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
Contents

Introduction

Related Work

Physical Wireless Methods for Extended Security

Simulation Tools For Wireless Extended Security

Case of Study

Conclusion
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

Introduction

Related Work

Physical Wireless Methods for Extended Security

Simulation Tools For Wireless Extended Security

Case of Study

Conclusion
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:

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

- Eavesdropper agent is passive.
Robust Slice Algorithm

1. $A$ or $B$ 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

Introduction

Related Work

Physical Wireless Methods for Extended Security

Simulation Tools For Wireless Extended Security

Case of Study

Conclusion
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

Introduction

Related Work

Physical Wireless Methods for Extended Security

Simulation Tools For Wireless Extended Security

Case of Study

Conclusion
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
By means of simulation, it has been proven that:

- An eavesdropper will generate the same key only at 0.01 m from $A$ or $B$.
- 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
References

- Airbus a320.  

- Google.  

- Web map service.  

  An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements.  
References II

Rapid prototyping for atm operational concepts development.

High-rate uncorrelated bit extraction for shared secret key generation from channel measurements.

Information-Theoretically secret key generation for fading wireless channels.