A Cost-Efficient RFI Localization Approach to Detect GNSS Jamming and Spoofing

Michael Felux, Valentin Fischer, Sophie Jochems, Okuary Osechas,
Manuel Waltert, Luciano Sarperi *Zurich University of Applied Sciences*
Martin Strohmeier, *armasuisse*

BIOGRAPHY

Michael Felux is a senior lecturer and leader of the Aviation Infrastructure Team at the Centre for Aviation at the Zurich University of Applied Sciences. He holds a PhD in Aerospace Engineering and has been working on safe and secure navigation for aviation for the past 14 years.

Valentin Fischer obtained a Bachelor of Science in aviation at the Zurich University of Applied Sciences (ZHAW) in summer 2022. In fall 2022, Mr. Fischer started his Master of Science in Aviation at the ZHAW. Since then, he has been working as a research assistant at the Center for Aviation within the research group Aviation Infrastructure. His research focuses on satellite navigation and aviation infrastructure topics.

Sophie Jochems graduated from the Zurich University of Applied Sciences (ZHAW) in summer 2019 with a Bachelor of Science in Aviation. Since July 2021, Ms. Jochems is working as a research assistant at the Center for Aviation at the ZHAW within the research group Aviation Infrastructure. Her research focus lies on satellite navigation and its use in the field of drone navigation. In fall 2023, Mrs. Jochems started her Master of Science in Data Science at the ZHAW.

Okuary Osechas is a researcher with the Center for Aviation at Zurich University of Applied Sciences. He has also worked for the German Aerospace Center (DLR) and the Mitsubishi Electric Research Lab. He received a Diploma in Electrical Engineering from Karlsruhe University and a PhD in Electrical Engineering from Tufts University.

Manuel Waltert is a research associate at the Centre for Aviation at the Zurich University of Applied Sciences. He holds a PhD in Transportation Sciences from Cranfield University and has been working on aviation-related research for the the past 10 years.

Luciano Sarperi has over 15 years of experience in R&D in the telecommunications sector and has been a lecturer in Wireless Communications at the Zurich University of Applied Sciences since 2017. His interests in applied R&D include wireless localization, IoT systems, mobile communications, and software defined radio applications.

Martin Strohmeier is a senior scientist at the Swiss Cyber-Defence Campus of armasuisse in Zurich, and also a visiting fellow of Kellogg College, University of Oxford. The main focus of his work has been the security analysis of critical infrastructures in the air, in space, and on ground. Martin is also a co-founder of the aviation research network OpenSky. He received his MSc degree from TU Kaiserslautern, Germany and joined Lancaster University's InfoLab21 and Lufthansa AG as a visiting researcher.

ABSTRACT

This paper introduces a novel method to identify the source of a Radio Frequency Interference (RFI) in an affordable and easily deployable way using UAVs. A payload consisting of two GNSS antennas and a directional antenna was attached to a UAV. A heading-capable GNSS receiver was fed with the signal of one GNSS antenna into the primary antenna port, and the combined signal of the directional antenna and the other GNSS antenna into the second antenna port as test statistic. In flight tests, the location of a jammer, i.e., the RFI source, was determined on the basis of the position and heading of the UAV using the difference of the average C/N0 values of the two antenna inputs. The heading of the UAV at which the proposed test statistic yields a maximum value, the direction towards the RFI source is established. The proposed method was tested in a field experiment consisting of two flights and involving a directional jammer, which was located approximately 1.5 km from the UAV. Results of the first test flight indicate that the heading corresponding to the spike in the test statistic correspond well to the true direction of the jammer. However, during the second test flight, when the directional antenna pointed at the source of RFI for short periods of time only, the test statistic showed more variation and a less distinct peak. Besides, the proposed setup was tested close to a 5G antenna to evaluate if the proximity of the frequency bands of 5G and GPS L1 signals affect the detection capability of the proposed measurement setup. The test statistic showed a discernible peak indicating significant interference with the test statistic. In this paper, the feasibility of the proposed method could be demonstrated.

