Sp-ATM

Techniques for spoofing detection and mitigation in Aeronautical receivers

Executive Summary Report

Version: 2.0

Date: 24/07/2020

Sp-ATM-ESR-OHB-TRP_AO9526

ESA UNCLASSIFIED

Project: TRP AO9526 – Sp-ATM - Techniques for spoofing detection and mitigation in Aeronautical receivers

ESA Contract No.: 4000127380/19/NL/CRD

Prepared by: OHB Digital Solutions (OHB), Graz, Austria

Supported by: Paris Lodron University of Salzburg, Aerospace Research Department (PLUS, Austria)

IntegriCom (IC, The Netherlands)

Signatures			
Function	**Name**	**Date**	**Signature**
(Main) Author	Philipp Berglez, OHB	24/07/2020	
Quality Manager	Philipp Berglez, OHB	24/07/2020	
Project Manager	Sascha Bartl, OHB	24/07/2020	

EUROPEAN SPACE AGENCY CONTRACT REPORT

The work described in this document was done under ESA Contract. Responsibility for the contents reside in the author or organisation that prepared it.

Document Information

THE INFORMATION IN THIS DOCUMENT IS **COMMERCIAL IN CONFIDENCE**
AND PROVIDED AS IS.
NO GUARANTEE OR WARRANTY IS GIVEN THAT THE INFORMATION IS FIT FOR ANY PURPOSE
OUTSIDE THE SCOPE OF THE **Sp-ATM** PROJECT.

Project:	Techniques for spoofing detection and mitigation in Aeronautical receivers
Project Short Title:	Sp-ATM
Document Title:	Sp-ATM-ESR-OHB-TRP_AO9526
Document ID:	Sp-ATM_FRP
DRD Reference:	1.1
Version:	2.0
Date:	24/07/2020
Number of Pages:	8
File Name:	Sp-ATM-ESR_Executive_Summary_Report_V2.0.docx

Authors:

Company	Author(s)	Chapters
OHB Digital Solutions	Dr. Philipp Berglez Sascha Bartl Manuel Kadletz Shahrzad Afroozeh	All
PLUS	Kurt Eschbacher Fritz Zobl Robert Marschallinger Carl-Herbert Rokitansky	All
IntegriCom	Bastiaan Ober	All

Approvals:

Function	Name	Date	Signature
(Main) Author	Philipp Berglez, OHB	24/07/2020	On file
Quality Manager	Philipp Berglez, OHB	24/07/2020	On file
Project Manager	Sacha Bartl, OHB	24/07/2020	On file
Customer	Gianluca Caparra, ESA		

Change Log:

Title:		**Sp-ATM_FRP – Change Log**			
2	0	22.07.2020	Version 2 for final data package. The following sections have been modified: • Amendments after updates of D501	S. Afroozeh, OHB Manuel Kadletz, OHB P.B. Ober, Integricom	P. Berglez, OHB
1	0	06/07/2020	1st release submitted for final review meeting	P. Berglez, OHB	P. Berglez, OHB
Issue	Revision	Date	Change Description	Prepared by	Released by

Applicable and Reference Documents

Applicable Documents:

[ESA-CON]	ESA Contract No.: 4000127390/19/NL/CRS Techniques for spoofing detection and mitigation in aeronautical receivers (Sp-ATM)
[ESA-PROP]	Techniques for spoofing detection and mitigation in aeronautical receivers (Sp-ATM) proposal, version 1.0

Scope of the Document

This document contains Executive Summary Report (ESR) for the TRP AO9526 - Techniques for spoofing detection and mitigation in aeronautical receivers (Sp-ATM) activity under ESA Contract No.: 4000127390/19/NL/CRS. The document was prepared and is managed by OHB Digital Solutions (OHB) (former TeleConsult Austria (TCA)) in cooperation with Paris Lodron University of Salzburg, Aerospace Research Department (PLUS) and IntegriCom (IC).

Note that in December 2018 TeleConsult Austria became part of the OHB SE group. In December 2019 the name was changed to OHB Digital Solutions.

This document describes the activities and main achievements of the TRP AO9526 - Techniques for spoofing detection and mitigation in aeronautical receivers (Sp-ATM) project.

