A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS

Task 4: Test Plan and Report

July 6, 2023

NOTICE

LEGAL DISCLAIMER

The information provided herein may include content supplied by third parties. Although the data and information contained herein has been produced or processed from sources believed to be reliable, the Federal Aviation Administration makes no warranty, expressed or implied, regarding the accuracy, adequacy, completeness, legality, reliability or usefulness of any information, conclusions or recommendations provided herein. Distribution of the information contained herein does not constitute an endorsement or warranty of the data or information provided herein by the Federal Aviation Administration or the U.S. Department of Transportation. Neither the Federal Aviation Administration nor the U.S. Department of Transportation shall be held liable for any improper or incorrect use of the information contained herein and assumes no responsibility for anyone's use of the information. The Federal Aviation Administration and U.S. Department of Transportation shall not be liable for any claim for any loss, harm, or other damages arising from access to or use of data or information, including without limitation any direct, indirect, incidental, exemplary, special or consequential damages, even if advised of the possibility of such damages. The Federal Aviation Administration shall not be liable to anyone for any decision made or action taken, or not taken, in reliance on the information contained herein.

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. A11L.UAS.86	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle A11L.UAS.86 - A44 Mitigating GPS and ADS-B Risks for UAS Task 4: Test, Analysis, and Demonstration of Mitigations Report		**5. Report Date** July 6, 2023 **6. Performing Organization Code**
7. Author(s) University of North Dakota William Semke, william.semke@und.edu Prakash Ranganathan, prakash.ranganathan@und.edu Kansas State University Randall Nichols, profrknichols@ksu.edu Embry-Riddle Aeronautical University Hever Moncayo, moncayoh@erau.edu Oregon State University Jihye Park, jihye.park@oregonstate.edu		**8. Performing Organization Report No.**
9. Performing Organization Name and Address University of North Dakota 243 Centennial Dr. Grand Forks, ND 58202		**10. Work Unit No.** **11. Contract or Grant No.**
12. Sponsoring Agency Name and Address FAA		**13. Type of Report and Period Covered** **14. Sponsoring Agency Code** 5401
15. Supplementary Notes		

16. Abstract

The A44 team has completed the testing, analysis, and demonstration of mitigations report which fulfills Task 4 for the A44 ASSURE project. Select mitigation strategies and test plans were chosen from previous reports. It prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable whose test plans were developed in the Task 3 report. It places particular emphasis on prioritizing mitigations that support sUAS operations that were tested in Task 4. The use of simulated flight data is a significant source of the test data used for evaluation.

17. Key Words GPS, ADS-B, signal dropouts, erroneous data, jamming, spoofing	**18. Distribution Statement** No restrictions. This document is available through the National Technical Information Service, Springfield, VA 22161.		
19. Security Classification (of this report) Unclassified	**20. Security Classification (of this page)** Unclassified	**21. No. of Pages** 101	**22. Price**

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TABLE OF ACRONYMS

1090ES	1090 Extended Squitter Data Link
A/C	Aircraft
ADS-B	Automatic Dependent Surveillance
A-GPS	Assisted Global Positioning System
ATC	Air Traffic Control
ATM	Air Traffic Management
ATS	Air Traffic Services
C2	Command and Control
C/A	Coarse Acquisition
CCC	Circular Cross Correlation
CD	Collective Detection
COTS	Commercial Off-The-Shelf
CTN	Course -Time Navigation
DAA	Detect and Avoid
ECD	Eichelberger's Collective Detection
EKF	Extended Kalman Filter
ESE	ERAU Simulation Environment
ERAU	Embry Riddle Aeronautical University
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
GMA	Geomagnetic Algorithm
GNAV	Geomagnetic based Navigation
GNSS	Global Navigation Satellite System
GSFD	Ground Station Flood Denial jamming
GPS	Global Positioning System
HOW	Hand-Over-Word
ICAO	International Civil Aviation Organization
IMU	Inertial Measurement Unit
KSU	Kansas State University
MLAT	Multilateration System
NAC	Navigation Accuracy Category
NDM	Navigation Data Modification
NIC	Navigation Integrity Category
OrSU	Oregon State University
PRN	Pseudo Random Noise
RINEX	Receiver Independent Exchange
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
SIB	System Information Block
SIB2	System Information Block Type 2
SIC	Successive Signal Interference Cancellation
SIL	Surveillance Integrity Level

SNR	Signal to Noise Ratio
SSLT	Seamless Satellite-Lock Takeover
SSR	Secondary Surveillance Radar
sUAS	Small Uncrewed Aircraft System
SV	Space Vehicle
TCAS	Traffic Collision Avoidance System
ToF	Time of Flight
UAS	Uncrewed Aircraft System
UAF	University of Alaska Fairbanks
UAV	Uncrewed Aerial Vehicle

EXECUTIVE SUMMARY

Unvalidated or unavailable Automatic Dependent Surveillance-Broadcast (ADS-B) and Global Position Systems (GPS) data poses security and safety risks to automated Uncrewed Aircraft Systems (UAS) navigation and to Detect and Avoid (DAA) operations. Erroneous, spoofed, jammed, or drop outs of GPS data may result in uncrewed aircraft position and navigation being incorrect. This may result in a fly away beyond radio control, flight into infrastructure, or flight into controlled airspace. Erroneous, spoofed, jammed, or drop outs of "ADSB-In" data may result in automated uncrewed aircraft being unable to detect and avoid other aircraft or result in detecting and avoiding illusionary aircraft. For automated DAA, a false ADS-B track can potentially be used to corral the uncrewed aircraft to fly towards controlled airspace, structures, terrain, and so on. This research is necessary to enable safe and secure automated small UAS (sUAS) navigation and DAA operations. Goals for the project include reports and recommendations useful for Federal Aviation Administration (FAA) policy development and UAS standards development. It is expected that this information will be used to better understand the risks and potential mitigations, and to help the FAA to reassess and refine FAA policy with respect to validation of ADS-B data.

The A44 team has completed the testing, analysis, and demonstration of mitigations report which fulfills Task 4 for the A44 ASSURE project. Select mitigation strategies and test plans were chosen from previous reports. This report prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. These test plans were developed in the Task 3 report. This report places particular emphasis on prioritizing mitigations that support sUAS operations that were tested in Task 4. The use of simulated flight data is a significant source of the test data used for evaluation.

The integrity of ADS-B and GPS navigation systems were tested to detect threats to the integrity and/or reliability of the data. These risks include dropped, erroneous, spoofed, and jammed data from GPS and/or ADS-B systems. Several mitigation schemes were flight and simulation tested based on their potential effectiveness in jamming and spoofing conditions. The mitigation schemes tested are cellular signal navigation, the Eichelberger's Collective Detection (ECD) method, optical flow, and geomagnetic navigation. Previous results indicate that these have an overall high effectiveness rating, while having varying effectiveness in the individual factors scored.

The UAS anomalies section focused on using ADS-B data sets to identify ADS-B anomalies that would result in ceasing operations and identify the scenarios that are most common. The data analyzed was collected by using flight test operations at UAF as well as from a unique case study of public use ADS-B data from the Dallas Fort Worth airport. Additional metrics are recommended for ADS-B reception quality and the distance and altitudes of the ADS-B receiver and transmitting aircraft. The DFW case clearly illustrated the possibility of extended loss of ADS-B signals and the subsequent need for mitigation strategies. In Section 3, flight tests were developed to record and utilize nearby LTE/4G cellular signals to inform a GNSS-independent positioning solution from a UAS-based receiver. The findings show precise cellular signal positioning approaches have strong potential for mitigating risk in UAS operations and should be considered a supporting navigation aide. For the spoofing chapter, the ECD method was studied in a simulation environment to produce preliminary data to assess its effectiveness. The research

efforts have shown the viability and unique capabilities of ECD to detect spoofed signals, mitigate the false and true signals, and recover the true signals. A functional GPS simulation model has been created as an initial step in establishing ECD validity. In Section 6, the evaluation of the capabilities, advantages, and limitations of optical flow and geomagnetic navigation techniques were tested using both flight and simulated data. These algorithms have demonstrated significant potential in improving the accuracy and robustness of navigation systems.

1. INTRODUCTION AND BACKGROUND

The FAA position communicated to Radio Technical Commission for Aeronautics Special Committee 228 is that UAS DAA systems should validate "ADS-B In" data before it is used to conduct DAA. A risk assessment and exploration of potential solutions is needed to inform potential policy updates for different types of UAS and operations for both GPS validation and ADS-B In validation. Potential risks and/or mitigations examples considered at the onset of the project are as follows:

- Potential Risk: If GPS data drops out or is jammed, the UAS may not know exactly where it is located and may fly away without anyone's knowledge of where it is. Note that sUAS are not tracked by Air Traffic Control (ATC) radar. Potential mitigations include means to detect broad area GPS jamming or GPS dropouts. Examples: monitor the known GPS position of a fixed GPS receiver on a cell phone, ground control station, tower, and other UAS that is on the ground. Alternatively, have an independent means of temporary navigation and UAS tracking sufficient to cease operations safely. Examples: Inertial Measurement Unit (IMU) navigation, UAS beacons (Radio Frequency (RF) or optical), vision-based navigation, rough triangulation or signal direction finding from the ground using Command and Control (C2) Signal to Noise Ratio (SNR) or time of flight analysis, etc.
- Potential Risk: If GPS signals are spoofed, the UAS may think it is in one location when it is actually at another location. This may result in the UAS crossing airspace boundaries, flying beyond radio control, sudden climbing to avoid terrain referenced onboard digital terrain elevation maps, etc. Potential mitigations could include means to detect broad are GPS spoofing. Examples: monitor the known GPS position of a fixed GPS receiver on a cell phone, Ground Control Station, tower, or other UAS that is on the ground. Alternatively, have an independent means of temporary navigation sufficient to cease operations. Potential examples may include temporary IMU navigation, navigation by C2 signal strength, UAS beacons (RF or optical), vision-based navigation, etc.
- Potential Risk: "ADS-B In" signals drop out or are jammed. This prevents UAS from detecting and avoiding other aircraft that are transmitting "ADS-B Out". Potential mitigations could include a means to detect ADS-B dropouts and jamming to cease UAS operations when jamming is detected. Example: monitor the signal from a fixed "ADS-B Out" source (potentially easy and low cost). Alternatively, potential mitigations could rely upon detecting jamming and a means to safely cease DAA operations.
- Potential Risk: A false "ADS-B In" signal is detected that harasses the UAS. If the UAS is automated to avoid collisions with other aircraft, there is the potential for false signals to harass and corral an automated UAS thereby directing it where a malicious actor desire it to fly (fly into infrastructure, terrain, controlled airspace, etc.). Potential mitigations could include having a means to validate "ADS-B In" tracks or detect false tracks. Example solutions: rough triangulation or signal direction finding from the ground using SNR or time of flight analysis. Have an ability for overriding UAS automated collision avoidance on unvalidated "ADS-B In" tracks. Cease UAS operations when false "ADS-B In" tracks are detected.

This Test, Analysis, and Demonstration Report fulfills Task 4 for the A44 ASSURE project. Task 3 prioritized the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable. The Task 4 testing and analysis places particular emphasis on prioritizing mitigations that support sUAS operations. The testing completed in Task 4 included the use of simulated flight data as a significant source of test data for evaluation.

The Task 4 Test, Analysis, and Demonstration Report contains testing results and analysis for UAS navigation anomalies including dropouts and erroneous data, GPS and ADS-B signal jamming, and GPS and ADS-B signal spoofing. The UAS anomalies section (Section 2) uses ADS-B data sets to identify ADS-B anomalies that would result in ceasing operations and identifies scenarios that are most common. Section 3 presents the findings and analysis from flight testing that utilized nearby LTE/4G cellular signals to inform a Global Navigation Satellite System (GNSS)-independent positioning solution from a UAS-based receiver. In Section 4, the ECD method is used in a simulation environment to produce data to assess its effectiveness in identifying spoofing as well as its ability to identify the true signal. Section 5 uses both flight and simulation data to evaluate the capabilities, advantages, and limitations of Optical Flow and Geomagnetic based Navigation (GNAV) techniques.

2. UAS NAVIGATIONAL ANOMALIES – DROPOUTS AND ERRONEOUS DATA TESTING AND DEMONSTRATION OF MITIGATIONS

The testing of UAS navigational anomalies including dropouts and erroneous data was accomplished by collecting ADS-B data from a custom receiver payload that was integrated and flown onboard a UAS. The payload flew multiple missions and collected data from a variety of local aircraft. The data was analyzed to determine the effect of aircraft altitude, size, range, and number of aircraft detected. Details of the payload, data processing, and analysis findings are presented in the subsequent sections. In addition, a study was done on a significant event where GPS interference around Dallas Fort Worth airport, that lasted for about 48 hours, and impacted 40 NM around the airport area. The event was analyzed and provided insights into this unique interference event.

2.1 Data Collection

2.1.1 Payload Construction

As part of the University of Alaska Fairbanks (UAF) contribution to the A44 efforts, a device to record ADS-B broadcasts with a timestamp was required. This was accomplished using a Raspberry Pi 3B+, a FlightAware ProStick+ ADS-B receiver, a Sparkfun NEO-M9N GPS breakout board, and a custom power and data breakout board. The Raspberry Pi was operated as the primary system controller, with the FlightAware ProStick+ connected via USB, and the GPS module connected via UART.

Dump-1090 was used to run the ProStick+, which outputs the collected information on a variety of Telnet ports. A shell script was used to connect to the telnet ports on the device, which then logged the data to a CSV file. As part of the requirements, the data needed to be timestamped accurately, which was made difficult due to how the raspberry pi handles its time synchronization. The Raspberry Pi has no Real Time Clock module to maintain its internal time during power off, so it assumes that no time has passed between shutdown and startup. Since it gets its time via Network Time Protocol, updating the time to the correct time is difficult, so the GPS module was added to map the local time on the raspberry pi to UTC time.

The GPS module is a breakout board of the uBlox NEO-M9N produced by SparkFun. A time offset was provided by the device. A python script was written to simultaneously collect the local time of the Pi and the UTC time from the GPS at startup.

Figure 1. ADSB Logger Payload tah was integrated into an Aurelia X6 hexacopter.

The payload was designed to be mounted on the top of one of an Aurelia X6 hexacopter and was powered using the adjustable voltage regulator from the main power bus of the aircraft.

2.1.2 ADS-B Payload Flights

Three flights were conducted across the UAF campus: one at Cornerstone Plaza, one in the Nenana Parking Lot across from the Student Recreation Center, and one in the front of Akasofu Parking Lot, as shown in Figure 2.

Figure 2. ADSB Flight Locations.

The Cornerstone Plaza location was chosen since it was the closest available location to an urban environment. It is the highest density location on campus, with closely spaced buildings and a large amount of foot traffic. It is also located approximately under the approach path for Runway 20 of Fairbanks International Airport. The Nenana lot location was chosen because it is near the foot of a large hill, potentially blocking signals. Finally, the Akasofu location was chosen as it is also near a few large buildings, as well as powerful RF emitters and has a clear view of the Fairbanks International Airport. During the flights, the UAS would ascend to 400 ft, in 100 ft increments, spending 5 minutes at each altitude.

2.2 File Pre-processing

UAF provided the data collected from flights conducted in the following formats:

a) **UAS Data:** (3) .tlog files
b) **ADSB data:** (1) .csv file

UAS data (location, speed, etc.) from the main controller of the Aurelia X6 hexacopter was provided as .tlog fil‘s. ‘.’log’ files are typically used by open-source autopilot software like ArduPilot and are not readily consumable by Python. Therefore, the .tlog files were converted to JSON TXT files using

Ardupilot Mission Planner. The resulting three JSON TXT files were parsed using a custom Python script, and the data was stored in a single CSV file. After this procedure, all data resided in two CSV files, the first with the UAS data (from .tlog files) and the second, provided by UAF, with ADS-B data collected from the payload of the UAS.

2.3 Data Exploration and Pre-processing

2.3.1 UAS data

This part of the dataset contains information about the parameters collected on the UAS that flew the payload. Start by exploring the UAS flight duration and trajectory data and then describe the pre-processing for time synchronization between the UAS and detected aircraft. Then an outlier removal algorithm is used to filter the time interval between consecutive ADS-B messages to get an estimate of the actual ADS-B message transmission rate of a given aircraft.

2.3.2 UAS Data Exploration

The UAS flight durations are listed in Table 1. All UAS flights were approximately 24 minutes in duration.

Table 1. UAS Flight Durations.

UAS Flight Number	Duration
1	24 min 28 Seconds
2	24 min 15 seconds
3	24 min 52 seconds

2.3.3 Flight Trajectories

A view of the entire flight trajectory is shown in a 3D scatter plot in Figure 3. The color of the points on the graph is indicative of time. Earlier times are in yellow, and the points become darker as time progresses. Figure 3 provides a holistic view of how the UAS flights were carried out.

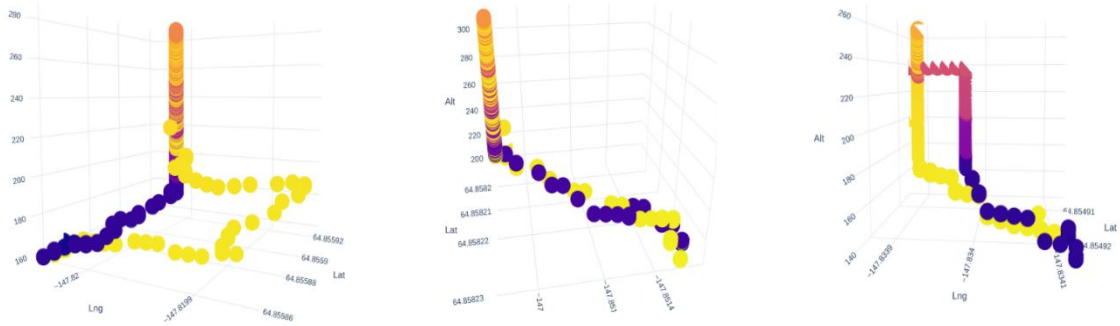


Figure 3. UAS Flight Trajectories.

2.4 Data Pre-processing

Data was stored on two independent devices, the UAS and Raspberry Pi within the ADS-B payload. The data collected on the Raspberry Pi maintained time independently of the UAS. A unique correction factor for each flight was applied to synchronize the time stamps.

2.5 ADS-B Data

This section explains the methodology for estimating the actual ADS-B message transmission rate of a given aircraft for the collected ADS-B. For this, an outlier removal algorithm is used to filter the time interval between consecutive ADS-B messages to estimate the ADS-B message transmission rate of each aircraft in the data set.

Since the recorded flights were for arbitrary aircraft entering the monitored region, it is difficult to establish what the actual time interval between the transmission of consecutive ADS-B messages (i.e. the ideal reception rate in the case of zero dropouts) is for a particular flight as there is no control data set with which to compare. However, Table 2 provides reported ADS-B message rates for different types of messages (“The 1090MHz Riddle” n.d.) and an estimate for the cumulative message frequency for airborne aircraft, which was used as a benchmark when comparing the collected data. Transmission rates were used for this benchmarking purpose since, in the ideal case of zero dropouts or lost messages, the transmission and reception rates would be equal. Therefore, the transmission rate provides an upper limit for the reception rate (or lower limit for analyzing time intervals between received messages).

Table 2. Reported transmission Rates of different ADS-B messages. Transmission rate provides an upper limit for reception rate, and transmission time interval provides a lower limit for reception time interval.

	Transmission Rate (Hz)		**Time Interval (s)**	
Message	Ground	Airborne	Ground	Airborne
Aircraft ID	0.1-0.2	0.2	5-10	5
Surface Position	0.2-2	-	0.5-5	-
Airborne Position	-	2	-	0.5
Airborne Velocity	-	2	-	0.5
Target States & Status	-	0.8	-	1.25
Aircraft Status				
No TCAS RA & Squawk change	0.2	0.2	5	5
Change in TCAS RA or Squawk	1.25	1.25	0.8	0.8
Operational Status				
No NIC/NAC/SIL change	0.2-0.4	0.4	2.5-5	2.5
Change in NIC/NAC/SIL	0.2-1.25	1.25	0.8-5	0.8
Cumulative Estimate		**8.1**		**0.123**

Additionally, the time interval between message reception many be influenced by atmospheric interference, physical obstruction, or limitations of receiver capabilities. Therefore, this analysis aims to estimate the mean time interval between ADS-B message transmission statistically for each flight from the messages received. This estimate is here referred to as the filtered mean time interval and has an associated upper bound. Time intervals greater than the upper bound are considered outliers and are not included in the calculation for the filtered mean time interval. If control data for transmission frequency could be obtained from an ADS-B transmitter, Algorithm 1 could be calibrated such that the upper bound corresponed to an instance of message dropout by finding the value of k that makes the filtered mean time interval of received messages equal to the average message rate of the transmitting device.