I. INTRODUCTION

Global Navigation Satellite Systems (GNSS) are the primary means of aeronautical navigation today. A wide variety of applications, such as Required Navigation Performance (RNP) approaches or accurate and reliable navigation in remote and oceanic areas are hardly possible without the use of GNSS. In Europe, the Commission Implementing Regulation (EU) 2018/1048 mandating the use of performance-based navigation for all phases of flight, except landing in CAT-II/III weather conditions, is in place and will come fully into effect in the year 2030. This will further increase the reliance of aeronautical navigation on GNSS. However, an increasing number of GNSS jamming and spoofing incidents have raised concerns in the aviation community regarding the vulnerability of aeronautical navigation systems (European Union Aviation Safety Agency, 2023). Ongoing jamming activities in the Eastern Mediterranean and in the vicinity of conflict areas around Ukraine and Iraq have been well documented and studied (Fol and Felux, 2022; Osechas et al., 2022; Felux et al., 2023). While large-scale Radio Frequency Interference (RFI) events have become a commonly observable phenomenon around conflict areas, significant GNSS signal disruptions have been observed in various other locations as well. Most prominently, two major incidents near Denver and Dallas that have impacted several thousand flights in the year 2022 (Cybersecurity & Infrastructure Securtiy Agency (CISA), 2022; Liu et al., 2023). With the increased reliance on GNSS-based navigation, addressing the impact of RFI on aviation is an urgent matter. While technological solutions are being developed that include hardening of the airborne receivers as well as developing suitable alternative or complementary navigation solutions that enable the same level of performance, these solutions will take many years until deployed on a large scale (Blois et al., 2023; Joseph et al., 2023). In the meantime, most aircraft with their current avionics will remain vulnerable to RFI. The research presented in this paper is therefore anchored in conceptualizing and developing an affordable and easily deployable RFI localization and detection system that enables a speedy localization of an RFI source. Liu et al. (2023) presented an approach to localize the source of RFI based on ADS-B data. However, the method heavily depends on the availability of trajectory data of aircraft affected by RFI. Our setup is designed as a supplementary payload for UAVs, particularly those already in use today, e.g., by emergency services and law enforcement, allowing swift deployment during critical navigation interference events. Furthermore, the technology requires no expert knowledge making it easy to use. When deploying several of those vehicles within a short period of time, several direction estimates from the deployed detectors can help localizing an RFI source rather quickly. This paper focuses on a feasibility study of the determination of the direction from where the interference is originating, relative to the jamming detector that is mounted on a UAV.

II. MATERIALS AND METHODS

This section describes the hardware setup including all components used for the tests, the measurements collected, and the methodology employed for determining the direction from the UAV to the RFI source.

1. Hardware setup

The payload was conceived such that it can be easily mounted on a UAV. The setup as flown is shown in Figure 1. For determining the location of an RFI source, the reference position of the detector has to be established first. While it is certainly possible to deploy the jammer localization hardware at a fixed known location, a conventional *Septentrio mosaic-H* GNSS receiver is used for positioning of the UAV with the mounted RFI localization equipment. This receiver features a dual-antenna input allowing for heading determination of the baseline between the two GNSS antennas. We flew two *Tallysman TW7972* multi-band GNSS antennas that were mounted onto a fixed carbon tube at a fixed baseline length. The receiver then determines the heading of the baseline between the two antennas. The signals of the main antenna were fed directly into the receiver, while the RF signals of the auxiliary GNSS antenna were combined with the signal of a directional antenna. We used a Yagi antenna mounted perpendicular to the baseline between the two GNSS antennas. Subsequently, the combined signal of the two antennas was fed into the auxiliary input of the GNSS receiver. This configuration allows the UAV to (i) determine its own position, (ii) determine the direction in which the directional antenna is pointed, and (iii) provide carrier to noise ratio (C/N0) information for both antennas inputs into the receiver. Determination of the direction towards the RFI source is based on the C/N0 outputs.

2. Measurements and Estimation of Direction to RFI Source

The airborne test equipment described provides measurements of C/N0 of both inputs, along with a heading estimate of the baseline between the two GNSS antennas. In order to account for the rather fast dynamics of the UAV, we used a sampling rate of 5 Hz to obtain sufficient directional resolution. The presence of an interference source would be indicated by a discernible change in C/N0 on the secondary antenna input, i.e., the combined signal of the GNSS and Yagi antenna, whenever the directional antenna is pointing in the direction of the RFI source. On the one hand, the C/N0 in the aux1 antenna would decrease when pointing at a jammer. On the other hand, when the RFI source is a spoofer, the C/N0 would increase. Both changes with respect to the rather constant reference signal of the main GNSS antenna can be identified.