The project in brief

Position, navigation and time solutions that use GNSS can be disrupted by jamming (overpowering the GNSS signals to prevent GNSS receivers to operate) or spoofing (cause a GNSS receiver to track fake signals and calculate an erroneous position).

In this project, we investigate, define and analyse GNSS interference and spoofing detection techniques relevant to the aeronautical domain, both for existing and future receivers. These investigation lead to the determination of most vulnerable phases of flight in addition to the best spoofing detector candidates. A combined weighted system of spoofing detectors was designed, implemented, and analysed. Based on our findings we have formulated guidelines and recommendations for future work and standardization activities.

Interference and spoofing threaten the use of GNSS

GNSS-based position, velocity, and timing services have steadily increased in importance over the past decades. However, there is growing awareness that these services are vulnerable to attacks to falsify the position and timing solutions, and such attacks have already been demonstrated in scientific and governmental publications. The availability and affordability of jamming and spoofing equipment increases the associated risks for GNSS users, including aviation.

Receiver techniques can make the position more resilient

To make GNSS more resilient, one can look at the properties of the Signal-In-Space (SIS), but changing these is expensive and time consuming. Receiver techniques have the potential to detect spoofing attacks at a much lower cost, and can sometimes even mitigate their effects. Interference- and spoofing-detection techniques improve the receiver's performance in the presence of interference and spoofing, as they allow detecting situations under which the nominal performance is degraded to the extent that GNSS has become unusable for the intended operation. Position output may still become unavailable, unless faulty signals can be effectively removed from the navigation solution.

Spoofing detectors impact the operational risks

The operational environment dictates the performance that is needed from the GNSS receivers and the criticality of correct information. Integrity risk is associated with the likelihood of using an erroneous position reading in the aircraft. Continuity risk captures the likelihood that no position if provided by the GNSS receiver at all. Different phases of flight have different allowances for acceptable integrity and continuity risk levels.

Spoofing and interference detectors for aviation receivers shall be designed to lower the impact of attacks, and in particular lower the integrity risks. Our study shows that the relation between 'detector-level' requirements and the operational risks is highly complex and involves many intricate dependencies. This makes it hard to follow a purely top-down or purely bottom-up approach to design and tune detectors: when working top-down, there is a danger that the requirements for the detectors are suboptimal and

become either impossible to meet or overly relaxed. When working bottom-up, the question becomes how to tune the detectors to give an optimal trade-off between integrity and continuity of service. What further complicates things is that achievable operational performance will finally depend on the likelihood of interference and successful spoofing attacks, which might change with time and location. Hence, in the end, an integral approach is needed that considers technical possibilities and operational requirements and their interactions together.

Operationally acceptable integrity and continuity risks can only be established from an overall analysis of the operational environment. While such an analysis was not the focal point of our study, we have investigated the relation between the operational risks and the performance that is needed from spoofing and interference detection techniques by integrity and continuity risk trees. These risk trees were used to assess the operational risks inflicted by the different attack scenarios in order to determine which attacks impose the largest risks.

We selected the attacks that impose the highest risks

Spoofing attacks can vary in the level of sophistication of equipment used, the knowledge needed about the targeted receiver, and can vary in the way they attack the receiver. When looking at aviation, it turns out that different phases are vulnerable to different types of attacks. Higher risks are associated with both the effort needed to attack and the impact on the airplane's position: attacks that are easier to perform are therefore likelier to occur, which increases the risk. On the other hand, more sophisticated attacks can increase the effectiveness of the spoofing and increase risk by increasing impact.

We have classified the different types of attacks, and ranked them in order of the risk they pose to aviation users. We have used criteria such as the availability and cost of hardware and software, the availability of information about the target receiver (for example its architecture, or its location), and the required logistics. Based on our engineering judgements, we have selected the four highest-risk attacks for further investigation:

- Meaconing / re-radiation of authentic signals by a malfunctioning GNSS repeater
- Airborne pin-point spoofing attack using a drone, with the goal of leading the aircraft on a false lateral path
- Ground-based pin-point spoofing attack from the ground, with the goal of leading the aircraft on a false vertical path
- A jamming attack on an approaching aircraft with the attacker located on the ground.

