Software detection and denying false GNSS data on open-source UAV autopilot

Bohdan Blazhei [1,†], Vitalii Larin[1,†] and Nataliia Kuzmenko[1,†]

[1] *National Aviation University, Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine*

Abstract

Performing safe flights of unmanned aerial vehicles (UAV) in busy areas is crucial to ensure their seamless integration into our modern-day tasks. The most popular UAV autopilot solutions show that safety could be easily tampered with by intended purposes or by interference caused by surrounding equipment. Modifications of the extended Kalman filter filter, which most autopilots use for navigation solution estimation, have been introduced in the paper to minimize the effect of interference. Results of the study present flight data collected and processed by common UAV autopilot unit during normal operation.

Keywords

air navigation, GNSS, extended Kalman filter, UAV, ardupilot, INS, FMU

1. Introduction

The technology of unmanned aviation is an excellent example of modern engineering where the interaction of the drone's design, its software-controlled electronic equipment, and information technology is combined. Only the combined interaction of these components makes both the flight of the unmanned aerial vehicle (UAV) and the maintenance of it and its ground station possible. The vast majority of professional and regular users, engineers, and UAV pilots are familiar with the flight planning software Mission Planner. Information technologies are used to solve tasks related to designing components of unmanned aviation systems, simulation of the flight of UAV, and simulating the characteristics of its components. The widespread use of software allows for the development of algorithms for upgrading and improving various aspects related to unmanned aviation systems. One of the most popular solutions for onboard software is Ardupilot and PX4, which are open-source flight control software that runs on standardized hardware of flight management unit.

CMSE'24: International Workshop on Computational Methods in Systems Engineering, June 17, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

4538392@stud.nau.edu.ua (B. Blazhei); vjlarin@gmail.com (V. Larin); nataliiakuzmenko@ukr.net (N. Kuzmenko)

0009-0005-3616-4239 (B. Blazhei); 0000-0002-5042-2426 (V. Larin); 0000-0002-1482-601X (N. Kuzmenko)

2. Related works

The main intellectual component of UAV is autopilot, which combines the aircraft control system and the navigation system. The navigation component of a UAV can be conditionally divided into two parts: one that depends on external signals and one that is autonomous. The set of navigation equipment on board a UAV is currently not clearly defined due to existing technical and organizational-regulatory issues. In the field of civil UAV applications, researchers pay considerable attention to aspects of ensuring UAV flight safety, which is the primary task of civil aviation. Flight safety depends on a significant number of factors. For example, an onboard weather radar is not standard equipment for UAVs, but its absence can, under certain circumstances, increase flight safety risks. The presence of such a component enhances the level of situational awareness about various meteorological phenomena. The algorithm presented in [1] will allow identifying the degree of turbulence intensity.

Much attention is paid to the search for new navigation solutions. For instance, navigation tasks are proposed to be solved through relative navigation of moving objects by correcting navigation decisions from mobile communication station signals [2]. Researchers also focus significantly on independent navigation systems. In [3], a local orientation system containing an inertial measurement unit and a magnetometric sensor is proposed, which algorithmically accounts for interference signals from powerful electromagnetic radiation sources. The improvement of navigation tools themselves is also being investigated.

Paper [4] proposes the structure of an inductive magnetometric sensor with non-orthogonal sensitivity axes, which is used to determine the course of the aircraft. The flight duration of electrically powered UAVs is influenced by the capacity of the battery.

The authors of [5] propose an algorithm for the onboard battery management system based on developed fuzzy logic rules, which allows predicting the impact of external factors such as temperature, humidity, and crosswind effects on the battery discharge rate. Algorithms for computing navigation data are also a relevant area of research.

In the articles [2, 6], an economic method, in terms of computational power, is developed to minimize the errors of trajectory measurements obtained from an automatic dependent surveillance device or a barometric altimeter. The issue of operational reliability is also an important research task.

Researchers [7] propose a hierarchical monitoring system built to support the life cycle of aviation equipment. The use of the regression model proposed by the authors [8] will improve the accuracy of assessing the degree of degradation of aviation tools.