The decision as to whether a jammer is present in a given direction was made by aggregating all available C/N0 values of the

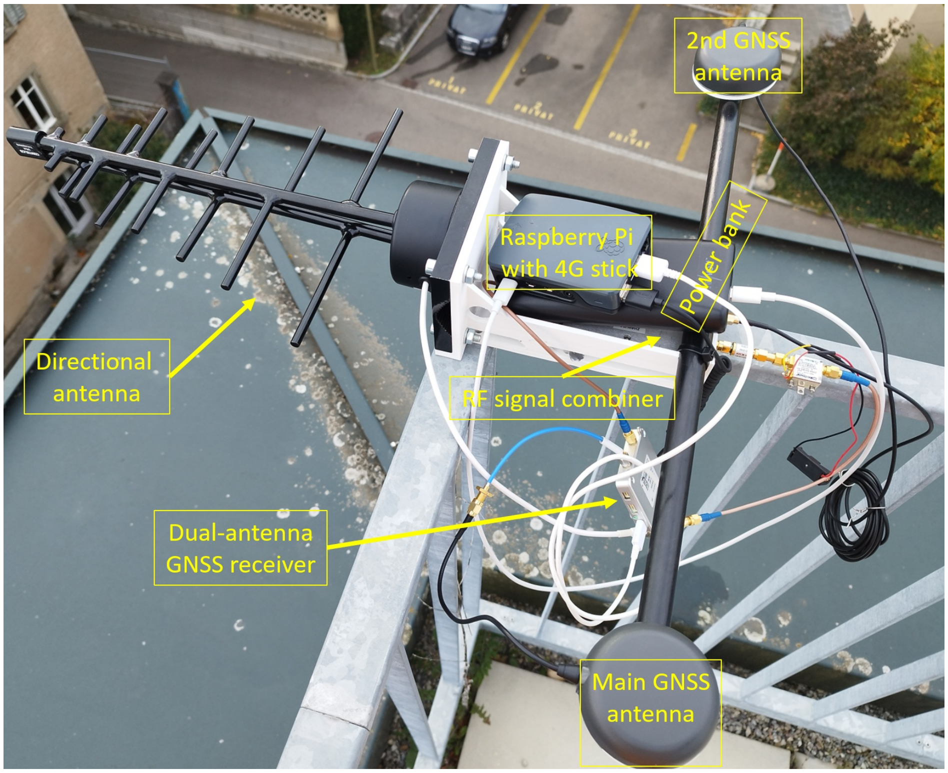

Figure 1: Deployable payload for determining the direction towards the RFI source.

L1 GPS and E1 Galileo signals. For the purpose of this paper, a distinction was made between C/N0 values measured through the main antenna and the auxiliary antenna. The proposed method averages the difference in C/N0 between the two antennas across all available satellite signals that are tracked on both input ports of the receiver. Consequently, the jamming metric T is the difference in average C/N0 between the main and aux1 port and can be written as

$$T = mean(C/N0_{main}) - mean(C/N0_{aux}). \tag{1}$$

As we were assuming that a jammer was present affecting the auxiliary antenna input, we determined the maximum value of T. The corresponding heading output by the receiver (adjusted by 90 ° due to the orientation of the directional antenna perpendicular to the GNSS antenna baseline) then showed the direction towards the RFI source.

3. Field testing with directional jammer

In order to test the setup under real-world jamming conditions, we had the opportunity to fly the equipment during an officially approved test of counter UAV equipment with a highly directional jammer. This directional antenna was pointed at the azimuth where the jamming detector was flown. However, the elevation angle of the jammer was deliberately pointed above the UAV. Completely jamming the detector system would have rendered the whole setup unusable, as the GNSS receiver on top of the UAV would neither have been able to determine its own location, nor establish the heading at which the directional antenna is pointed. Moreover, in case that both GNSS antennas are fully jammed, it is not possible to detect any discernible difference in the observed C/N0 values.

