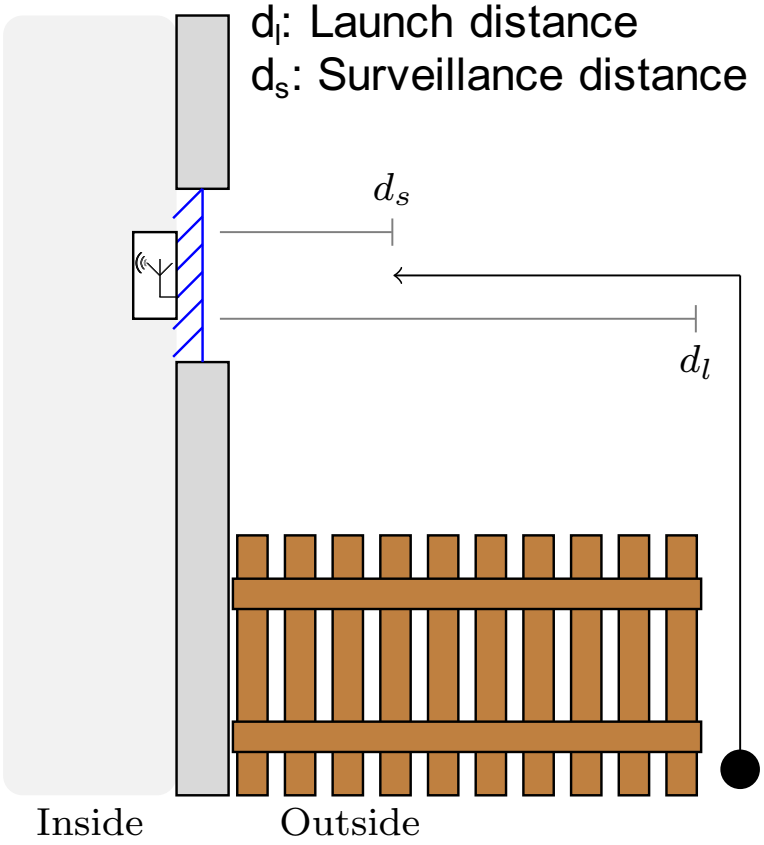


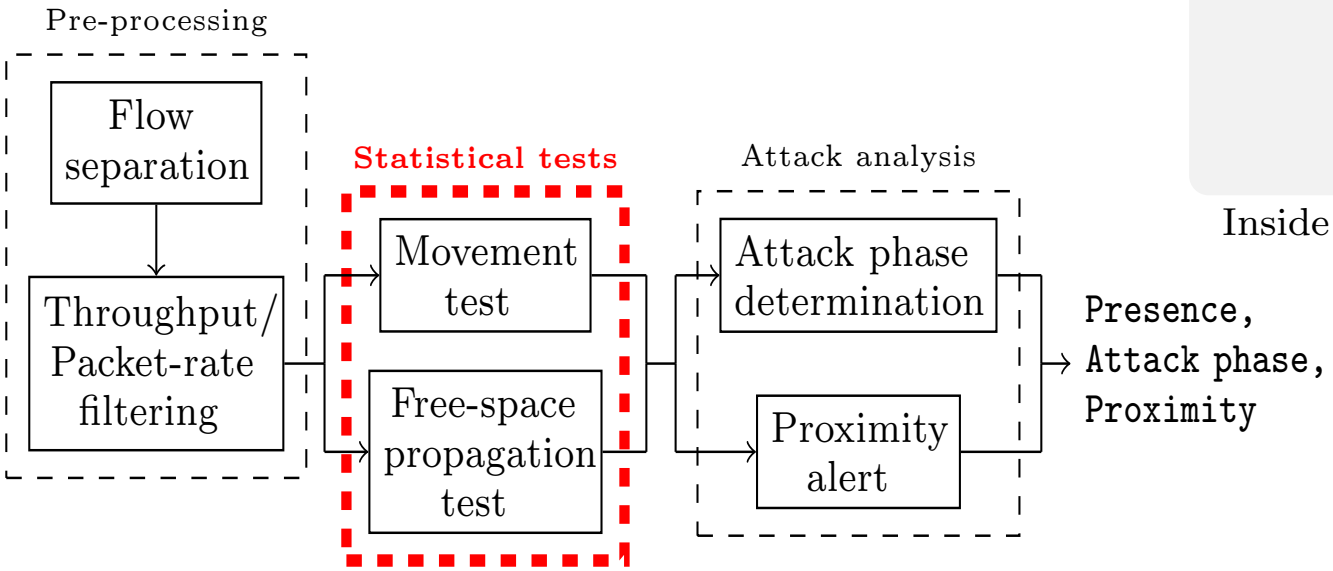
Using RF signals for drone detection

- Detecting drones by analyzing radio environment
- Detection of different phases: approach, surveillance, departure

Drone detection

- Developed statistical methods to detect drone invasions
- Computationally lightweight
- Implementable on a smartphone

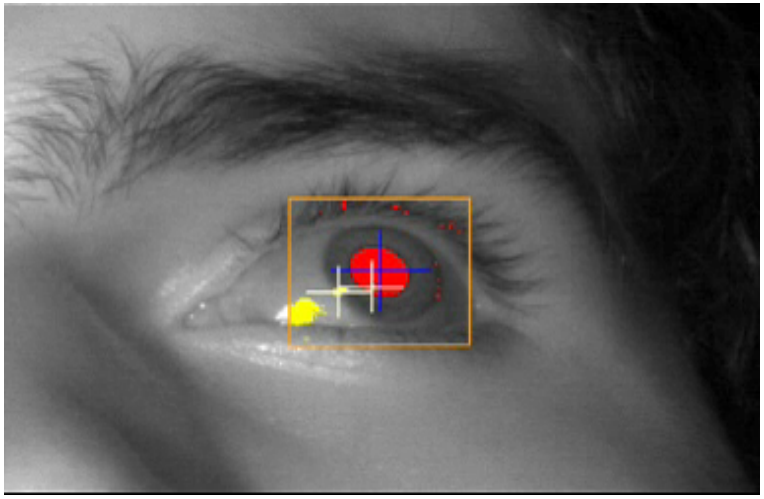


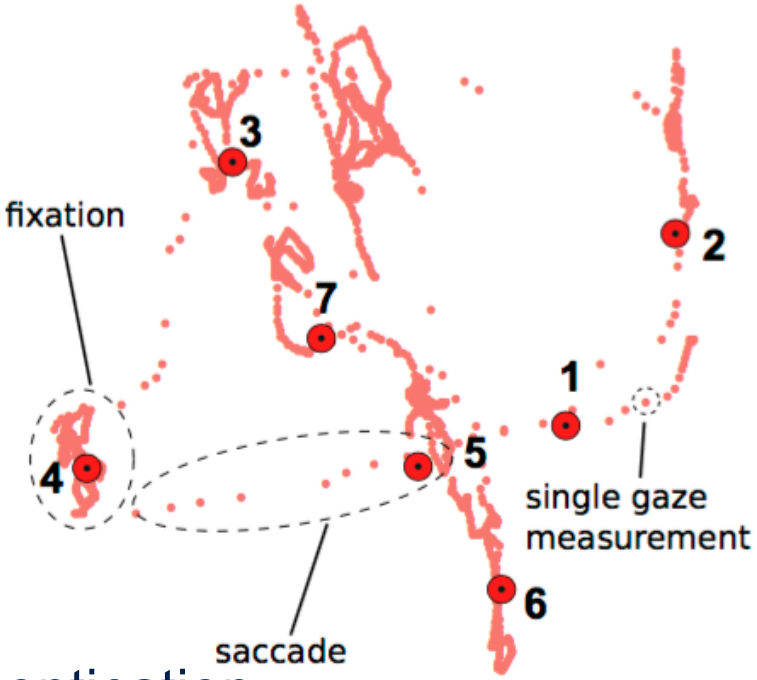


Wi-Fly: Detecting Privacy Invasion Attacks by Consumer Drones. S. Birnbach, R. Baker and I. Martinovic. NDSS 2017.

Continuous Authentication using Eye Movements

Eye movements are used to design a *challenge-response authentication protocol with freshness guarantees.*



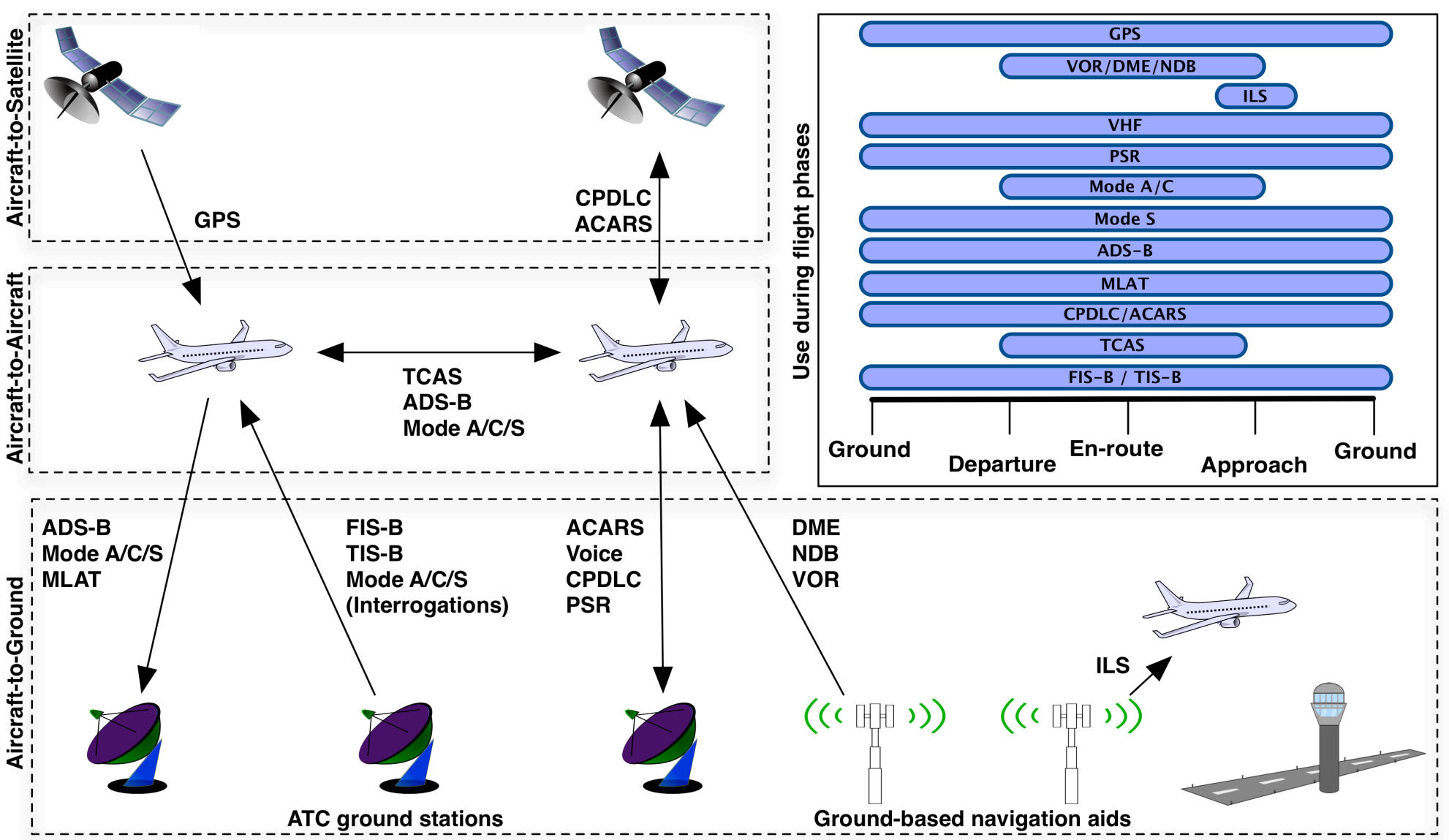


Microsecond response → fast user authentication

Using Reflexive Eye Movements For Fast Challenge–Response Authentication.
I. Sluganovic, M. Roeschlin, K.B. Rasmussen, I. Martinovic. ACM CCS 2016.

A BRIEF INTRODUCTION TO AIR TRAFFIC CONTROL

The Big Picture of Air Traffic Communication



Air Traffic Control – PSR

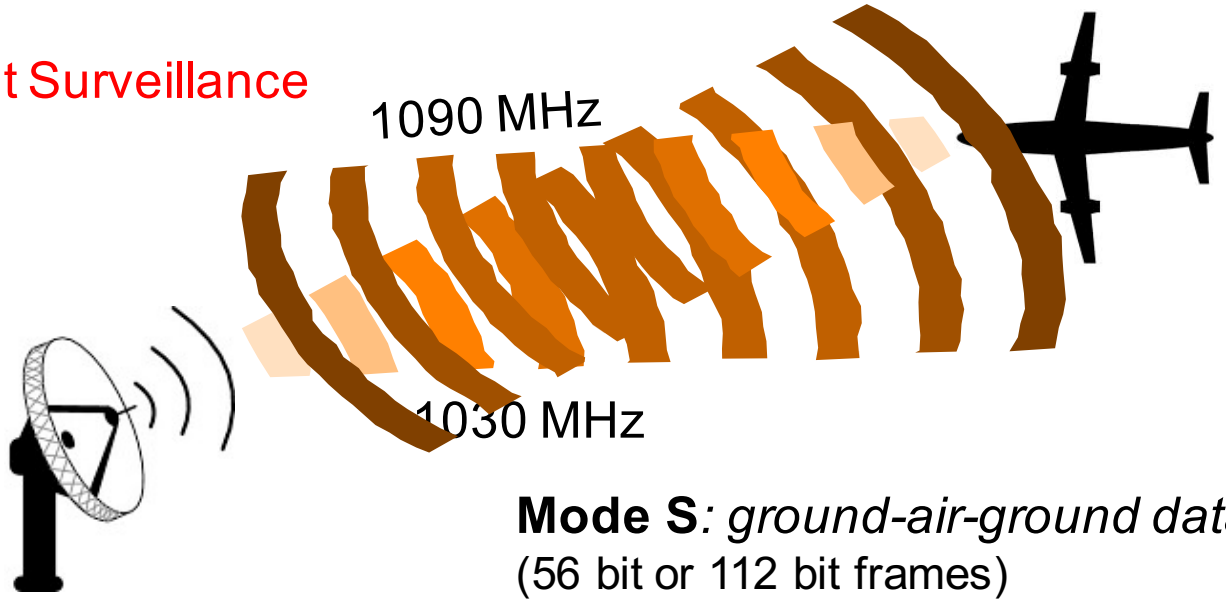
- Primary Surveillance Radar (PSR)
  - Ground based radar
  - Measures the time difference between the signal transmission and reflection (12.36 microseconds is known as a radar-mile)

→ Independent Surveillance

Air Traffic Control – SSR

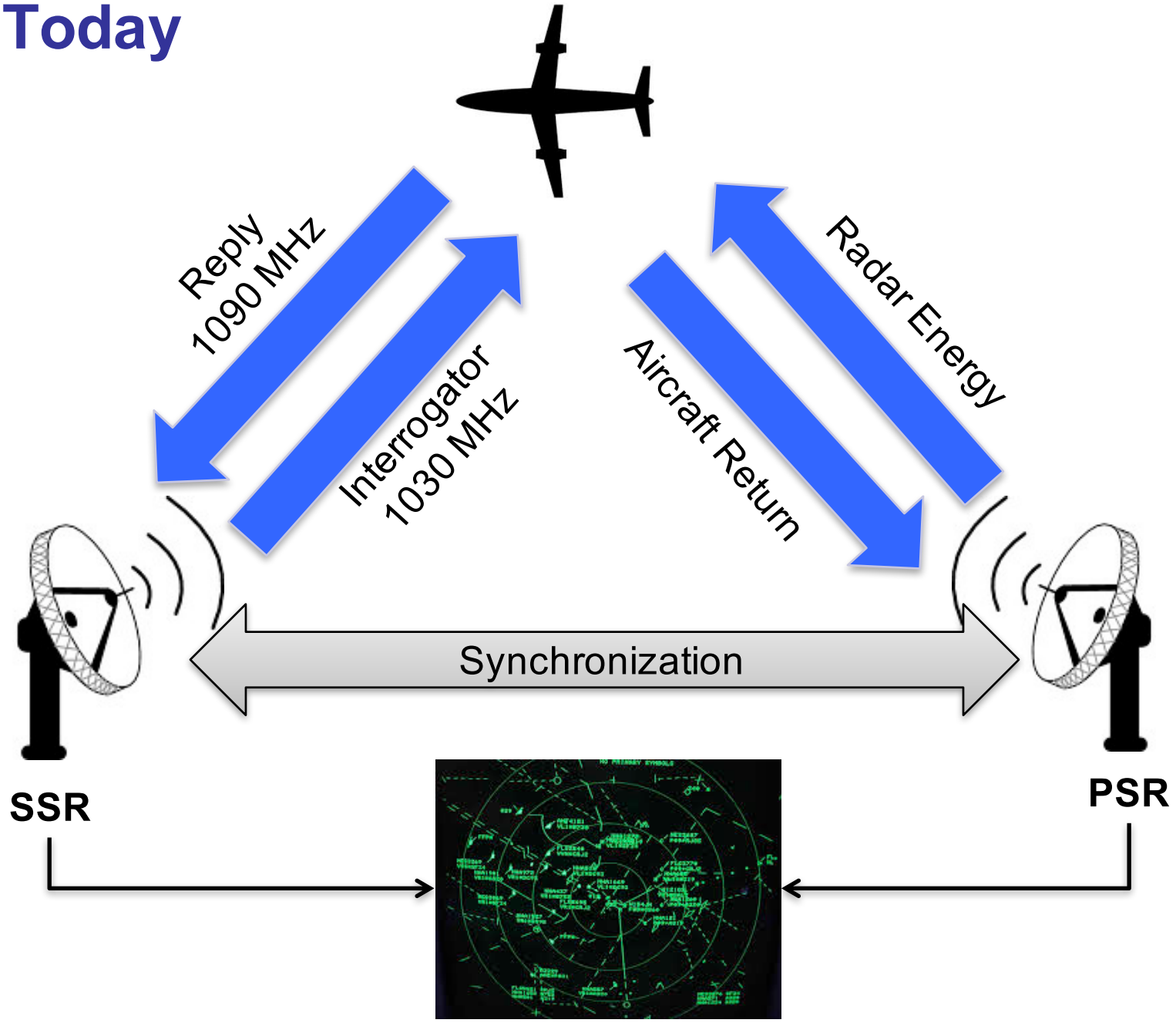
- Secondary Surveillance Radar (SSR)
  - Inspired by Identify Friend or Foe (IFF) during WWII
  - Transponder-based interrogation
  - Mode A: identification code only
  - Mode C: identification code and barometric altitude
  - Mode S: *selective* addressing to interrogate just one aircraft
  - Mode S is used in **Traffic Alert and Collision Avoidance System**