The authors [9] examine a 15-state extended Kalman filter (EKF) and a hybrid architecture combining a six-state nonlinear complementary filter (NCF) with a nine-state EKF. They integrate GPS data with inertial measurement units, which include three-axis accelerometers, three-axis rate gyros, and a three-axis magnetometer, in an open-loop configuration to estimate navigation states. These architectures were assessed in the closed-loop guidance of the Black-Kite MAV using a software-in-the-loop simulation (SILS) setup. Both algorithms are validated using flight test data recorded by an on-board data logger on an off-the-shelf autopilot board (Ardupilot Mega APM-2.5) mounted on the “Slybird” UAV [10, 11]. The proposed architectures

are crucial for achieving fusion of inertial navigation system and global navigation satellite system (GNSS) sensors, which is essential for the autonomous guidance and navigation of UAVs. The paper presents two INS/GNSS fusion/filter algorithms for Black-Kite MAV, evaluating their performance in the SILS setup. The filters are evaluated with position, velocity, attitude, and heading estimates from both fusion architectures. The performance of both filters is compared with the flight test data of SLYBIRDUAV, obtained from the autopilot board ARDUPILOT MEGA (APM-2.5) with onboard MEMS sensors and data logger. The paper presents two INS/GNSS mathematical model formulations: first, 15-state EKF, and second, NCF-EKF split architecture with six-state NCF and nine-state EKF [12]. The MEMS sensor suit for signal measurements consists of tri-axial accelerometers, tri-axial gyroscopes, tri-axial magnetometer, and GNSS. The constant bias components are constant null-shift bias terms, while the accelerometer measurements are modeled as zero mean, band-limited AWGN processes with covariances. The 15-state EKFN model excludes the effect of Earth's rotation rate, and the INS/GNSS model in the local North-East-Down frame is used. The six-state NCF is used for estimating attitudes and rates bias, while the nine-state EKF is used for estimating position and velocity. This approach allows for practical realization of estimation problems, such as providing decent attitude solutions during GNSS outages. Spoofing is the practice of replicating false signals with the same code phase, carrier frequency, and Doppler frequency shift as the real navigation satellite signal to achieve interference and capture [13].

After introduction of GNSS spoofing technology, the research progress of GNSS anti-spoofing technology over the last decade is summarized. A new classification standard is proposed for anti-spoofing technology and the implementation difficulty, effect, and adaptability of the current main spoofing detection technologies are analyzed and compared. Spoofing is the practice of replicating false signals with the same code phase, carrier frequency, and Doppler frequency shift as the real navigation satellite signal to achieve interference and capture. It has become a hotspot for satellite navigation interference technology due to its advantages in interference concealment and efficiency. Spoofing of GNSS involves broadcasting false signals to make the victim receiver misunderstand them as real signals, leading to incorrect positioning and timing, potentially causing dangerous behavior. GNSS anti-spoofing technology aims to detect attacks and warn victims that their navigation and clock are unreliable. Onboard receivers with receiver autonomous integration monitoring technology (RAIM) use redundant signals by default to generate multiple positions for comparison. However, some spoofing methods may exceed USE's basic defense capability. This paper introduces the development of satellite navigation spoofing technology, focusing on GNSS positioning principles, vulnerabilities, spoofing attack methods, and defense methods. GNSS vulnerability is based on three main factors: disclosure of navigation signal format, disclosure of navigation data format, and an unprotected broadcast channel. GNSS uses three public frequencies which expose the spectrum characteristics, signal modulation format, and pseudo-random code sequence. This allows spoofers to take targeted spoofing actions based on relevant signal parameters and characteristics. GNSS message data, such as ephemeris, almanac, satellite clock parameters, and ionosphere/troposphere, are disclosed to facilitate user use. GNSS's broadcast communication mode exposes its communication channel to interference, monitoring, and tampering. GNSS

spoofing involves transmitting a signal with the same structure and power as the satellite signal, causing the target to mistakenly think it is a real signal and search for and capture it. Spoofing affects satellite navigation signal processing, which includes RF front-end processing, baseband IF signal processing, and navigation information output [10].

