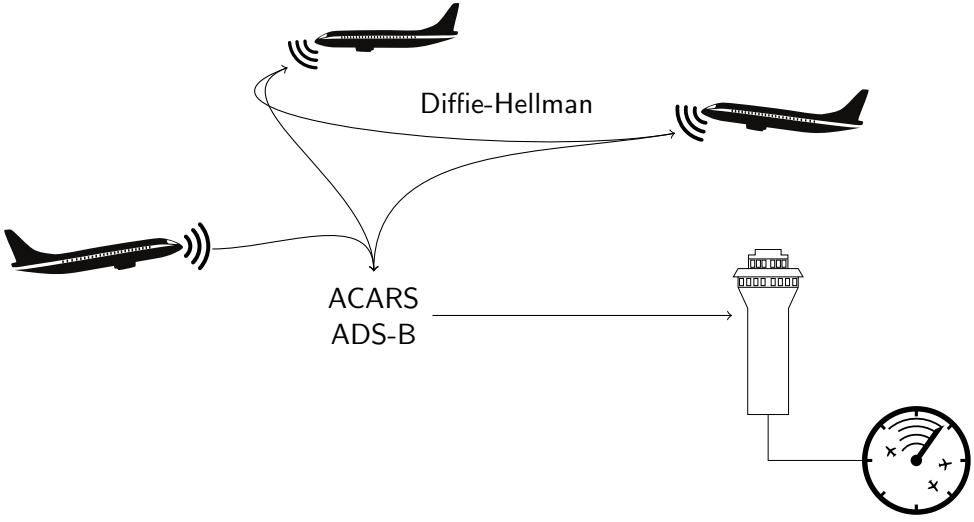


ACARS: Aircraft Communication Addressing and Reporting System
ADS-B: Automatic Dependent Surveillance-Broadcast

Evaluation of a wireless physical security method for flying objects based on the frequency selectivity of the propagation channel

Adrián Expósito García, Héctor Esteban González, Lorenzo Rubio Arjona, Martin Kubisch, Dominic Schupke

adrian.exposito-garcia@airbus.com, +498960728609

Wednesday 20th March, 2019

AIRBUS

Contents

- High-Rate Uncorrelated Bit Extraction (HRUBE) [Patwari et al., 2010].
- [Ben Hamida et al., 2009] identifies weakness of existing key generation algorithms.
- [Ye et al., 2010] uses Rayleigh and Rician models to generate richly scattering environments.

Contents

Assumptions taken

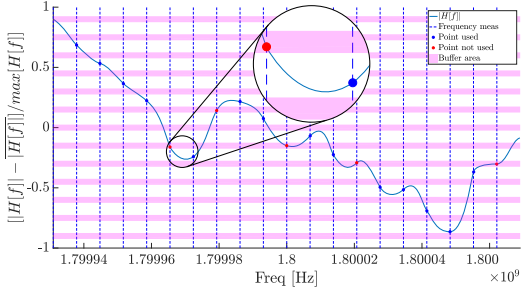
- Information reconciliation is part of system design, an important aspect in key generation, nevertheless, out of scope in this research. [Patwari et al., 2010]
- Synchronous measurements.
- Absence of noise:

$$|H_{\mathcal{AB}}[f]| = |H_{\mathcal{BA}}[f]|$$

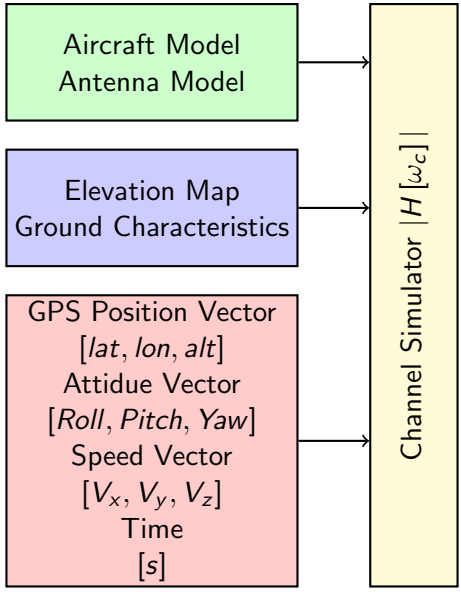
- Eavesdropper agent is passive.