We flew two different tests each lasting between five and seven minutes. During the first test, the detector was flown just about two m above ground at a distance of about 1480 m from the RFI source. The RFI source was pointed at an elevation angle of 15 ° and thus significantly above the UAV. The line of sight was blocked by trees close to the transmitter. The jammer was turned on while the UAV was already flying. We then rotated the UAV to collect data with the directional antenna pointing at different azimuth angles. The second test was conducted at the same location. This time, the beam of the jamming antenna was lowered by 5 ° and the UAV was flown at heights between two m and 30 m above ground in order to determine if there is a discernible impact on the observed C/N0 values while the UAV was moving closer to the main lobe of the jammer. Nevertheless, the detector remained below the main beam of the jammer at all times during the second test flight.

4. Impact of 5G Ground Stations as RFI Sources

One aspect of this research with significant potential for impact is the presence of 5G ground stations which may act as RFI sources for the detector. The 5G network in Switzerland uses, among others, frequencies in the range of 1442 MHz and 1517 MHz, which is just below the L1 frequency of 1575 MHz. Depending on the hardware and frequency susceptibility of the equipment used, the 5G antennas may thus cause false detections for the proposed setup. We therefore also investigated the behavior of the equipment in an urban scenario on the roof top of a building with a 5G antenna 40 m away from the test setup.

III. RESULTS

This section presents the results of the jamming tests, as well as the impact of 5G antennas on the setup.

1. Field testing with directional jammer

The left plot in Figure 2 depicts the average C/N0 values for both antennas observed during the first flight. The jammer was located at a heading of approximately 248 ° from the location where the detector was flown. This corresponds well to a significant drop in average C/N0 of the aux1 antenna for headings around that value. At the same time the average C/N0 of the main antenna varies as well but to a much lesser degree. For headings between about 350 ° and 90 ° the UAV was hovering and pointing in the same direction for extended time periods leading to visible aggregations of data points. It can be noted that despite the UAV pointing in a constant direction, the average C/N0 value varies by up to two dB, however, the effect is visible on both antenna inputs.

The right plot in Figure 2 shows the corresponding test statistic. To enhance the clarity of the illustration, the periods of static hovering were trimmed from the test statistic plot. During this test, a clear peak with the maximum value of T reaching almost four dB at a heading of approximately 243 ° is observable. The triangular shape of the test statistic is consistent with the beam width of the antenna gain pattern of a directional antenna.

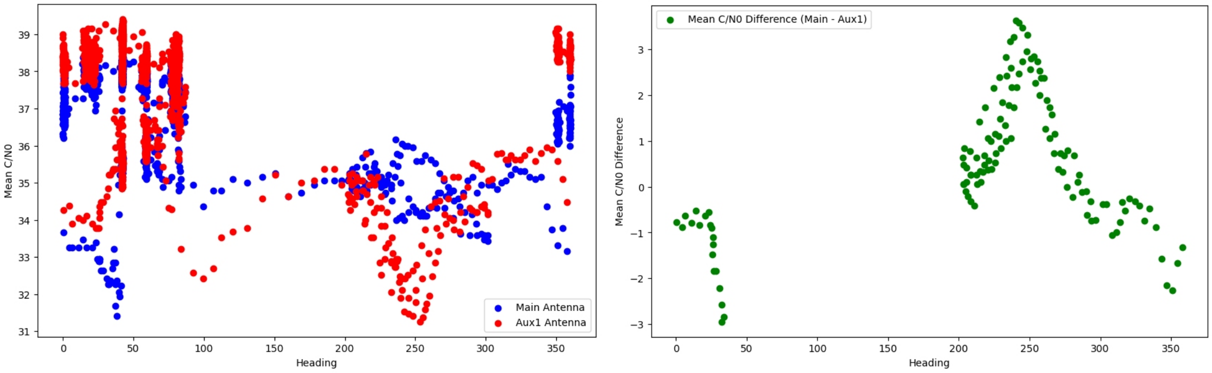

Figure 2: Average C/N0 values of main and auxiliary antenna for the first flight (left plot). Test statistic for first flight (right plot).