The researchers [14, 15] propose a Kalman Filter design to detect spoofing using residual analysis and provide countermeasures. The performance of the filter is tested using Monte-Carlo simulations. The results show that the proposed filter is successful in detecting spoofing attacks and correcting position and velocity estimations, reducing vulnerability against spoofing and increasing the robustness of the navigation solution. The Kalman Filter design is proposed for detecting spoofing attacks in GNSS receivers. The filter structure includes initial states, error covariance matrix, and state estimations. The filter operates at a frequency of 5 Hz, with GNSS measurements coming every 1 second. The residual generation is added to the filter to detect anomalies. When an anomaly is detected for 10 time steps, it is considered a spoofing attack.

Dynamic calibration and compensation method is proposed in [16] for errors caused by time-gap between two asynchronous INS in carriers. The method analyzes and models the causes of asynchronous time from different INSs, establishing an online estimation and compensation Kalman filter for asynchronous time. Simulation results show the proposed method can achieve an estimation accuracy of 0.027ms for the asynchronous time between different INSs, improving the accuracy and stability of the fusion algorithm. A framework for GNSS spoofing detection combines multiple metrics with a fixed false alert probability, achieving over 70% reduction in worst-case missed detection probability compared to conventional metric combination techniques. This is particularly important for real-time applications [17]. Based on the traditional principle of using a multi-antenna carrier phase to solve DOA, this paper [18] innovatively solves the following problems: the poor direction-finding accuracy caused by the unstable phase center of low-cost commercial antennas, the low success rate of spoofing detection in a multipath environment, and the inconsistent sampling time among multiple low-cost commercial GNSS boards. Monte Carlo simulations are carried out to verify our analysis, which shows the effectiveness of the Kalman filter innovation-based spoofing detection method against ramp-type fault profiles and the advantages of measurement averaging over innovation averaging in certain spoofing scenarios [19]. In the GNSS/RINS integrated navigation system, the results of RINS are free from external interference and have sufficient accuracy in a short time [20].

The paper [21] analyzes the detection performance of a signal quality monitoring (SQM) method for detecting GNSS spoofing, focusing on the fusion of metrics using an “OR” rule and determining optimal thresholds and detection probability. To effectively combat intermediate spoofing signals, this paper presents an enhanced spoofing detection method based on abnormal energy of the quadrature (Q) channel correlators [22]. The extended Kalman filter estimated position and velocity of the receiver is used along with the satellite position and velocity computed from ephemeris to find out the range and range rate of each of the satellites to the receiver [23].

The test [24] is based on the generalized likelihood ratio test (GLRT) paradigm and essentially performs a consistency check between the set of observed range measurements and known information about the satellite topology and the geometry of the receiver constellation. This

paper [25] presents a framework for GNSS spoofing detection using the Generalized Likelihood Ratio Test, demonstrating robustness against various attack modes and ensuring false alert probability under the Neyman-Pearson paradigm.

3. Problem statement

A receiver of GNSS is an integral component of most UAV navigation systems. Today, several GNSS are actively functioning, with dozens of satellites in Earth's orbits providing signals to users and enabling highly accurate determination of object coordinates.

One of the weaknesses of satellite navigation is the vulnerability of the signals received by the onboard navigation system receiver to external interference of natural and artificial origin. An especially dangerous factor affecting UAV navigation systems is deliberate interference, which involves substituting the true satellite system signals with an external “satellite-like” false signal, usually of higher power. This allows the owner of such a signal, by generating the required sequences, to direct the UAV's flight according to their own scenario. This type of interference is known as "spoofing". Spoofing is more subtle than jamming and relies on generating a counterfeit signal with just the right strength to “lift” a timer or navigation receiver from the legitimate signal [14]. The ultimate goal of such spoofing influence is either an aviation disaster of the affected UAV or diverting the UAV significantly away from the flight path designated by preprogrammed waypoints.