Algorithm 1. Iterative outlier filtering of time intervals between consecutive ADS-B messages.ss

$k \equiv const.$

$for\ FLIGHT\ in\ FLIGHTS\ do$

$\mathcal{S} \equiv set\ of\ time\ intervals,\ \Delta t,\ between\ conseutive\ messages\ in\ FLIGHT$

$\mathbb{Q} = \mathcal{S},\ filtered\ set\ of\ \Delta t$

$\overline{\Delta t} \equiv mean\ \Delta t\ \forall\ (\Delta t\ \epsilon\ \mathbb{Q}),\ changes\ with\ \Delta t\ \epsilon\ \mathbb{Q}$

$UpperBound = 0$

$while\ \big((\Delta t > UpperBound)\ \epsilon\ \mathbb{Q}\big)\ do$

$$\sigma = \sqrt{\frac{\sum \left(\Delta t - \overline{\Delta t}\right)^2}{length(\mathbb{Q})}}$$

$UpperBound = \overline{\Delta t} + k \times \sigma$

$\mathbb{Q} = [(\Delta t\ \epsilon\ \mathbb{Q}) < UpperBound]$

$FilteredMean = \overline{\Delta t}$

ADS-B messages from a total of 48 aircraft were captured during data collection. Of these flights, some did not contain location data and others did not contain enough messages for reliable statistical analysis. Therefore, analysis was performed only on flights records that contained location data and that had at least 100 messages. These criteria were met by 34 of the 48 total flights detected, which are shown in Figure 4. Analysis results for these flights are shown in Table 3 where the filtered mean time interval and upper bound were calculated via Algorithm 1 with k=2.

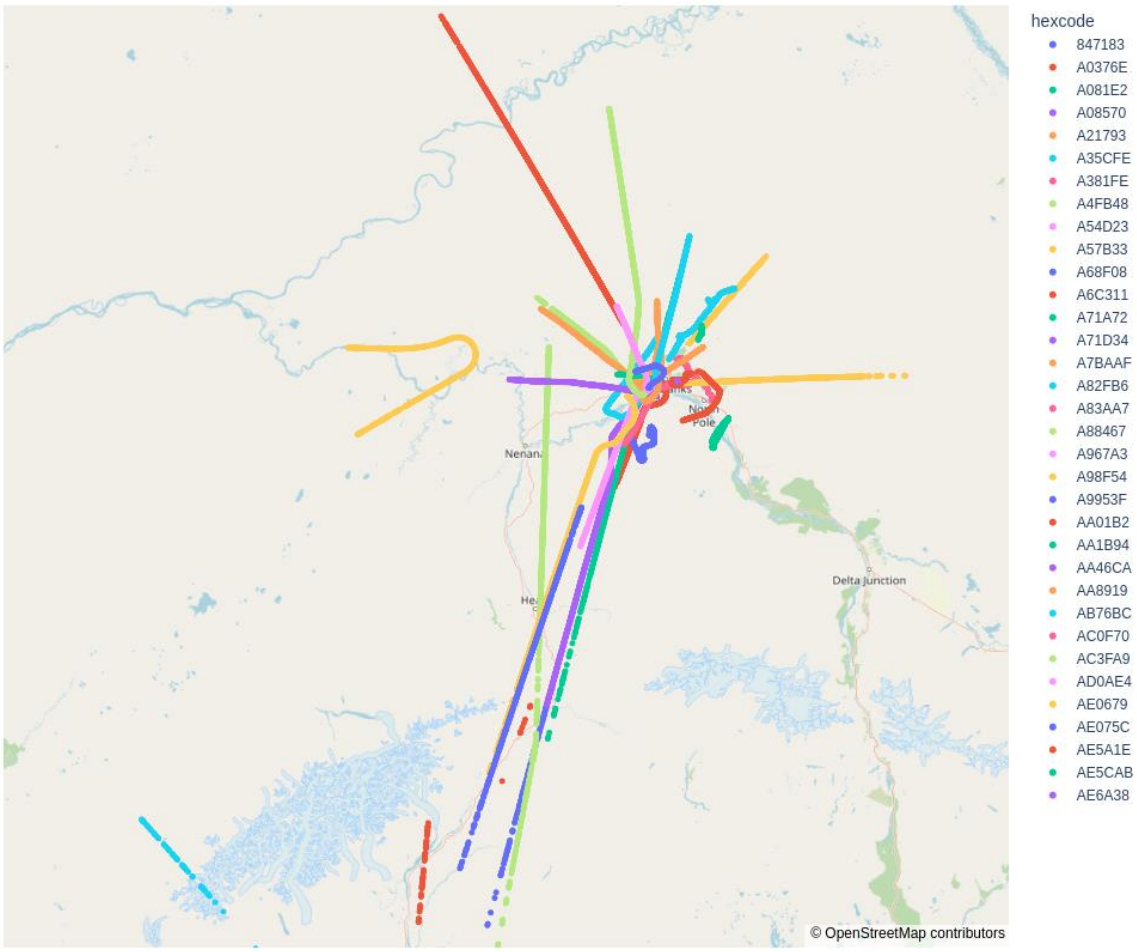


Figure 4. Trajectories for 34 flights visualized.

Table 3. Iterative outlier filtering results with k=2.

Aircraft	Flight Time (H:M:S)	Filtered Mean Time Interval (s)	Upper Bound of Filter (s)	Max Altitude (Ft)	ICAO	Size
Boeing 747-8KZF	0:14:14	0.447	1.083	33025	847183	Large
BEECH 1900C	0:36:14	0.254	0.688	21075	A0376E	Medium

Cessna 208B	0:09:41	0.236	0.66	4800	A081E2	Small
Cessna 208B C20	0:02:45	0.266	0.712	1900	A08570	Small
PIPER PA-31-350	0:49:35	0.597	1.231	0	A21793	Small
Boeing 737-852 (SF)(W)	0:06:54	0.582	1.325	41000	A35CFE	Medium
Bombardier CL-600-2B16 Challenger 605	0:41:10	0.000	0.001	2525	A381FE	Medium
PIPER PA-31-350	0:17:28	0.123	0.281	6800	A4FB48	Small
Cessna 172G	0:00:48	0.264	0.636	0	A54D23	Small
Cessna 208B	0:11:18	0.195	0.599	7750	A57B33	Small
PIPER PA-28-180	0:38:25	0.208	0.608	4350	A68F08	Small
Boeing 737-890 (W)	0:10:25	0.583	1.296	36700	A6C311	Medium
No data	0:16:28	0.079	0.188	35000	A71A72	Unknown
Boeing 737-890 (W)	0:19:26	0.137	0.321	25900	A71D34	Medium
PIPER PA-31-350	1:12:48	0.156	0.361	7600	A7BAAF	Small
Cessna 182R	1:29:26	0.200	0.603	4900	A82FB6	Small
Cessna T182T	0:11:14	0.000	0.001	3825	A83AA7	Small
EMBRAER ERJ-175LR (170-200LR)	0:21:34	0.149	0.344	36000	A88467	Medium
FOKKER F.27MK 500	0:14:52	0.091	0.218	19000	A967A3	Medium
Cessna 208B	0:23:39	0.213	0.624	10750	A98F54	Medium

PIPER PA-31-350	0:18:02	0.415	0.757	0	A9953F	Small
Pilatus PC-12/47	0:34:04	0.197	0.456	24000	AA01B2	Small
Cessna 208B	1:04:11	0.222	0.641	6075	AA1B94	Medium
Cessna 208B	0:14:21	0.209	0.615	7700	AA46CA	Medium
DOUGLAS DC-6A	0:37:03	0.210	0.622	3825	AA8919	Large
Cessna 208B	0:16:47	0.220	0.625	8800	AB76BC	Medium
Cessna TU206F	0:43:37	4.531	11.824	0	AC0F70	Small
Dehavilland DHC-8-102	0:20:24	0.132	0.312	18800	AC3FA9	Medium
Cessna 208B	0:10:08	0.219	0.639	5125	AD0AE4	Small
Boeing C-17A Globemaster III	1:38:08	0.119	0.282	23200	AE0679	Large
Beech C-12F	0:41:24	0.002	0.004	25025	AE075C	Small
No data	1:18:43	0.116	0.273	1600	AE5A1E	Unknown
Sikorsky UH-60M Blackhawk	0:31:58	0.243	0.578	3600	AE5CAB	Small
No data	0:29:25	0.787	1.464	0	AE6A38	Unknown

ADS-B transmission rates vary depending on message type, but in general grounded aircraft transmit at a slower rate compared to airborne aircraft. This trend can be seen when comparing the mean filtered time interval of flights with a maximum altitude of 0 Ft to flights that were airborne. Additionally, stationary aircraft have transmission frequencies as low as 0.1Hz (10 s/msg) which may explain the larger values for the Cessna TU206F with International Civil Aviation Organization (ICAO) AC0F70. Figure 5 shows boxplots for the flight times, filtered mean time intervals, and upper bounds listed, where the mean values across all flights are listed. Averaging across all flights gives a

mean filtered time interval of 0.4 s and an upper bound of 0.9 s, suggesting that for airborne flights time gaps in reception > 1 s may indicate message loss. Outliers in Figure 5 appear to correspond to grounded aircraft.

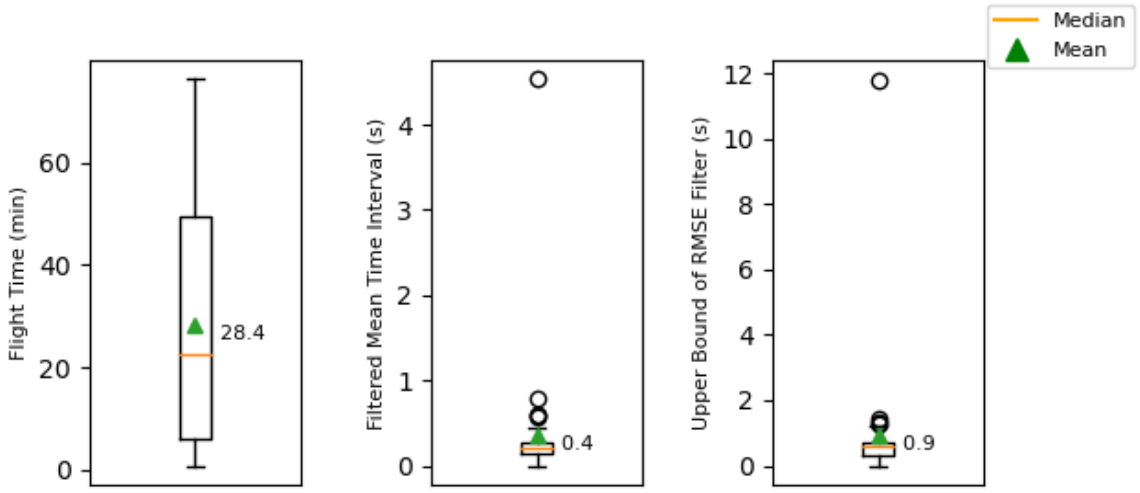


Figure 5. Statistical analysis of flight time filtered mean time interval, and upper bound across all flights.

2.6 Analysis

2.6.1 Effect of Aircraft Altitude on ADS-B Reception Rate

Figure 6 shows boxplots of the time intervals between messages (unfiltered) binned by maximum flight altitude where the average value across all data points is reported. The range of each bin is 1,000 Ft and is labeled by the maximum value for that bin. For example, the bin labeled 2000 contains data from flights with maximum altitudes > 1,000 Ft and ≤ 2,000 Ft. The maximum average time interval of 3.9 s is reported for aircraft that remained grounded (maximum altitude = 0 Ft.) which corresponds reasonably well to reported transmission rates of grounded aircraft of 0.1 and 0.2 Hz (10 and 5 s/msg) for different message types. Most of data from flights that were airborne had an average time interval near 0.5 s corresponding to a message frequency of 2 Hz (typical for airborne aircraft), except for the data from the flights with the two highest values of maximum altitude (37,000 and 41,000 Ft).

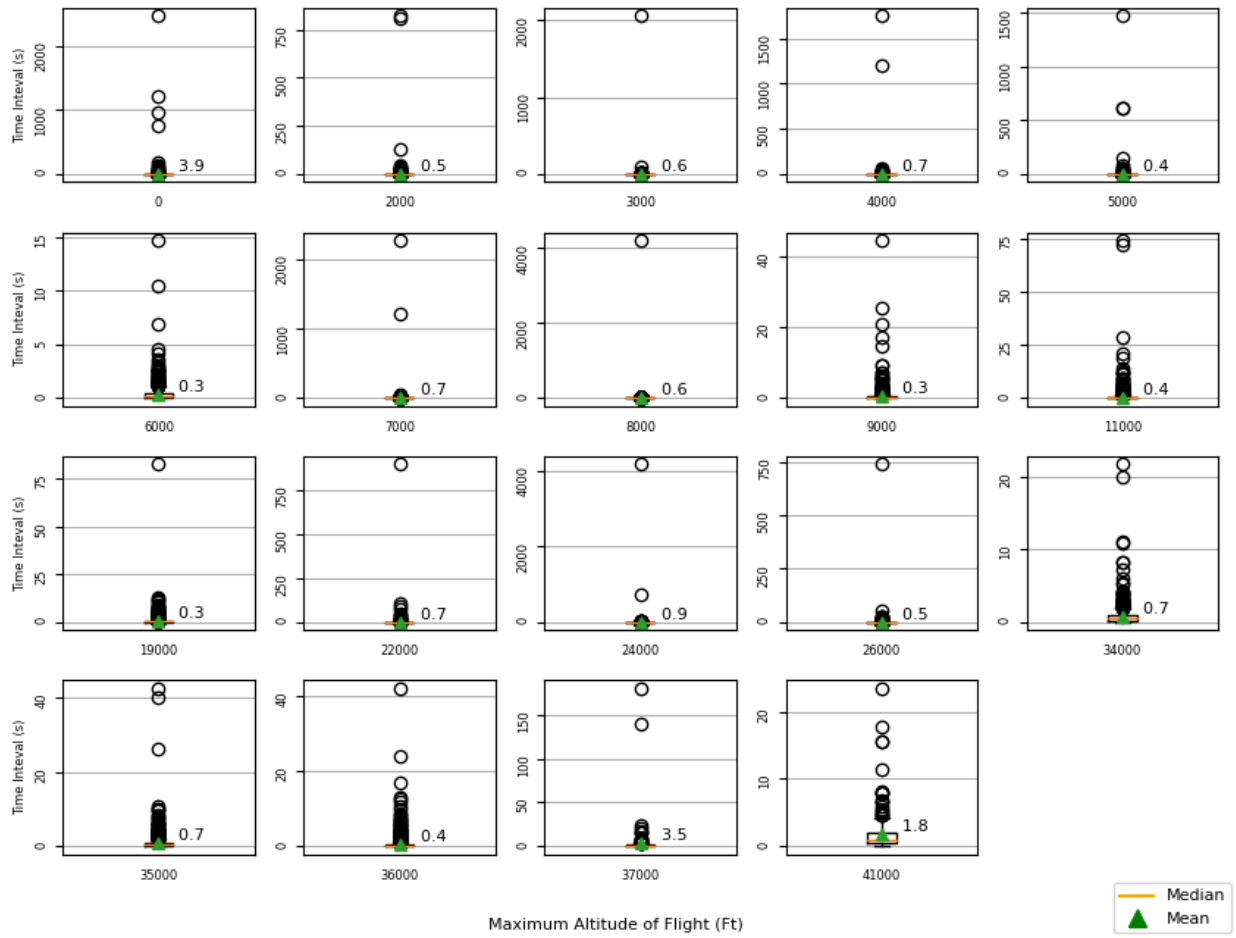


Figure 6. Time intervals binned by maximum flight altitude in 1,000 Ft bins. Bins are labeled by maximum value.

2.6.2 Effect of Aircraft Size on ADS-B Reception Rate

Bins for aircraft size were determined by weight as reported in Table 4. Since some ICAO numbers did not correspond to any aircraft type (Aircraft with type "No data" in Table 3), an additional "unknown" category was included when analyzing dropout instances and duration by aircraft size.

Table 4. Classification of aircraft by size.

Size Category	Weight (lbs.)
large	> 255,000
medium	< 255,000 & > 41,000

small	< 41,000

A dropout was considered any time interval between consecutive ADS-B messages exceeding 10 s. Dropout instances are reported as the average number of dropouts per hour and are shown in Figure 7 for the selected aircraft size categories. This data shows a trend with larger aircraft having less instances of dropout, however this difference is not statistically significant.

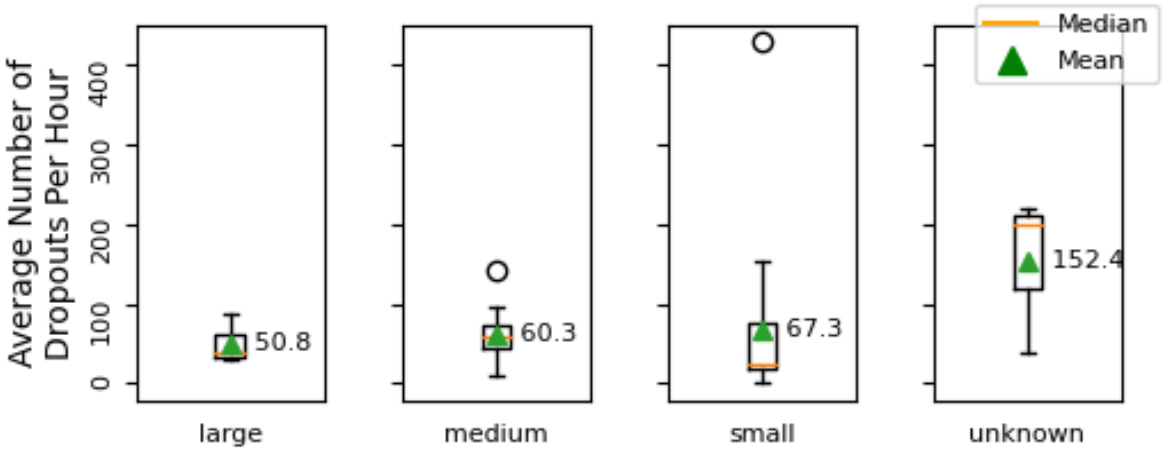


Figure 7. Effect of the aircraft size on the average number of dropouts per hour.

Dropout duration was calculated as the time interval between consecutive messages for each time interval > 10 s. Average dropout duration was calculated over a given flight (ICAO) and is reported in Figure 8 for the aircraft size categories. The data displayed in Figure 8 shows that individual dropouts can persist for a long-time interval, with the maximum exceeding 2000 s (30 min). However, no significant correlation is observed between the average dropout duration of different size categories.

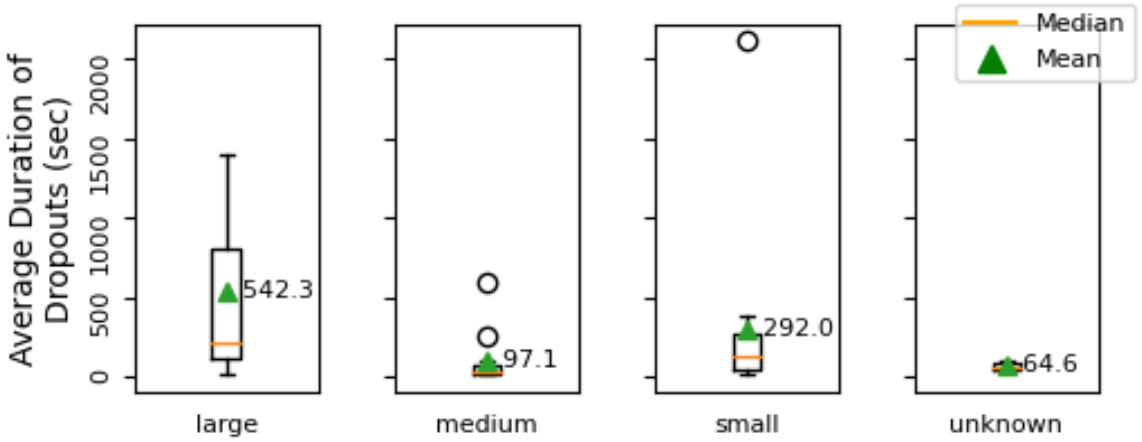


Figure 8. Effect of the aircraft size on the average dropout duration.

Mean time intervals were also analyzed with respect to aircraft sizes. This quantity differs from average dropout duration in that an average of all mean time intervals is taken for each aircraft size bin, whereas for dropout duration, only mean time intervals > 10 s are included in the average. Figure 9 shows the effect of aircraft size on mean time interval, for time intervals between consecutive ADS-B messages of any type (ΔT_msg) and time intervals between consecutive ADS-B location messages (ΔT_loc). No clear trend can be observed for the mean time interval for different aircraft sizes, however the aircraft in the large category had the largest values for both total messages and location messages.