How spoofing detectors can observe attacks

Apart from the final position outcome, spoofing and interference affect a wide variety of variables in the receiver. Each of these offers opportunities to detect an attack by observing its value and checking it for anomalies. We have implemented a variety of detectors into our software-defined receiver, which we'll briefly summarize below.

- RAIM and ARAIM detectors: RAIM failure detection and exclusion algorithms are implemented in existing aviation receivers. They are designed to deal with individual satellite errors, and can only detect a single faulty signal at a time. ARAIM is an evolution of RAIM that is currently being developed for future multi-constellation receivers. It is designed to deal with multiple faults in satellites, but the number of simultaneous faults that can be effectively detected is still limited. While not being designed for interference and spoofing attacks, these detectors are part of current and future receiver standards. Therefore, it makes sense to investigate their capabilities to detect and mitigate the effects of such attacks.
- CNR Detector: The carrier-to-noise ratio (CNR or C/N0) describes the ratio of the received modulated carrier signal power and the received noise power spectral density. It is estimated by the receiver and can be fairly well predicted, due to the open sky environment with low multipath/fading. If the estimated CNR deviates significantly from the predicted value, this is a strong indication of either jamming (that increases the noise levels) or spoofing (that increases the signal levels).
- Correlation Peak Detector: by transmitting GNSS-like signals, a spoofer tries to take over the tracking of an authentic correlation peak, often causing deformation of the correlation peak. Monitoring the shape of the correlation peak can therefore be used to detect spoofing signals. As soon as the authentic and spoofed correlation-peak are separated by at least ½ chip, the correlation function can also be searched for more than one significant correlation peaks and thus can be used to find additional signals.
- Clock Detector: a spoofer aims to take over the tracking loops of the airborne receiver using spoofed GNSS signals. As it is challenging for spoofer's to estimate the receiver position, the spoofing signals cannot fully compensate for the transmission delay or Doppler shift of actual signals. This causes the receiver's clock bias estimate to jump. Additionally, there is potential for this bias to experience excessive drift. Both effects can be exploited to detect the occurrence of a spoofing attack.
- Spatial Correlation Peak Detector: when spoofing signals are transmitted from a single source by an attacker, the signal errors show higher correlations than signal errors that come from actual GNSS satellites. This characteristic can be exploited for detection, but is expected to fail for highly sophisticated spoofing attacks that transmit signals from different locations.

Multiple detectors are combined using a weighting scheme

We have found considerable overlap between the capabilities of different spoofing detectors to detect specific attacks. We exploit that fact by combining the output of multiple detectors using a simple weighting scheme to improve overall performance.

The idea is that the most effective and reliable detectors function as 'primary detectors' with a weight of 1. The 'secondary detectors' are given a lower weight. A single detection of a primary detector would immediately lead to a system warning. In the case of the detection of a primary detector, either a confirmation of sufficiently enough secondary

detectors or the approval of a second primary detector is required to raise the system state from warning to alarm. This way, the secondary detectors can be used to confirm a detection or to suppress false alarms. On the other hand, they function as a backup: if multiple secondary detectors fire, this makes it highly likely that there is a problem, even if the primary detector has not detected it.

Conclusions and Recommendations

All designed spoofing and jamming scenarios have been successfully carried out and lead to some new insights on the behaviour of both current aviation receivers and the added value of our proposed, combined detection system.

Based on the performed work we identified some fields of potential future work on the path of spoofing detection being certified and implemented in the aviation domain.

- With the lessons learnt during this activity, more simulation and validation of the proposed detection system has to be conducted. In order to confirm the KPIs on a more robust basis, longer periods of simulation would be required.
- Expand the range of potential spoofing attacks and variations to validate the threat space coverage of the proposed detection system.
- The work during this task showed that the jamming detection at the beginning of a spoofing attack currently is over-sensitive. In order to tune the system to meet the false alarm requirement, precise definitions of the detection criteria for jamming detection have to be provided.

Based on the lessons learned from the simulations, the detection system must be tested and validated with real-world data in future activities.

Finally, guidelines for aeronautical GNSS anti-spoofing techniques have been provided in our study, but consolidation is necessary within the standardization community. These guidelines shall summarize the aeronautical spoofing threat space and the proposed anti-spoofing techniques.

END OF DOCUMENT