One of the most common open-source software environments for UAV flight control today is Ardupilot, which can interact with a wide range of hardware systems. When performing UAV flights using Ardupilot as an autopilot in complex radio conditions with standard onboard GNSS receivers, a threatening situation may arise during the flight. When the UAV enters a zone with satellite navigation signal suppression, the GNSS receiver data transmitted to the flight controller is incorrect, specifically exhibiting a jumpy, prolonged change in the current coordinates and flight altitude reported by the receiver. This problem is quite relevant as it significantly and directly affects the safety of UAV flights.

4. Data acquired during GNSS jamming and spoofing

In order to proceed with practical data gathering a test environment was setup. An electronic warfare system Bukovel-AD was used [26]. Test airframe type is VTOL (vertical take-off and landing) airplane. Flight plan included takeoff on VTOL to height of 50m, climb to 900m AGL (above ground level), performing flight in range of 10 km from Bukovel-AD.

During the test flight the following equipment have been used: HEX Cube Orange+ (autopilot); ArduPlane V 4.4.1 (firmware), and Ublox F9P (GNSS receiver). Trajectory data for test flight are presented in Figure 1 and Figure 2.

Climbing mode is indicated from 22:21 until 22:29 in Figure 1. At 22:29:45 we get first signs of sudden dip in altitude received from Ublox F9P. Next 22:30:20 we get second sudden dip in altitude, at 22:34 we see that spoofing modified altitude of receiver up to 2100m AGL in less than 5s time, after which telemetry link also has been jammed and ground station stop receive any data.

Figure 2 is showing data correlation between altitude reported by GNSS receiver, satellites visibility and EKF vertical variance. We can clearly see pattern, when spoofing is engaged satellites visibility suddenly drops to about 2-4 satellites and variance error rising.

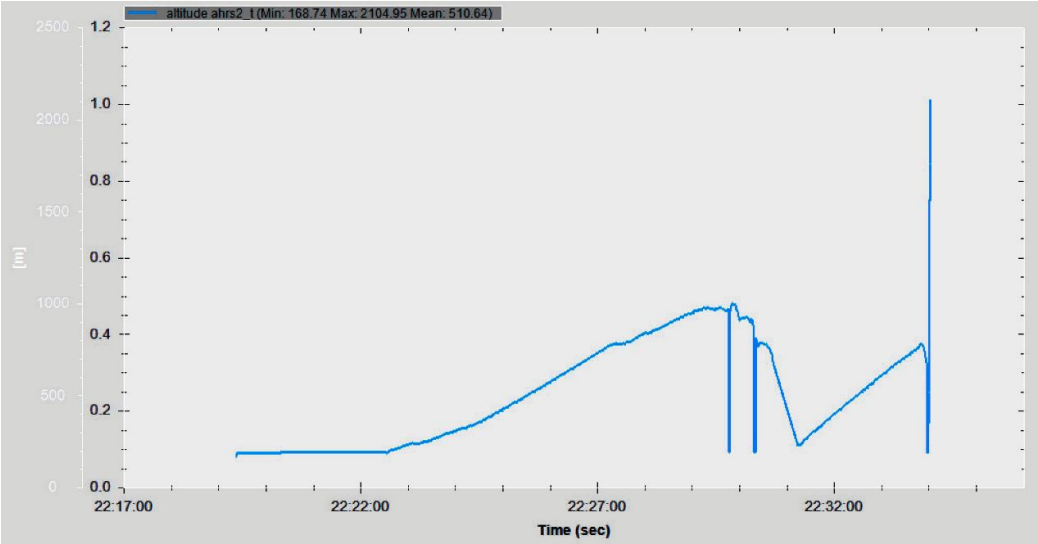

Figure 1: Altitude interference of GNSS receiver.