→ Dependent Surveillance

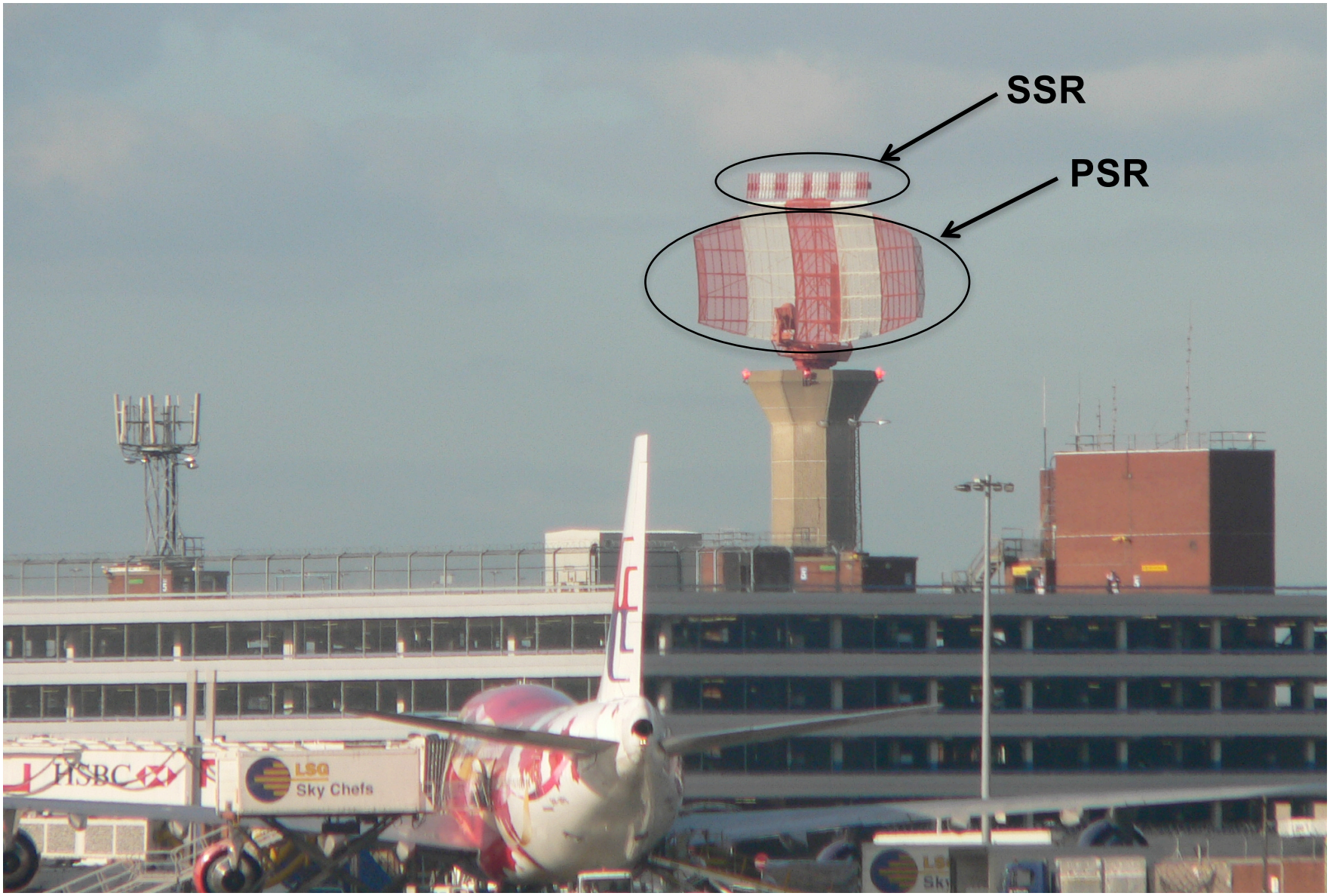


Mode S*: ground-air-ground data link*
(56 bit or 112 bit frames)

ATC Today


Reply
1090 MHz
Interrogator
1030 MHz
Aircraft Return
Radar Energy
Synchronization
SSR
PSR

PSR and SSR (London Heathrow)



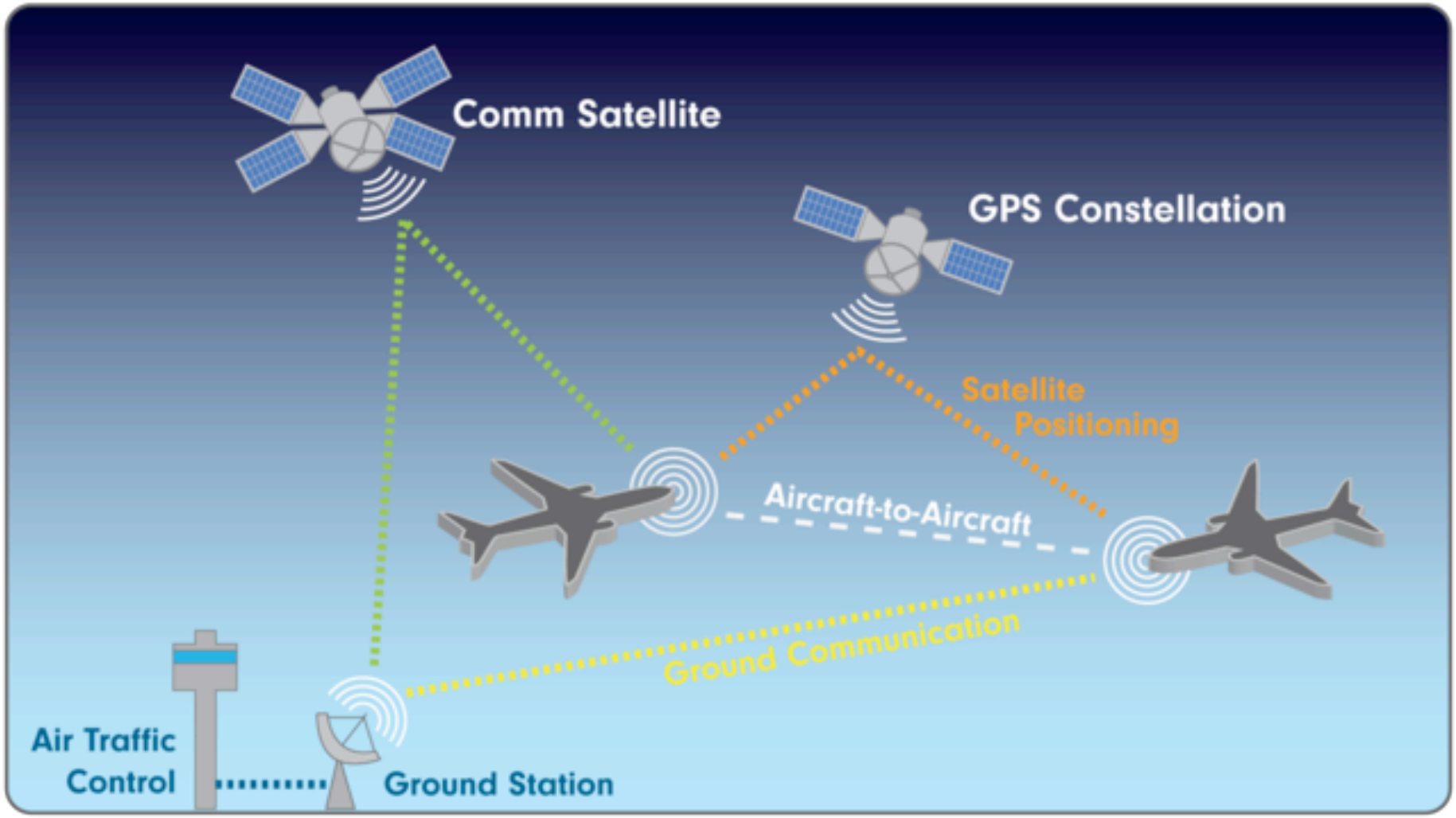
Problems of Today's ATC

- Enormous cost of operation; insufficient accuracy
- PSR
  - Does not provide identity
  - Often reports false targets
  - High transmission power required for long-range performance
  - Expensive to install and maintain
- SSR
  - Can sometimes report false targets or position (reflections, multipath)
  - Systems are expensive to install and maintain
  - Systems require optimum site with unobstructed view to aircraft

→ **Large separation minima is required**
→ **Complex collision avoidance**

Air Traffic Management of Tomorrow

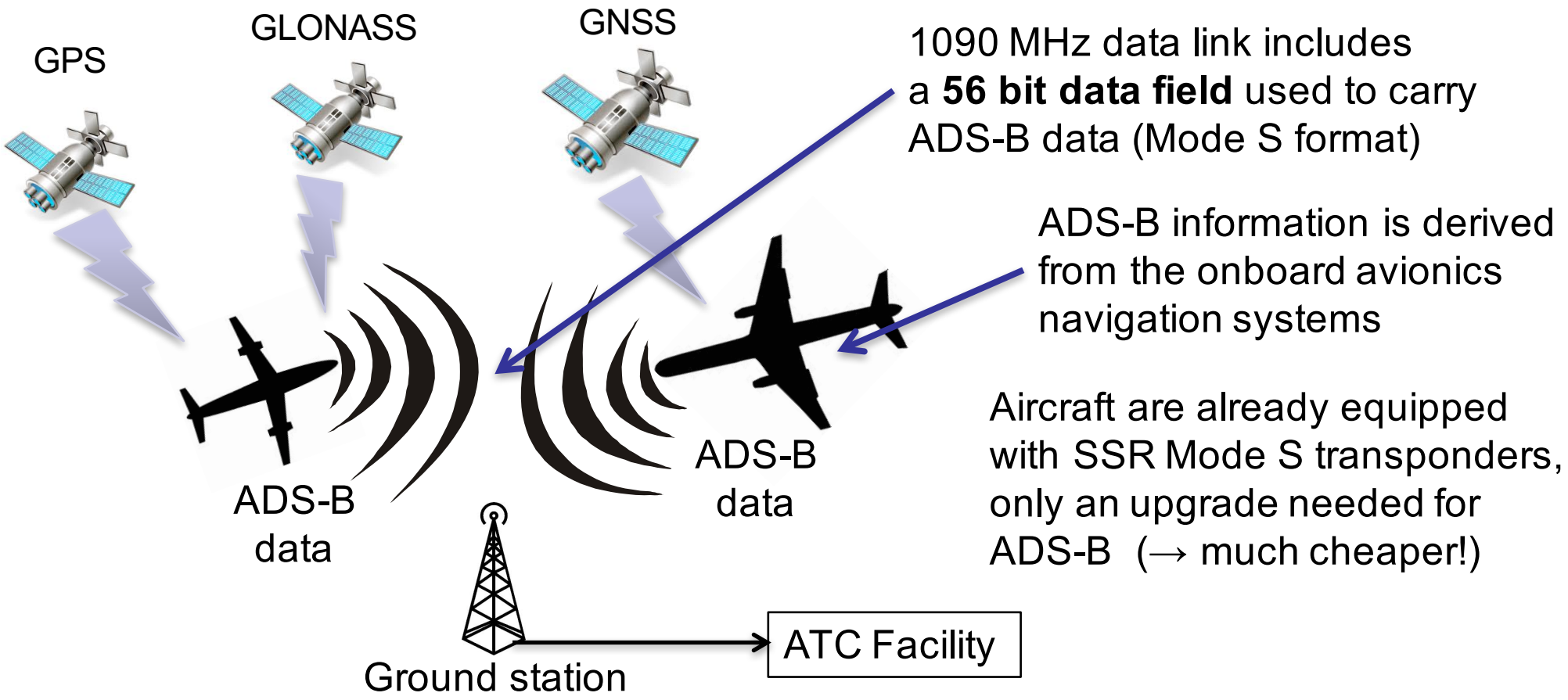
- Main objectives: higher accuracy and cost-efficiency



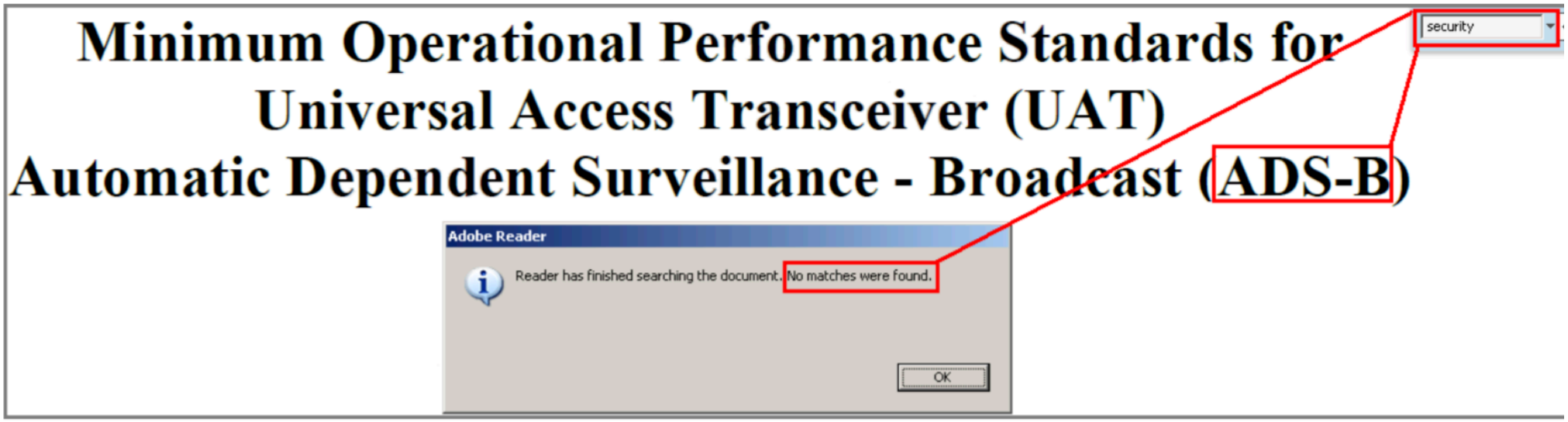
Source: www.airfactsjournal.com

ADS-B

Automatic: Always on (no explicit interrogation necessary)
Dependent: On-board system provides surveillance information to other parties
Surveillance: Provides precise position, altitude, speed, heading, identification,…
Broadcast: Sent to any aircraft or ground station equipped to receive the data



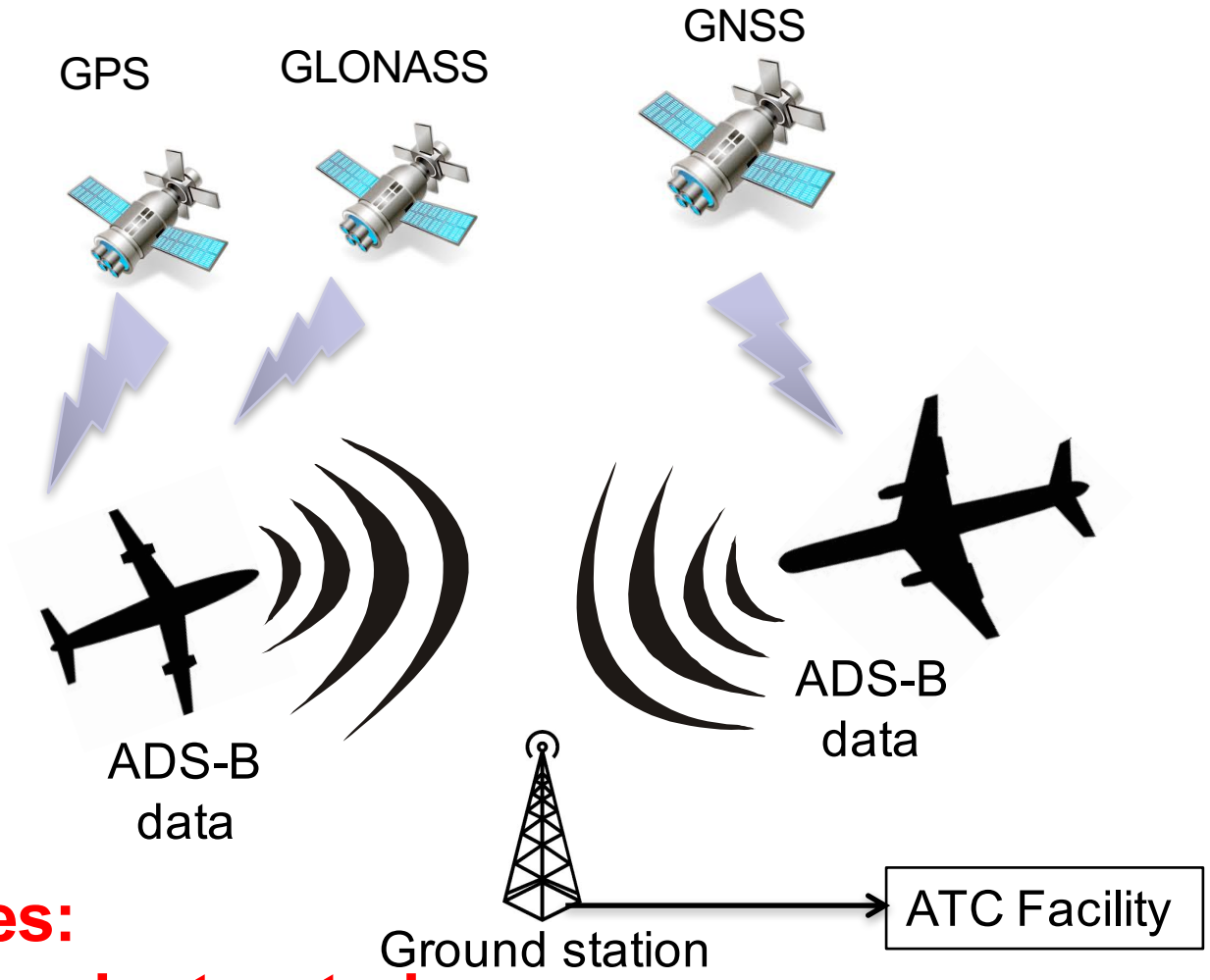
SECURITY OF ATC



Credit: A. Costin

Adversary meets ADS-B

No authentication.
No authorization.
No confidentiality.
No integrity.