Robust Slice Algorithm

1. $\mathcal{A}$ or $\mathcal{B}$ is defined as the master node.
2. $k[n]$ is calculated based on:
   - 2.1 d_{buff}
   - 2.2 d_{key}
   - 2.3 $|H[f_n]|$
3. Non-used sampling frequencies are shared from the master node.
4. Key is then generated on both sides excluding the non-used sampling frequencies.



Contents


Aircraft Model
Antenna Model
Elevation Map
Ground Characteristics
GPS Position Vector
$[lat, lon, alt]$
Attidue Vector
$[Roll, Pitch, Yaw]$
Speed Vector
$[V_x, V_y, V_z]$
Time
$[s]$
Channel Simulator $|H[\omega_c]|$

Contents

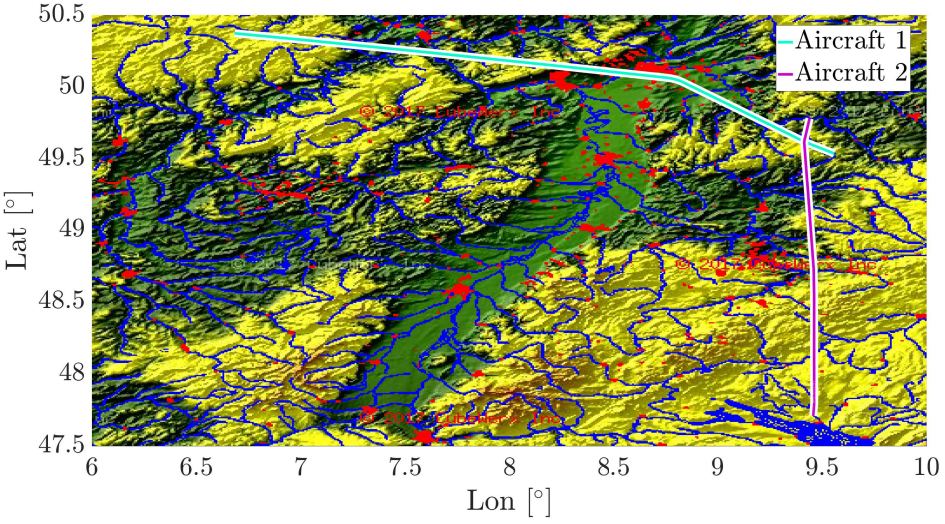
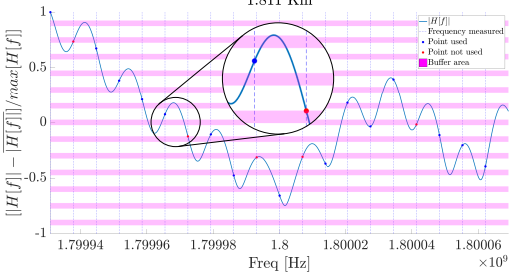
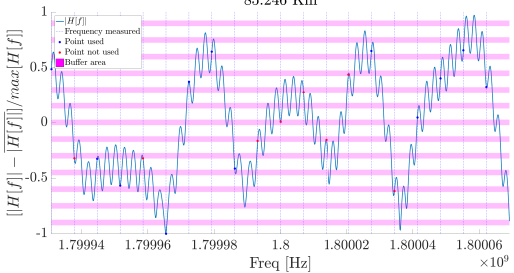
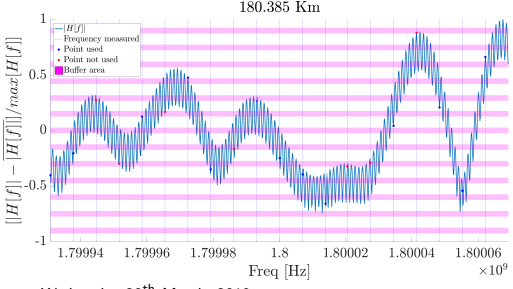