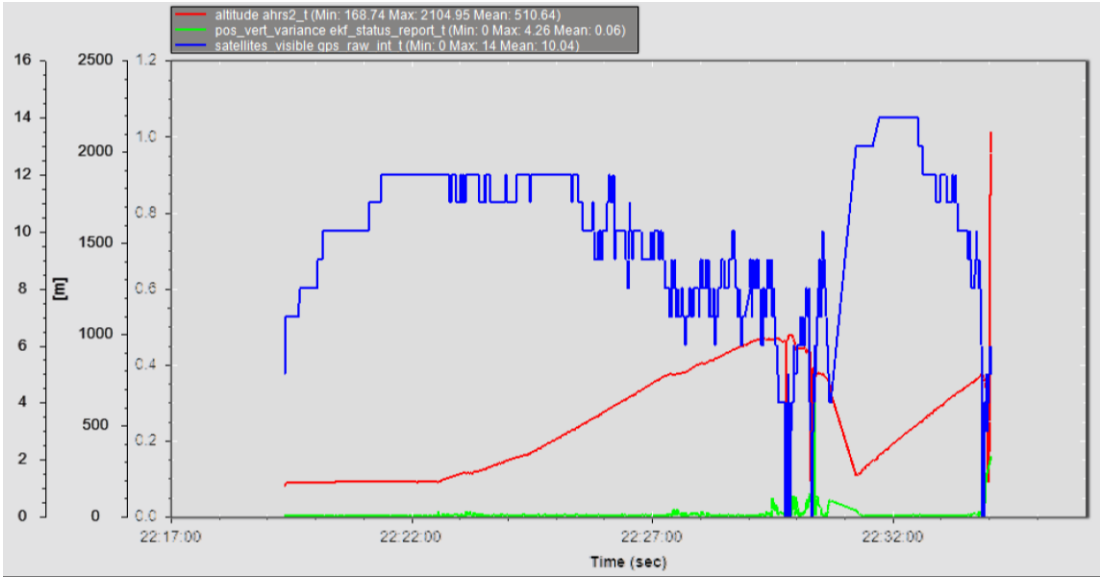

Figure 2: Satellite status, EKF vertical variance and altitude.

Figure 3 shows real time EKF status during active spoofing. Almost all lanes of EKF processing inconsistent data and trying to deny any false data but after sustained amount of time under influence it cannot longer provide stable flight.

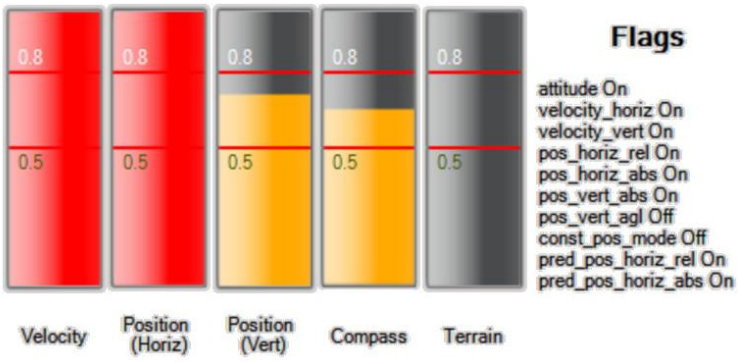

Figure 3: EKF Status during interference.

The objective of this research is to create a method to counteract or eliminate spoofing signals through the implementation of relatively simple algorithms, if possible, which can be realized by modifying the widely used UAV flight control software, specifically Ardupilot, thanks to its open-source code.

5. Automatic data selection algorithm for EKF

As is known, various modifications of the Kalman filter are used in integrated navigation systems for UAVs. The Extended Kalman Filter (EKF) algorithm is employed to estimate position, speed, and angular orientation based on measurements from gyroscopes, accelerometers, compasses, GNSS, velocity, and barometric pressure. The advantage of EKF over simpler complementary filter algorithms, such as the direct cosine matrix (DCM), is that it effectively rejects data from measurements containing significant errors through the comprehensive processing of all available measurements. This makes the aircraft less sensitive to temporary failures of a single sensor. EKF also allows for the inclusion of measurements from other sensors, such as optical flow sensors and laser rangefinders, which are used as auxiliary tools in navigation [13].