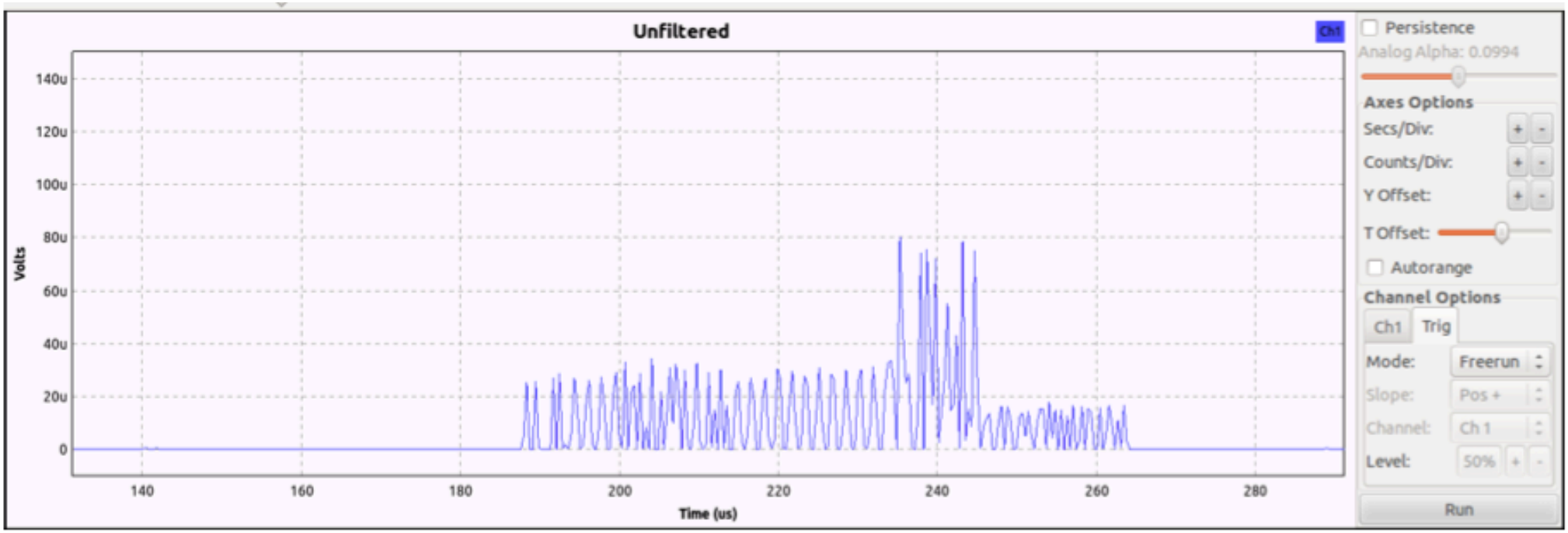


ADS-B system assumes:
- Received GPS data can be trusted
- Data broadcast over 1090ES data link can be trusted

PASSIVE THREATS?

Eavesdropping on ADS-B Data

- Receiving **raw** ADS-B data is easy
  - ADS-B uses Mode S
  - Mode S: Pulse Position Modulation
  - Software Defined Radio (GNU Radio) implementation of Mode S receiver exists (credit: Nick Foster)
    - https://github.com/bistromath/gr-air-modes



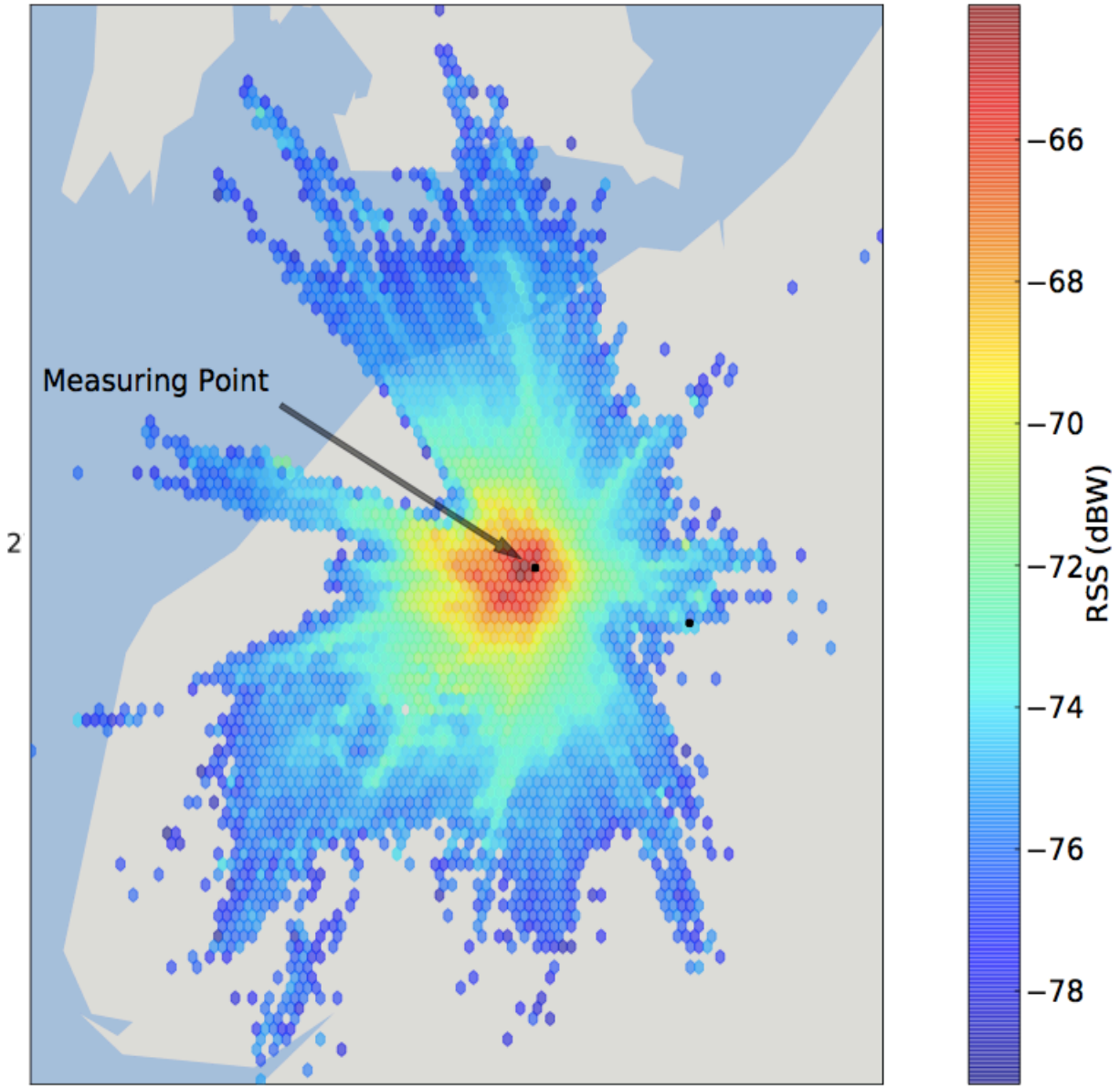
Receiving ADS-B Data using COTS Hardware

- Many cheap Mode-S/ADS-B receivers available

  (btw, DVB-T USB stick for 30$ works, too!)

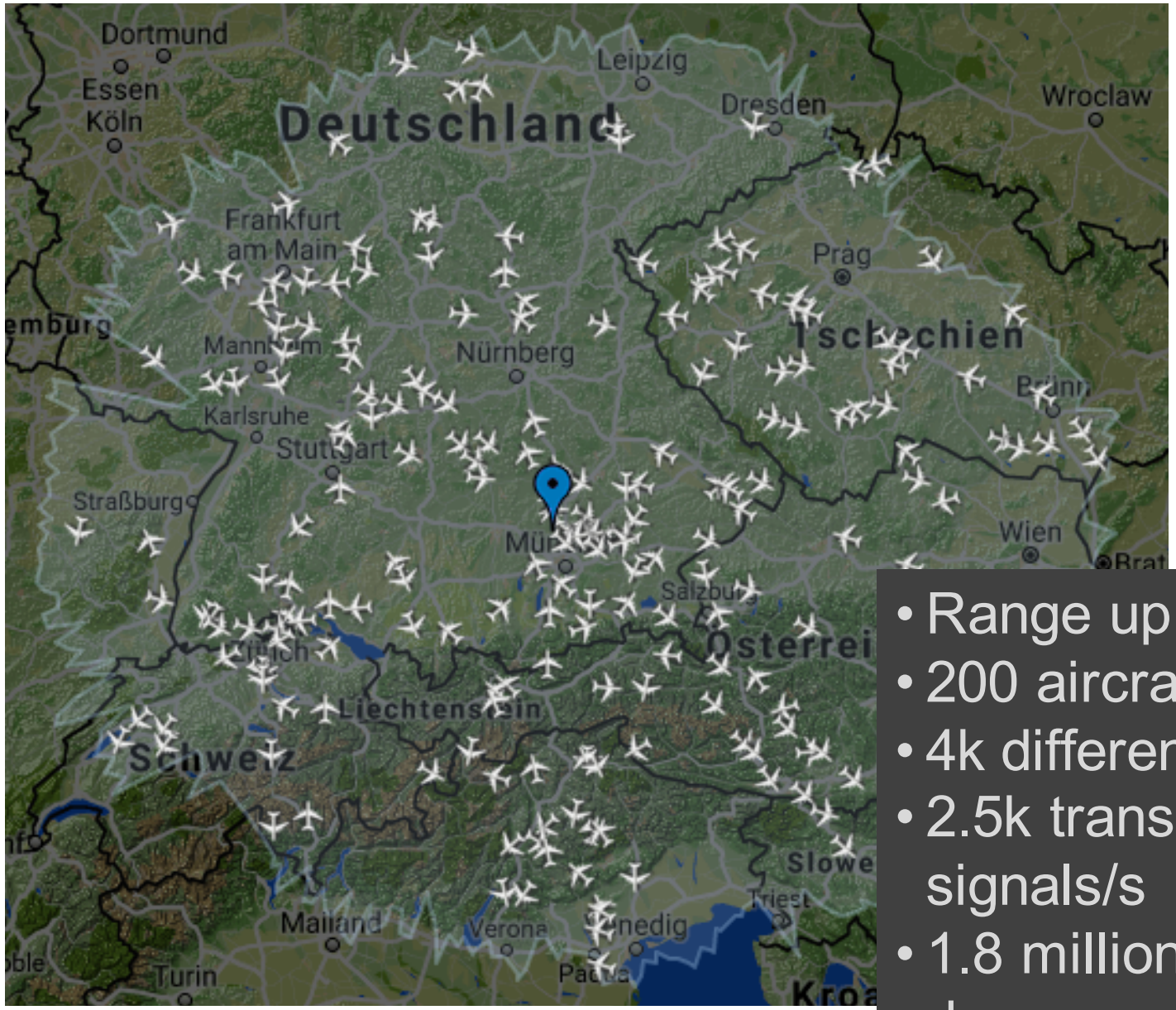
Receiving ADS-B data using USRP/GNURadio

- *Home-made* Receiver
  - USRP N210
  - SBX daughterboard
  - Kinetic Avionic MD1105 antenna (1090 MHz)



- Bit-error detection
- Preamble
- RSS
- SNR
- other PHY-data

OpenSky: Receiver View



- Range up to 600 km
- 200 aircraft at a time
- 4k different aircraft/day
- 2.5k transponder signals/s
- 1.8 million signals per day

Eavesdropping on ADS-B transmissions

Raw ADS-B data (real-time):

- Call sign
- ICAO ID
- Position
- Altitude
- Heading
- Speed
- Climbing rate

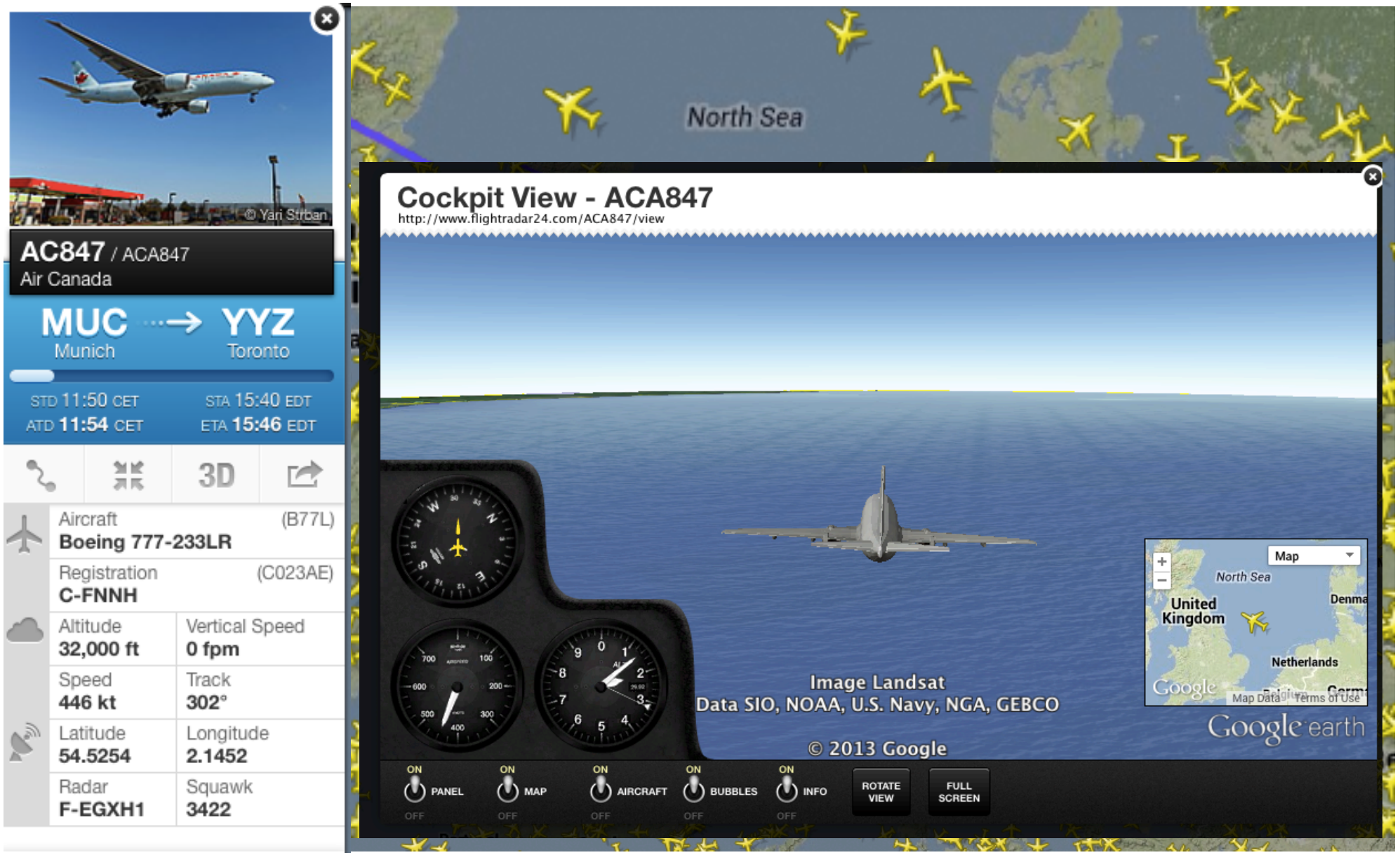
Publicly available data:

- Flight No.
- Owner
- Start position
- Destination
- Scheduled arrival
- Aircraft Model
- Engine