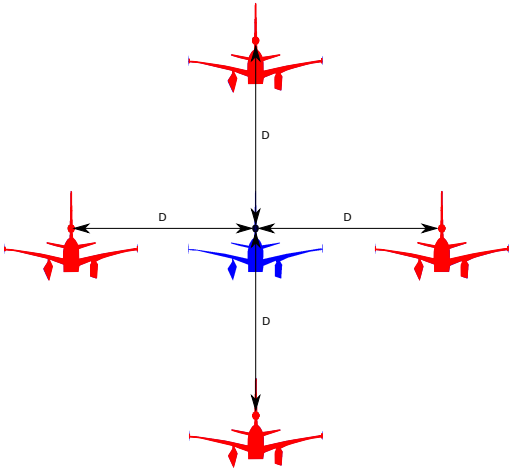
Figure: Trajectory [C.Edinger and A.Schmitt, 2013]

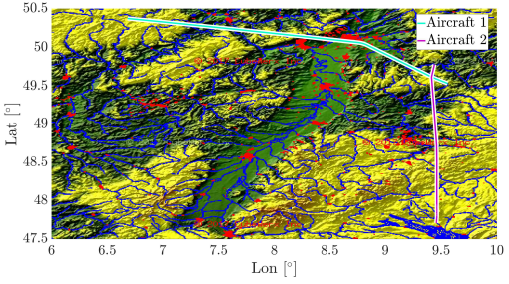


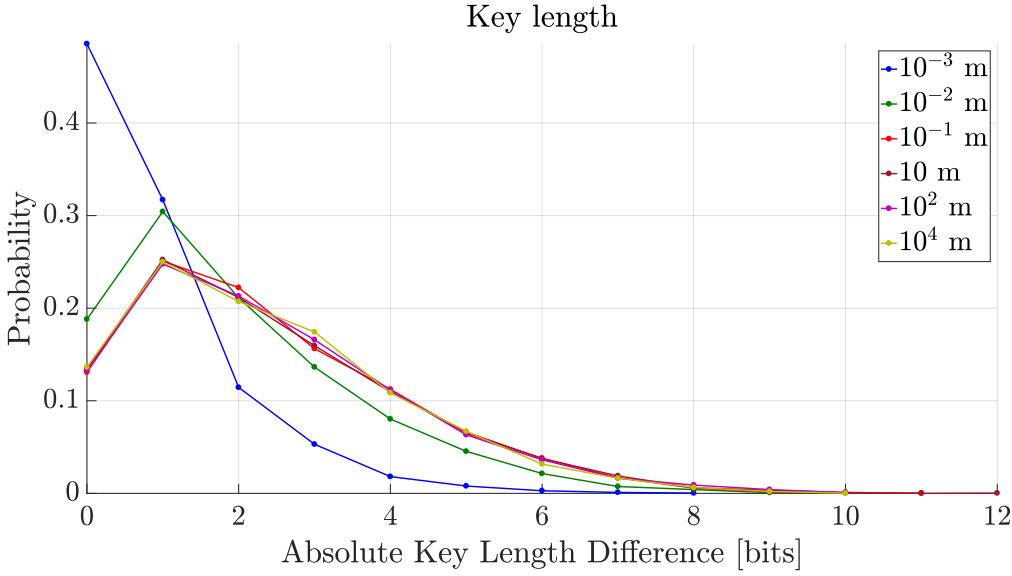


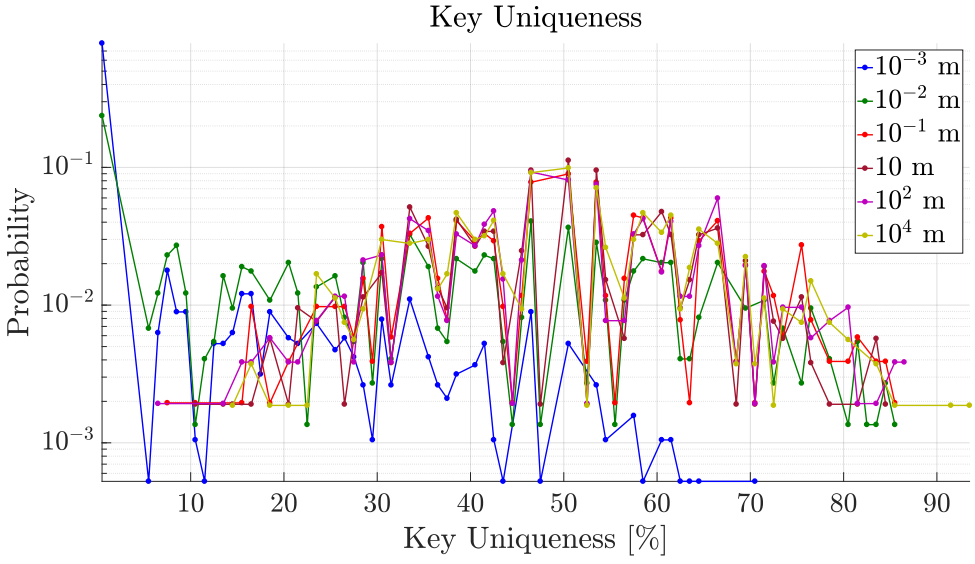


Distance	Generated Key	Length of generated key
180 km	1100011011000011	16 bit
85 km	101100101011101	15 bit
1.81 km	01111101000110	14 bit


D
D
D
D


Aircraft 1
Aircraft 2
Lat [°]
Lon [°]
50.5
50
49.5
49
48.5
48
47.5
6
6.5
7
7.5
8
8.5
9
9.5
10


Key length
Probability
Absolute Key Length Difference [bits]
0
0.1
0.2
0.3
0.4
0
2
4
6
8
10
12
10^{-3} m
10^{-2} m
10^{-1} m
10 m
10^{2} m
10^{4} m


Key Uniqueness
Probability
Key Uniqueness [%]
10^{-1}
10^{-2}
10^{-3}
10
20
30
40
50
60
70
80
90
10^{-3} m
10^{-2} m
10^{-1} m
10 m
10^{2} m
10^{4} m

Contents

- By means of simulation, it has been proven that:
  - An eavesdropper will generate the same key only at 0.01 m from $\mathcal{A}$ or $\mathcal{B}$.
  - Channel possess sufficient randomness to generate keys.
  - PHYSEC is a viable and secure wireless physical security method for flying objects.
- Open research paths:
  - Test PHYSEC on real conditions.
  - Study scenarios such as approach or taxi.

Evaluation of a wireless physical security method for flying objects based on the frequency selectivity of the propagation channel