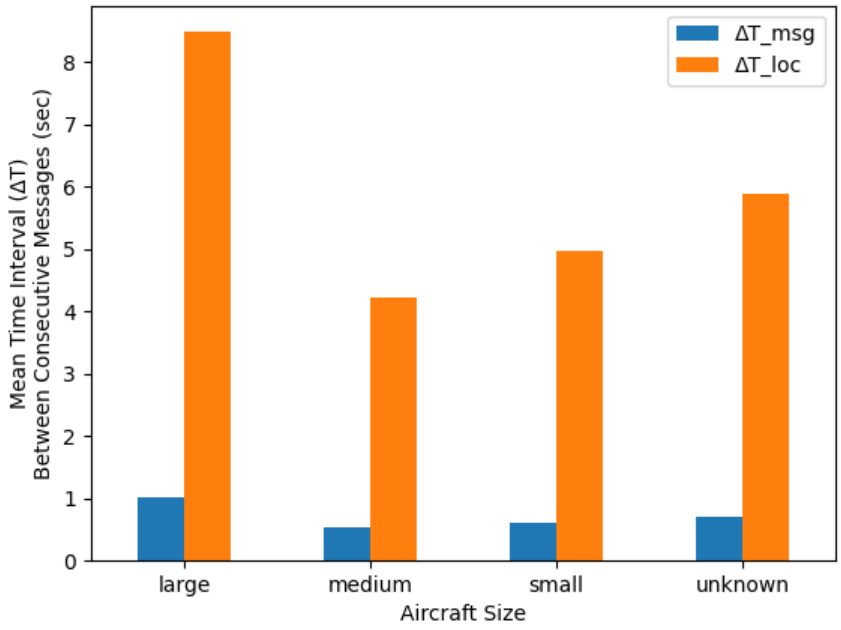


Figure 9. Aircraft size vs Mean time interval between messages.

2.6.3 Effect of Distance from Receiver on ADS-B Reception Rate

The effect of the distance of the aircraft from the UAS-mounted receiver on mean time interval was also analyzed. Since a time interval is taken between two consecutive ADS-B messages, the distance category was assigned according to the average distance from the receiver for the consecutive messages. Four equally sized distance bins were constructed between the minimum and maximum distances from the receiver in the ADS-B data set. As with the aircraft size analysis (Section 2.6.2), a dropout was considered any time interval between consecutive ADS-B messages exceeding 10 s. Dropout instances are reported as the average number of dropouts per hour and are shown in Figure 10 for each of the distance bins. This data suggests that the aircraft closest to the receiver exhibit the highest frequency of dropouts, however this may be due to the large quantity of grounded aircraft at the nearby Fairbanks airport, which can intermittently turn off and on. Further analysis needs to be performed to investigate this possibility.

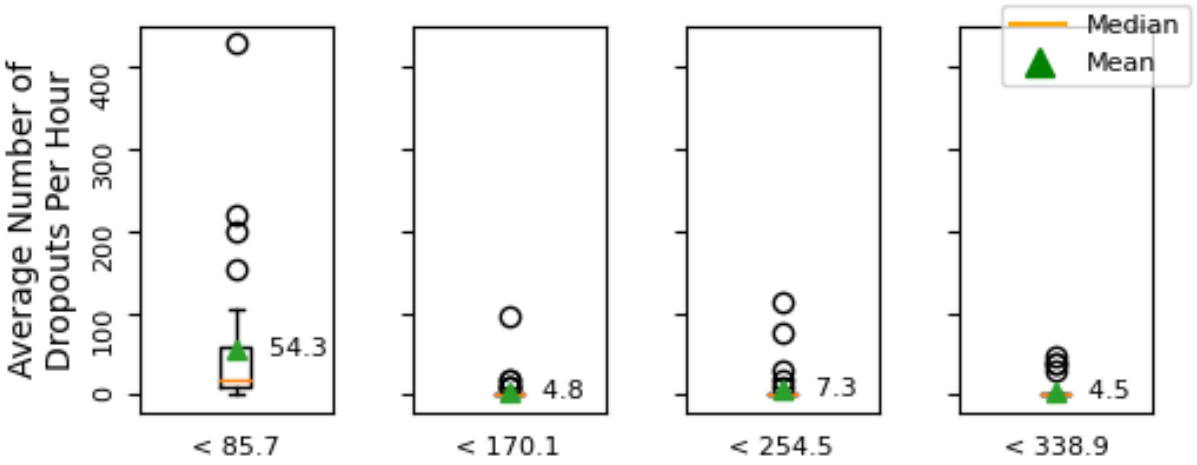


Figure 10. Effect of the distance (km) from the receiver on the average number of dropouts per hour.

As with the aircraft size analysis (Section 2.6.2), dropout duration was calculated as the time interval between consecutive messages for each time interval > 10 s. Average dropout duration was calculated over a given flight (ICAO) and is reported in Figure 11 for the different distance bins. Although many of the longer durations in the shortest distance category (< 85.7 km) may be due to grounded nearby aircraft turning on and off, the trend of farther aircraft exhibiting shorter dropout durations persists for the other three distance bins. Further analysis must be performed to eliminate any skewing of the first bin that may result from grounded, noncontinuous ADS-B transmitters.

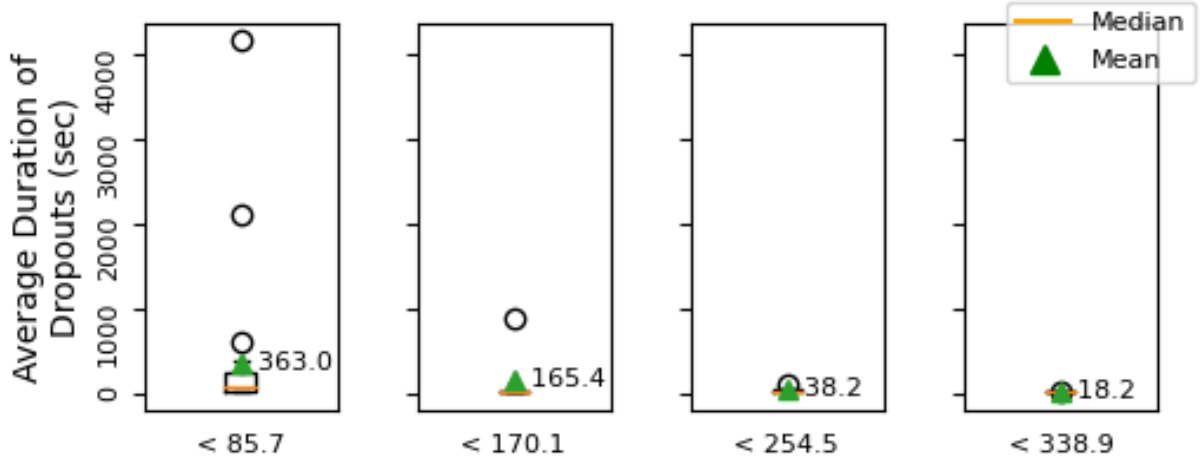


Figure 11. Effect of the distance (km) from receiver on the average dropout duration.

Mean time intervals were also analyzed relative to distance from receiver. This quantity differs from average dropout duration in that an average of all mean time intervals is taken for each distance and aircraft size bin, whereas for dropout duration, only mean time intervals > 10 s are included in the average. Figure 12 shows the effect of receiver distance on mean time interval for time intervals

between consecutive ADS-B messages of any type (ΔT_msg) and time intervals between consecutive ADS-B location messages (ΔT_loc). Except for location messages of aircraft in the smallest distance bin (< 85.7 km), the frequency of both location messages and total messages appears to decrease with increasing distance from the receiver. However, this does not result in increased dropout frequency (see Figure 10) when defining dropout as a > 10 s gap between messages.

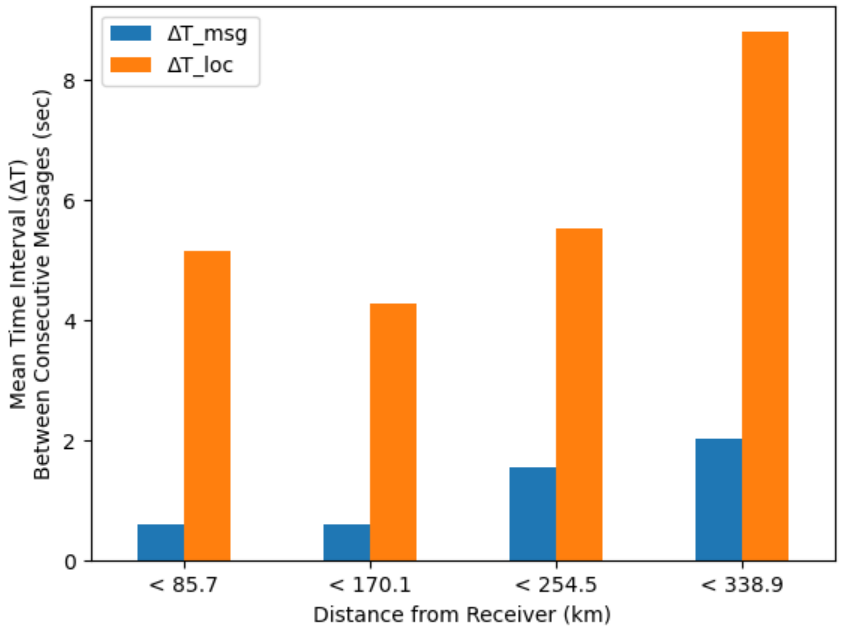


Figure 12. Distance from Receiver vs mean time interval between messages.

2.6.4.3 Recommendations from ADS-B Payload

For airborne aircraft, a cumulative estimate for message transmission rate of 8.1 Hz (0.123 msg/s) (Table 2) was generated by summing the transmission rates of each individual message type (i.e., each row in the airborne transmission rate category of Table 2). This estimate incorporates rates of all message types of airborne aircraft (aircraft ID, airborne position, airborne velocity, target states/status, and aircraft and operational status messages. This cumulative message transmission rate is used as an upper bound for the cumulative reception rate since these rates would be equal in the ideal case of no lost messages. From comparing the reception data to this upper bound, message loss appears to be a frequent occurrence, given that the filtered mean time interval of 0.4 msg/s for all flights analyzed is considerably larger than that of the estimate for transmission (0.123 msg/s). Therefore, metrics other than dropout may be needed to comprehensively characterize ADS-B reception quality, such as an estimated percentage of lost messages in reference to the expected rate of 8.1 Hz. This conclusion is supported by the observation that greater distances between the receiver and transmitting aircraft result in increased mean time intervals but not increased occurrences of

dropouts, suggesting that dropout alone may not be an adequate metric. Grounded Aircraft (Max Altitude of 0 Ft) had the largest mean time interval which agrees with reported ADS-B messaging rates for grounded and airborne aircraft. Additionally, aircraft size did not significantly affect the rate or duration of dropouts due to the large variance in the size category data sets. Finally, increasing the altitude of the ADS-B receiver resulted in an increased number of detected aircraft, and a Chi^2 test was used to rule out the null hypothesis that receiver altitude and number of detected aircraft were statistically uncorrelated. Recommendations based on these observations are summarized as follows:

1. Apply an additional metric such as "estimated percent message loss" to characterize ADS-B reception quality.
2. The distance between the ADS-B receiver and transmitting aircraft should be accounted for when determining the location of an ADS-B receiver station.
3. ADS-B reception may be improved by increasing the altitude of the receiver.

3. DFW INTERFERENCE ANALYSIS

3.1 Introduction

3.1.1 The opensky Network

Opensky network is a non-profit, crowd-sourced, off-the-shelf ADS-B receiver network that has collected data from volunteers worldwide since 2013. This data is processed and stored in a central database (Schäfer et al. 2014). The database contains positional – Airborne and Surface, Identification, Velocity, operational status, and uncertainty metrics transmitted by aircraft with ADS-B in the range of volunteer-operated sensors. Open Sky uses an Impala database for the storage of ADS-B messages. The data that interests the researchers is stored in state_vectors_data_4 and operational_status_data4. The operating status messages table uses min and max time as parameters to keep track of Navigation Integrity Category (NIC) instead of state vectors, which uses epoch time every second.

The Open Sky database holds NIC in a separate table, in which the NIC is logged between timestamps (min. time and max. time) instead of a single timestamp as used the state vectors data. To draw conclusions and analyze areas of interference, it would first be required to combine NIC with the state_vectors_data4. A program that does exactly this was designed. Given a query for the state_vectors_data4 table, it connects to the Open Sky IMPALA database, runs the query, and saves the data obtained from the query to disk. Once saved, it obtains the unique identifiers of aircraft in the data obtained. With these unique aircraft, it queries the position_data4 table, obtains the NIC value, matches the timestamps, creates files for each aircraft with the NIC and Navigation Accuracy Category (NAC) value (where available), and combines them. It can also catch authentication time-out errors. If these errors occur, the query resumes from the last obtained call to rerun, thus automating the process of obtaining data from the Open Sky, which is a time-consuming task, and freeing the user from waiting for long queries to complete. On successfully obtaining the data from the remote database, it becomes easily available for analysis and processing.

3.2 Analysis and Conclusion

3.2.1. GPS interference event

As per multiple reports (*Bloomberg.Com* 2022) (Goodin 2022) ("Runway Now Open at DFW Airport after Faulty GPS Signal Prompts Temporary Closure" 2022), there was GPS interference around Dallas Fort Worth airport, that lasted for about 48 hours, and impacted 40 NM around the airport area. The researchers analyzed and provided insights into this interference event with open-source ADS-B data from the Open Sky Network.

3.2.2 Data Acquisition

The data set used for analysis is from the Open Sky network. The database was queried in temporally smaller chunks of about four hours to obtain data from 20:00:00 Oct 17th, 2022, to 23:59:59 October 18th, 2022, 40 Nautical Miles (NM) around DFW airport. The dataset contains 5,747,931 data points and about 2,559 unique aircraft. This dataset was analyzed with NIC as the primary parameter to study its properties during a GPS interference event.

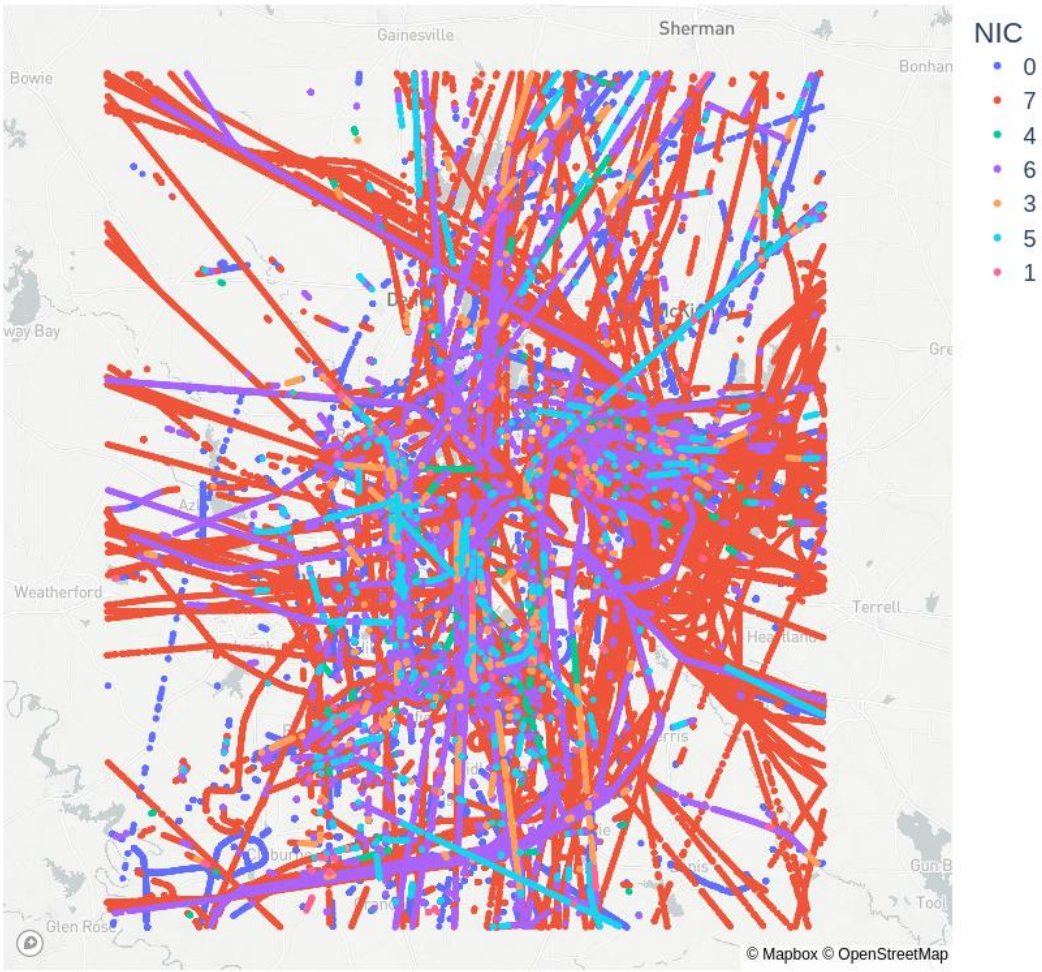


Figure 13. Overview of datapoints with NIC7 and below.

Figure 13 is a Geo scatter plot showing every data point where the NIC has dropped to seven or below. The visualization is intended to give a holistic view of the dataset.

3.2.3 Analysis

The dataset was analyzed with NIC as the primary parameter to understand its properties during a GPS interference event.

Altitude:

It is common to find points with low NIC values at lower altitudes. This is because obstructions like trees or high-rise buildings or mountains can obscure a portion of the sky, denying the GPS receiver from being able to view the intended constellation of satellites intended to get a good position fix. However, this is not the case with airborne aircraft. Given their altitude and larger horizon, they would easily get more satellites than what is expected to get a proper position fix. However, Figure 14, a violin plot with altitude in the y-axis and NIC values in the X-axis, indicates there are many data points from about 9,000 to 15,000 m altitude whose NIC has dropped to 0.

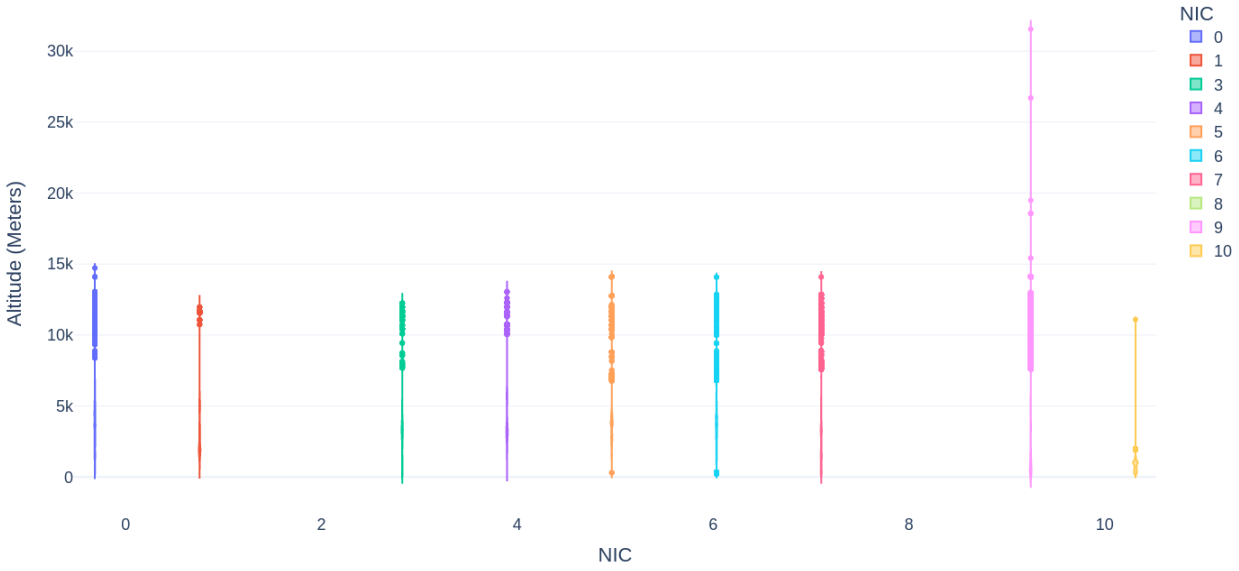


Figure 14. NIC by Altitude.

Change in NIC:

This analysis also revealed that when the NIC drops to 0 and recovers, the most typical pattern is a drop from 9 to 0 and a recovery from 0 to 9. This occurs a total of 559 times in the entire dataset. Figure 15 is a bar chart with the count on the y-axis and the change category on the x-axis that visualizes the number of times a category of change in NIC occurs.