To prevent interference in the operation of the extended Kalman filter, a modification has been proposed. The essence of this modification is to prevent unreliable data from affecting the navigation calculation system by modifying the EKF3 algorithm in the Ardupilot software [25]. The modification is possible because Ardupilot software has an open codebase, fully allowing the implementation of custom scenarios. The proposed modification involves incorporating a subroutine in EKF3 to filter values from the GNSS receiver, such as altitude and ground speed. This comparison of values will occur within the AP_NavEKF3_core [14]. The algorithm provides for the automatic disconnection of GNSS data from EKF3 when the threshold difference values between INS (inertial navigation system) and GNSS measurements are exceeded, enabling the UAV to switch to flight mode based solely on INS data. Re-enabling GNSS can be done either automatically or by modifying the software of the ground control station, Mission Planner. Figure 4 presents an option for introducing an additional GNSS state switching command in the program interface. To implement this function, the software of Mission Planner and Ardupilot was modified. The command is sent via Mavlink2 message through the telemetry link. Figure 5 shows what sensors are EKF processing.

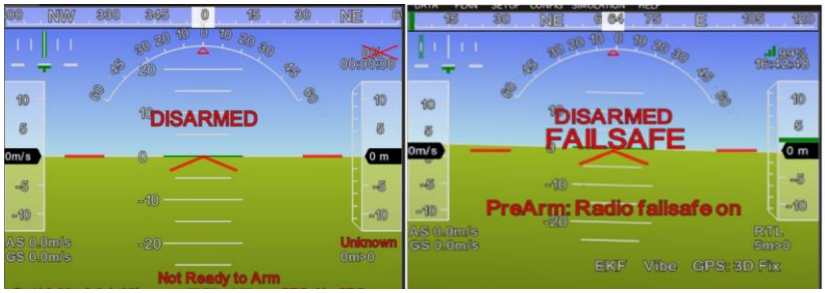

Figure 4: Manual GNSS disable/enable function.

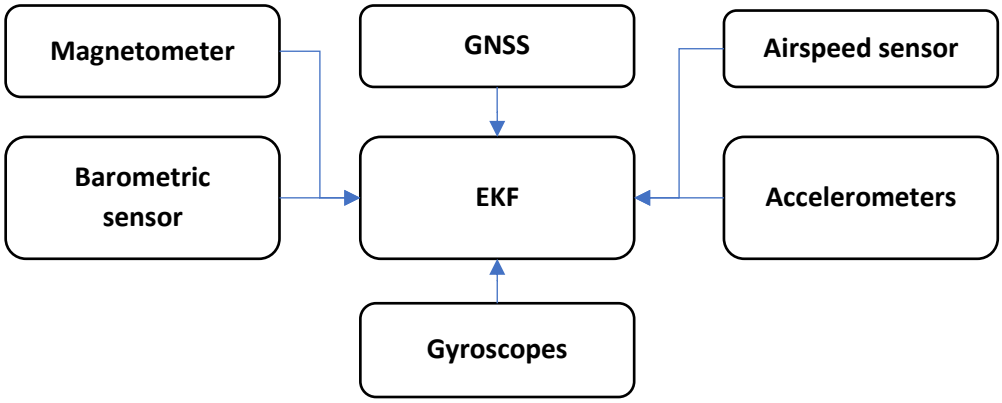

Figure 5: Operation during manually disabled GNSS data.

The EKF instantiates multiple instances of the filter called “lanes”. The primary lane is the one that provides state estimates, rest are updated in the background and available for switching to. The number of possible lanes is exactly equal to the number of IMUs enabled for use. Conventionally, each lane uses the primary instance of the Airspeed, Barometer, GNSS and Magnetometer sensors.

6. Conclusions

The study highlights the susceptibility of UAV navigation systems to external interference, particularly spoofing, which can lead to aviation disasters or significant deviations from the flight path. A modification to the EKF3 algorithm in the Ardupilot software is proposed to filter out unreliable GNSS data, enhancing the safety and reliability of UAV flights. Automatic Data Selection, modified algorithm allows for the automatic disconnection of GNSS data when discrepancies with INS measurements are detected, enabling the UAV to rely solely on INS data for navigation.

