Integrity of a GNSS/IMU hybridization against GNSS spoofing

Mathieu HUSSONG

Doctoral fellow in the Signav research team at ENAC

Thesis supervised by Carl MILNER & Axel GARCIA-PENA

mathieu.hussong@enac.fr

What is spoofing ?

Civil aviation relies on GNSS positioning to ensure a continuous level of safety during all phases of flight. For multiple reasons, GNSS signals might be miss-interpreted by the receiver, because of an external agent's interference with the GNSS frequencies. **Intrusions of external agents into the GNSS cycle** are defined as spoofing whenever the GNSS receiver location might be mislead by the counterfeit signal [1].

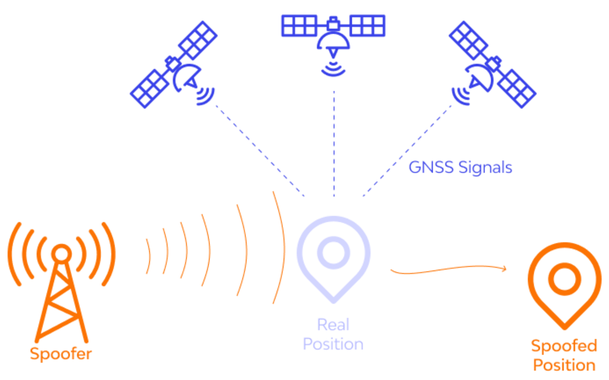

Figure 1: Example of a GNSS spoofing scenario luring the receiver location

Civil aviation started to consider spoofing issues back in 2001 [2] with the ambition to build anti-spoofing receivers based on spoof-affected observables. The first reported and confirmed spoofing attack took place in 2010 in Hannover, Germany [3]. GPS repeaters were installed to test the GNSS-exploiting avionics of business jets inside a hangar 1km away from the runway threshold. If the repeaters were in use with the hangar doors open, aircraft taxiing to the runway threshold experienced problems with GPS-driven instrumentation. Several pilots reported the displayed position of their aircraft shifted to coincide with the position of the hangar, while experiencing warning alarms and positioning alerts. Although this incident did not cause any injuries or material disaster, it provoked a **massive confusion** that postponed and diverted planes during the unintended attack, leading to huge traffic delays and **fear of other spoofing events**.

More recently, rumours of sophisticated spoofing cases are spreading. On December 4th, 2011, Iran captured a U.S. Lockheed Martin RQ-170 drone, claiming to have spoofed GPS, landing the drone in Iran instead of Afghanistan [4]. No certification have been disclosed about this event. Beside civil aviation, numerous GNSS spoofing attacks have been reported over the Black sea in June 2017 [5]. Ships notified that their GPS navigation system incorrectly placed them at airports many (up to 150) miles away from where they were sailing offshore. Years before, dynamic and **life-threatening spoofing attack** experimentations have been conducted onboard a 213-foot yacht [6]. Spoofing devices broadcast false GPS signals from the ship's upper deck to its antennas, and have been able to turn the yacht slightly off its original course. GPS tracking in the command room showed the yacht traveling along a straight line despite the maneuvers made.

"I didn't know, until we performed this experiment, just how possible it is to spoof a vessel and how difficult it is to detect this attack."

Todd Humphreys, 2013, [6]

Main Objectives

Spoofing evidences become mainstream and are feared to skyrocket during the next decades. When it comes to **ensuring the integrity of the civil aircraft positioning**, the necessity to detect and avoid spoofing events soar up to the number one priority of the civil aviation institutions. This thesis intends to mitigate spoofing threats in civil aircrafts by monitoring the GNSS/IMU hybridization observables. Within three years, experiments and analyses expect :

- to exhaustively enumerate the spoofing scenarios that loom on civil aviation
- to assess the resistance of civil aircrafts against these spoofing threats
- to define alert limits to bound the integrity risk of a position failure
- to come up with new methods and hybridization-driven algorithms to detect and exclude spoofing events
- to modernize international telecommunication regulations to safely face spoofing
- to extend the use of GNSS driven-procedures in critical phases of flight.