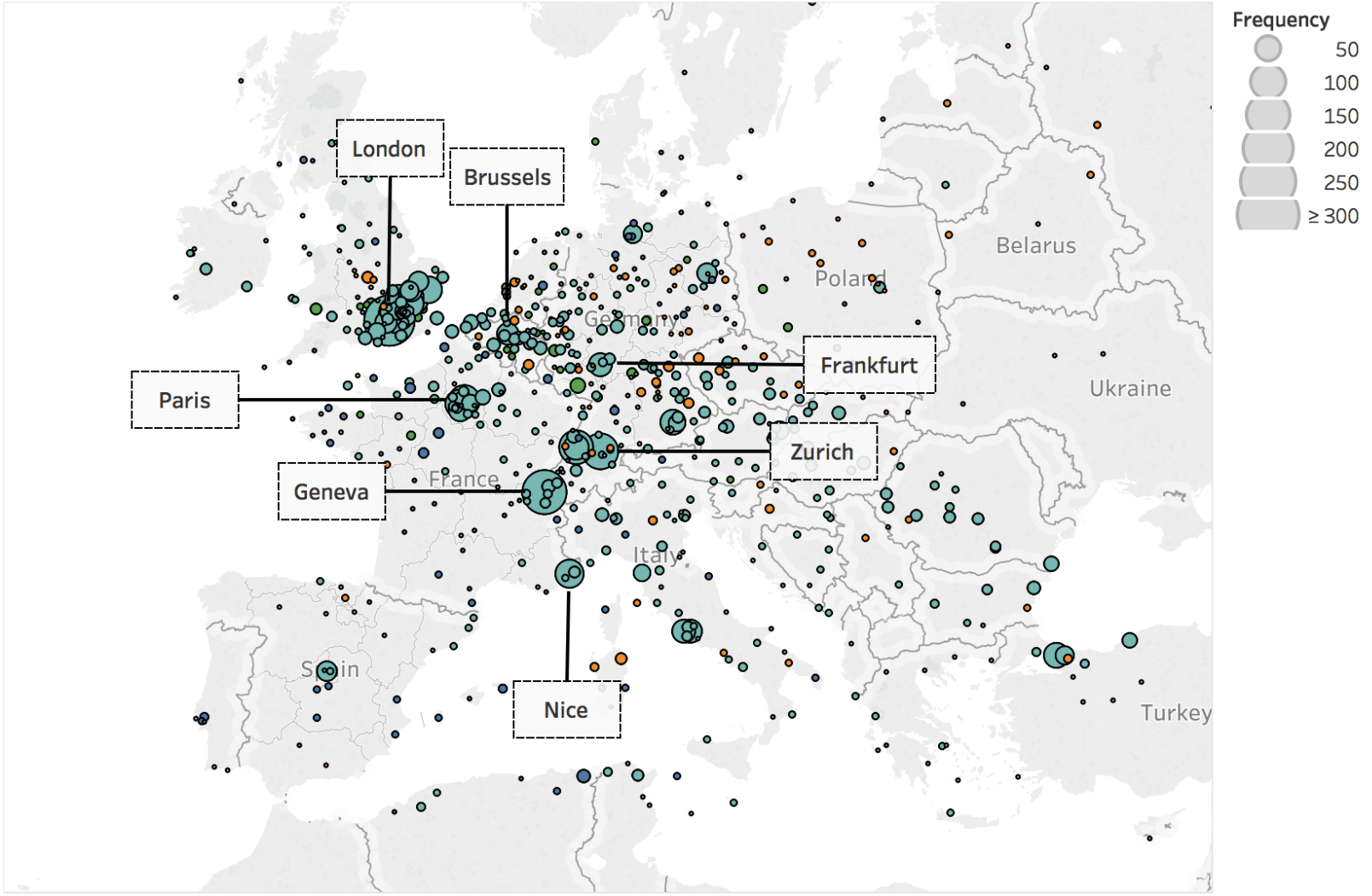
EUROCONTROL

FEDERAL AVIATION ADMINISTRATION

Receiving ADS-B Data: Feature or Flaw?



Privacy leakage from air-traffic?



The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication. Martin Strohmeier, Matthew Smith, Vincent Lenders and Ivan Martinovic. *In IEEE European Symposium on Security and Privacy (EuroS&P) 2018.* IEEE. April, 2018.

ACARS Messages (encrypted)

	Txt	Registration
1	06cE5gC7M) g.9DgggC)f7. .7L??D7os437g(`7g:).7...C7hhhhh	D-AERO
2	09|\L46c+BhhNBo444BZ4ch8hcGeeocPr!(c4shZc41B,c888Bcbbbbb	D-AERO
3	09|\L46c+BhB41o448hN6c644cGeeocPr!(c4shZc4Z48c888,cbbbbb	D-AERO
4	05JO4jd)]C9jo9Xjjjj`B)joe)w)w)j`9B)jBu`)jBCu)jjd7C	D-AFUN
5	03m0>xJqLDt-J9fxxxDx(qx9xq#q#qxP(VqttDPqtJJ(qxxP$-	D-AFUN
6	08msWL}ZqvY`KY~LLL}KcZLacZ=yy~Z=yP\ZLK}LZYLeeZYLvLZLYL[K	D-AJET
7	08,suL}ZqvY``}~LLL`t}ZLKLZ=yy~Z=yP\ZLK}LZYLe`ZYLvLZLYL[}	D-AJET
8	09|\L46c+B4B1so444N,4c4ZNcGe-Wc-GrPc4s64c8hhNc8N8Zc44Z5h	D-AJET
9	08,suL}ZqvL}`c~LLLeYvZYc`Z=yP\ZP=|0ZLK}LZYeetZY`YtZLLc[K	D-AJET
10	06cE5gC7M9`9(:Dggg)C97C9g7aLso7L??D7g(Cg7.`g:7.`C:7gg),C	D-AJET
11	09|\L46c+B4hs6o444BBhchBNc-GrPcGeeoc4s64c8Z86c8Z61c44B58	D-AJET
12	03m0>xJqL-VJt-fxx(t9-q-txq.T+lq!1mlqxPJtqxetDqxe-Pqxx9$9	N415QS
13	03m0>xJqLDt-DVfxxxxDeqtJPq!Odbq+oofqxPJtqxV-DqxVDeq#####	D-AERO
14	03m0>xJqLDtJee+xxxJD-qt9Jq#q#qxPJtqtt-tqtJJxq#####	D-AERO
15	02N;E,0lrQ---9/,,3-])l,),lvE<hlXO::l,A,3l30-]l300ml,,mT3	CS-DKF
16	02Xe|,0lrQ3m99/,,0-]]lm0,lvk1ilXkrrl,A,3l3Q,)l3QQml(((((	N719SH
17	03m0>xJqLDtDJ(fxx-xPtq-Jxq!Odbq+OLLqx9xtqtDtJqtDDDq#####	N719SH
18	021244 EGLL KMSP6 112701 853350	N827MH

Bad crypto in aviation systems

Key identifier

```
07*?X.0)Emk.;M].;4;Dm)m..) Y(*)]s($).M4U).U;;).MmD)..D+0
07*?X.0)EmUmkm]..D00M)4k.)]rr6) Y-\).k.<);4<k);000).;;+U
07*?X.0)EmUmUU]..D0Mk)m;.)]E{-) 6-r).k.;);;;;);4;;)..U+.
```

- ACARS encryption using a weak substitution cipher broken in minutes.
- Used by a wide range of private, military and government aircraft.

Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS, in *Financial Cryptography and Data Security 2017.*

Eavesdropping on Data Links: Medical Issues

Passenger

Status of unwell passengers reported to the ground to request assistance

RE PAX SALLY SHE
IT
FEELING A LITTLE
BETTER
NO FURTHER
ASSISTANCE
NEEDED.THANKS

PAX SALLY
HAS COLLAPSED
AGAIN
HAVE DECLARED
MEDICAL
EMERGENCY

Departure & arrival airports

Detailed treatment information passed on to medical staff on the ground

/EGKK KHOU 21 104017
NO MEDLINK.
PAX TOM 27A HAS LEUKEMIA. GIVEN 2
PUFFS OF INHALER. 325MG ASPIRIN. ON
DRIP FOR REHYDRATION. APPEARS TO
HAVE CHEST INFECTION. BP STAB

Eavesdropping on Data Links: Possessions at Risk

Forgotten belongings, including hotel name, room number and specific items

DEAR CCO COULD U PLS
ADVSE CAPT PAUL
TO RECOVER PASSPORT AND PERSONL
BELONGING LEFT
THAT CAPT JOHN LEFT IN ROOM 522
HOTEL WESTIN WASHINGTON DULLES
AIRPORT

Credit card details, sufficient to make a card-not-present transaction

FR2200
PLS VERIFY CREDIT
CARD:
MASTERCARD
1234 5678 1234 5678 EXP
10/20
USD 552

Card type

Card number & expiry date

Our work on privacy in ATC

Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS). Accepted for publication at PETS. Feb. 1 2018. Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders and Ivan Martinovic.

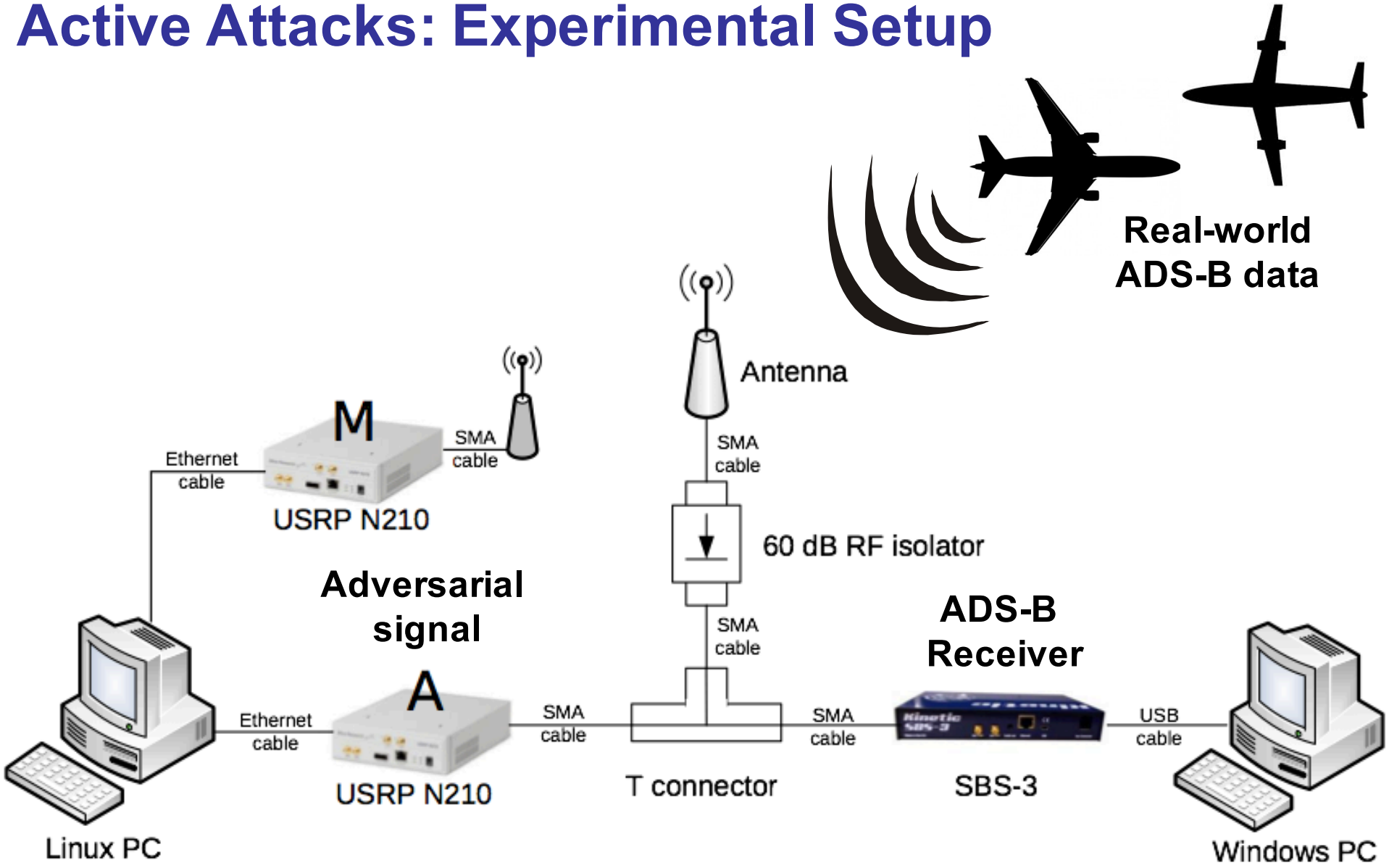
Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS, Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders and Ivan Martinovic. *International Conference on Financial Cryptography and Data Security 2017*. April, 2017.

On Perception and Reality in Wireless Air Traffic Communications Security, Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. In IEEE Transactions on Intelligent Transportation Systems. June, 2017.

On the Security and Privacy of ACARS. Matt Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. *Integrated Communications Navigation and Surveillance (ICNS)*. 2016.

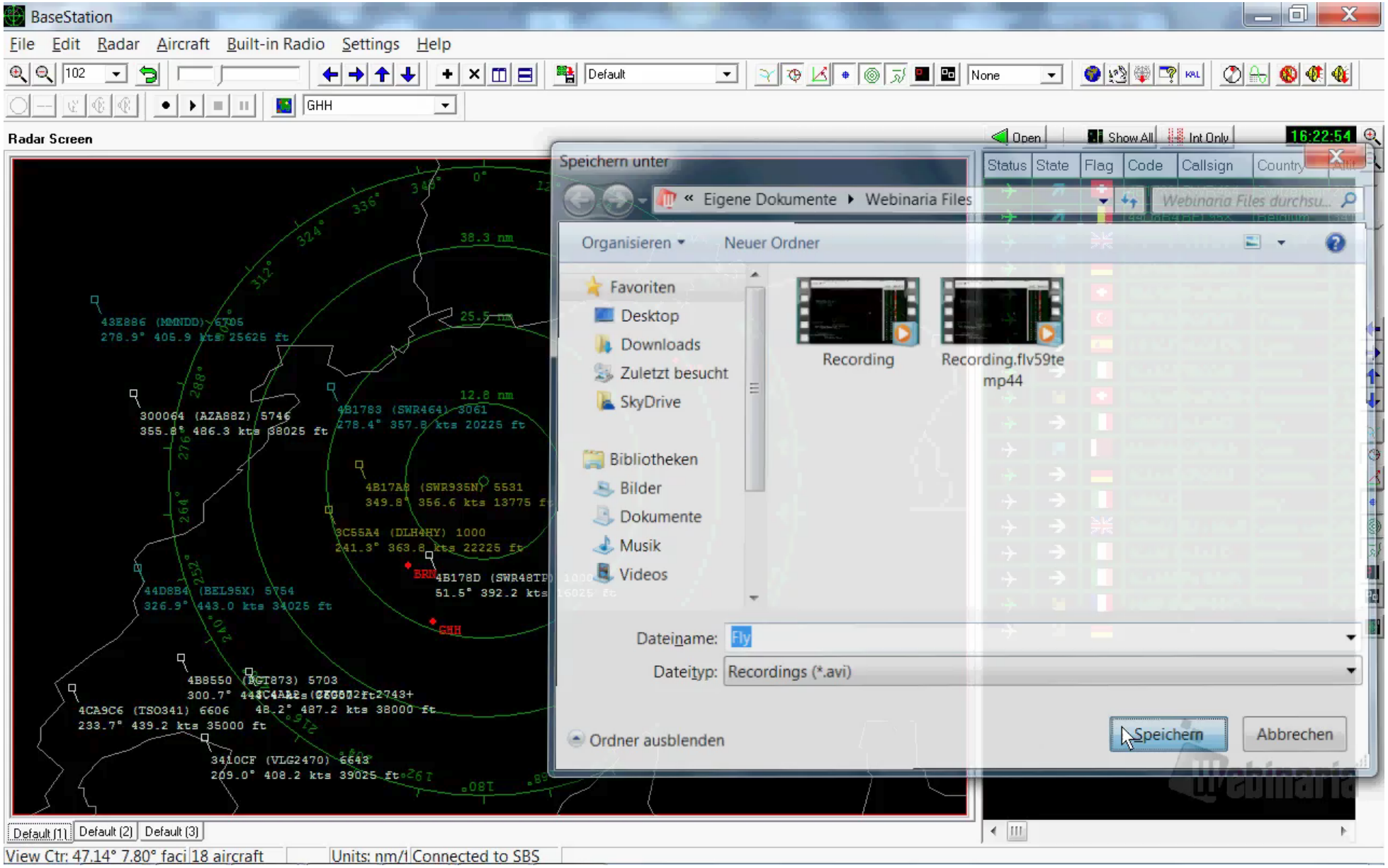
ACTIVE THREATS?