References

[1] Y. Averyanova, V. Larin, N. Kuzmenko, I. Ostroumov, M. Zaliskyi, O. Solomentsev, O. Sushchenko, Y. Bezkorovainyi, Turbulence detection and classification algorithm using data

from AWR, in: Proceedings of IEEE 2nd Ukrainian Microwave Week (UkrMW), Kyiv, Ukraine, 2022, pp. 518–522. doi: 10.1109/UkrMW58013.2022.10037172.

[2] I. Ostroumov, N. Kuzmenko, Y. Bezkorovainyi, Y. Averyanova, V. Larin, O. Sushchenko, M. Zaliskyi, O. Solomentsev, Relative navigation for vehicle formation movement, in: Proceedings of the 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 2022, pp. 1–4. doi: 10.1109/KhPIWeek57572.2022.9916414.

[3] O. Sushchenko, Y. Bezkorovainyi, V. Golitsyn, N. Kuzmenko, Y. Averyanova, M. Zaliskyi, I. Ostroumov, V. Larin, O. Solomentsev, Integration of MEMS inertial and magnetic field sensors for tracking power lines, in: Proceedings of the XVIII International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2022, Polyana, Ukraine, 2022, pp. 33–36. doi: 10.1109/MEMSTECH55132.2022.10002907.

[4] O. Sushchenko, Y. Bezkorovainyi, O. Solomentsev, N. Kuzmenko, Y. Averyanova, M. Zaliskyi, I. Ostroumov, V. Larin, V. Golitsyn, Airborne sensor for measuring components of terrestrial magnetic field, in: Proceedings of the 41st International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2022, pp. 687–691. doi: 10.1109/ELNANO54667.2022.9926760.

[5] V. Larin, O. Solomentsev, M. Zaliskyi, A. Shcherban, Y. Averyanova, I. Ostroumov, N. Kuzmenko, O. Sushchenko, Y. Bezkorovainyi, Prediction of the final discharge of the UAV battery based on fuzzy logic estimation of information and influencing parameters, in: Proceedings of the 3rd KhPI Week on Advanced Technology (KhPIWeek), Kharkiv Ukraine, 2022, pp. 1–6. doi: 10.1109/KhPIWeek57572.2022.9916490.

[6] N. Kuzmenko, I. Ostroumov, Y. Bezkorovainyi, Y. Averyanova, V. Larin, O. Sushchenko, M. Zaliskyi, O. Solomentsev, Airplane flight phase identification using maximum posterior probability method, in: Proceedings of the 3rd International Conference on System Analysis & Intelligent Computing (SAIC), Kyiv, Ukraine, 2022, pp. 1–5. doi: 10.1109/SAIC57818.2022.9922913.

[7] O. Solomentsev, M. Zaliskyi, O. Sushchenko, Y. Bezkorovainyi, Y. Averyanova, I. Ostroumov, V. Larin, N. Kuzmenko, Data processing through the lifecycle of aviation radio equipment. in: Proceedings of the 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022, pp. 146–151. doi: 10.1109/CSIT56902.2022.10000844.

[8] M. Zaliskyi, O. Solomentsev, V. Larin, Y. Averyanova, N. Kuzmenko, I. Ostroumov, O. Sushchenko, Y. Bezkorovainyi, Model building for diagnostic variables during aviation equipment maintenance, in: Proceedings of the 17th International Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 2022, pp. 160–164. doi: 10.1109/CSIT56902.2022.10000556.

[9] A. Sanketh, INS/GPS Fusion Architectures for Unmanned Aerial Vehicles, International journal of intelligent unmanned Systems 2 (2014) 154–167. doi:10.1108/IJIUS-03-2014-0001.