References

[1] "Threats and Countermeasures for Aviation Applications : Vol.7", EU-U.S. Cooperation on Satellite Navigation, WG-C Service Resilience Sub-Group, 2019

[2] "Vulnerability assessment of the transportation infrastructure relying on the global position- ing system", John A. Volpe National Transportation Systems Center, Office of the Assistant Secretary for Transportation Policy, U.S. Department of Transportation, 2001

[3] "GNSS Spoofing and Aviation: An Evolving Relationship", Gerhard (Gary) Berz, EUROCONTROL, 2018

[4] "Detecting GNSS spoofing attacks using INS coupling", C. TANIL, Illinois Institute of Technology, 2016

[5] "Above Us Only Stars : Exposing GPS Spoofing in Russia and Syria", C4ADS, 2019

[6] "Researchers successfully spoof an 80 million dollar yacht at sea", Phys.org, University of Texas at Austin, 2013

[7] "Springer Handbook of Global Navigation Satellite Systems", P.J.G. Teunissen, Oliver Montenbruck, Springer, 2017

[8] "Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System", Y. LIU , S. LI , Q. FU , Z. LIU , Q. ZHOU, IEEE Sensors journal, 2019

[9] Jafarnia-Jahromi, A., Lin, T., Broumandan, A., Nielsen, J., Lachapelle, G., "Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver," Proceedings of the 2012 International Technical Meeting of The Institute of Navigation, Newport Beach, CA, January 2012, pp. 790-800.

[10] "Detecting GNSS Spoofing Using Inertial Sensors", B. PERVAN, MMAE Department, Rettaliata Engineering Center, Illinois Institute of Navigation, 2019

five-month results

This thesis is running for five months. Beside the state of the art that lasted four months, four software beta-versions have be implemented. These softwares have been designed to generate spoofing realistic scenarios based on pre-determined modelizations. They are currently under validation process and are described hereafter.

Aircraft trajectory generator software

Realistic 7D (3D for space, 1D for time, 3D for attitude) aircraft trajectories are needed for this thesis in order to simulate both IMU and GNSS aircraft outputs, then spoofing corruption and mitigation. The generation can be done with any desired flight plan by mentioning the 7D waypoints that should feature the flight profile. The software interpolates the 7D-position in-between the waypoints with a realistic behaviour taking into account the dynamic flight equations, the inertia of the aircraft, the Earth curvature, auto-pilot responses, and acceleration human-oriented profiles. Wind gusts and turbulence drawn from the discrete Dryden model can also be added. Figures 2 to 4 highlight some features of the software generation.

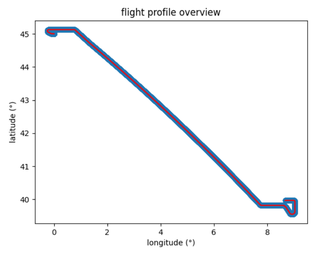

Figure 2: Whole flight trajectory

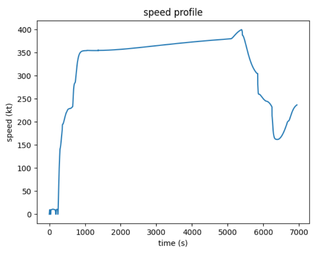

Figure 3: Whole flight speed profile

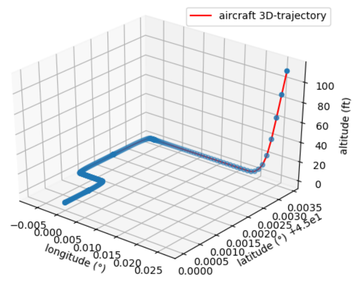

Figure 4: Taxi and Take-off 3D-view

IMU output generator software

From the profiles generated by the aircraft trajectory generator software, the IMU outputs are derived thanks to the IMU output generator. The required high precision of the generation is achieved with the inclusion in the software of the Earth rotation, repeatability biases, stability drifts, IO scale factors, misalignement matrices, random walk errors and white noise. Figure 5 depicts the IMU outputs computed from the generated flight profile.