Active Attacks: Experimental Setup

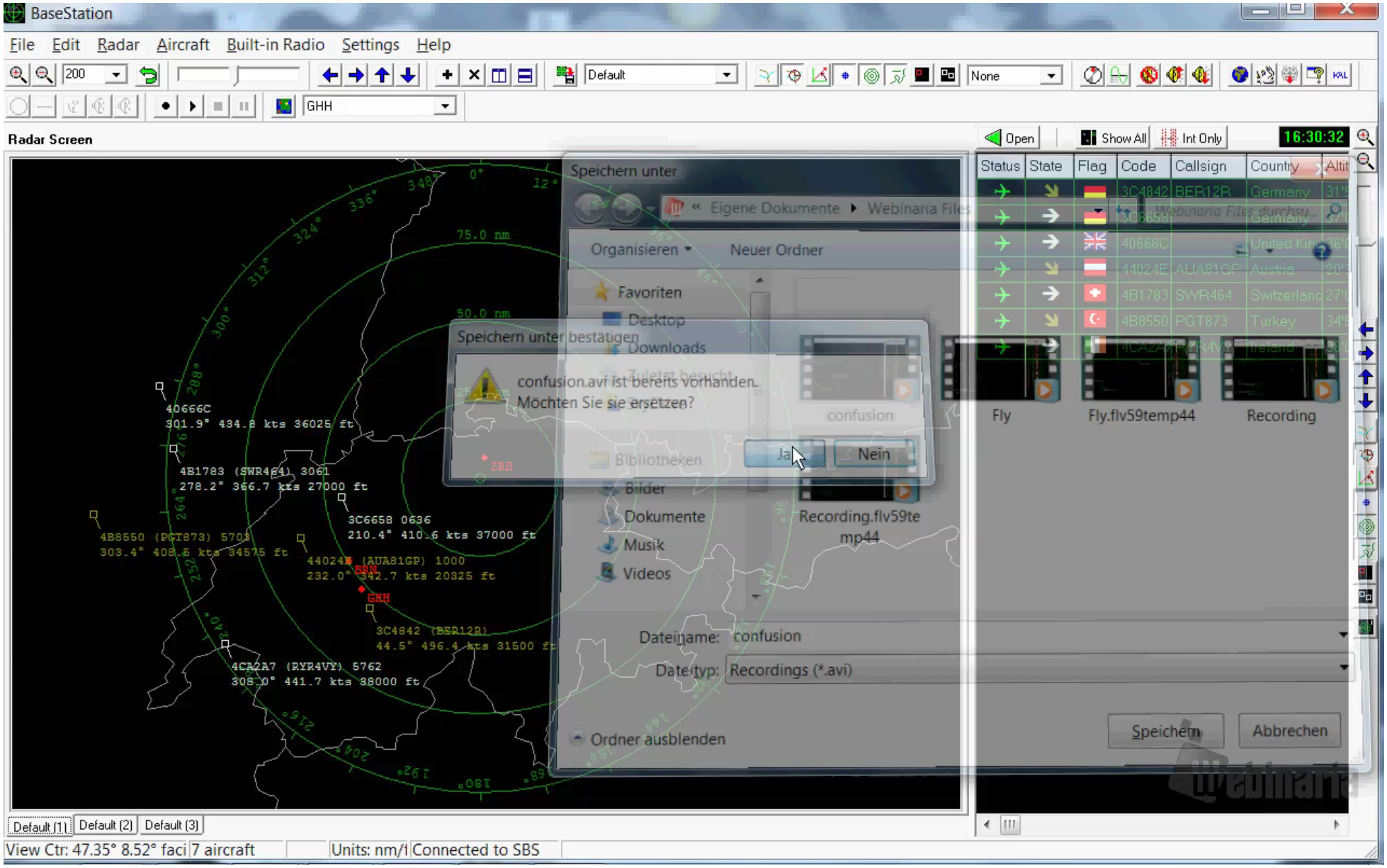


***Experimental Analysis of Attacks on Next Generation Air Traffic Communication*.**
M. Schaefer, V. Lenders and I. Martinovic. ACNS 2013.

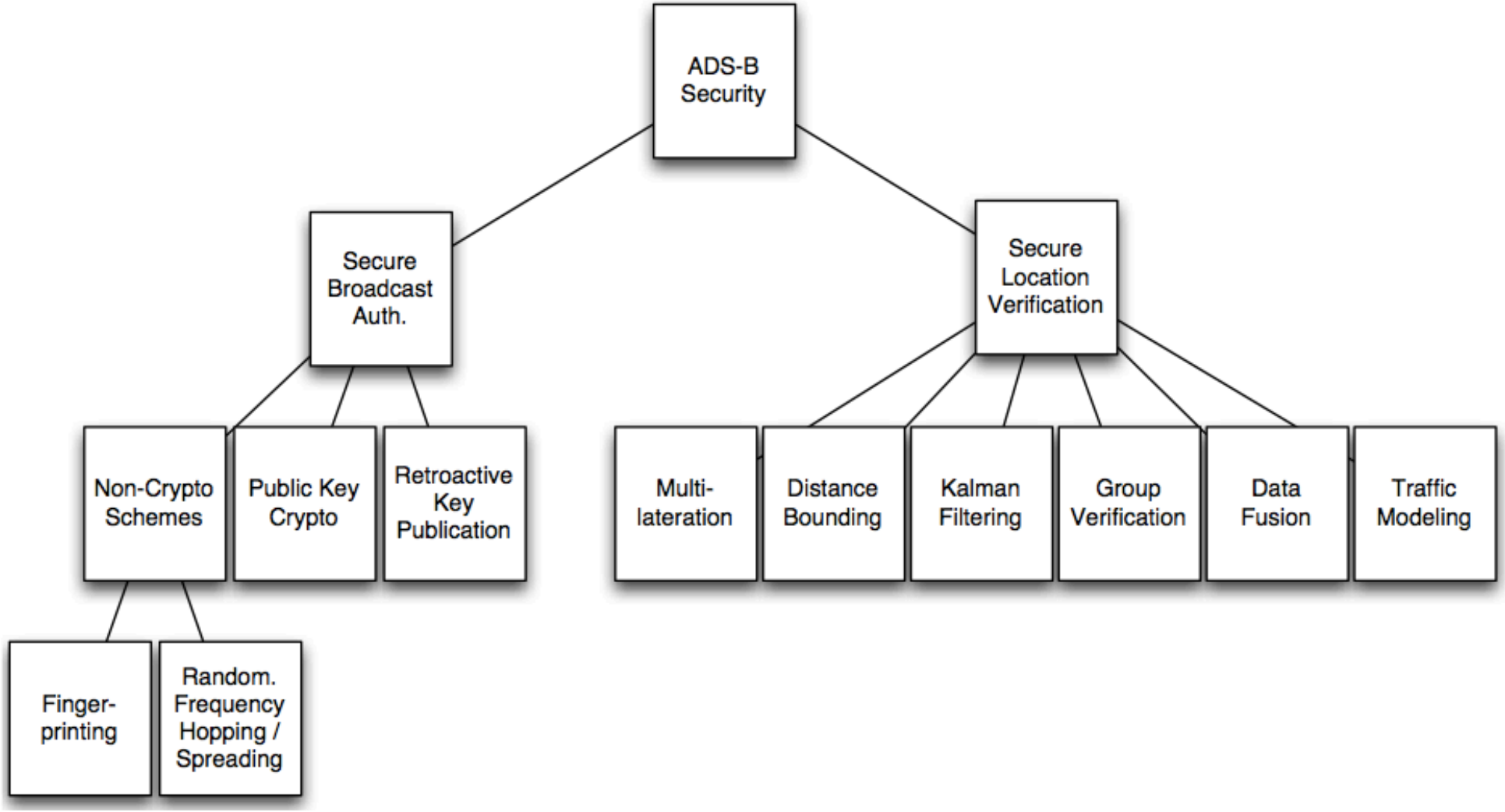
Demo – Ghost Aircraft Injection Attack



Demo – Ghost Aircraft Flooding Attack



Solutions?



- ***On the Security of the Automatic Dependent Surveillance – Broadcast Protocol*. M. Strohmeier, V. Lenders and I. Martinovic. *IEEE Communications Surveys & Tutorials. 2016.***

Security (research/hacker) community

News

Hackers say coming air traffic control system lets them hijack planes

FAA says it can spot hacking attempts, but won't allow independent 'stress tests'

By Taylor Armerding, CSO
January 11, 2013 08:12 AM ET

Add a comment Print Share 23 +1 Like 143 More

CSO - An ongoing multibillion-dollar overhaul of the natio
system is designed to make commercial aviation more efi
friendly and safer by 2025.

Sleeping air traffic controllers get federal wakeup

But some white-hat hackers are questioning the safety pa
Transportation System (NextGen) will rely on Global Posi
of radar. And so far, several hackers have said they were
capability to hijack aircraft by spoofing their GPS components.

Researcher: New air traffic control system is hackable

By **Heather Kelly**, CNN
July 26, 2012 -- Updated 2249 GMT (0649 HKT) | Filed under: **Web**

Air Traffic Control of the Future Is (Still) Incredibly Hackable

WIRED

Defcon Researchers Build Tool To Track the Planes of the Rich and Famous

5. Researcher demonstra
traffic control system

In another Black Hat presentation, Andrei Cos

Air Traffic Controllers Pick the Wrong Week to Quit Using Radar

CNN

Hacker Shows Air Traffic Control Danger With 'Ghost Planes'

Posted 09.26.2012 | **Travel**

Read More: Air Force One, Air Traffic Control, Faa, Travel News, Air Travel, Airlines, Hacking, Black Hat, Travel News

Andrei Costin, a Cypriad hacker, gave an unnerving demonstration outlining the weaknesses of air traffic control systems today at the Black Hat hackin...

Read Whole Story

SECURITY | 7/25/2012 @ 1:54PM | 17,036 views

Next-Gen Air Traffic Control Vulnerable To Hackers Spoofing Planes Out Of Thin Air

4 comments, 3 called-out + Comment Now + Follow Comments

Aviation Community Responses

THE SKY IS CALLING, NOT FALLING

Tim Taylor talks about the disturb
as if the ongoing roll-out of ADS-I
peril. He recommends:

Indeed, the FAA expounded on a larger concern–the number of functions that prudently should be contained in one box of avionics. Just as the value of real estate is based on the cliché, "location, location, location," air safety is built on the trinity of "redundancy, redundancy, redundancy." If TCAS

1) Relax, the situation is OK, bordering on "normal." – The FAA says it has procedures in place to prevent that, and that system security is integral to ADS-B technical specifications. At minimum the subject
engineering circles – by people who are
who have had more than a decade to co
over this.

- tons of redundancy

AINonline BIZAV AIR TRANSPORT DEFENSE

AIR TRANSPORT

Hackers, FAA Disagree Over ADS-B Vulnerability

by Matt Thurber - August 21, 2012, 4:15 PM

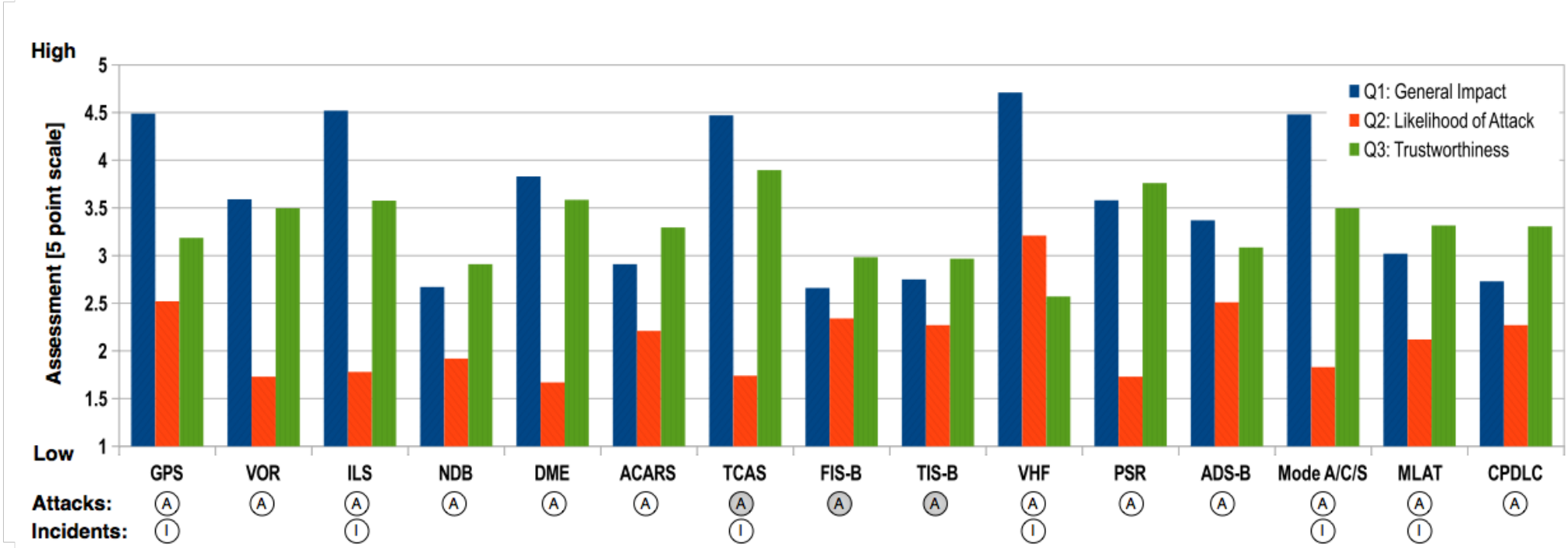
The FAA said that the ADS-B system is secure
displays. "An FAA ADS-B security action plan identified and mitigated risks and monitors the progress of
corrective action," an FAA spoke

FAA Denies Vulnerabilities In New Air Traffic Control System

Posted by **Soulskill** on Wednesday August 22, 2012 @05:23PM
from the what's-the-worst-that-could-happen dept.

A spokeswoman for key ADS-B
security certification and accredi
security features built in, including features to protect against...spoofing attacks. [This] is provided through multiple means of independent validation hat a target is where it is reported to be."

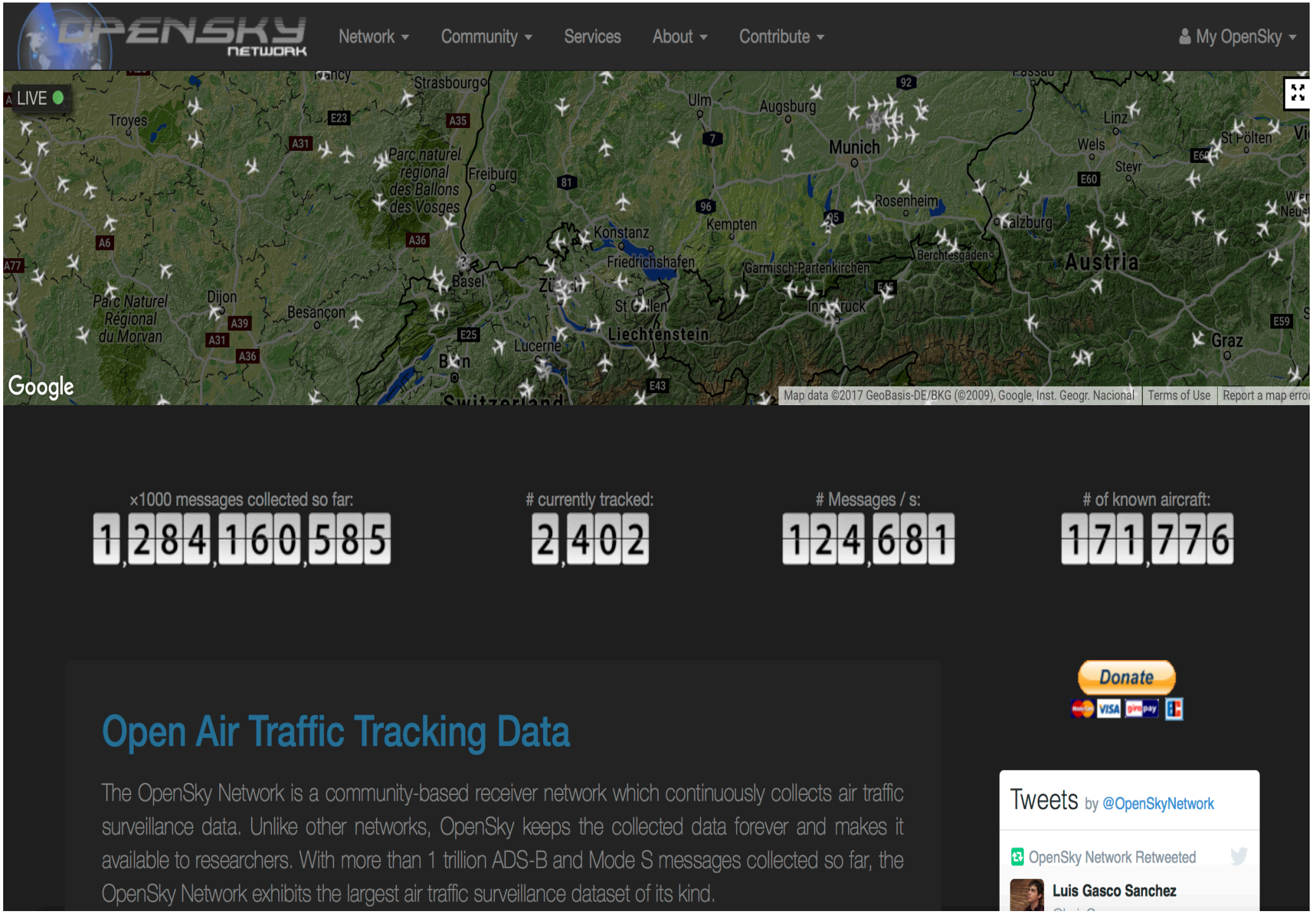
Aviation Expert Opinions – Survey, n=253