[10] M. Lianxiao, L. Yang, W. Yang, L. Zhang, A Survey of GNSS Spoofing and Anti-Spoofing Technology, Remote Sensing 14 (2022) 4826. doi:10.3390/rs14194826.

[11] Dronecode Foundation. (2023, January 31). Standards - Pixhawk. Pixhawk. URL: https://pixhawk.org/standards.
[12] Extended Kalman Filter (EKF), Copter documentation. URL: https://ardupilot.org/copter/docs/common-apm-navigation-extended-kalman-filter-overview.html.
[13] D. Schmidt, K. Radke, S. Camtepe, E. Foo, M. Ren, A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures, ACM Computing Surveys 48 (2016) 1–31.
[14] ArduPilot. GitHub. ArduPilot/ardupilot: ArduPlane, ArduCopter, ArduRover, ArduSub source. GitHub. URL: https://github.com/ArduPilot/ardupilot.
[15] H. Akcay, E. Onat, Kalman Filter Design For Spoofing Detection and Anti-Spoofing in GNSS Receivers. 2022.
[16] W. Liang, K. Li, A Dynamic Calibration and Compensation Method for the Asynchronous Time Between Two Inertial Navigation Systems, IEEE Sensors Journal 21(8) (2021) 10091–10101. doi:10.1109/JSEN.2021.3049122.
[17] F. Rothmaier, Y. Chen, S. Lo, T. Walter, A Framework for GNSS Spoofing Detection Through Combinations of Metrics, IEEE Transactions on Aerospace and Electronic Systems 57(6) (2021) 3633–3647. doi:10.1109/TAES.2021.3082673.
[18] P. Mao, H. Yuan, X. Chen, Y. Gong, S. Li, R. Li, R. Luo, G. Zhao, C. Fu, J. Xu, A GNSS Spoofing Detection and Direction-Finding Method based on Low-Cost commercial board components. Remote Sensing 15(11) (2023) 2781. doi:10.3390/rs15112781.
[19] Y. Liu, S. Li, Q. Fu, Z. Liu, Q. Zhou, Analysis of Kalman Filter Innovation-Based GNSS Spoofing Detection Method for INS/GNSS Integrated Navigation System, IEEE Sensors Journal 19(13) (2019) 5167–5178. doi:10.1109/JSEN.2019.2902178.
[20] W. Liang, K. Li, Q. Li, Anti-spoofing Kalman filter for GPS/rotational INS integration, Measurement 193 (2022) 110962. doi:10.1016/j.measurement.2022.110962.
[21] K. Benachenhou, M. Bencheikh, Detection of global positioning system spoofing using fusion of signal quality monitoring metrics, Computers & Electrical Engineering 92 (2021) 107159. doi:10.1016/j.compeleceng.2021.107159.
[22] J. Wang, X. Tang, P. Ma, J. Wu, C. Ma, G. Sun, GNSS Spoofing Detection Using Q Channel Energy, Remote Sensing 15(22) (2022) 5337. doi:10.3390/rs15225337.
[23] V. Vinoj, V. Lalu, INS aided spoofing detection of high dynamic GNSS receiver for launch vehicle applications: A loosely coupled approach, Advances in Space Research 3 (2024) 18. doi:10.1016/j.asr.2024.03.018.
[24] A. Kalantari, E. Larsson, Statistical test for GNSS spoofing attack detection by using multiple receivers on a rigid body, EURASIP Journal on Advances in Signal Processing 1 (2020) 1–16. doi:10.1186/s13634-020-0663-z.
[25] F. Rothmaier, L. Taleghani, Y. Chen, S. Lo, E. Phelts, T. Walter, GNSS Spoofing Detection through Metric Combinations: Calibration and Application of a General Framework, In: 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, Missouri, 2021, pp. 4249–4263. doi:10.33012/2021.18126.
[26] Bukovel-AD Technical manual. URL: https://spetstechnoexport.com/product/bukovel-ad.
[27] EKF3 Affinity and lane switching. Copter documentation. URL: https://ardupilot.org/copter/docs/common-ek3-affinity-lane-switching.html.