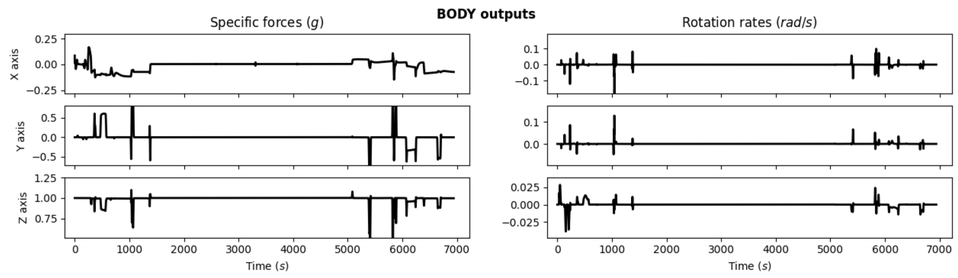

Figure 5: IMU outputs as generated by the software during the whole flight

GNSS observable generator software

A third software provides the outputs of a GNSS receiver from any flight profile. It has been designed to produce code and phase pseudodistances with a centimetric accuracy. The computations integrates ephemeris errors, satellite clock and hardware errors, carrier phase wind-up errors, carrier phase integer ambiguity terms, special and general relativity effects, ionospheric and tropospheric delays, multipaths, receiver clock and hardware errors, and thermal noise. The generator handles multi-constellation and multi-frequency scenarios. The code pseudodistance for L1 during the whole flight profile is given as an example on figure 6.

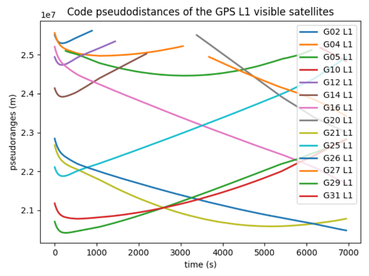

Figure 6: GPS L1 C/A code pseudodistances as generated over the whole flight

GNSS precise point positioning software

In order to loosely-hybridize the GNSS and the IMU outputs, it is required to build a GNSS positioning software. As the modelization and the generation are precise up to the centimeter level, a precise point positioning user algorithm has been implemented to take advantage of the position accuracy. The software models the same error sources than the GNSS observable generator software, rendering a positioning error lesser than 50cm both with real data and generated ones. The performances of this software are exhibited on figures 7 to 9.

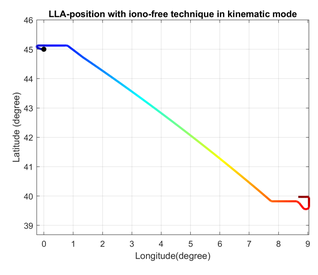

Figure 7: Trajectory estimation

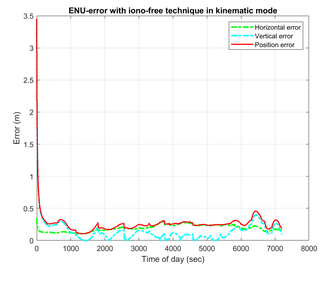

Figure 8: Positioning error

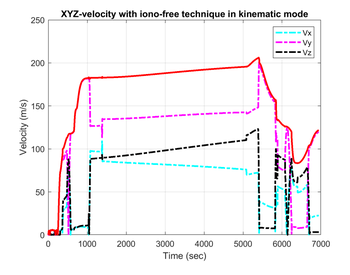

Figure 9: Estimated velocity

Forthcoming Research

The next two years of the thesis will be dedicated to the validation of the four above-mentioned softwares, and the proceeding of the thesis agenda. It is unfortunately too early to say if the results would lead to updates of the civil aviation regulation or definition of new integrity standards. Stay tuned to witness what these future years hold!