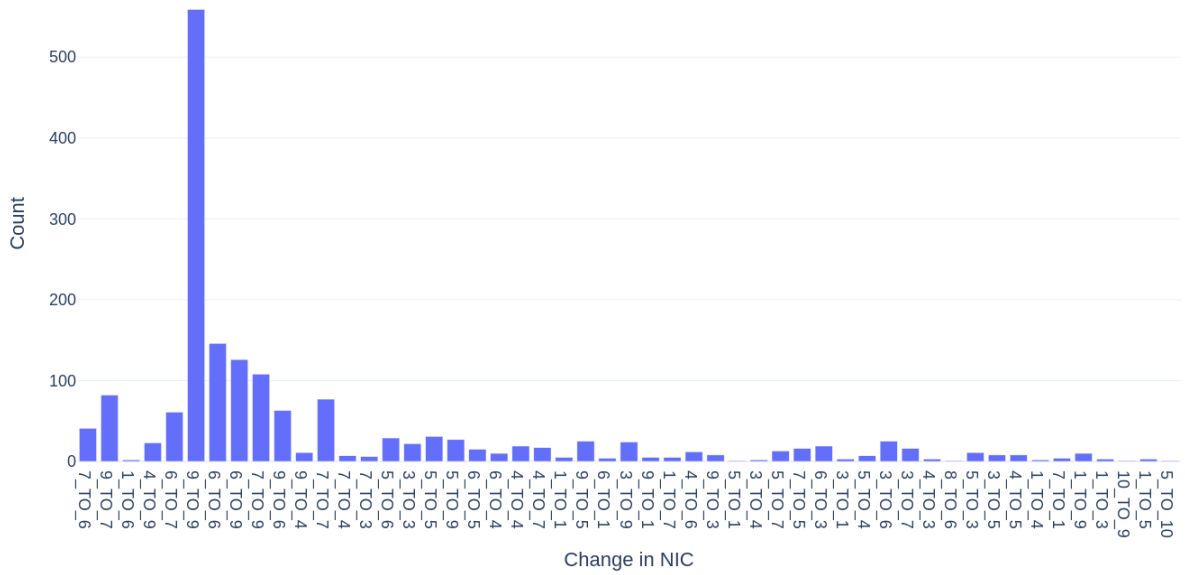


Figure 15. Count of Change in NIC by Category.

Aircraft Heading:

Aircraft were analyzed by heading, and it was found that a drop in NIC of 7 or below was experienced by aircraft heading south-westerly and southern direction. Figure 16 and Figure 17 are polar bar charts where the bars represent the count of aircraft. . These plots indicate that though the count of aircraft heading in various directions is similar, a higher number of aircraft experienced a drop in NIC when heading in the south and south westerly direction.

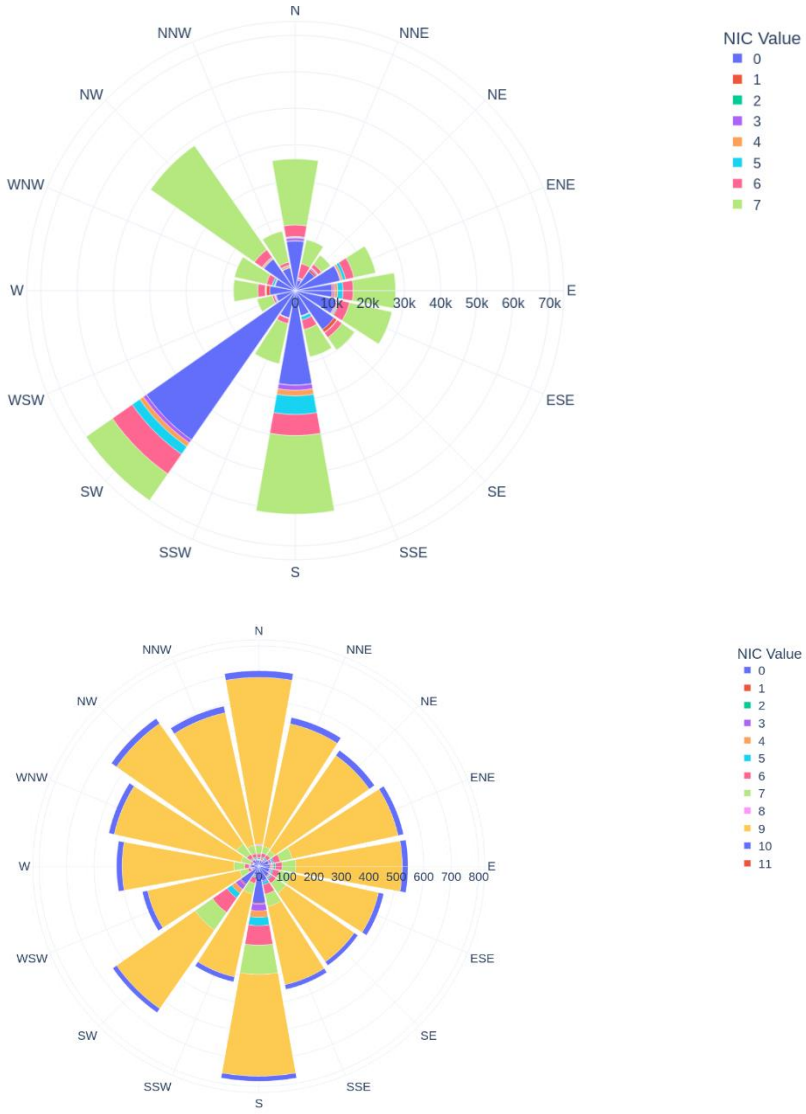


Figure 16. Aircraft Count by heading: all NIC values..

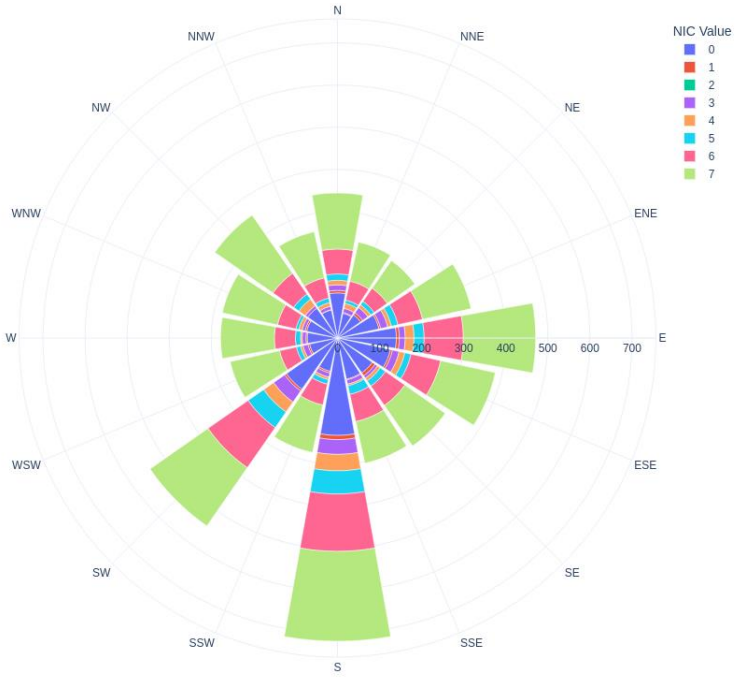


Figure 17. Aircraft Count by heading: NIC 7 and below.

3.2.4 Conclusion

This Analysis provides the following insight into the properties of NIC during the interference event:

- Aircraft as high as 9 – 13,000 meters were affected by GPS interference.
- The most typical change in NIC was found to be from 9 to 0 and recovery back to 9, followed by 6 to 0 and back 6 and 6 to 0 and back to 9. It is possible that this pattern of change in NIC could be indicative of an intentional GPS jamming incident. Further research is warranted to determine the exact cause. Some of the possible reasons for NIC values to go back and forth could be: 1. Intentional jamming/spoofing, 2. Unknown reasons, 3. Environmental/atmospheric interference 4. Interaction with nearby transceivers or satellite constellations affecting the ADS-B/GPS signal quality. In terms of heading, it was found that most of the aircraft that experienced a drop in NIC were heading in the southern or southwestern direction.

4. CELLULAR NAVIGATION

4.1 Introduction

In this section of the Task 4 report, a cellular navigation mitigation strategy utilizes nearby LTE/4G cellular signals to assist the UAS navigation in GNSS challenging environments. Considering possible safety risks due to the erroneous, jammed or dropped GNSS data, published cellular navigation approaches, in combination with expanding cellular infrastructure, have strong potential to assist UAS navigation, and should be further investigated.

Oregon State University (OrSU) investigated this topic within Tasks 3 and 4 and collaborated with the UAF team to conduct flight testing and manage UAS and sensor equipment logistics. OrSU performed the data processing, interpretation, and discussion components using the acquired test data. Within Task 4, OrSU performed the following tasks: (1) assess accuracy of a signal-strength informed cellular positioning solution, (2) test hybrid integration with a GNSS-based solution acquired in tandem, and (3) contextualize results as they relate to applications in practical, law-abiding UAS operations.

4.2 Background

4.2.1 Cellular signal-based range estimation techniques

In the event of a GNSS signal loss due to obstructions, multipath, intentional/unintentional jamming, etc., the aircraft's positioning performance is degraded. A simplified illustration of this scenario is depicted in Figure 18 where the aircraft receives GNSS signals from three of the four satellites as one satellite's signal is occluded by a building. Thus, rendering a GNSS position estimation is not achievable because the minimum required GNSS satellites for positioning is four. However, signals from nearby terrestrial cellular towers could be used as a "pseudo" GNSS satellite. In the figure, signals from two cell towers are utilized along with the three GNSS satellites to estimate the aircraft position.

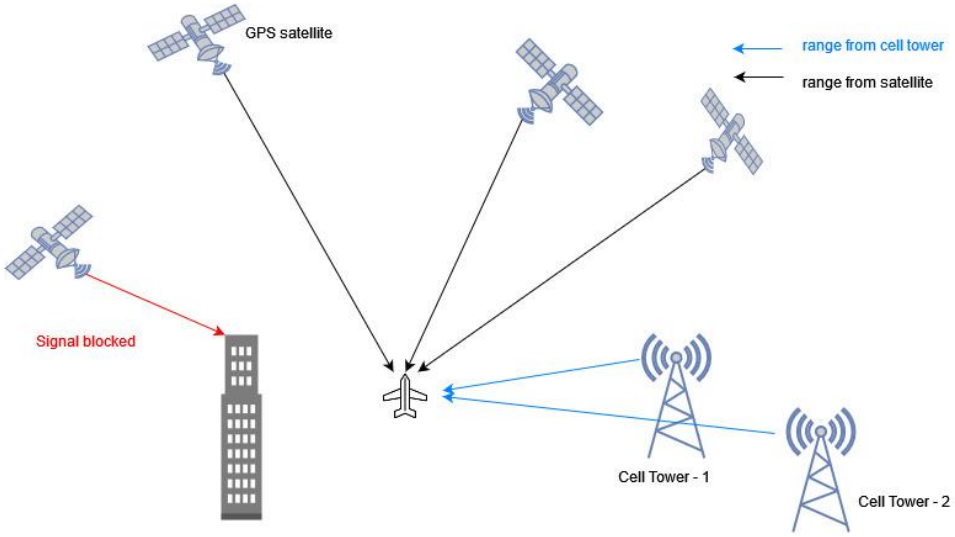


Figure 18. Conceptual diagram of cell towers augmenting GNSS positioning of an aircraft when a satellite signal is blocked.

Position estimation is based on a trilateration technique where range measurements from four or more beacons (GNSS, cell towers, etc.) of known location are used to calculate position. Various prominent techniques used to estimate range between a cell tower and cellular receiver exist in the literature, including:

1. Signal time of arrival
2. Signal direction of arrival
3. Received signal strength

These techniques can be leveraged with the different generations of cellular signals, and in user-based or network-based navigation approaches**.** Uncertainty estimation varies based on methods, flight and processing par–meters – from hundreds of meters in signal-strength approaches, to potential meter or submeter accuracy shown in cases of carrier phase time of arrival positioning with 5G signals (Khalife, Bhattacharya, and Kassas 2018; Shamaei and Kassas 2019).

Received signal strength-based range estimation involves minimal hardware complexity, as radio systems commonly measure and report received signal strength, though the approach produces a lower accuracy threshold compared to other presented methods. Given the constraints of the project timeline and equipment budget, the researchers adopted the signal strength-based range estimation approach for Task 4 experiment. In the next section, various techniques to estimate a range from received signal strength are discussed.

4.2.2 Path loss models to estimate range from signal strength

Using the received signal strength (measured by the radio system) and the transmitted signal strength (communicated in the signal from the tower), the path loss between the tower and the UAS can be calculated. Path loss is the ratio of the transmitted (P_t) and the received power (P_r), with power expressed in Watts as shown in Eqn. (1)

$$PL(dB) = 10 \log_{10} P_t / P_r \quad (1)$$

There exist many models which define the relationship between the path loss and the range between the tower and the user, depending on the radio signals frequency, and the properties of the medium/environment in which it travels. Notable theoretical models include the Free Space Model (Seyed A. Zekavat and R. Michael Buehrer 2012), and Open Field Model (Alan Bensky, 2008) in addition to a variety of empirical/analytic models. The Hata Path Loss Model is used in this study for its applicability to a small city environment and repeated published use in cellular signal literature, detailed below:

Hata model – The Hata model is a city-based empirical model for calculating path loss in cellular transmission by considering the effects of diffraction, reflection and scattering caused by city structures. The parameters in the model vary depending on the size of the city: small, medium, and large (Hata, 1980). The details of the model are as shown:

Model applicability:

Frequency: 500 – 1500 MHz

Range: 1 – 10 km (2)Path loss equation:

$$L_u = 69.55 + 26.16 \log_{10} f - 13.82 \log_{10} h_t - C_h + [44.9 - 6.55 \log_{10} h_t] \log_{10} d \quad (2)$$

where:

L_u = path loss in urban environment (dB)

h_t = height of the tower (m)

f = frequency of the signal (MHz)

d = distance between tower and the user/UAS (km),

C_h = antenna height correction factor

The antenna height correction factor varies based on the size of the city. For small or medium sized cities,

$$C_h = 0.8 + [1.1 \log_{10} f - 0.7] h_u - 1.56 \log_{10} f. \quad (3)$$

For large cities, the antenna height correction is different for different frequency ranges. If 150 MHz < f < 200 MHz,

$$C_h = 8.29 \ (\log_{10}(1.54 \log_{10} h_u))\text{^}2 - 1.1. \quad (4)$$

If 200 MHz < f < 1500 MHz,

$$C_h = \ 3.2\ (\log_{10}(11.75 \log_{10} h_u))\text{^}2 - 4.97. \quad (5)$$

where h_u = height of the tower (m).

In the suburban environment, the path loss model is following.

$$L_{su} = \ \mathrm{L_u}\ -2\ [\log_{10} \frac{f}{28}]^2 - 5.4 \quad (6)$$

where L_{su} = path loss in suburban environment (dB).

In the open areas,

$$L_o = \ \mathrm{L_u}\ -4.78\ [\log_{10} f]^2 + 18.33 \log_{10} f - 40.94 \quad (7)$$

where L_o = path loss in open area

4.2.3. Math theory of hybrid GNSS and cellular position estimation

The range solution calculated from each cellular tower to the user, using the path loss model described in the previous section, is combined with the range measurements from the GNSS satellites to estimate a hybrid navigation solution. A simple non-linear least squares technique, which uses the combined range estimates from GNSS and cell towers, estimates the UAS position.

The range between a GNSS satellite position (r_s) and UAS position (r_u) is:

$$\rho_{GPS} = ||r_s - \ r_u|| + b \quad (8)$$

where:

r_s = earth centered earth fixed (ECEF) position of the satellite
r_u = UAS ECEF position
b = GNSS receiver clock bias

Similarly, the range between a cell tower position (r_c) and UAS (r_u) is:

$$\rho_{LTE} = ||r_c - \ r_u|| \quad (9)$$

Due to the non-linear range equations, researchers use incremental variables (d_{r_u}, db) in the observation equation by linearizing at an assumed or known UAS location of given epoch:

$$\begin{bmatrix} \Delta\rho_{GPS,1} \\ . \\ . \\ \Delta\rho_{GPS,N} \\ \Delta\rho_{LTE,1} \\ . \\ . \\ \Delta\rho_{LTE,M} \end{bmatrix} = \begin{vmatrix} -1^{x}_{\mathrm{GNSS},1} - 1^{y}_{\mathrm{GNSS},1} - 1^{z}_{\mathrm{GNSS},1} & 1 \\ . & \\ . & \\ -1^{x}_{\mathrm{GNSS},N} - 1^{y}_{\mathrm{GNSS},N} - 1^{z}_{\mathrm{GNSS},N} & 1 \\ -1^{x}_{\mathrm{LTE},1} - 1^{y}_{\mathrm{LTE},1} - 1^{z}_{\mathrm{LTE},1} & 0 \\ . & \\ . & \\ -1^{x}_{\mathrm{LTE},M} - 1^{y}_{\mathrm{LTE},M} - 1^{z}_{\mathrm{LTE},M} & 0 \end{vmatrix} \begin{bmatrix} dr_u^x \\ dr_u^y \\ dr_u^z \\ db \end{bmatrix} \tag{10}$$

*w*here:
$\Delta\rho$ = range residual
1 = unit vector to the UAS from a LTE cell tower or a GNSS satellite
dr_u = incremental UAS position estimate
M = visible cell towers at epoch *t*
N = visible GNSS satellites at epoch *t*

An iterative least squares solution to calculate the incremental variable is:

$$\mathrm{dX} = (H^T H)^{-1} H^T y \tag{11}$$

where:

$$\mathrm{y} = \begin{bmatrix} \Delta\rho_{GPS,1} \\ . \\ . \\ \Delta\rho_{GPS,N} \\ \Delta\rho_{LTE,1} \\ . \\ . \\ \Delta\rho_{LTE,M} \end{bmatrix} ; \mathrm{H} = \begin{vmatrix} -1^{x}_{\mathrm{GNSS},1} - 1^{y}_{\mathrm{GNSS},1} - 1^{z}_{\mathrm{GNSS},1} & 1 \\ . & \\ . & \\ -1^{x}_{\mathrm{GNSS},N} - 1^{y}_{\mathrm{GNSS},N} - 1^{z}_{\mathrm{GNSS},N} & 1 \\ -1^{x}_{\mathrm{LTE},1} - 1^{y}_{\mathrm{LTE},1} - 1^{z}_{\mathrm{LTE},1} & 0 \\ . & \\ . & \\ -1^{x}_{\mathrm{LTE},M} - 1^{y}_{\mathrm{LTE},M} - 1^{z}_{\mathrm{LTE},M} & 0 \end{vmatrix} \text{ and } \mathrm{dX} = \begin{bmatrix} dr_u^x \\ dr_u^y \\ dr_u^z \\ b \end{bmatrix}$$

The UAS position estimate at epoch *t* is defined as:

$$X_t = X_{t-1} + dX. \tag{12}$$

4.3 Experimental Methods and Results

4.3.1 Equipment

The PriSM Network Scanner (manufactured by Epiq Solutions) is a mobile radio frequency multi-tool instrument used for cellular network surveying, scanning and spectrum analysis (Figure 19). It

is capable of logging all available bands and subchannels in semi-real time, including the fields: received signal strength, System Information Block (SIB) messages, and cell ID.

Figure 19. Prism scanner is the black unit with the antenna (detached).

A Pixhawk-operated hexcopter UAS was leveraged for flight tests, including a payload of two sensors (Figure 20).

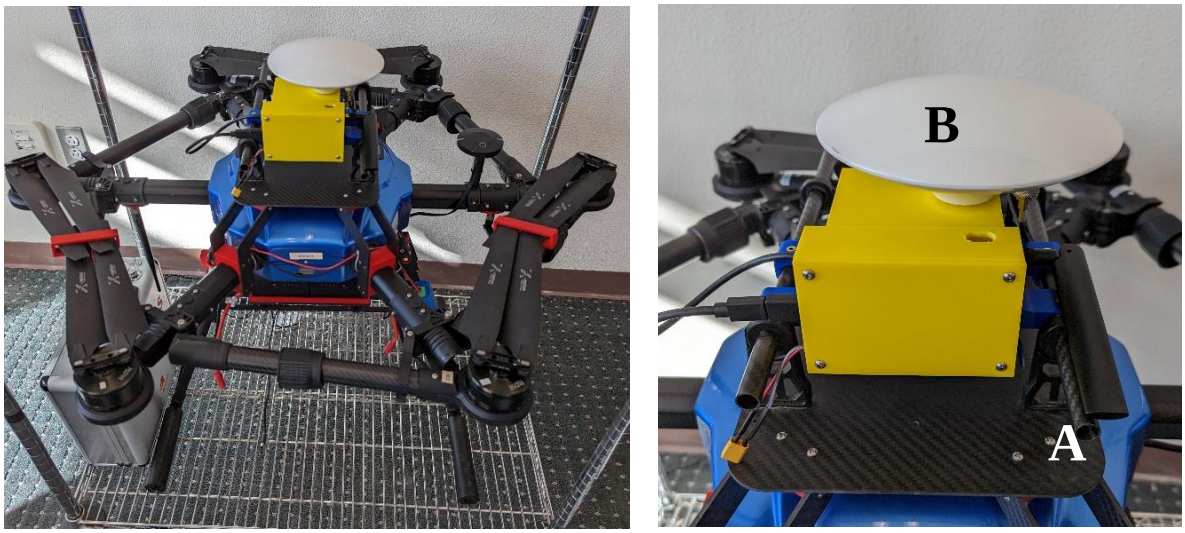


Figure 20. Images of flight test vehicle (left); cellular (A) and GNSS (B) antennae on payload

The supporting sensor, a high-rate, multi-constellation GNSS receiver (SparkFun ZED-F9R) paired with a dual band antenna (SparkFun TOP106) combination was used for GNSS signal collection (Figure 21).