Figure 3 contains the observed C/N0 values of both antennas during the second flight, during which the beam of the jamming antenna was lowered by five ° and the UAV was flown at varying altitudes. There is a clear decreasing trend in the C/N0 on both antennas from about 38 dB to just about 26 dB while the UAV was ascending by about 22 m. The reduction in average C/N0 is similar for both antennas, consistent with the UAV being increasingly affected by the jammer as its altitude increases.

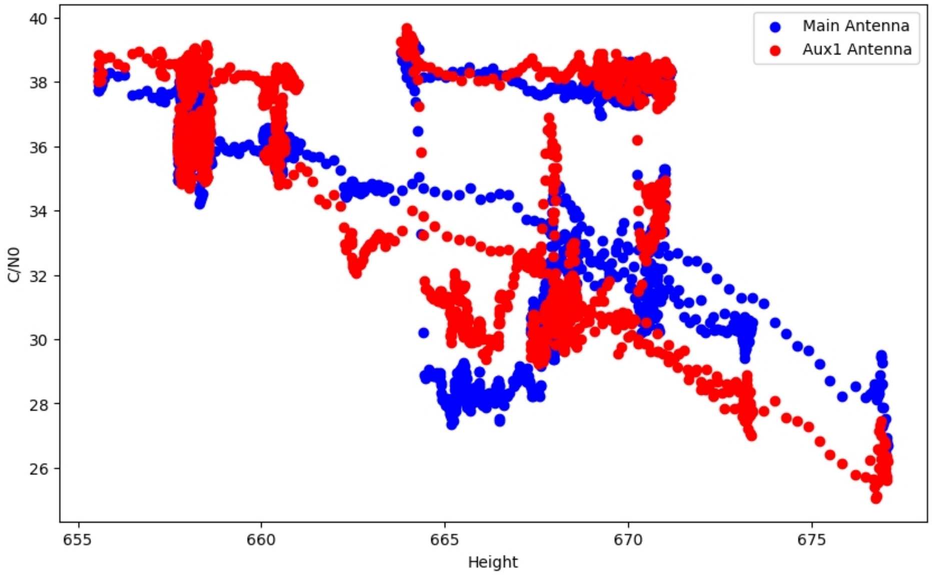

Figure 3: C/N0 of both antennas as a function of height while moving into the jamming signal from below.

Figure 4 shows the corresponding test statistic of the second flight. In comparison with the first test, this test statistic contains more variation. The peak value for T is slightly higher than four dB and consists of less data points, as the directional antenna was pointing towards the jammer for short periods only. It should be noted here that, despite not visible in the plot, the receiver was unable to determine the heading repeatedly.

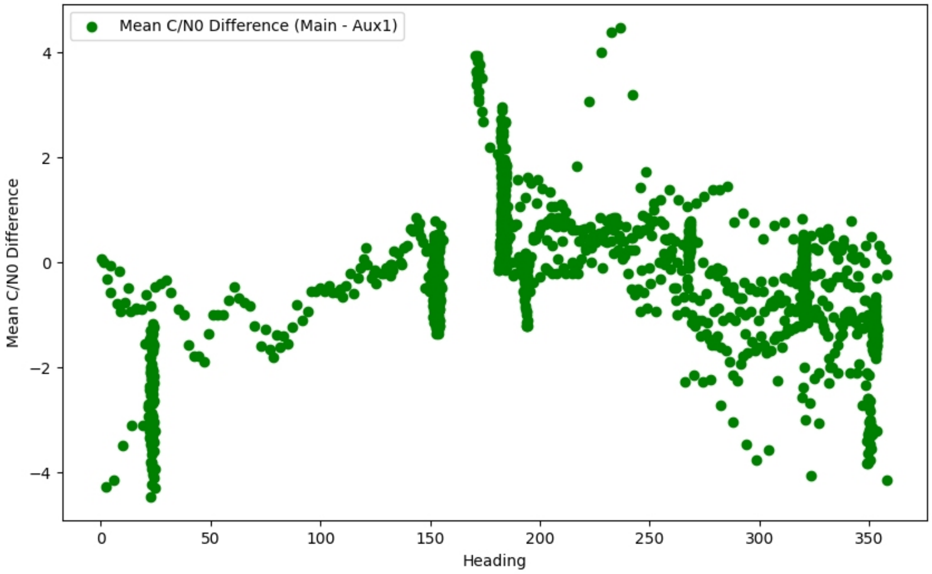

Figure 4: Test statistic of the second flight.