Adrián Expósito García, Héctor Esteban González, Lorenzo Rubio Arjona, Martin Kubisch, Dominic Schupke

adrian.exposito-garcia@airbus.com, +498960728609

Wednesday 20th March, 2019

AIRBUS

References I

- Airbus a320.
  https://grabcad.com/library/airbus-a320--1 Accessed: 2019-11-03.
- Google.
  http://www.google.com/apis/maps/signup.html. Accessed: 2019-11-03.
- Web map service.
  http://www.pvretano.com/cubewerx/cubeserv? Accessed: 2019-11-03.
- Ben Hamida, S. T., Pierrot, J.-B., and Castelluccia, C. (2009).
  An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements.
  2009 3rd International Conference on New Technologies, Mobility and Security, pages 1–5.

References II


C.Edinger and A.Schmitt (2013).
Rapid prototyping for atm operational concepts development.
Deutsche Nationalbibliothek (urn:nbn:de:101:1-201302088769). Deutscher Luft- und Raumfahrtkongress 2012, 10.-12. Sep 2012, Berlin, Deutschland.


Patwari, N., Croft, J., Jana, S., and Kasera, S. K. (2010).
High-rate uncorrelated bit extraction for shared secret key generation from channel measurements.
IEEE Transactions on Mobile Computing, 9(1):17–30.


Ye, C., Mathur, S., Reznik, A., Shah, Y., Trappe, W., and Mandayam, N. B. (2010).
Information-Theoretically secret key generation for fading wireless channels.
IEEE Transactions on Information Forensics and Security, 5(2):240–254.