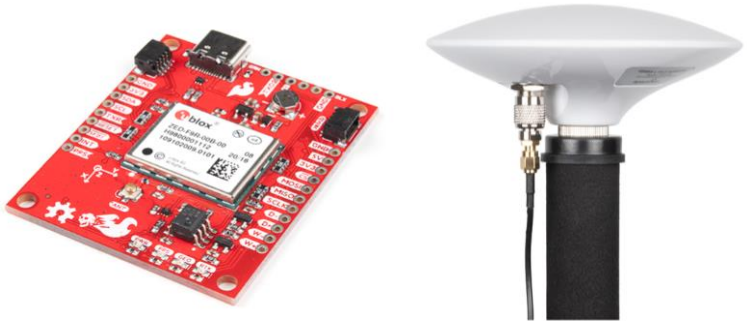


Figure 21. GNSS SparkFun ZED-F9R receiver (left) and SparkFun TOP106 antenna (right)

4.3.2 Data acquisition and analysis

Four data collections campaigns were conducted during Task 4:

1. Preliminary data collection (indoor, static occupation)
2. Outdoor environment (static occupation)
3. Outdoor environment flight trials
4. Clean visibility collection (static occupation)

The first two acquisitions were completed as preliminary assessment of the signal environment and scanner logging behavior, which informed flight test planning. Hardware limitations identified in the second and third campaigns prompted a final standalone cellular collection, and reoriented processing project 4.3.2.1 Preliminary data collection (Indoor environment)

For knowledge about the cellular scanning sensor and the cellular signals, a preliminary logging session was collected within an indoor environment to:

- Assess data for any teething issues.
- Understand the structure of the exported log files in preparation for data processing.
- Identify the tracked cell IDs to begin geolocating source cell towers.
- Note prominent frequencies present in the local environment for use in future spectrum masking to achieve optimal scanner logging rate.

The findings from this early occupation are reported within the framework of the various components and subprocesses involved in accomplishing the signal strength-based positioning technique.

It should be noted that the researchers applied another path loss model for indoor use, that is the ITU model because the Free space, Open field, and Hata models are all designed for the outdoor environment. More details about the ITU model are described in this section.

Visible cell IDs

A cell ID is a standardized, unique identification code associated with a specific transmitting cell (antenna), usually elevated by a tower-like foundation. Multiple cells are commonly arranged in an array structure on a single tower, oriented in different azimuth directions to maximize cellular coverage.

During the three-hour logging session, ten cell IDs were recorded by the scanner. In Figure 22, placeholder values for the actual cell ID codes are represented on the y-axis. An example of the actual cell ID visible in the indoor environment is 125711126, which is mapped to value 5 in the y-axis.

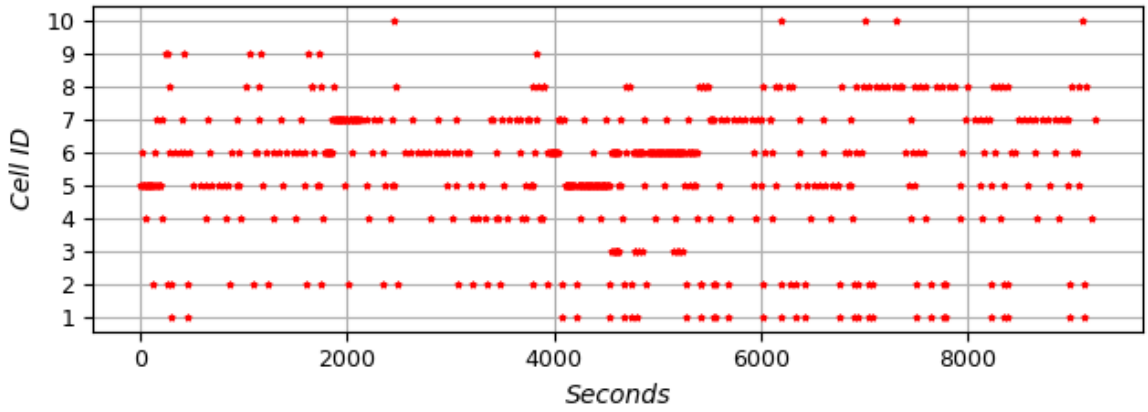


Figure 22. Cell IDs visible from an indoor environment.

As the scanner is iterating through the North American LTE spectrum, a portion of cell IDs (5, 6, 7) are tracked consistently for the 3-hour duration (Figure 23). Cell IDs 3, 9 and 10 are only tracked for a brief period. It should be noted that across the ten tracked cell IDs, all are shared among only three distinct cellular towers.

Identification of reliable cell IDs (and towers) can inform tower candidates for the positioning solution, as well as recurring frequencies which can influence the band masking for the flight collection, as covered in the next section.

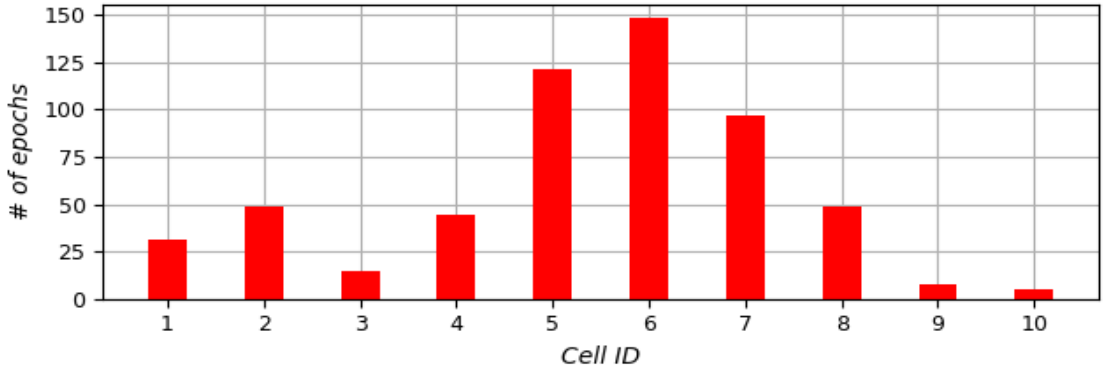


Figure 23. Cell IDs visible from an indoor environment.

Visible bands/frequencies

The PRiSM scanner has the capability to toggle on and off specified bands within the logging session settings, effectively omitting portions of the spectrum during a collection. Where iterating through the complete NA spectrum can take close to 30 minutes, masking the majority of the available bands to focus on those with high signal presence in the local environment will ideally reduce the iteration time to minutes or less. The preliminary office data presented some potential bands (Figure 24), where most recorded cell IDs transmit in band 4, 66, or 13. Of those results, 6 out of 10 cell IDs are band 4 signals whose frequencies are 2115, 2127.5, 2140 and 2150 MHz.

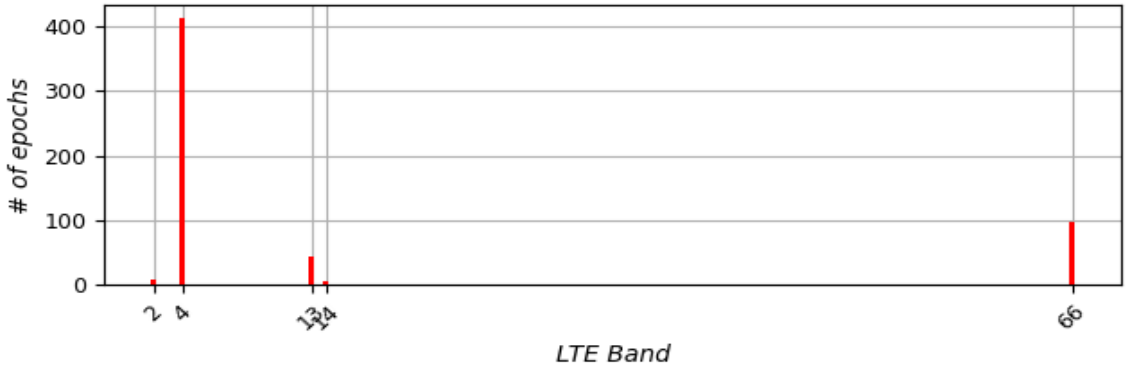


Figure 24. Cellular band channels visible from an indoor environment.

Received signal power

The cellular scanner logs the received signal power through “Reference signal received power” field along with other indicators like Received Signal Strength Indicator (RSSI), reference signal received quality, and signal-to-noise ratio.

Signal transmit power

Cell towers communicate the frequency and power of the source reference signal from each cell in a System Information Block Type 2 (SIB2) message.

A sample SIB2 hexadecimal value at a given epoch:

0830992b7ec9294ab81d0400c0002002029dcaaf082000c

01ddc801c64c000c0a20000700060021462a440c400000

Various resources can decode the SIB2 message, such as a browser-based tool hosted by Marben Products ("MARBEN ASN.1 Solutions: 3GPP LTE Messages Decoder" n.d.). Once translated, the reference signal transmit power is available within the <referenceSignalPower> tag:

```
<pdsch-ConfigCommon>
        <referenceSignalPower>

        </referenceSignalPower>
        <p-b>
                1
        </p-b>
</pdsch-ConfigCommon>
```

In this example, a particular cell reference signal transmit power is 20 dBm (highlighted).

During the office occupation, the transmit power of six cell IDs ranged between 18-21 dBm (Figure 25). Note the lack of variation in each respective signal transmit power. While fluctuation would easily be accounted for in the presented path loss math models, no SIB2 messages indicated noticeable change in transmitted power across all collections completed for Task 4.

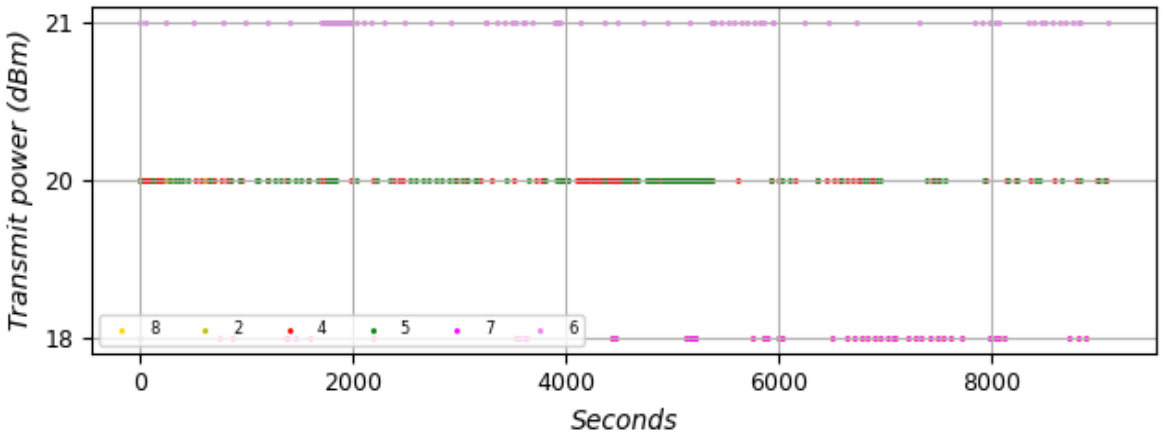


Figure 25. Signal transmit power per cell ID decoded from SIB2 messages, collected in an indoor environment.

Cell ID and tower matching

To calculate range from existing path loss models, the horizontal location and vertical height of the signal source, or cell, also needs to be known. While the PriSM receiver collects signal information from all mobile network providers within range, the only tower-related information logged is the unique cell ID, which provides no explicit details related to signal origin, which is the location of tower location. Communication tower construction and modification are regulated and documented by the Federal Communications Commission (FCC), and in the state of Alaska, by the local Borough. Tower permit records for all communication infrastructure currently in operation and within 10km of Fairbanks city limits were obtained from both sources: via an automated pull request on the Antenna Structure Registration online database for the FCC, and a formal public records request to the Fairbanks North Star Borough. These documents provide reliable location coordinates for towers that meet the criteria of the search parameters, as well as tower height, but still no directly related fields to match with the cell ID acquired in flight tests.

CellMapper and OpenCellID are two open access cell tower databases identified as potential intermediary resources for matching together the PriSM logs and permitting records. Both gather and compile crowdsourced cellular signal data recorded by smartphones of participating users. OpenCellID, which hosts a CSV download of the database of cellular towers on a global scale, includes cell ID, mobile network (MNC), and approximate location fields. This tabular data was initially used as a quality check, verifying similar cell ID values in the scanner logs were overlapping with the Fairbanks region cell IDs in addition to pairing the network provider to each cell ID though the MNC field. CellMapper is hosted on a browser interface that (1) provides more fields for each cell ID, (2) groups cell IDs into respective eNB ID, or unique tower identifier, and (3) offers a cell ID to eNB ID conversion tool on the same site. Similar to a cell and its designated cell ID, each cellular tower has a standardized unique identification number named eNodeB ID (eNB ID), which can act as the intermediary field needed. Using the CellMapper conversion tool to calculate the eNB ID term, tower cell IDs were able to be matched to tower location through crosschecking CellMapper

with Google Maps Street View imagery, and finally verifying the coordinates recorded in the FCC permit and/or Borough records matched.

Range estimation using ITU Indoor model

By obtaining transmit power and received power, the signal path loss is calculated. The relation between path loss (*PL*) and distance (*d*), as a function of frequency (*f*), path loss exponent (*N*) and number of floors (*n*) in a building is given by (ITU-Indoor model) (ITU-R P.1238 1, 1997, p.3):

$$PL\ (in\ dBm) = 20\log(f) + 10\,N\log(d) + L_f(n)\ - 28 \qquad (13)$$

For simplicity, *N* is considered 3 for all frequencies (*N* = 3 is valid for freq. around 2000 MHz), and the loss due to various floors is not considered. The true range is calculated from the location of the towers as well as an approximate location of the office using GNSS.

Table 5 shows the list of cell IDs, their signal frequencies, the range calculated using tower location from Open cell ID and Google Earth, and the range calculated using the path loss model. All the cell IDs shown in the table are from a single tower, with its location verified following the steps in the previous section. The true distance between the tower and the office is 1230 m, calculated within Google Earth Pro.

Table 5. Preliminary ranging results from the ITU Indoor Model.

Cell ID	Frequency [MHz]	Distance b/w GE and Office [m]	Range using ITU indoor model [m]
125711126	2140	~1230	954
126735112	1982.5	~1230	762
126735275	763	~1230	807

The range error calculated from the path loss model for the 3 cell IDs are 276, 468 and 423 m.

4.3.2.2 Static ground and flight occupations in the outdoor environment

From the preliminary data collection experiment, the payload and sensors were prepared for data collection in the field. For the outdoor environment testing, two planned acquisition campaigns were drafted and completed.

First, a series of three ~10 minutes occupations in the expected flight area (Figure 26). Cellular and GNSS signals were logged at each site with the sensors positioned in their flight payload structure (Figure 19), placed on the ground during logging. This data was assessed during the scheduling and drafting of the flight tests, with the intention to identify both prominent, reoccurring frequencies and

cell ID fields. Using common frequencies, a spectrum mask was developed to maximize the scanner sampling rate while maintaining a usable count of towers to produce a positioning result. With cell ID values, the tower matching process could begin to enable early path loss model testing using signal source location.

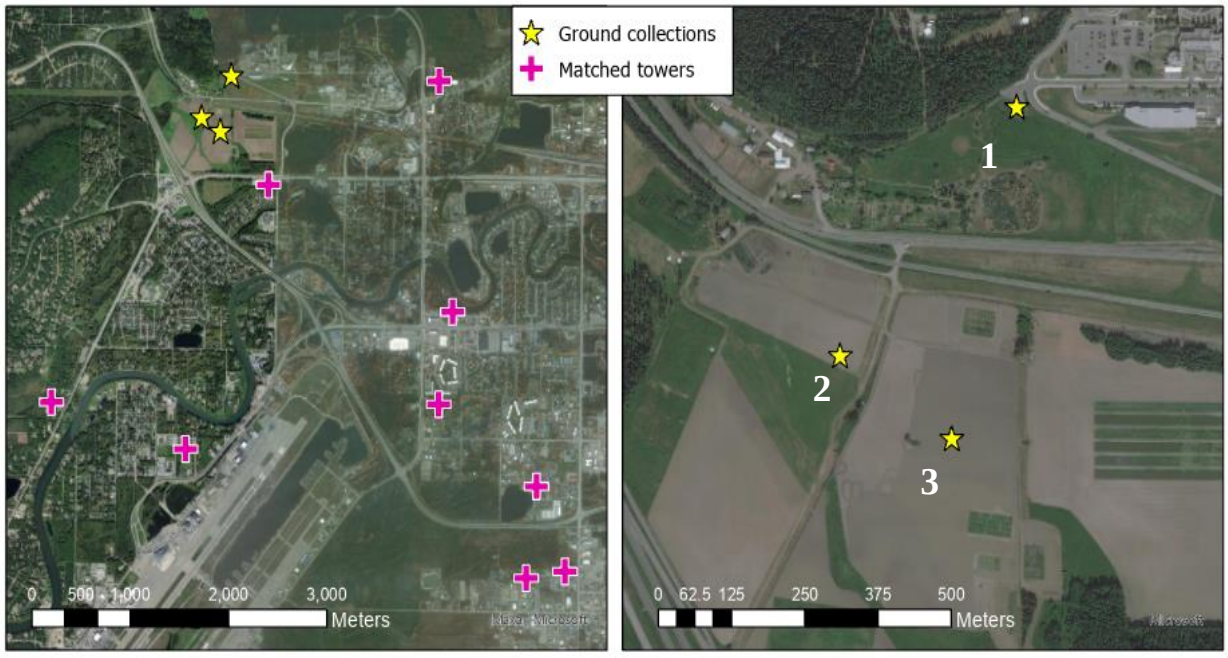


Figure 26. Subset of local towers matched to logged cell IDs fields in the ground occupations (left) and ground-based static collection sites (right).

Discrepancy in range estimation from a tower to two adjacent sites

The true range from a cell ID to sites 1 and 2 are 3520 m and 3120 m, respectively. The signal is transmitted at 751 MHz. Hence, Hata model is used for range estimation as it is valid from 500-1500 MHz.

The range error from sites 1 and 2 are shown in the left and right half of the Figure 27, respectively.

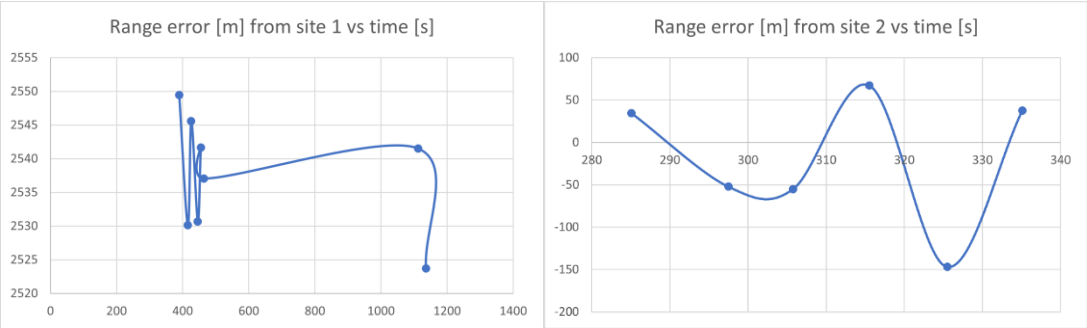


Figure 27. Range errors from Site 1 (left) and Site 2 (right).

Preliminary observations and discussion

The received signal power from the cell ID does not record with consistent intervals that are shown in the left plot in Figure 27. There were regular measurements from 400 s to 480 s, but no measurements until 1100 s. This is likely due to the scanner unnecessarily scanning for all the cell IDs and bands, as the current version of the firmware does not support the filtering.

Range error from site 1 is very high, ~ 2.5 km, but it is less than 150 m from site 2. There is no visible obstruction in the line-of-sight vector from the tower to sites 1 and 2 to explain the loss of received signal strength over 400 m distance. This may be due to the limitations in collecting ground data, or the applicability of the model.