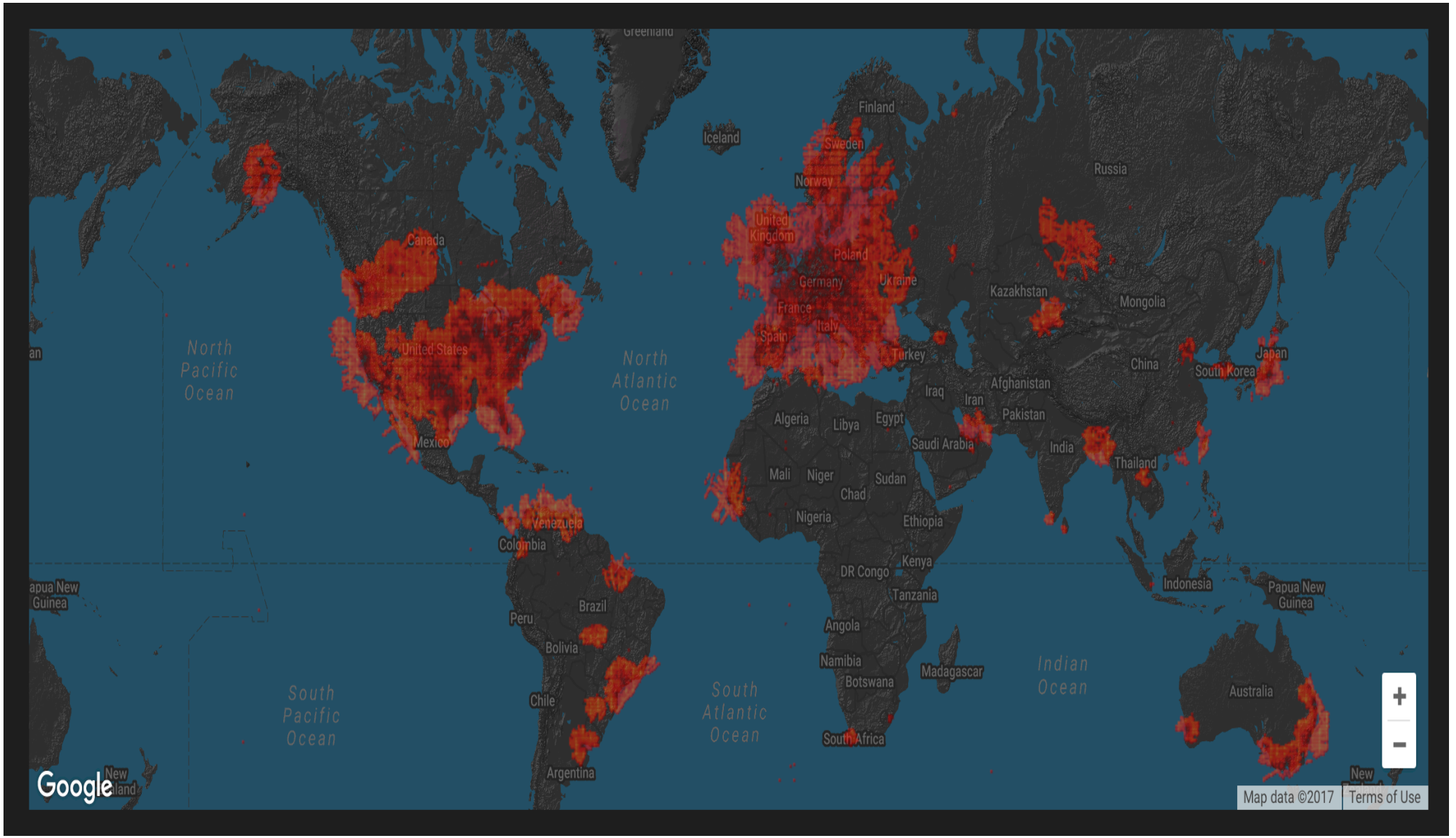
On Perception and Reality in Wireless Air Traffic Communications Security, by Strohmeier, Martin; Schäfer, Matthias; Pinheiro, Rui; Lenders, Vincent; Martinovic, Ivan. In IEEE Transactions on Intelligent Transportation Systems. 2016.

Attack Simulator: Cockpit Systems

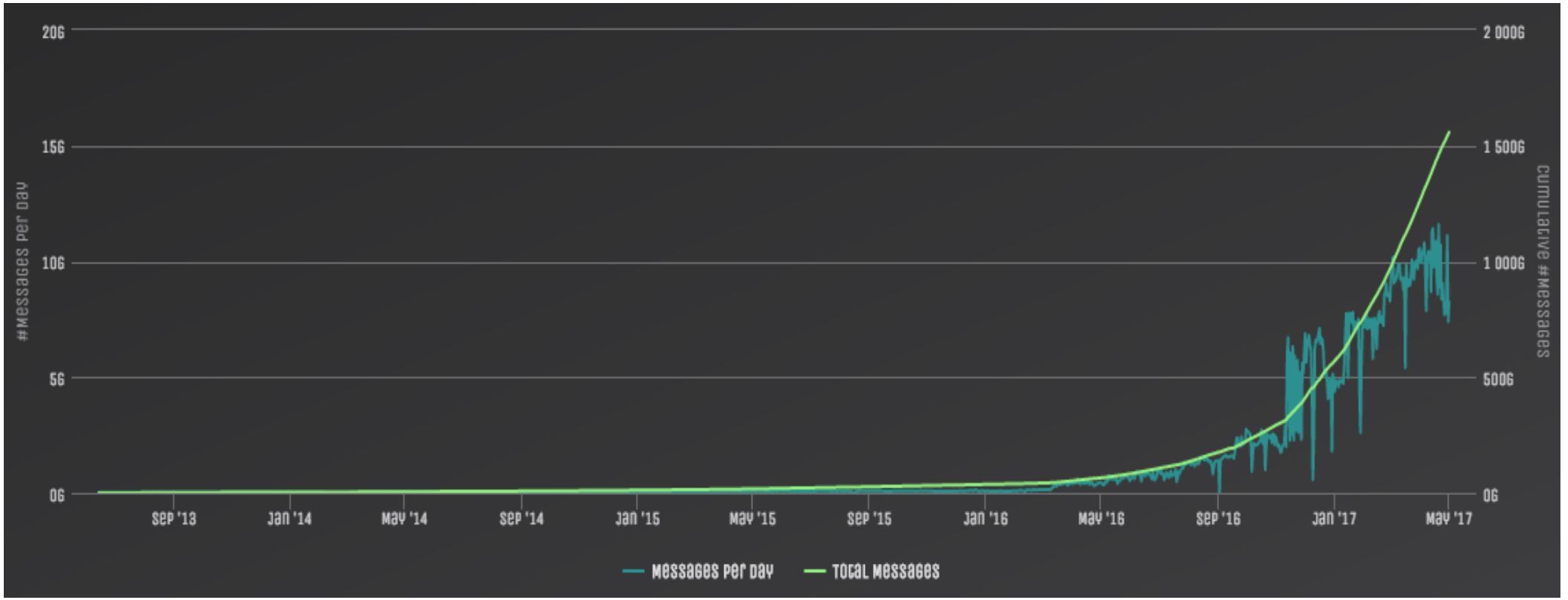
- X-Plane Flight Simulator
- Goal: Extending the simulator to include various attack


OPENSKY NETWORK
Network
Community
Services
About
Contribute
My OpenSky
LIVE
Strasbourg
Troyes
Ulm
Augsburg
Munich
Linz
Wels
Steyr
St Pölten
Freiburg
Parc naturel régional des Ballons des Vosges
Rosenheim
Kempten
Konstanz
Friedrichshafen
Salzburg
Berchtesgaden
Garmisch-Partenkirchen
Austria
Basel
Zürich
St Gallen
Innsbruck
Liechtenstein
Parc Naturel Régional du Morvan
Dijon
Besançon
Lucerne
Bern
Graz
Google
Map data ©2017 GeoBasis-DE/BKG (©2009), Google, Inst. Geogr. Nacional
Terms of Use
Report a map error
×1000 messages collected so far:
1,284,160,585
currently tracked:
2,402
Messages / s:
124,681
# of known aircraft:
171,776
Donate
Open Air Traffic Tracking Data
The OpenSky Network is a community-based receiver network which continuously collects air traffic surveillance data. Unlike other networks, OpenSky keeps the collected data forever and makes it available to researchers. With more than 1 trillion ADS-B and Mode S messages collected so far, the OpenSky Network exhibits the largest air traffic surveillance dataset of its kind.
Tweets by @OpenSkyNetwork
OpenSky Network Retweeted
Luis Gasco Sanchez

OPENSKY 2017



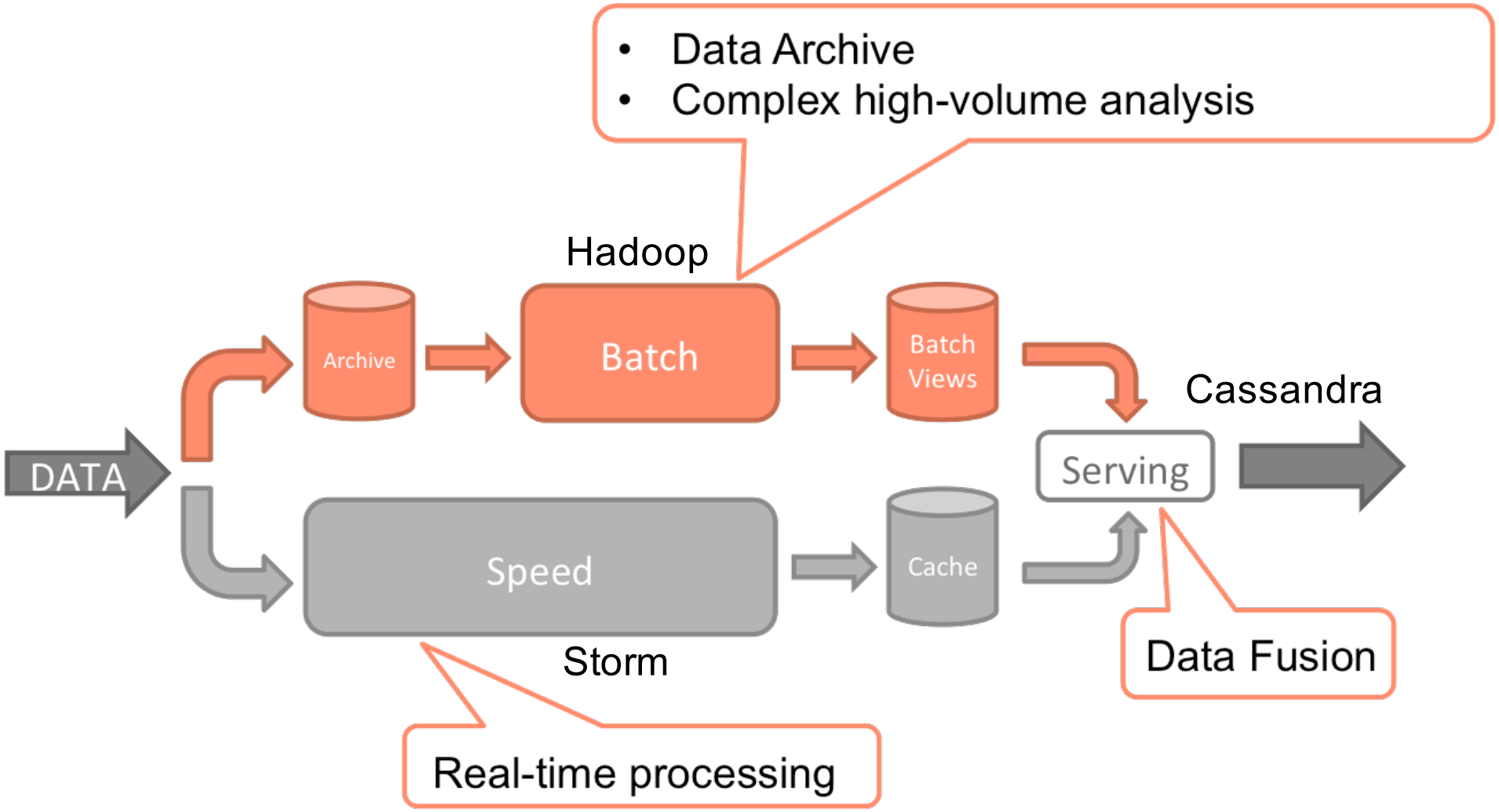
OpenSky's View (1)



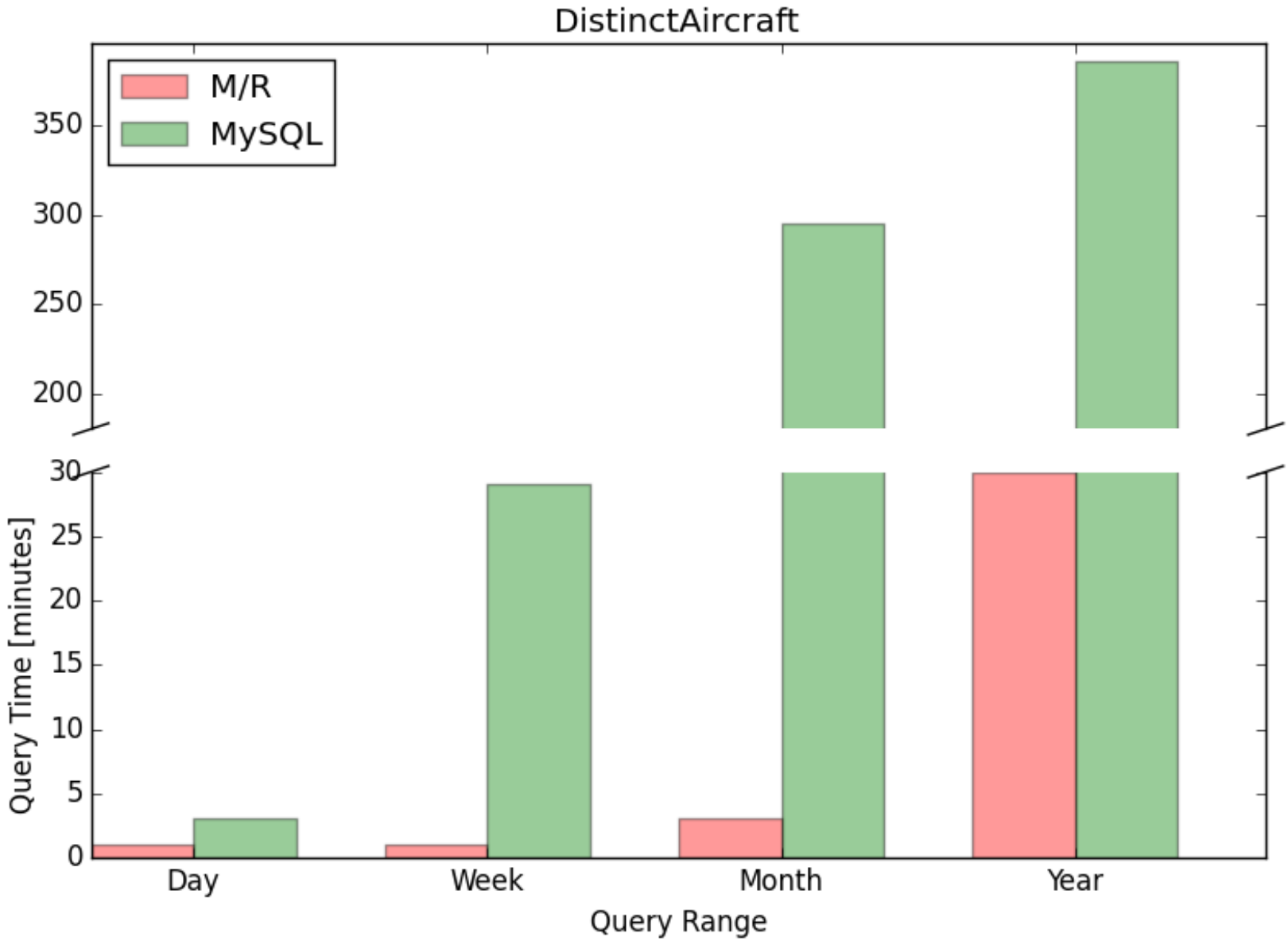
- 1.6 trillion messages since June 2013
- Currently ~10 billion signals per day
- Up to 4k aircraft at a time
- 200k transponder signals per second (peak)