2. Impact of 5G Ground Stations

The setup was also examined at a distance of approximately 40 meters from a 5G base station antenna, as the proximity of the 5G frequency bands may have an impact on the detection capability. This test was conducted by just using the payload without having it mounted and flown on a UAV. The close proximity of the 5G frequency band to the GNSS L1 band resulted in discernible interference for the GPS L1 signals. Figure 5 depicts the observed average C/N0 values for the main and aux1 antenna port on the left and the corresponding test statistic on the right. The test statistic T reaches a maximum value of over 15 dB in this scenario. The corresponding heading output of the receiver is 206 ° with the true heading being 204 °.

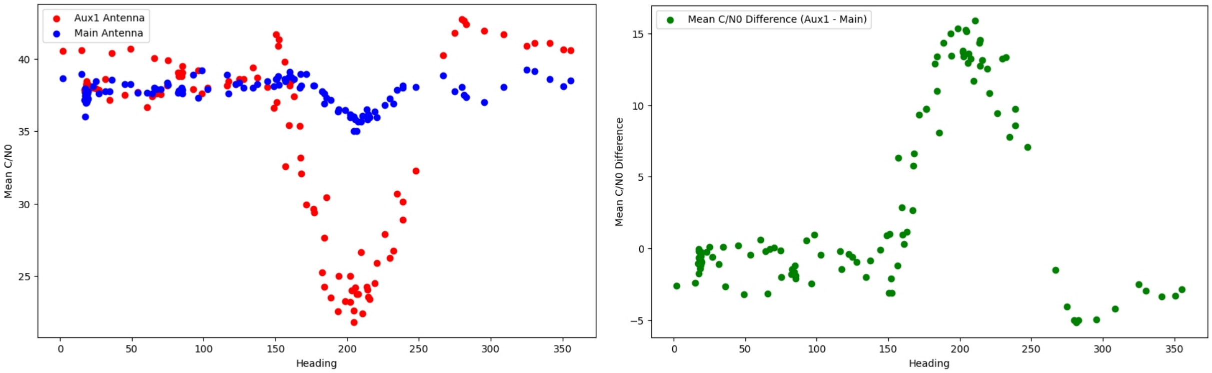

Figure 5: Average C/N0 values of main and aux antenna (left plot) and test statistic (right plot).

IV. DISCUSSION

The experimental results of this study, which are based on field tests with a directional jammer, suggest that the direction towards an RFI source can be determined using the measurement setup described. While being rather low-cost as well as easy to build and deploy, the proposed method also has several limitations. As indicated by the results, especially for the second test, the mean difference of the observed C/N0 values of the two antenna inputs exhibits a rather noisy behavior. One reason may lie within the test setup itself. The wiring, especially the power and USB cables, as well as the 4G mobile unit that was used for real-time monitoring may cause some level of unwanted interference with an impact on the received C/N0 values. Another issue may result from the antenna near field properties and different multipath effects on both antennas. The algorithm to estimate the jammer direction currently takes the maximum value of the test statistic with the corresponding heading as direction estimate. However, if the setup is not subject to jamming or the jamming power that is picked up does not lead to a test statistic that is large enough to create a clear signal in the noisy measurements, there is a high chance of obtaining an erroneous direction estimate. Furthermore, the method is limited to a minimum and a maximum use distance. On the one hand, if operated below the minimum distance to a jammer, the detector will not be able to determine a reliable heading anymore, or lose tracking altogether. Loss of track will first occur on the port with the combined GNSS and directional antenna resulting in a gap in the heading estimate and a loss of track of satellites. In that case, a reliable determination of the jammer direction becomes impossible. On the other hand, the maximum distance is limited by a minimum discernible change in C/N0 difference as described above. The test statistic may also be influenced by other signals in neighbouring frequency bands. The results shown for the test with a 5G base station antenna yielded a very significant peak in the test statistic. This may lead to wrongfully identifying other transmitters as potential jammers.