Static flight tests data may reveal suitability of the model as human interference while collecting data wouldn't be there as the scanner will be mounted on an UAS.

Post-acquisition briefings from UAF and review of the preliminary ground-based data outlined above, hardware-specific limitations were identified that impacted future planning related to processing and flight test components, to be addressed in following sections. Limitations include:

1. The network scanner can only toggle *bands* in the scanned spectrum, not specific frequencies. This introduces iteration across a larger spectrum of frequencies than desired, and significantly decreases sampling rate of the logging session.
2. The scanner logs are unable to be synced to GNSS, device, or local time.

i. Flight tests and planning

Initial flight plans included two sets of flights, representing ideal and challenging signal environments respectively, comprised of waypoint-based static and trajectory occupations at varying altitudes, with intent to analyze static and real-time dynamic UAS flight. However, due to the discovery of limitations in the cellular hardware and challenges in flight timeframe and logistics, the original flight itinerary was adjusted and reduced.

Stationary acquisitions of incremental altitude were prioritized to account for asynchronous timestamps between sensors and UAS, and to record variation in received signals as verticality increases. Three static occupations of 6 to 10 minute duration at 15ft, 150ft, and 400ft AGL were manually flown and logged in a designated flight area, with flight crew manually marking down local timestamps of occupation start and end in reference to the isolated scanner clock (Figure 29).

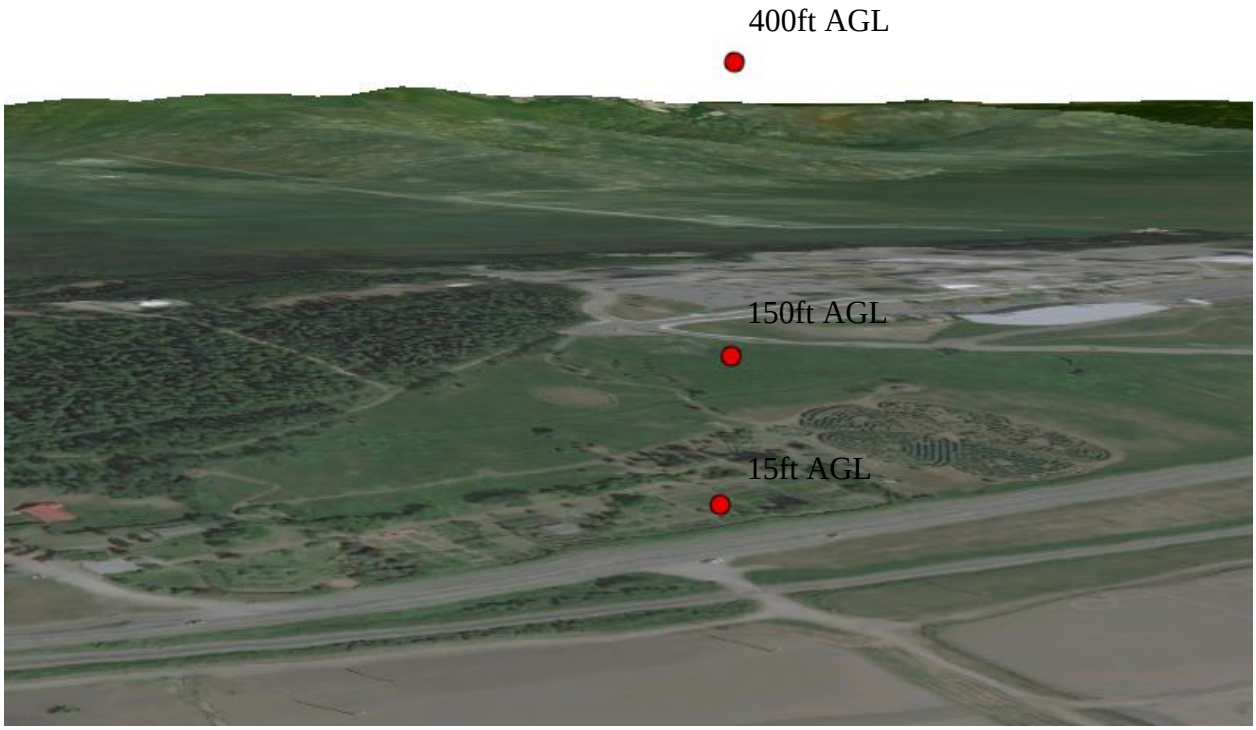


Figure 28. 3-D Scene visualizing the 15ft, 150ft, and 400ft AGL flight tests flown SW of the Univ. of AK campus.

Initial analysis of preliminary data noted strong variation in select towers' signal strength between each flight, and the preliminary ground-based data. The similarity between occupations and vicinity to reliable signal sources is expected to produce consistent signal clarity across the collections and days of acquisition. As represented in Figure 25, and seen in the variation of RSSI in the data logs, the tower transmit power remained constant, further supporting likelihood of an unidentified bias. Review of the antenna orientation (Figure 20) within the payload infrastructure was the primary theory for these unexpected fluctuations.

To accommodate the limited Task 4 timeframe, one more cellular-based collection was planned with the intention to compare results of the current data to a 'clean' occupation and identify the typical signal strength benchmark for locally available cell IDs. This will validate the existence of bias in the flight data and allow for testing suitability of introduced path loss models.

To validate the sub-optimal antenna placement, a 15-minute, ground-based occupation was collected with the standalone PriSM scanner. The collection was requested with intention to process a static, non-time dependent dataset with minimal visibility concerns in all azimuth directions. The device was placed in the same general area as the flight trials in Figure 29, atop a truck roof to reduce potential multipath effects with the omni-direction antenna tip pointed in the zenith direction. Figure 29 shows the "clean" data collection with the "correct" configuration of the antenna.

Figure 29. 'Clean' near-ground static cellular occupation collected at flight area with PriSM scanner.

Path loss comparison between "clean" and "challenged" scenarios

On average, a 3 dB power loss is observed from the flight data to the final 'clean' cellular occupation across three towers consistently shared between the dataset that is shown in Figure 30. This confirmed the likelihood of antenna placement as the cause of the unexpected flight data fluctuations.

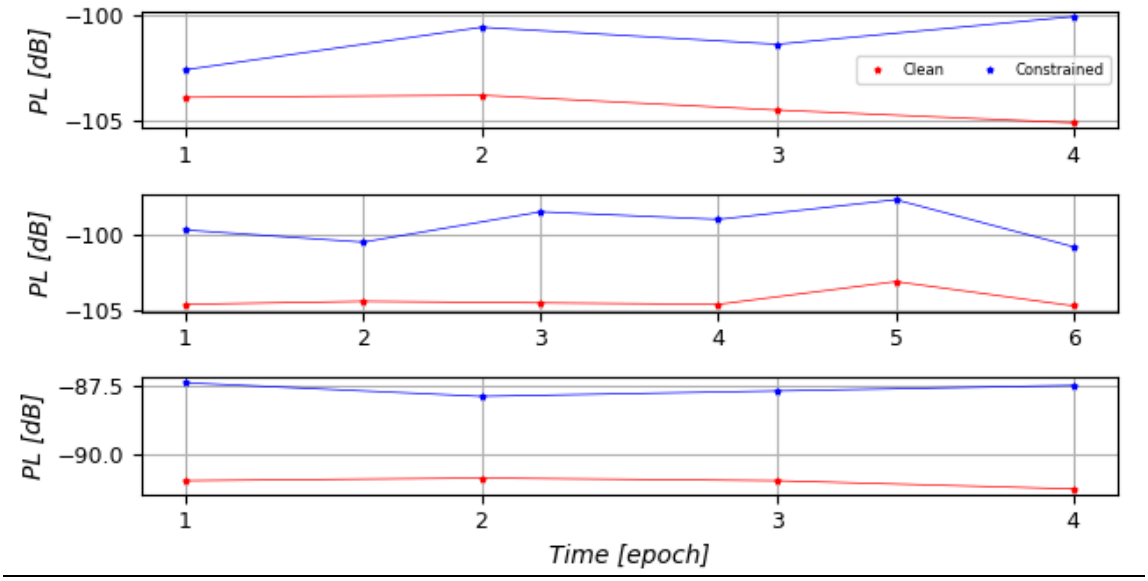


Figure 30. Path loss estimates for a clean (red) and challenged (blue) scanner antenna from 3 LTE tower.

Position estimation using GPS and LTE tower range measurements

Though the antenna position was sub-optimal during the flight trials, the researchers would like to demonstrate the usability of the cell tower measurements in UAS position estimation in GNSS-denied environments. The following approach was accomplished through post-processing, as a proof of concept, but can be applicable for onboard real-time implementation.

For the 150 ft flight, the researchers selected a cell tower that had the least range error (~ 500 m) to the UAS. Two case studies are pursued in which UAS position is estimated using:

1. 4 GPS satellites.
2. 3 GPS satellites and 1 LTE tower.

Note that both cases are extremely limited GNSS environment. In general, there are more than 6 GPS satellites in an open sky environment and the number of visible satellites becomes double or more if counting multi-constellation GNSS. However, considering the receiver and antenna grades on small UASs which usually receive GPS only, and flying in an urban canyon, visible satellites are limited that causes positioning degradation. In Case 1, the coordinates of UAS can be mathematically calculated, but a large error is expected because of the limited number of observations. In Case 2, only three GPS satellites are visible that cannot compute a position. To get 'any' level of position result, use a range estimate from a nearby cell tower and calculate a solution using hybrid positioning (introduced in Section 2C).

The true position of the 150 ft flight, the position estimated using 4 GPS satellites, and the position estimated using 3 GPS satellites and 1 LTE tower are shown in Figure 31. With only 3 GPS satellites, position estimation is not possible, but augmenting the algorithm with the range estimate from a

single tower, one can determine the position of UAS. The position error for this single epoch-based estimation is 594 m, considering the noisy range estimates from the cell tower, as well as the non-availability of other nearby LTE towers due to the challenged antenna position (Figure 31).

Despite summarized accuracy thresholds for this signal strength method, this result shows potential, in specific scenarios, to augment or aid the GNSS based positioning with measurements from LTE towers in a non-challenged antenna scenario.

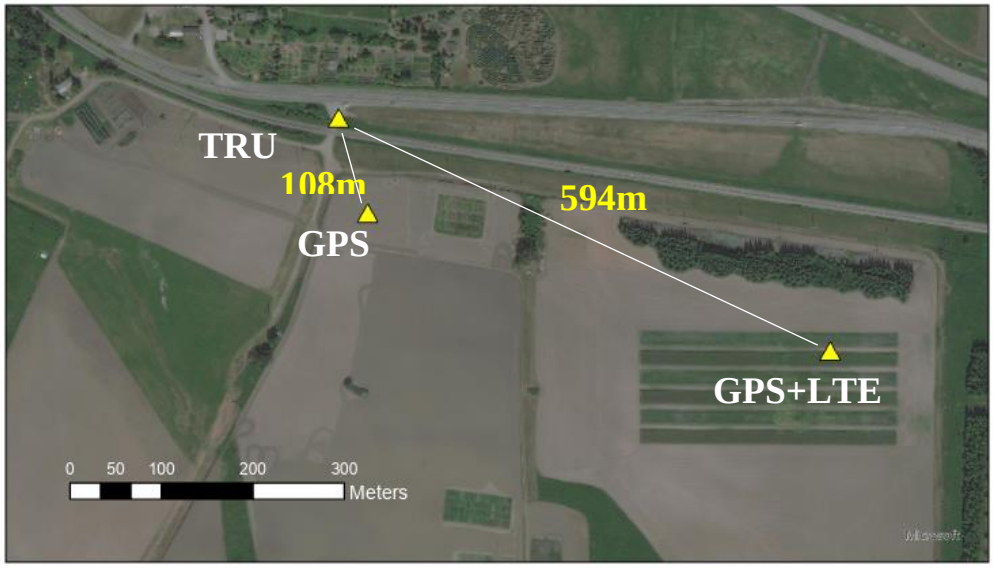


Figure 31. Visualization of the position estimate results for the 'challenged' 150ft flight, in case of 3 available GPS satellites.

4.4 Conclusion

4.4.1 Review of findings

Though hardware and logistical components limited the flight and processing potential for a true signal strength-based method in Task 4, productive characteristics and methods for leveraging cellular signals as a UAS-based navigation source can be identified from the case study.

RSSI-informed cellular positioning approaches fundamentally yield an accuracy threshold in the range of hundreds of meters, in-line with results found in the flight data analysis. This level of uncertainty can be utilized in very specific dropout conditions but is too high for practical and reliable application in real-time UAS operations. However, more precise methods available in literature such as carrier phase positioning, with use of a software defined receiver, have shown potential for meter to sub-meter in early test cases.

In the ideal scenario of achievable accuracy in cellular-based approach, an efficient method of locating and characterizing cellular tower parameters is still required to calculate a solution. This

report outlines available public resources and a viable approach to match local towers through intermediary cross-checks and redundant datasets, successful for the scope and scale of the tests conducted in Fairbanks, AK. For nation-wide UAS operations to plausibly leverage existing cellular networks as a positioning source, a database of tower infrastructure attributes would need to be available and regularly updated for public use, or through partnership avenues with network providers.

Current cellular infrastructure provided sufficient signal overlap in flight scans for this study area. When surveying the occurrence of unique visible cell IDs recorded during scanner occupations, cell ID counts from the 150ft and 400ft sessions were significantly higher than the 'clean' standalone PRiSM collection; even considering the two to three times shorter flight occupations, and cellular antenna visibility obstructions associated with the UAS payload. This indicates that existing 4G cell infrastructure can provide usable signals of opportunity throughout the current sUAS vertical flight space of 400ft altitude and below. Assuming this is true in a given location outside of the study area, it could be plausible to broadly consider most environments semi-ideal for eavesdropping on cell signals. Exceptions would notably include the urban canyon, or regions of high topographic variability, where obstructions create a challenging multipath environment even at higher AGL elevations. However, current projections of 5G infrastructure in urban environments could involve a dense next generation cellular network that could be considered for such scenarios in future UAS cellular navigation.

5 SPOOF – PROOF GPS AND ADS-B SECURITY CONSIDERATIONS & INTEGRATION OF ECD ALGORITHM TO ERAU SIMULATION ENVIRONMENT

5.1 Motivation

The motivation for the research conducted on ECD as mitigation scheme is that that both GPS (part of the GNSS family) and ADS-B systems are vulnerable to spoofing attacks on both manned and unmanned aircraft. In general, GPS vulnerabilities translate down to the more specific ADS-B subset which has its own vulnerabilities. This section will describe the work of Dr. Michael Eichelberger on *Robust Global Localization using GPS and Aircraft Signals*. He describes a functional tool known as CD to detect, mitigate and counter spoofing attacks on all stages of GPS. (Eichelberger 2019). The attacks on GPS then become part of the spoofing of the ADS-B systems that incorporate the GPS information within its data stream. However, since the spoofed GPS is part of the ADS-B data stream the same techniques can be used utilize to detect, mitigate, and counter spoofing attacks on the ADS-B system.

GPS is ubiquitous and is incorporated into so many applications (aircraft, ship, car /truck navigation; train routing and control; cellular network, stock market, and power grid synchronization) that it

makes a “rich” target for spoofing a receiver’s perceived location or time. Wrong information in time or space can have severe consequences.

ATC is partially transitioning from radar to a scheme in which Aircraft (A/C) transmit their current location twice per second, through ADS-B messages. This system is mandated in Europe and well under way in the US from 2020. The A/C determines their own location using GPS. If a wrong location is estimated by the on-board GPS receiver due to spoofing, wrong routing instructions will be delivered due to a wrong reported A/C location, leading to a potential A/C crash.

Ships depend heavily on GPS. They have few reference points to localize themselves apart from GPS. Wrong location indication can strand a ship, cause a collision, push off course into dangerous waters, ground a ship, or turn a ship into a ghost or a missile. 2017 incidents in the Black Sea and South China Seas have been documented. (Randall K Nichols et al. 2019) (Burgees 2017).

While planes and ships suffer spoofing attacks in the domain of location, an attacker may also try to change the perceived time of a GPS receiver. Cellular networks rely on accurate time synchronization for exchanging communication data packets between ground antennas and mobile handsets in the same network cell. Also, all neighboring cells of the network need to be time synchronized for seamless call handoffs of handsets switching cells and coordinating data transmissions in overlapping coverage areas. Since most cellular ground stations get their timing information from GPS, a signal spoofing attacker could decouple cells from the common network time. Overlapping cells might send data at the same time and frequencies, leading to message collisions and losses (Microsemi 2014). Failing communications networks can disrupt emergency services and businesses (Eichelberger 2019).

5.2 Spoofing

Threats and weaknesses show that large damages (even fatal or catastrophic) can be caused by transmitting forged GPS signals. False signal generators may cost only a few hundred dollars of software and hardware. Spoofing of location fixes for critical stakeholders can mean complete failure of mission.

A GPS receiver computing its location incorrectly or even failing to estimate any location at all can have different causes. Wrong localization solutions come from 1) a low SNR of the signal (examples: inside a building or below trees in a canyon); 2) reflected signals in multipath scenarios, or 3) deliberately spoofed signals. (Eichelberger 2019) discusses mitigating low SNR and multipath reflected signals. Signal spoofing is the most difficult case since the attacker can freely choose the signal power and delays for each satellite individually (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019).

Before discussing ECD – Collective detection maximum likelihood localization approach, (Eichelberger 2019) it is best to step back and briefly discuss GPS signals, classical GPS receivers, Assisted GPS (A-GPS), and snapshot receivers. Then the ECD approach to spoofing will show some real power by comparison. The power of the method is defined as enhanced spoofing detection, mitigation, and signal recovery capabilities.

5.3 Select locations with the most vulnerability to GPS spoofing

There have been select locations in the world identified as the most vulnerable to GPS spoofing based on lack of self-healing equipment. To combat the vulnerability, ECD hardens individual systems thus reducing reliance on networks like Differential Global Positioning Systems (DGPS) and Wide Area Augmentation System (WAAS).

Three examples:

- DGPS & WAAS (plus foreign equivalents): ground –based GPS correctional systems meant to help with GPS errors caused by Jamming/Spoofing/Environmental factors,
- Specific focus areas: Ukraine, CENTCOM, sea lanes in the Atlantic and Pacific, international navigation, South China Seas, Taiwan, Hawaii, Prepositioned S&R and oil drilling, and
- Locations without ground-based redundancy, making GPS - reliant operations more vulnerable.

5.4 GPS Signal

The GPS system consists of a control segment, space segment and user segment. The space segment contains the 24 orbiting satellites. The network monitor stations and ground control stations, and their antennas make up the control segment. The third and most important are the receivers which make up the user segment (USGPO 2021).

Satellites transmit signals in different frequency bands. These include the L1 and L2 frequency bands at 1.57542 GHz and 1.2276 GHz. Signals from different satellites may be distinguished and extracted from background noise using code division multiple access protocol (Department of Defense 2008). Each satellite has a unique Coarse / Acquisition code (C/A) of 1023 bits. The C/A codes are Pseudo Random Noise (PRN) sequences transmitted at 10.23 MHz which means they repeat every millisecond. The C/A code is merged using an XOR before being with the L1 or L2 carrier. The data broadcast has a timestamp called Hand Over Word (HOW) which is used to compute the location of the satellite when the packet was transmitted. The receiver needs accurate orbital information (aka ephemeris) about the satellite which changes over time. The timestamp is broadcast every six seconds, the ephemeris data can only be received if the receiver can decode at least 30 seconds of signal (Eichelberger 2019).

5.5 Classical Receivers

Classical GPS receivers use three stages when obtaining a location fix. They are Acquisition, Tracking, and localization.

Acquisition. The relative speed between satellite and receiver introduces a significant Doppler shift to the carrier frequency. GPS receiver locates the set of available satellites. This is achieved by correlating the received signal with the known C/A codes from satellites. (Eichelberger 2019).

Tracking. After a set of satellites has been acquired, the data contained in the broadcast signal is decoded. Doppler shifts and C/A code phase are tracked using tracking loops. After the receiver obtains the ephemeris data and HOW timestamps from at least four satellites, it can start to compute its location (Eichelberger 2019).

Localization. Localization in GPS is achieved using signal Time of Flight (ToF) measurements. ToFs are the difference between the arrival times of the HOW timestamps decoded in the tracking stage of the receiver and those signal transmission timestamps themselves. The local time at the receiver is unknown and the localization is done using pseudo-ranges. The receiver location is usually found using least-squares optimization (Eichelberger 2019) (Wikipedia 2023).

A main disadvantage of GPS is the low bit rate of the navigation data encoded in the signals transmitted by the satellites. The minimal data necessary to compute a location fix, which includes the ephemerides of the satellites, repeats only every 30 seconds.