OpenSky 2.0: The λ-Architecture

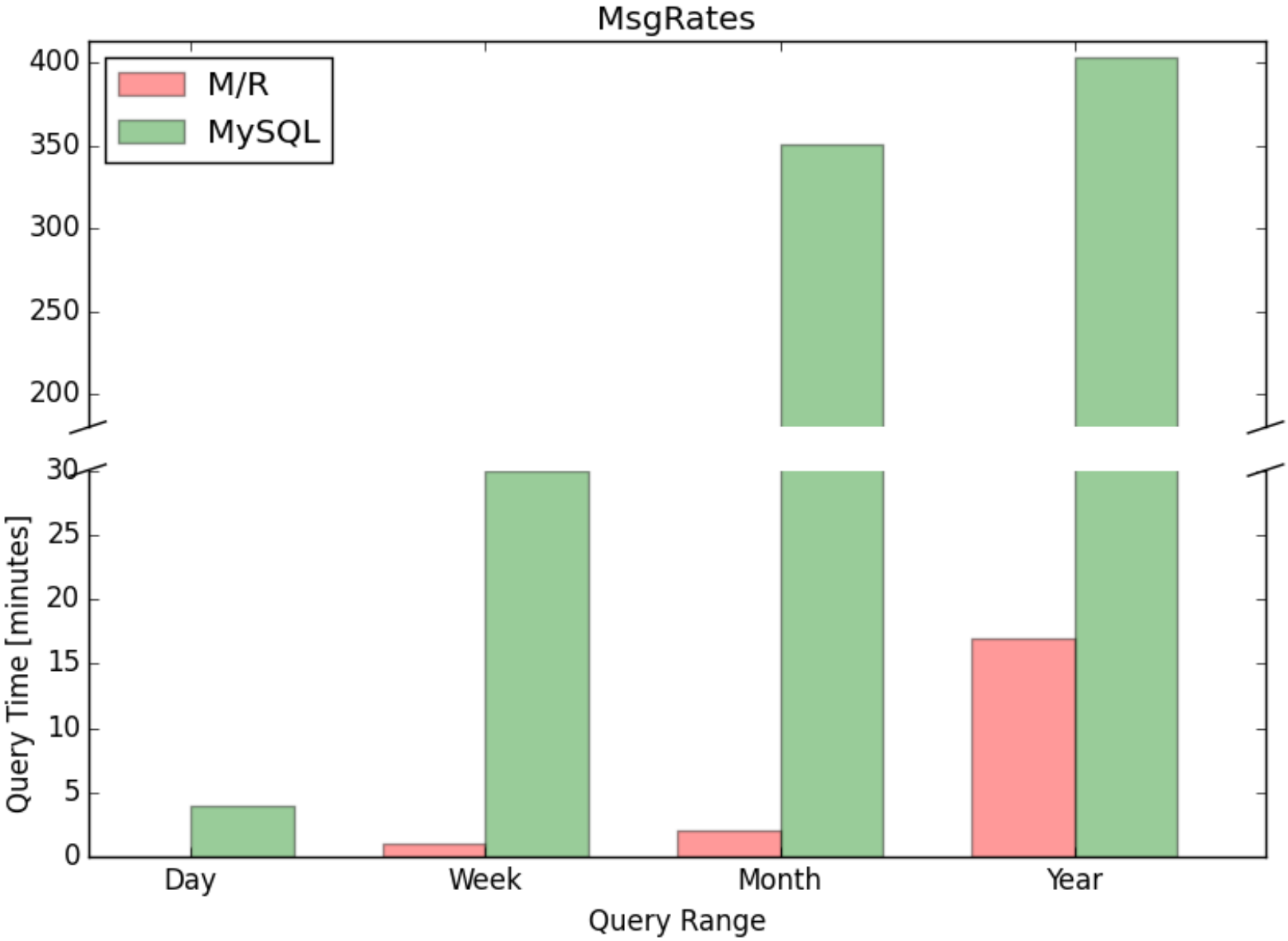
Proposed by Nathan Marz (2013))



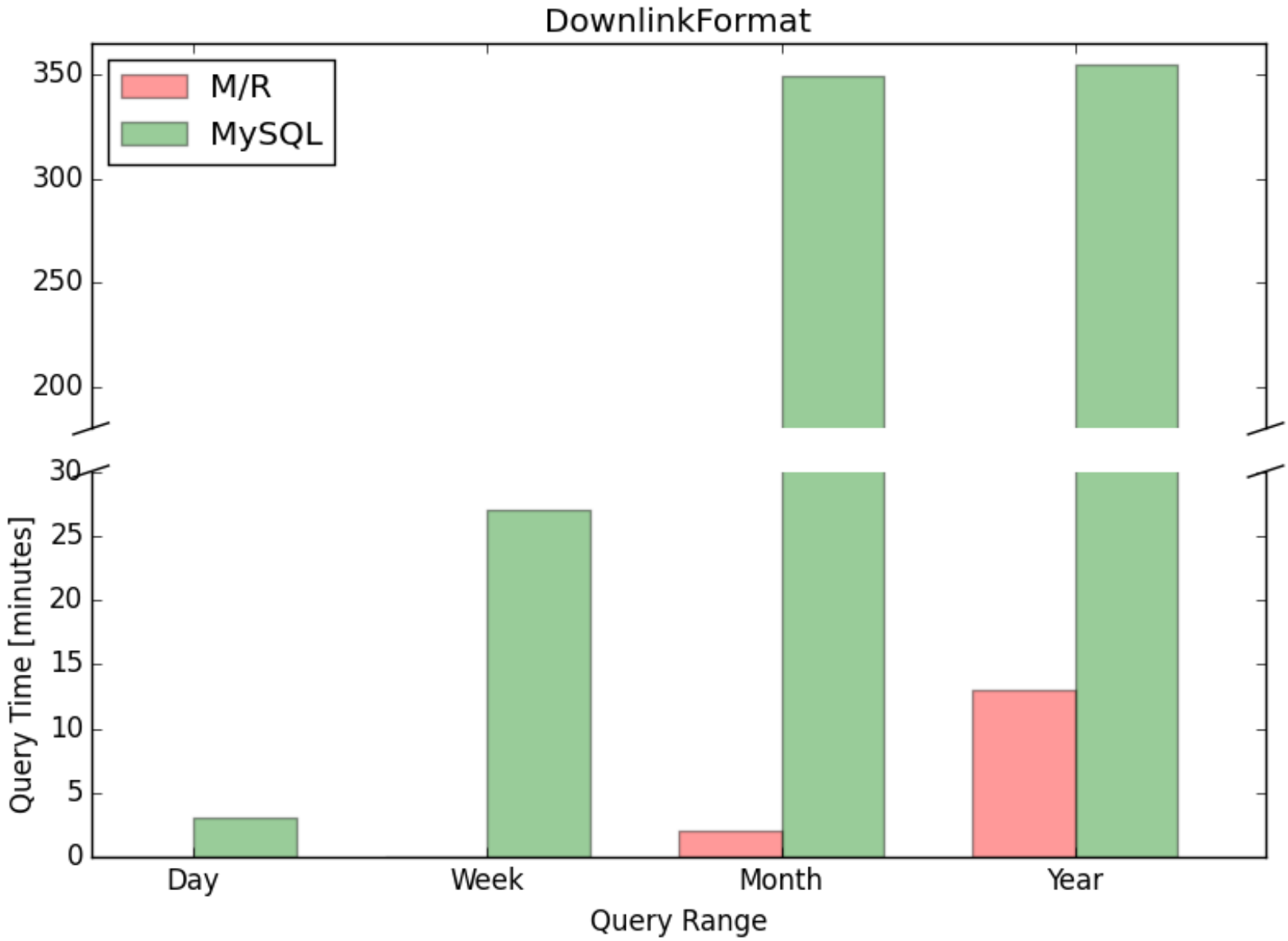
OpenSky: Query Performance (1)



OpenSky: Query Performance (2)

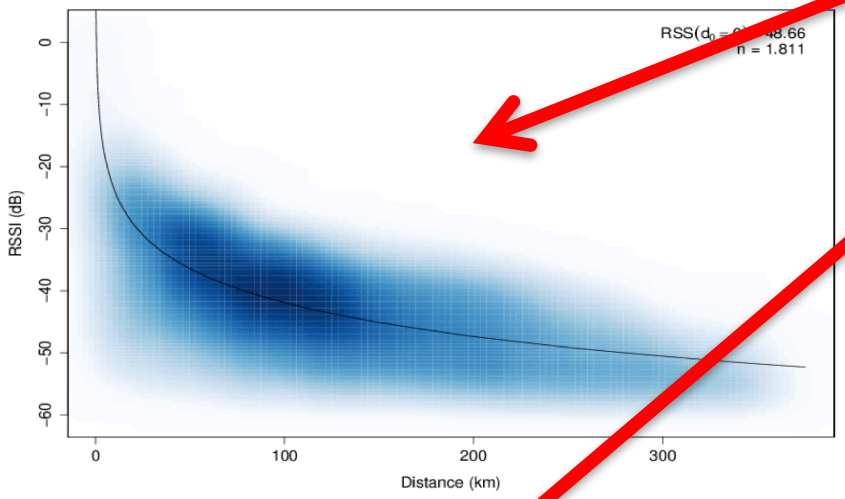


OpenSky: Query Performance (3)



OpenSky: Channel Analysis

Propagation Model



Log-distance Path Loss Model (LDPL)

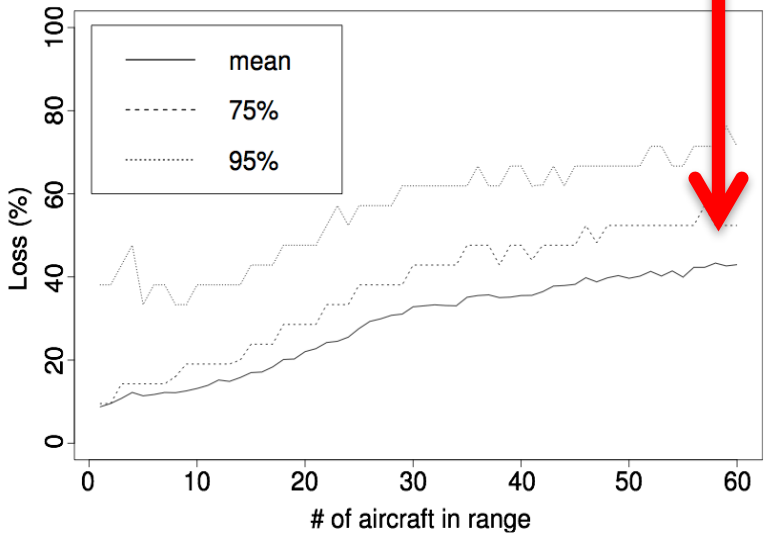
Doughnut effect: noticeable drop in reception quality of messages sent in close proximity to a receiver.

1090 MHz channel utilization is very high

60 aircraft → 40% message loss

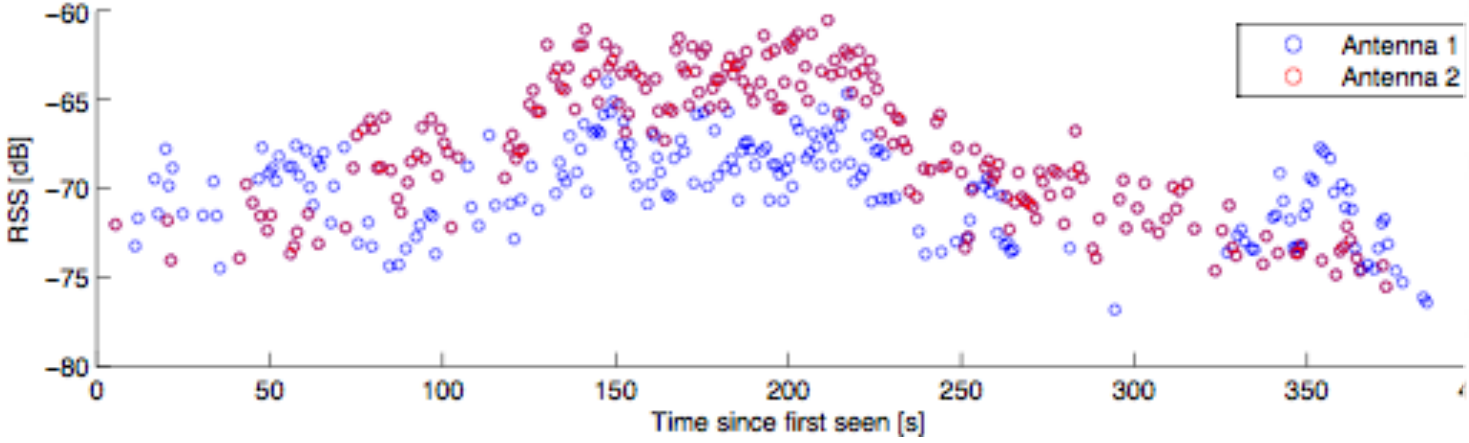
Loss vs. Distance

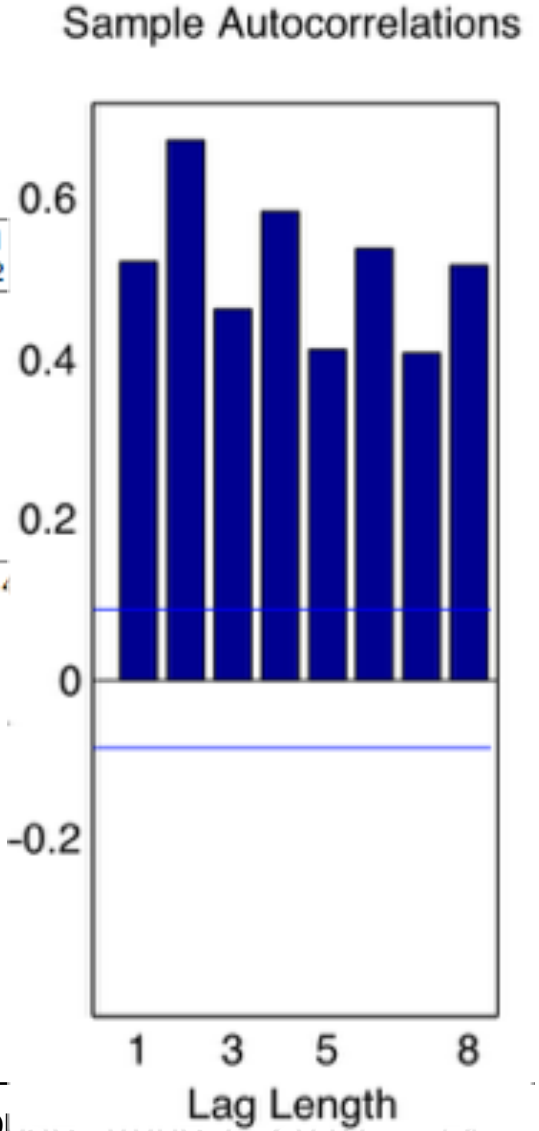
Loss vs. Traffic



Solutions: PHY-based Anomaly Detection

- Detect non-adjusting (constant/random sending power) attackers based on their TX patterns and correlation with claimed distances.

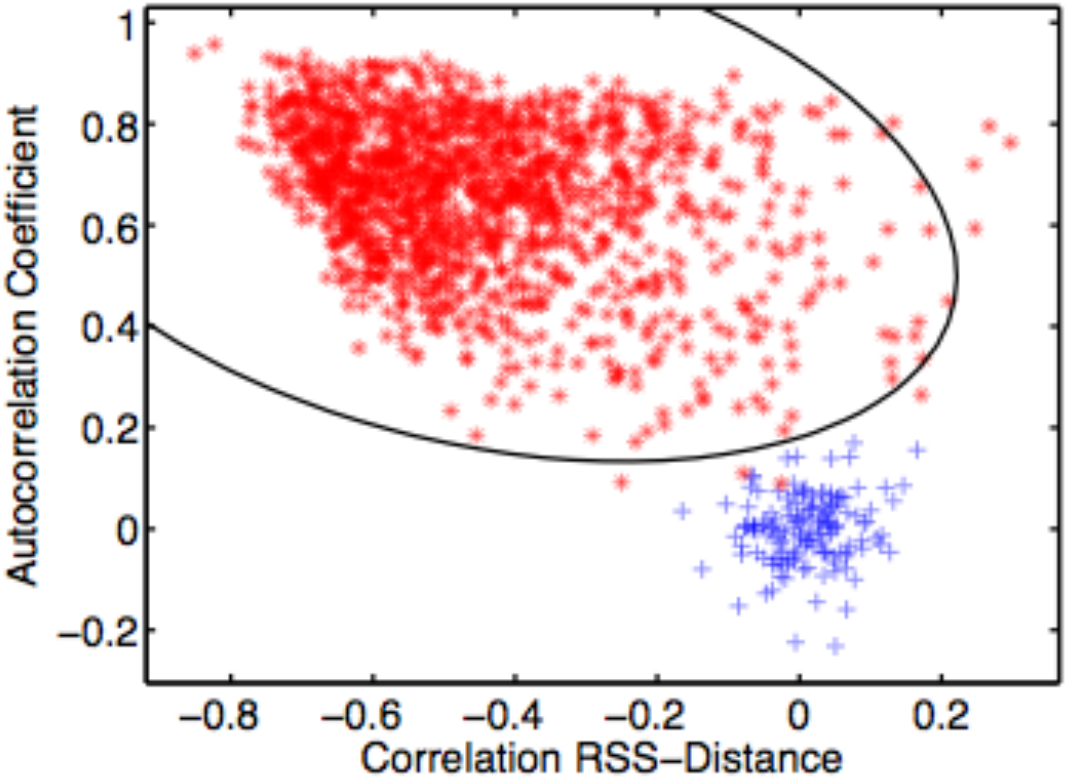


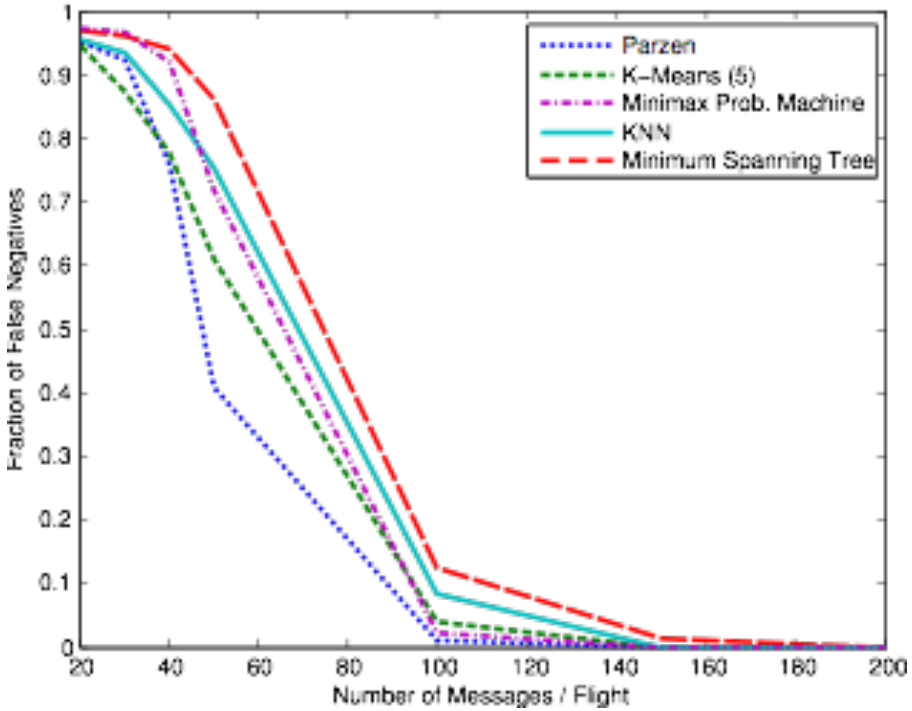


- Easily detect single-antenna attackers with high certainty by exploiting autocorrelation