The proposed detection metric of using the difference of the average C/N0 still has potential for improvement. Depending on the impact the jammer creates, it might be beneficial to focus more on the satellites with high C/N0-values (to remain more robust in case of a stronger impact) or focus on satellites with low C/N0 in case of weak jamming impact as it might be more visible in these satellites. Moreover, the beam width of the directional antenna used is another key element of the method as it dictates the precision and accuracy of the estimation, which yields the bearing to the potential RFI source. The narrower the beam, the better the estimate can become. A reduction of the beam-width must typically be traded against increasing cost of the antenna. Furthermore, more dedicated filters blocking out signals from signals bands outside the GNSS frequency spectrum could be helpful in reducing the potential impact of 5G and other signal sourced that may impact the performance of the setup.

V. CONCLUSIONS AND OUTLOOK

As various RFI events in the past have impressively demonstrated, there is now a lack in the capability of timely locating sources of RFI. The method presented in this paper for identifying the direction of a jammer resembles a first step towards remedying this deficiency. Especially with the increased reliance on GNSS-based approach guidance in Europe mandated by the PBN implementation rule, it becomes highly important to be able to react quickly to potential RFI events. This is especially true as long as no aircraft-based solutions providing resilient GNSS navigation are widely available and in use. The results of this study suggest that it is feasible to determine the direction of arrival of RFI signals using heading information, two GNSS antennas, and a directional antenna. The current implementation aggregates C/N0 values for GPS and Galileo signals. However, the available hardware is also able to acquire signals from other constellations. Especially Glonass with its FDMA signal structure may be useful to increase robustness. Furthermore, depending on receiver capabilities, also using multiple frequencies can substantially improve the reliability and robustness of the results if jamming only affects one frequency band. The inclusion of other constellations and other frequencies is an item for future work.

When the direction estimation process is executed by several UAVs and the information about the estimated direction is shared, it may be possible to locate RFI sources rather quickly. Localizing the source based on a number of different direction estimates with varying quality and reliability poses its own challenges and is subject to further study. Also subject to future work is the communication aspect of how the information can be shared and aggregated.

ACKNOWLEDGEMENTS

This project was funded by armasuisse W+T under grant number 047-26. The authors greatly appreciate the support!

REFERENCES

Blois, M., Studenny, J., O'Keefe, K., and Liu, B. (2023). Baseline Spoofing Detection for Aircraft with Standard Navigation Hardware. pages 824–835, Denver, Colorado.

Cybersecurity & Infrastructure Securtiy Agency (CISA) (2022). Global Positioning System (GPS) Interference.

European Union Aviation Safety Agency (2023). *Safety Information Bulletin Operations–ATM/ANS Revision 2, Global Navigation Satellite System Outage and Alterations Leading to Navigation / Surveillance Degradation*. `https://ad.easa.europa.eu/blob/EASA_SIB_2022_02R2.pdf/SIB_2022-02R2_1`.

Felux, M., Figuet, B., Waltert, M., Fol, P., Strohmeier, M., and Olive, X. (2023). Analysis of GNSS disruptions in European Airspace. pages 315–326, Long Beach, California.

Fol, P. and Felux, M. (2022). Identification and operational impact analysis of GNSS RFI based on flight crew reports and ADS-B data. In *7th International Workshop on ATM/CNS (IWAC), Tokyo, Japan (online), 25-27 October 2022*, pages 33–40. Electronic Navigation Research Institute.

Joseph, A., Griggs, J., Bartolone, P., Schnaufer, B., Phan, H., and Malhotra, V. (2023). GNSS Radio Frequency Interference Mitigation in Collins Commercial Airborne Receivers. pages 836–855, Denver, Colorado.

Liu, Z., Blanch, J., Lo, S., and Walter, T. (2023). Investigation of GPS Interference Events with Refinement on the Localization Algorithm. pages 327–338, Long Beach, CA, USA. ISSN: 2330-3646.

Osechas, O., Fohlmeister, F., Dautermann, T., and Felux, M. (2022). Impact of gnss-band radio interference on operational avionics. *NAVIGATION: Journal of the Institute of Navigation*, 69(2).