5.6 A-GPS (ASSISTED GPS) – Reducing the Start-up Time

Assisted GPS (A-GPS) drastically reduces the start-up time by fetching the navigation data over the Internet, commonly by connecting via a cellular network. Data transmission over cellular networks is faster than decoding the GPS signals and normally only takes a few seconds. The ephemeris data is valid for 30 minutes. Using that data, the acquisition time can be reduced since the available satellites can be estimated along with their expected Doppler shifts. With A-GPS, the receiver still needs to extract the HOW timestamps from the signal. However, these timestamps are transmitted every six seconds, which translates to how much time it takes the A-GPS receiver to compute a location fix. (Eichelberger 2019)

5.7 Coarse - Time Navigation

Coarse -Time Navigation (CTN) is an A-GPS technique which drops the requirement to decode the HOW timestamps from the GPS signals. The only information used from the GPS signals are the phases of the C/A code sequences which are detected by a matched filter. Those C/A code arrival times are related to the sub-milliseconds unambiguously, the deviation may be no more than 150 km

from the correct values. Since the PRN sequences repeat every millisecond, without considering navigation data flips in the signal, CTN can in theory compute a location from one millisecond of the sampled signal. Noise can be an issue with such short signal recordings because it cannot be filtered out the same way with longer recordings of several seconds. The big advantage is that signal processing is fast and power- efficient and reduces the latency of the first fix. Since no metadata is extracted from the GPS signal, CTN can often compute a location even in the presence of noise or attenuation (Van Diggelen 2009).

5.7 Snapshot Receivers

Snapshot receivers aim at the remaining latency that results from transmission of timestamps from satellites every six seconds. Snapshot receivers can determine the ranges to the satellite modulo 1 ms, which corresponds to 300 km.

5.8 Collective Detection

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combines all the available information and decide only at the end of the computation. This technique is critical to the (Eichelberger 2019) (R K Nichols et al. 2022) invention to mitigate spoofing attacks on GPS or ADS-B. CD can tolerate a few low-quality satellite signals and is more robust than CTN. CD requires a lot of computational power. CD can be sped up by a branch and bound approach which reduces the computational power per location fixed to the order of one second even for uncertainties of 100 km and a minute. CD improvements and research has been plentiful (Eichelberger 2019) (AXELRAD et al. 2011; Liu et al. 2012) (Bissig, Eichelberger, and Wattenhofer 2017a).

5.9 ECD

Dr. Manuel Eichelberger's *CD – Collective detection maximum likelihood localization approach*, his method not only can *detect* spoofing attacks but also *mitigate* and recover the true signal. The ECD approach is a robust algorithm to mitigate spoofing. ECD can differentiate closer differences between the correct and spoofed locations than previously known approaches (Eichelberger 2019). Commercial Of The Shelf (COTS) products have little spoofing integrated defenses. Military receivers use symmetrically encrypted GPS signals which are subject to a "replay" attack with a small delay to confuse receivers.

ECD solves even the toughest type of GPS spoofing attack which consists of spoofed signals with power levels similar to the authentic signals. (Eichelberger 2019) ECD achieves median errors under 19 m on the TEXBAT dataset, which is the de facto reference dataset for testing GPS anti-spoofing algorithms (Ranganathan, Ólafsdóttir, and Capkun 2016) (Wesson 2014). The ECD approach uses

only a few milliseconds worth of raw GPS signals, so called snapshots, for each location fix. This enables offloading the computation into the Cloud, which allows knowledge of observed attacks. Existing spoofing mitigation methods require a constant stream of GPS signals and track those signals over time. Computational load is increased because fake signals have to be detected, removed, or bypassed (Eichelberger 2019).

5.10 RESEARCH TO 2016: SURVEY OF EFFECTIVE GPS SPOOFING COUNTERMEASURES

Because of the overwhelming dependence on GPS in every sector, ranging from civilian to military, researchers have been trying to desperately find a complete solution to meet spoofing threat. To understand that ECD (the following sections) is a significant and impactful departure from past efforts, it is necessary to briefly cover the prevailing contemporary literature. Haider and Khalid in 2016 published an adequate survey of spoofing countermeasures up through the end of 2016. (Haider and Khalid 2016).

5.10.1 Spoofing Techniques

According to (Haider & Khalid, 2016) there are three common GPS Spoofing techniques with different sophistication levels. They are simplistic, intermediate, and sophisticated (Humphreys et al., n.d.).

The ***simplistic spoofing attack*** is the most commonly used technique to spoof GPS receivers. It only requires a COTS GPS signal simulator, amplifier, and antenna to broadcast signals towards the GPS receiver. It was performed successfully by Los Alamos National Laboratory in 2002 (Warner and Johnston 2003). Simplistic spoofing attacks can be expensive as the GPS simulator can run $400K and heavy (not mobile). Simulator signals are not synchronized by the available GPS signal and detection is easy.

In the ***intermediate spoofing attack***, the spoofing component consists of GPS receiver to receiver genuine GPS signal and spoofing device to transmit a fake GPS signal. The idea is to estimate the target receiver antenna position and velocity and then broadcast a fake signal relative to the genuine GPS signal. This type of spoofing attack is difficult to detect and can be partially prevented by use of an IMU (Humphreys et al., n.d.).

In ***sophisticated spoofing attacks***, multiple receiver-spoofer devices target the GPS receiver from different angles and directions. The angle-of-attack defense against GPS spoofing in which the angle of reception is monitored to detect spoofing fails in this scenario. The only known defense successful against such an attack is cryptographic authentication (Humphreys et al., n.d.).

Note that prior research on spoofing was to exclude the fake signals and focus on a single satellite. ECD includes the fake signal on a minimum of four satellites, and then progressively / selectively eliminates their effect until the real weaker GPS signals become apparent (Eichelberger 2019).

5.11 GPS SPOOFING RESEARCH: IMPACT AND SIGNIFICANCE OF THE ECD DEFENSE

Three tracks of research are most relevant to ECD / CD**:** Maximum Likelihood Localization, Spoofing Mitigation algorithms and Successive Signal Interference Cancellation (SIC). Note that historical spoofing research focusses primarily on detection of singular Standard Positioning Service (SPS) source attacks. The focus on mitigation, correction and recovery attending to multiple spoofing signals on multiple satellite attack surface is the hallmark of ECD.

5.11.1 Maximum Likelihood Localization

CD is a maximum likelihood GPS localization technique. It was proposed it 1996 but considered computationally infeasible at that time (Spilker and Parkinson 1996). CD was first implemented by Axelrad et al. in 2011 (AXELRAD et al. 2011). The search space contained millions or more location hypotheses. Improvements in the computational burden were found using various heuristics (Zhengxuan 2016) (Cheong et al., n.d.). A breakthrough came with the proposal of a branch-and-bound algorithm that finds the optimal solution within ten seconds running on a single CPU thread (Bissig, Eichelberger, and Wattenhofer 2017b).

5.11.2 Spoofing Mitigation

GPS spoofing defenses have been intensively studied. Most of them focus on detecting spoofing attacks. There is a paucity of prior research for spoofing mitigation and recovering from successful attacks by finding and authenticating the correct signals (Psiaki and Humphreys 2016). In contrast to the vast research on GPS spoofing, there is a lack of commercial, civil receivers with anti-spoofing capabilities. ECD inherently mitigates spoofing attacks and is anticipated to be a very impactful tool in mitigating the attacks.

Spoofing hardware performing a sophisticated seamless satellite-lock takeover attack has been built (Humphreys & al., 2008). Challenges associated with spoofing are matching the spoofed and authentic signals ‘amplitudes at the receiver, which might not be in line of sight and moving (Schmidt & al, 2016).

It is practically feasible for a spoofer to erase the authentic signals at a 180-degree phase offset (M.L. Psiaki & Humphreys, 2016). This is one of the strongest attacks that can only be detected with multiple receiver antennas or by a moving receiver (M.L. Psiaki & Humphreys, 2016). For signal erasure to be feasible, the spoofer needs to know the receiver location more accurately than the GPS

L1 wavelength, which is 19 cm. Receivers with only a single antenna cannot withstand such an erasure attack. ECD targets single-antenna receivers and does not deal with signal erasure (Eichelberger 2019). In all other types of spoofing attacks, including signal replay and multiple transmission antenna implementations, the original signals are still present and ECD remains robust (Eichelberger 2019). Detecting multi-antenna receivers and differentiating signal timing consistencies is covered in (Tippenhauer et al. 2011).

The GPS anti-spoofing work most relevant to ECD is based on joint processing of satellite signals and the maximum likelihood localization. One method is able to mitigate a limited number of spoofed signals by vector tracking of all satellite signals (Jafarnia-Jahromi et al. 2012). A similar technique is shown to be robust against jamming and signal replay (Ng and Gao 2016).

5.11.3 Successive Signal Interference Cancellation

A key factor in the effectiveness of ECD is it uses an iterative signal damping technique with spoofing signals similar to SIC. SIC removes the strongest received signals one by one in order to find the weaker signals and have been used with GPS signals before (López-Risueño and Seco-Granados 2005) (Madhani et al. 2003). That work is based on a classical receiver architecture which only keeps a signal's timing, amplitude, and phase. The ECD has its own snapshot receiver based on CD, which directly operates in the localization domain and does not identify individual signals in an intermediate stage. It is impossible to differentiate between authentic and spoofed signal, *a priori*, ECD does not remove signals from the sample data. Otherwise, the localization algorithm might lose the information from authentic signals. Instead, ECD dampens strong signals by 60% to reveal weaker signals. This can reveal localization solutions with lower CD likelihood (Eichelberger 2019).

5.11.4 GPS Signal Jamming

The easiest way to prevent a receiver from finding a GPS location is jamming the GPS frequency band. GPS signals are weak and require sophisticated processing to be found. Satellite signal jamming worsens the SNR of the satellite signal acquisition results. ECD algorithms achieve a better SNR than classical receivers and are able to tolerate more noise or stronger jamming (Eichelberger 2019).

A jammed receiver is less likely to detect spoofing since the original signals cannot be accurately determined. The receiver tries to acquire any satellite signals it can find. The attacker only needs to send a set of valid GPS satellite signals stronger than the noise floor, without any synchronization with the authentic signals (Eichelberger 2019).

There is a more powerful and subtle attack on top of the jammed signal that may be utilized. The spoofer can send a set of satellite signals with adjusted power levels and synchronized to the authentic

signals to successfully spoof the receiver (Eichelberger 2019). So even if the receiver has countermeasures to differentiate the jamming, the spoofer signals will be accepted as authentic.(R K Nichols et al. 2022).

5.11.5 Two Robust GPS Signal Spoofing Attacks and ECD

Two of the most powerful GPS signal spoofing attacks are: Seamless Satellite-Lock Takeover (SSLT) and Navigation Data Modification (NDM). A description of the performance of ECD in each is provided.

5.11.6 Seamless Satellite-Lock Takeover (SSLT)

The most powerful attack is a *seamless satellite-lock takeover*. In such an attack, the original and counterfeit signals are identical with respect to the satellite code, navigation data, code phase, transmission frequency, and received power. This requires the attacker to know the location of the spoofed device precisely, so that ToF and power losses over a distance can be factored in. After matching the spoofed signals with the authentic ones, the spoofer can send its own signals with a small power advantage to trick the receiver into tracking those instead of the authentic signals. A classical receiver without spoofing countermeasures, like tracking multiple peaks, is unable to mitigate or detect the SSLT attack, and there is no indication of interruption of the receiver's signal tracking (Eichelberger 2019).

5.11.7 Navigation Data Modification (NDM)

In NDM the attacker has two attack vectors: modifying the signals code phase or altering the navigation data. The former changes the signal arrival time measurements. The latter affects the perceived satellite locations. Both influence the calculated receiver location. ECD works with snapshot GPS receivers and are not vulnerable to NDM changes as they fetch information from other sources like the Internet. ECD deals with modified, wireless GPS signals.

5.11.8 ECD Algorithm Design

ECD is aimed at single-antenna receivers. Its spoofing mitigation algorithm object is to identify all localization solutions. It is based on CD because 1) CD has improved noise tolerance compared to classical receivers, 2) CD is suitable for snapshot receivers, 3) CD is not susceptible to navigation data modifications, and 4) CD computes a location likelihood distribution which can reveal all likely receiver locations including the actual location, independent of the number of spoofed and multipath signals. ECD avoids all the spoofing pitfalls and signal selection problems by joining and

transforming all signals into a location likelihood distribution. Therefore, it defeats the top two GPS spoofing signal attacks (Eichelberger 2019).

Relating to the 4th point, spoofing and multi-path signals are similar from a receiver's perspective. Both result in several observed signals from the same satellite. The difference is that multipath signals have a delay dependent on the environment while spoofing signals can be crafted to yield consistent localization solution at the receiver. In order to detect spoofing and multipath signals, classical receivers can be modified to track an arbitrary number of signals per satellite, instead of only one (Shaukat et al., n.d.). In such a receiver, the set of authentic signals – one signal from each satellite – would have to be correctly identified. Any selection of signals can be checked for consistency by verification that the resulting residual error of the localization algorithm is exceedingly small. This is a combinatorically difficult problem. For n satellites and m transmitted sets of spoofed signals, there are $(m+1)^n$ possibilities for the receiver to select a set of signals. Only m + 1 of those will result in a consistent localization solution, which represents the actual location and m spoofed locations. ECD avoids this signal selection problem by joining and transforming all signals into a location likelihood distribution (Eichelberger 2019).

ECD only shows consistent signals, since just a few signals overlapping (synced) for some location hypotheses do not accumulate a significant likelihood. All plausible receiver locations – given the observed–signals - have a high likelihood. Finding these locations in four dimensions, space, and time, is computationally expensive (Bissig, Eichelberger, and Wattenhofer 2017b).

5.11.9 Branch and Bound

To reduce the computational load comparing to exhaustively enumerating all the location hypotheses in the search space, a fast CD leveraging branch and bound algorithm is employed. (Eichelberger 2019) describes the modifications to the B&B algorithm for ECD in copious detail in chapter 6. Eichelberger also discusses acquisition, receiver implementation and experiments using the TEXBAT database. One of the key points under the receiver implementation concerns correlation of C/A codes.

The highest correlation is theoretically achieved when the C/A code in the received signal is aligned with the reference C/A code. Due to the pseudo-random nature of the C/A codes, a shift larger than one code chip from the correct location results in a low correlation value. Since one code chip has a duration of 1/1023 ms, the width of the peaks found in the acquisition vector is less than 2% of the total vector size. ECD reduces the maximum peak by 60% in each vector. A detection for partially overlapping peaks prevents changes to those peaks. Reducing the signal rather than eliminating it has little negative impact on accuracy. Before using these vectors in the next iteration of the algorithm, the acquisition result vectors are normalized again. This reduces the search space based on the prior iteration (Eichelberger 2019).

5.11.10 ADS-B Security

We next move into the subset problem, namely ADS-B systems on aircraft both manned and unmanned. ADS-B ubiquitously uses GPS location and signal receiver technologies. ADS-B has an extremely high dependency on communication and navigation (GNSS) systems. This is a fundamental cause of insecurity in the ADS-B system. It inherits the vulnerabilities of those systems and results in increased Risk and additional threats (Randall K Nichols et al. 2019; R K Nichols et al. 2022). Another vulnerability of the ADS-B system is its broadcast nature without security measures. These can easily be exploited to cause other threats such as eavesdropping aircraft movement with the intention to harm, message deletion, and modification. The system's dependency on the on-board transponder is also considered a major vulnerability, which is shared by the Secondary Surveillance Radar (SSR). This vulnerability can be exploited by aircraft hijackers to make the aircraft movements invisible (ALI 2019).

5.11.10.1 ADS-B Standards

ICAO has stressed including provisions for the protection of critical information and communication technology systems against cyberattacks and interference as stated in the Aviation Security Manual Document 8973/8 (ICAO 2021). This was further emphasized in Air Traffic Management (ATM) Security Manual Document 9985 AN/492 to protect ATMs against cyberattacks (ICAO 2021). There is a current IEEE 4-PAR standard in the works (proposed 25 April 2023 by SC 5 on Self-Healing systems) entitled: "Title: Standard for Self-healing GPS Navigation Signals that have been Jammed, Spoofed or otherwise Degraded."

5.11.10.2 ADS-B Security Requirements

Strohmeier, et al. (Strohmeier, Lenders, and Martinovic 2014) and Nichols, et al. (Randall K Nichols et al. 2019) have both outlined a set of security requirements for piloted aircraft and unmanned aircraft, respectively. Here are the combined security requirements for the ADS-B system coordinated with the standard information security paradigm of Confidentiality, Integrity & Availability:

- Data integrity
    - The system security should be able to ensure that ADS-B data received by the ground station or other aircraft (A/C) or UAS (if equipped) are the exact message transmitted by the A/C. It should also be able to detect any malicious modification to the data during the broadcast.
- Source integrity

    - The system security should be able to verify that the ADS-B message received is sent by the actual owner (correct A/C) of the message.
- Data origin (location / position fix) authentication
    - The system security should be able to verify that the positioning information in the ADS-B message received is the original position of the A/C at the time of transmission.
- Low impact on current operations
    - The system security hardware / software should be compatible with the current ADS-B installation and standards.
- Sufficiently quick and correct detection of incidents
- Secure against DOS attacks against computing power
- System security functions need to be scalable irrespective of traffic density
- Robustness to packet loss

5.11.10.3 Vulnerabilities in ADS-B system

Vulnerability in this section refers to the Ryan Nichols (RN) equations for information Risk determination. A vulnerability is a weakness in the system that makes it susceptible to exploitation via a threat or various types of threats (Randall K Nichols et al. 2019). ADS-B system is vulnerable to security threats. The Risk Assessment is covered in CHAPTER 3: SPACE ELECTRONIC WARFARE, SIGNAL INTERCEPTION, ISR, JAMMING, SPOOFING, & ECD (NICHOLS & MAI) of (R.K.Nichols & et.al., 2022). It is also discussed briefly in CHAPTER 10: SPACE ELECTRONIC WARFARE (NICHOLS) an upcoming textbook (Nichols & Carter, CHAPTER 10: SPACE ELECTRONIC WARFARE (NICHOLS), 2023).

5.11.11 Broadcast Nature of RF Communications

ADS-B principle of operation, system components, integration and operational environment are adequately discussed in Chapter 4 of (ALI 2019). The ADS-B system broadcasts ADS-B messages containing A/C state vector information and identity information via RF communication links such as 1090 Extended Squitter Data Link (1090ES), universal access transceiver or VHF data link Mode 4. The broadcast nature of the wireless networks without additional security measures is the main vulnerability in the system (R K Nichols et al. 2022).

5.11.12 No Cryptographic Mechanisms

Neither ADS-B messages are encrypted by the sender at the point of origin, nor the transmission links. There are no authentication mechanisms based on robust cryptographic security protocols. The ICAO ("What Is a NOTAM? | AIRPORTS AUTHORITY OF INDIA," n.d.) has verified that there is no cryptographic mechanism implemented in the ADS-B protocol. Newer implementations have additional protections, however UAS systems are notoriously weak in terms of security.

5.11.13 ADS-B COTS

ADS-B receivers are available in COTS at affordable prices. The receiver can be used to track ADS-B capable A/C flying within a specific range of the receiver. The number of ADS-B tracking gadgets for all kinds of media is growing every year. They can be used to hack the systems on UAS (Randall K Nichols et al. 2019).

5.11.13.1 Shared Data

As a result of COTS availability of ADS-B receivers, various parties, both private and public, are sharing real-time air traffic information on A/C on the internet. There are numerous websites on the internet that provide digitized live ADS-B traffic data to the public, e.g., flightradar24.com, radarvirtuel.com, and Flightaware. The available of the data and the capability to track individual A/C movements open the door to malicious parties to perform undesired acts that may have safety implications (ALI 2019).

5.11.14 ASTERIX Data Format

All-purpose Structured EUROCONTROL Surveillance Information eXchange (ASTERIX) is a binary format for information exchange in aviation (EUROCONTROL 2013). ADS-B data is encoded into ASTERIX CAT 21 format and transmitted by ADS-B equipped A/C to ADS_B ground stations. The data is then decoded into usable form for ATC use. The ASTERIX format decoding guidance, source code and tools are widely available in the public domain (ALI 2019).

5.11.15 Dependency on the On-Board Transponder

ADS-B encoding, and broadcast are performed by either the transponder (for 1090ES) or an emitter (for universal access transceiver / VHF data link Mode 4) on board the A/C. Therefore, the ADS-B aircraft surveillance is dependent on the on-board equipment. There is a vulnerability (not cyber or spoofing) whereby the transponder or emitter can be turned off inside the cockpit. Obviously, the A/C becomes invisible and SSR and Traffic Collision Avoidance System (TCAS) operation integrity is affected.