Solutions: PHY-based Anomaly Detection

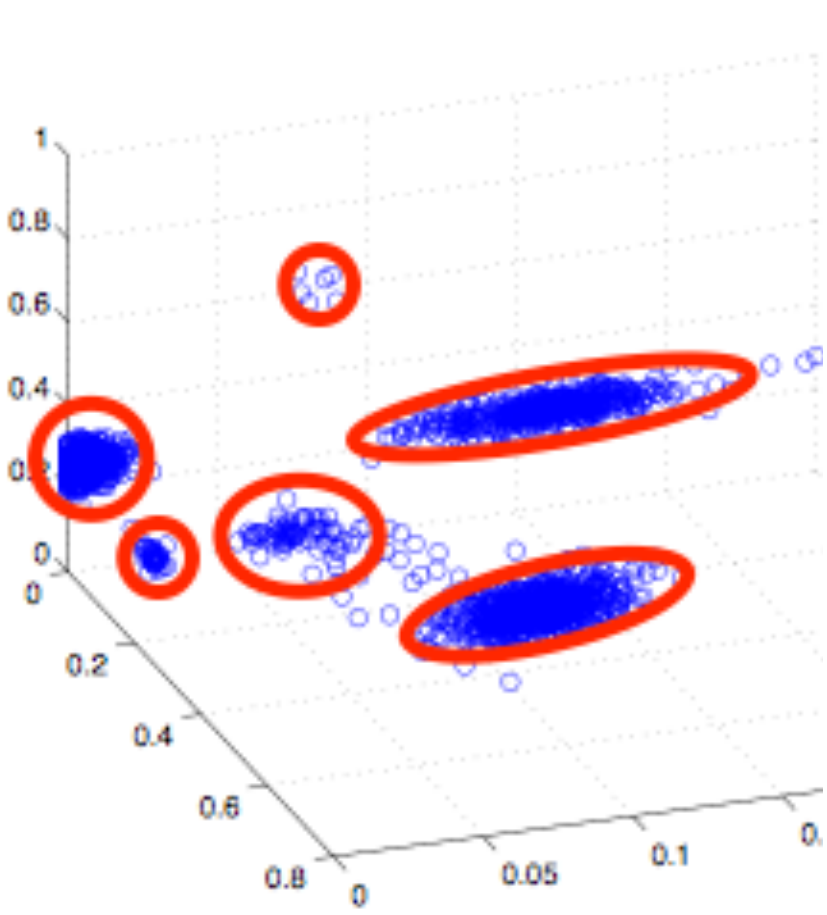
- Learn normal state of various features.
- Detect attackers that don't conform to the expected behaviour.

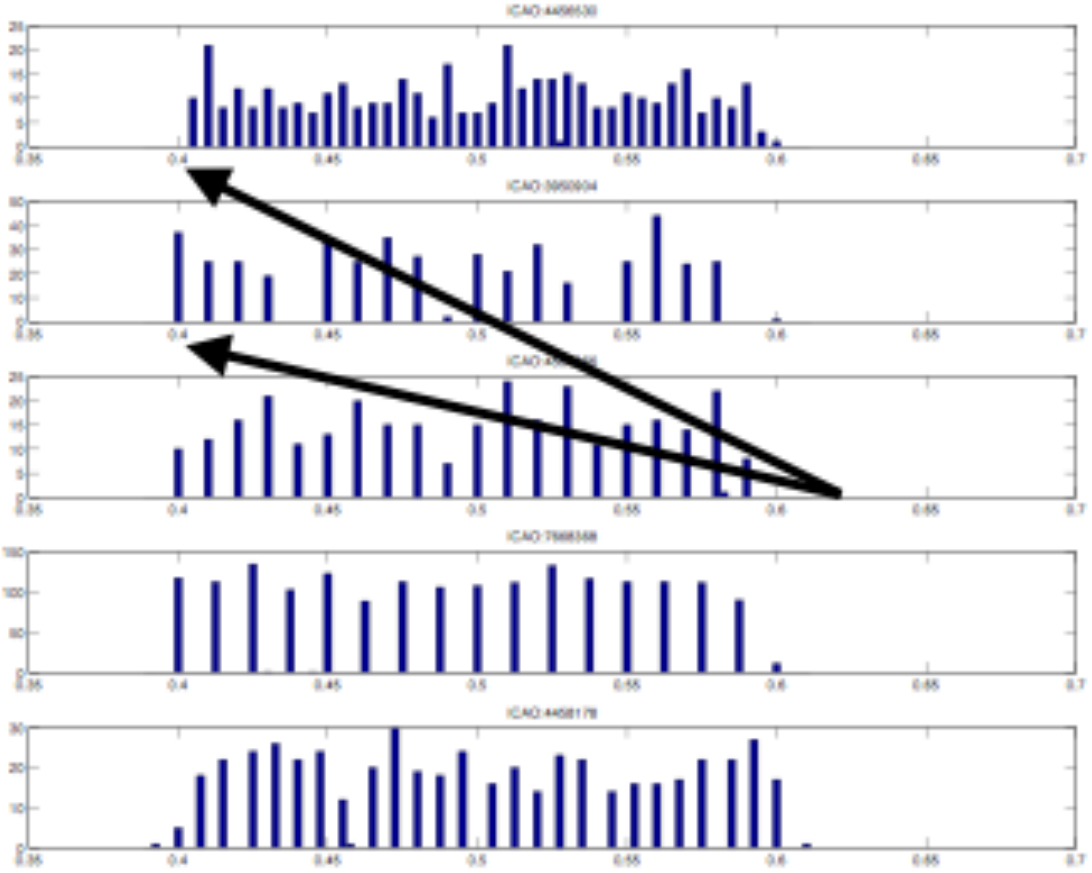




Solutions: Transponder Fingerprinting

- Different ADS-B transponder types / implementations used in the commercial aviation market.
- Features based on random backoff behaviour deduced from message interarrival times

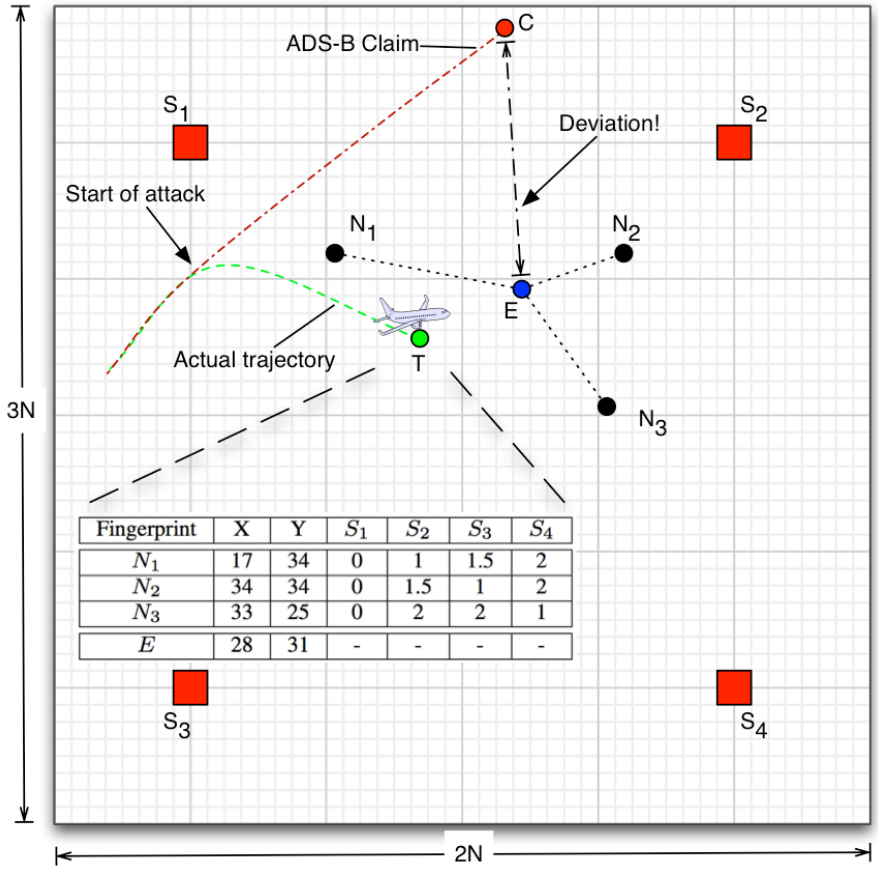




Solutions: Aircraft Location Verification

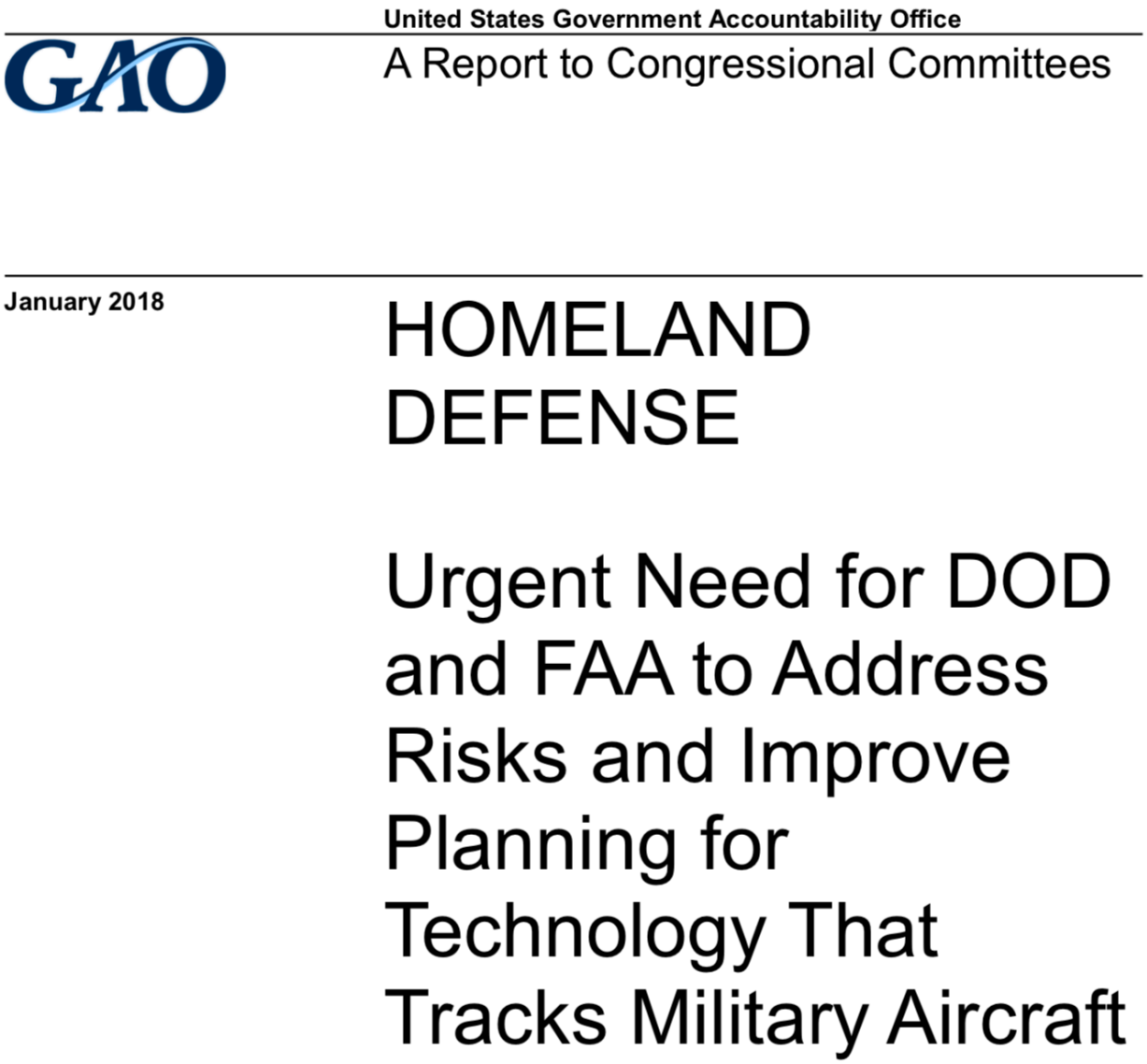
- Goal: Improve multilateration coverage (less than 4% utilization) by using simple statistical and machine learning algorithms on time differences of arrival

- Massively improved detection range and speed (up to 20 times more messages used);
- Much cheaper than multilateration



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	-	-	-	-

Research Impact



United States Government Accountability Office

GAO

A Report to Congressional Committees

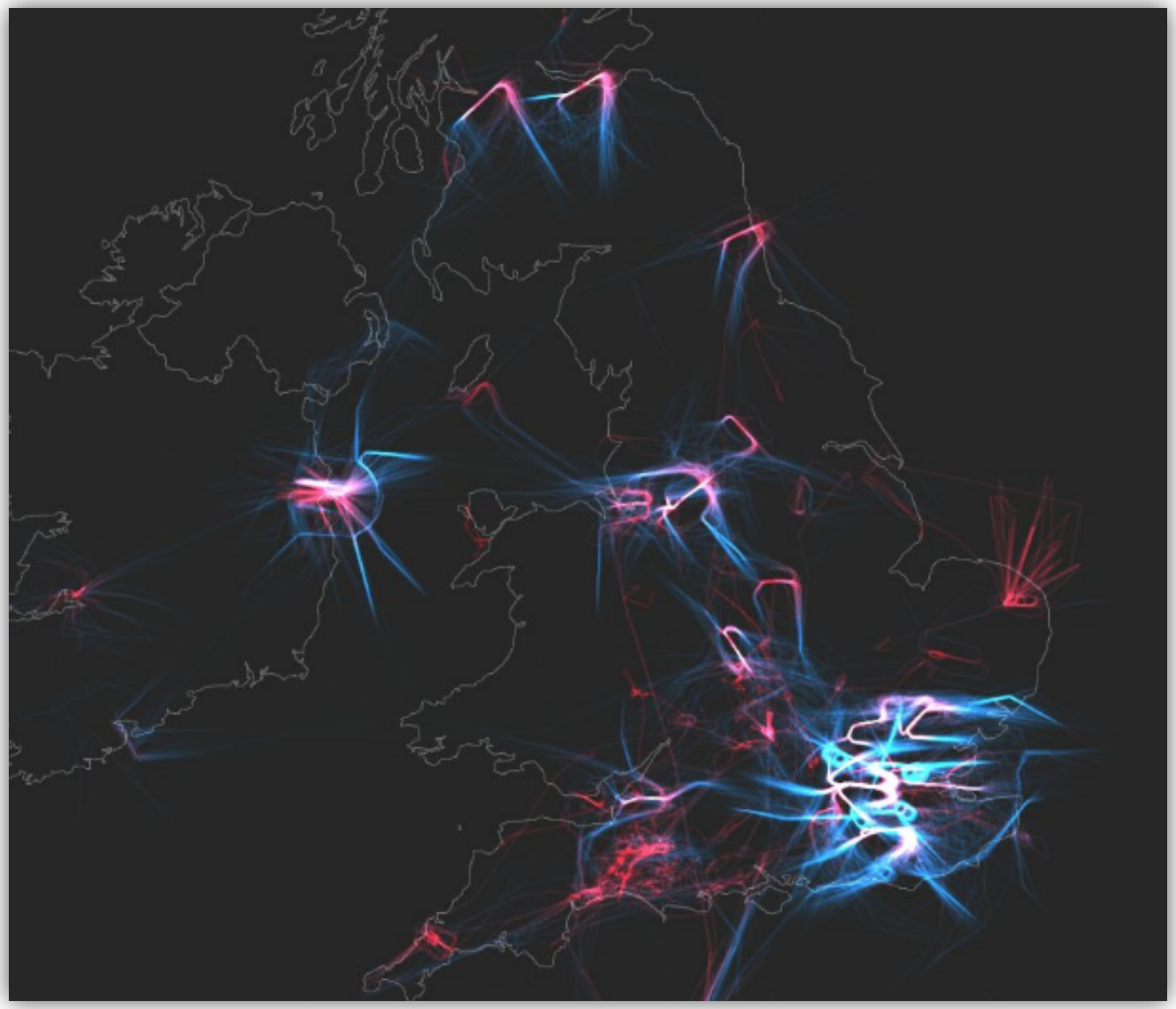
January 2018

HOMELAND DEFENSE

Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft

#dataviz

UK's air traffic density



#dataviz

© https://twitter.com/robhawkes

Conclusions

- Security awareness is still very low in aviation at large. [Defensiveness on security issues and belief in traditional safety mechanisms such as redundancy is prevalent.]
- But: Safety is not security and both cannot be solved the same way.
- Many issues will only be fully solved with new technologies/protocols that include security by design.
  - Introducing new technologies takes in this sector takes decades!
- Can crowdsourcing in ATC help mitigate future attacks and improve security efficiently?

Conclusions

- Next generation of air-traffic surveillance systems is coming
  - Worlds of safety and security
  - Trends towards digital datalinks
  - Two different worlds meet: safety and security
- At the moment, no really good solution in sight
  - However, PSR/SSR & MLAT will still be used for some time
- Enough time to think about threats based on unprotected ADS-B data
  - Inspiration from VANETS, MANETS, etc.