5.11.16 Complex System Architecture and Passthrough of GNSS Vulnerabilities

ADS-B is an integrated system, dependent on an on-board navigation system to obtain information about the state of the A/C as well as a communication data link to broadcast the information to ATC on the ground and other ADS-B equipped A/C. The system interacts with external elements such as humans (controllers and pilots) and environmental factors. The integrated nature of the system increases the system's vulnerability. The vulnerabilities of the GNSS on which the system relies to obtain A/C positioning information are inherited by the system. Vulnerabilities of the

communications links are also inherited by the ADS-B system (ALI 2019) (Eichelberger 2019) (The Royal Academy of Engineering 2011).

5.11.17 Threats in ADS-B system

Threats in this section refers to the Ryan Nichols (RN) equations for information Risk determination. A threat is an action exploiting a vulnerability in the system to cause damage or harm specifically to A/C and to the Air Traffic Services (ATS), intentionally or unintentionally (Randall K Nichols et al. 2019) ADS-B system is vulnerable to security threats.

5.11.18 Eavesdropping

The broadcast nature of ADS-B RF communication links without additional security measures (cryptographic mechanisms) enables the act of eavesdropping into the transmission. Eavesdropping can lead to serious threats such as targeting specific A/C movement information with intention to harm the A/C. This can be done with more sophisticated traffic and signal analysis using available sources such as Mode S and ASDS-B capable open-source GNU Radio modules or Software Defined Radio. Eavesdropping is a violation of confidentiality and compromises system security (ALI 2019).

5.11.19 Data-Link Jamming

Data-link jamming is an act of deliberate / non-deliberate blocking, jamming, or causing interference in wireless communications (Randall K Nichols and Lekkas 2002). Deliberate jamming using a radio jammer device aims to disrupt information flow (message sending /receiving) between users within a wireless network. Jammer devices can be easily obtained as COTS devices (Strohmeier, Lenders, and Martinovic 2014) (Randall K Nichols and Lekkas 2002). Using the Ryan Nichols equations, the impact is severe in aviation due to the large coverage area (airspace) which is impossible to control. It involves safety critical data; hence the computed Risk / lethality level is high (Randall K Nichols and Lekkas 2002). The information security quality affected is availability because jamming stops the A/C or ground stations or multiple users within a specific area from communicating. On Air Traffic Control

Jamming is performed on ADS-B frequencies, e.g., 1090MHz. Targeted jamming attack would disable ATS at any airport using air traffic control center. Jamming a moving A/C is difficult but feasible (Strohmeier, Lenders, and Martinovic 2014).

ADS-B system transmitting on 1090ES is prone to unintentional signal jamming due to the use of the same frequency (Mode S 1090 MHz) by many systems such as SSR, TCAS, Multilateration System (MLAT), and ADS-B, particularly in dense space (ALI 2019). Not only is ADS-B prone to jamming, so is SSR (Adamy 2001).

While the ADS-B signal may be jammed, there is still some of the remaining signal that the ECD method can use to detect, mitigate and counter spoofing attacks. Therefore, the ECD method is still effective in determining the true signal and mitigate the threat.

5.11.19.1 Two Types of Jamming Threats for ADS-B

Apart from GNSS (positioning source for ADS-B) jamming, the main jamming threats for the ADS-B system include GS Flood Denial and A/C Flood Denial.

5.11.19.1.1 Ground Station Flood Denial (GSFD)

The GSFD blocks 1090 MHz transmissions at the ADS-B ground station. There is no difficulty in gaining close proximity to a ground station. Jamming can be performed using a low-power jamming device to block ADS-B signals from A/C to the ground station. The threat does not target individual A/C. It blocks ADS-B signals from all A/C within the range of the ground station.

5.11.19.1.2 Aircraft Flood Denial

Aircraft Flood Denial jamming blocks signal transmission to the A/C. This threat disables the reception of ADS-B IN messages, TCAS and interrogation from wide area multilateration/MLAT and SSR. It is exceedingly difficult to gain close proximity to a moving A/C. The attacker needs to use a high-powered jamming device. According to (McCallie, Butts, and Mills 2011) , these devices are not easy to obtain at the time of the study. What is true is the jamming function will be ineffective as soon as the A/C moves out of the specific range of the jamming device. Better attempts can be made from within the A/C through the use of miniature electronics.

5.11.20 ADS-B Signal Spoofing

ADS-B signal spoofing attempts to deceive an ADS-B receiver by broadcasting fake ADS-B signals, structured to resemble a set of normal ADS-B signals or by re-broadcasting genuine signals captured elsewhere or at a different time. Spoofing an ADS-B system is also known as message injection because fake (ghost) A/C are introduced into the air traffic. The vulnerability of the system – having no authentication measures implemented at the system's data link layer – enables this threat. Spoofing is a hit on the security goal of Integrity. This leads to undesired operational decisions by controllers or surveillance operations in the air or on ground. The threat affects both ADS-B IN and OUT systems (ALI 2019). Spoofing threats are of two basic varieties: Ground Station Target Ghost Injection / Flooding and Ground Station Target Ghost Injection / Flooding.

5.11.20.1 Ground Station Target Ghost Injection / Flooding

Ground Station Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single A/C or multiple fake (ghost) A/C into a ground station. This will cause single /multiple fake (ghost) A/C to appear on the controller's working position (radar screen).

5.11.20.2 Aircraft Target Ghost Injection / Flooding

Aircraft Target Ghost Injection / Flooding is performed by injecting ADS-B signals from a single A/C or multiple fake (ghost) A/C into an airplane in flight. This will cause ghost A/C to appear on the TCAS and Cockpit Display of Traffic Information (CDTI) screens in the cockpit to go irrational. Making the situation worse, the fake data will also be used by airborne operations such as Airborne Collision Avoidance System, Air Traffic Situational Awareness, in trail procedure and others for aiding A/C navigation operations (ALI 2019).

5.11.20.3 ADS-B message deletion

An A/C can be made to look like it has vanished from the ADS-B based air traffic by deleting ADS-B message broadcast from the A/C. This can be done by two methods: destructive interference and constructive interference. Destructive interference is performed by transmitting an inverse of an actual ADS-B signal to an ADS-B receiver. Constructive interference is performed by transmitting a duplicate of the ADS-B signal and adding the two signal waves (original and duplicate). The two signal waves have to be of the same frequency, phase and travelling in the same direction. Both approaches will be result in discarded by the ADS-B receiver as corrupt (ALI 2019).

5.11.20.4 ADS-B Message Modification

ADS-B message modification is feasible on the physical layer during transmission via datalinks using two methods: Signal Overshadowing and Bit-flipping. Signal overshadowing is done by sending a stronger signal to the ADS-B receiver, whereby only the stronger of the two colliding signals is received. This method will replace either the whole target message or part of it. Bit flipping is an algorithmic manipulation of bits. The attacker changes bits from 1 to 0 or vice versa. This will modify the ADS-B message and is a clear violation of the security goal of Integrity (Strohmeier, Lenders, and Martinovic 2014) (Strohmeier, 2015). This attack will disrupt ATC operations or A/C navigation.

5.12 ECD effectiveness to identified threats and vulnerabilities

All of the ADS-B vulnerabilities and threats identified and discussed are amenable to ECD mitigation if sufficient computing horsepower is available. ECD can detect as well as mitigate and resolve the fake signals thereby reducing system risk. For an A/C or ground station this condition is generally

readily achievable, although for a UAS or sUAS it is not as easily accomplished. However, recent advances in embedded software and offloading calculations to the cloud have eased the burden.

5.13 Mitigation Plan

To prove the viability and robustness of ECD**,** Kansas State University (KSU) devised an ECD mitigation plan requiring simulation to demonstrate its effectiveness. This was chosen as flight testing was not a valid option because of funding and competing workloads in the A44 project. A baseline testing scenario was developed to exercise and demonstrate the ECD simulation.

5.13.1 Mitigation Plan for ECD using Simulation Datasets

The plan developed is a testing scenario to exercise the ECD method in a simulation environment. The intention of the plan is to gather data in a scenario that is challenging but is not intended to establish future testing standards or criteria, nor is it sufficient to demonstrate the effectiveness under all threats.

1. Establish a base case scenario in an urban location.
    a. The scenario will be transporting vital organ delivery by UAS between hospitals during 4-hour max transport time to be used for patient life support. [FAILURE = COMPLETE FAILURE OF MISSION]
    b. Organ & carry case weight 5 lbs.
2. Establish 3–5-mile route based on 1 satellite GPS dataset. Establish routing and performance characteristics for successful delivery run.
3. Establish Spoofing case where 2/3 satellites are sending ghost signals that change GPS received signals to show / command UAS false route.
    a. False Route change must be significant enough to cause Failure of Mission (20% deviation in heading) and measurable in a real time visual display.
4. Engage ECD as countermeasure:
    a. detect / differentiate all three satellites ECD must indicate correct satellite and reject 2 false ghosts
    b. mitigate route deviation (return to correct mission route) to meet life mission time and delivery specs
    c. recover correct signals and log same
5. Collect as much supplemental data from each interaction to be used to perturb parameters and/or verify ECD perform to 4A-C above.

It is understood that datasets would be batch runs. Embry Riddle Aeronautical University's (ERAU's) team has created the required signals and case datasets to send to Manuel to be run in his ECD models. Manuel would send results back to ERAU's team for additional simulations and verification that ECD solved the 4A-C goals. In addition to proof of concept, data should be collected to estimate in flight, real-time use of ECD effectiveness in further studies. This process resulted in

difficulties for both teams as communication delays and batch runs were difficult hurdles to surmount.

5.13.2 Integration of ECD Algorithm to ERAU Simulation Environment

The ECD algorithm requires I/Q (in-phase/quadrature) GPS signals. ERAU Simulation Environment (ESE) did not have the capability to emulate the GPS waveform. Therefore, to accomplish integration of ECD into the ESE, a MATLAB code was written to achieve the goal of generating the GPS waveform data in the form of I/Q signals. This data resembles the received signal from an actual GPS satellite. The data produced by this code is an accordance with IS-GPS-200L ("NAVSTAR GLOBAL POSITIONING SYSTEM INTERFACE SPECIFICATION IS-GPS-200 Revision D Navstar GPS Space Segment/Navigation User Interfaces" 2006). The following provides a general description of the different components of the process of generating the I/Q data as shown in

Figure 32.

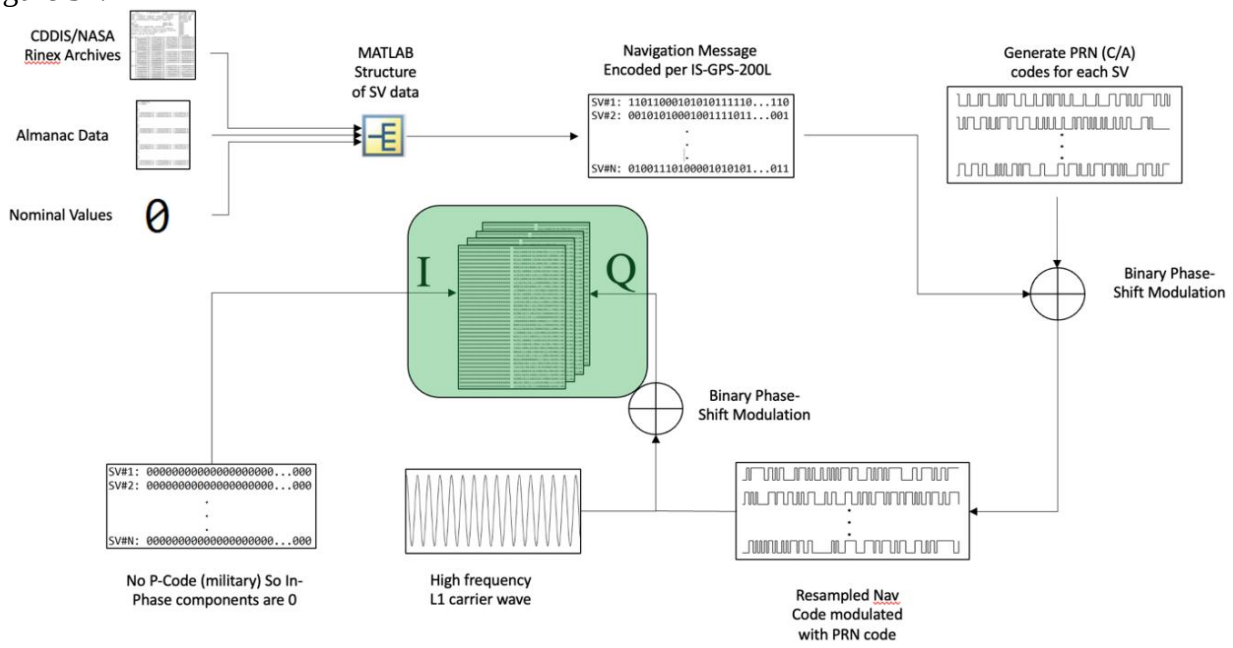


Figure 32. Process of generating I/Q data for a GPS receiver.

In practice, the data sent in the GPS signals is either computed onboard the GPS Space Vehicle (SV) or transmitted to the SV by means of a GPS ground station. For simulation purposes, this data needs to be known before creating the signal and thus must come from an existing real GPS reception. Most of the data in the navigation message is ephemeris, almanac, clock, and health data along with correction coefficients regarding the ionosphere and clock data. Ephemeris data contains information regarding the SV's orbital parameters. This information was obtained from two sources. The almanac data was downloaded from the CelesTrak website ("CelesTrak" n.d.), and the ephemeris and correction data were downloaded from NASA's CDDIS website ("CDDIS |" n.d.). This data comes

in the form of Receiver Independent Exchange (RINEX) format files. The MATLAB code reads both files and stores pertinent data in a data structure for all relevant SVs. The SV produces binary navigation data onboard with a frequency of 50 Hz. This encoded navigation data is a series of 1s and 0s and contains various information regarding satellite ephemeris data, signal health data, correction data, etc. The data is in the legacy navigation format. Then, in accordance with section 20.3 in IS-GPS-200L (IS-GPS-200G 2013), the navigation message is then created as 37500 bits long and takes 12.5 minutes to transmit. Figure 33 illustrates an example of the code plotting the localization of the GPS Satellites and the receiver using RINEX format files.

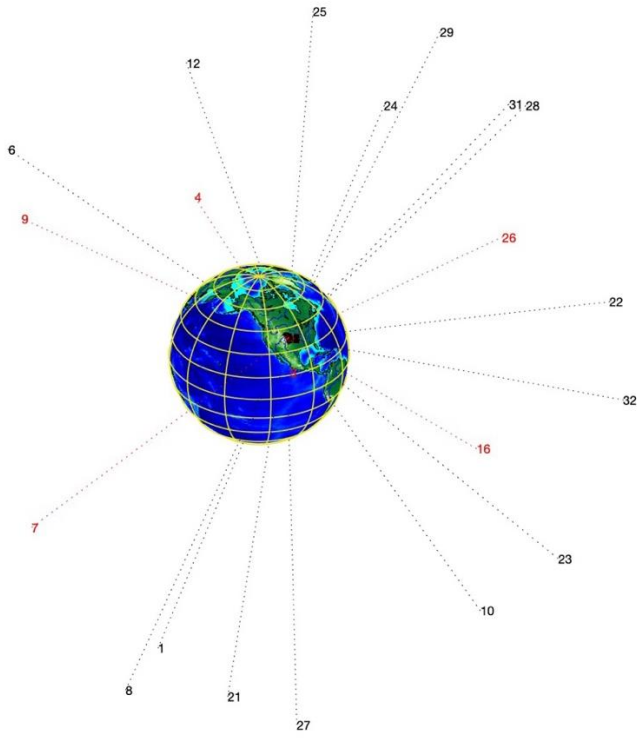


Figure 33. Example of plotting GPS Satellites and Receiver Localizations.

The GPS data typically contains a train of Binary Phase Shift Key modulated in binary bits and further modulated to a 1575.42 MHz carrier wave. The I/Q signals refer to two sinusoidal signals that are 90 degrees apart in phase (i.e., sine and cosine). In order for the receiver to identify which SV signal is being received, the navigation data is modulated with two types of PRN codes. The PRN codes are created using 10 and 12 stage shift registers. The Binary Phase Shift Key modulation is performed with MATLAB bitxor() command. These codes are a higher frequency bit train produced by the SV themselves and each SV has its own unique PRN code. The two types of codes are coarse acquisition C/A and Precise (P), as illustrated in Figure 34. The C/A code has a total length of 1023 bits and is sent with a frequency of 1.023 MHz. The P code has a total length of 228.922848 terabits and is sent with a frequency of 10.23 MHz. After the navigation message is modulated with either of the two PRN codes, it is then modulated onto the L1 carrier wave. The signal that gets the P code

modulated data is called the in-phase and the signal that gets the C/A code modulated data is called the quadrature. If multiple signals are being created, then the signals are summed together to represent a single signal reception from a receiver. After the two modulations with the PRN codes are performed, the L1 carrier wave is modulated with these binary data trains for creating the I and Q data. The data is finally written to a binary file due to the large size of the resulting data files. Figure 34 illustrates the process of generating I/Q binary data from C/A Code and P Code using the available legacy navigation data. Figure 35 shows an example of the code output generating a signal representation of the Q data associated to a frequency and phase characteristics of the GPS information obtained by the receiver.

It is important to notice that the Q data signal, as illustrated in Figure 35, is prone to spoofing attacks that in consequence would change the actual estimation of the localization provided by the receiver. This attack can be simulated by adding a new signal to the Q date which would result in a change of phase and frequency properties of the localization signal.

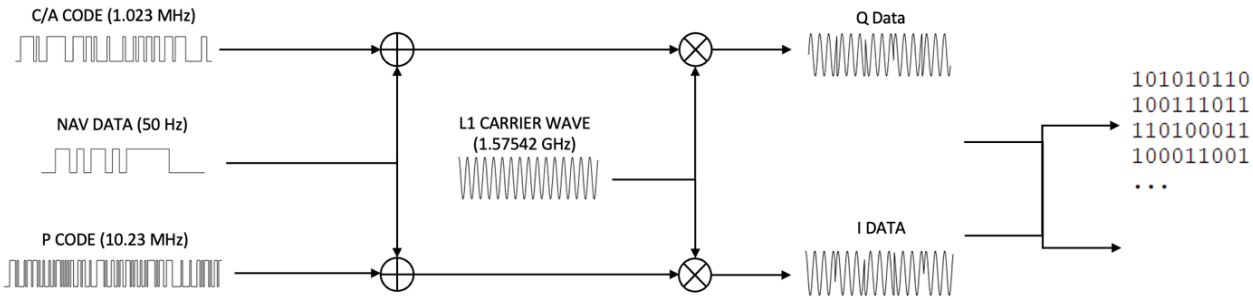


Figure 34. Illustration of the Generation of I/Q binary data using C/A and P codes.

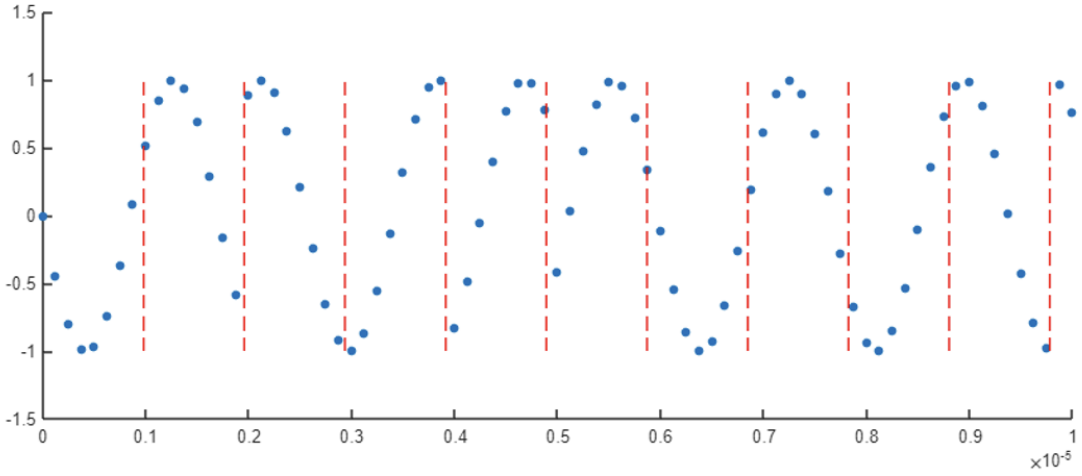


Figure 35. First 10 microseconds of Q data. Red lines are C/A chip width.

5.13.3 Scope of ECD simulation results

Both research teams have performed in an exemplary way to prove the value of ECD as a GNSS / GPS / ADS-B spoofing countermeasure for attacks against navigation communication signals. In 2022, because of the difficult nature of the data development (3 dimensions, time, ephemeris, satellite, and ground station considerations) and building a model for simulation ab initio, KSU and ERAU leads decided to not spend funds or time on flight testing. They chose a difficult case to solve assuming a complete simulation model could be achieved in the schedule and funds allotted. Theoretically and from published data the case was provable (Eichelberger 2019) (R K Nichols et al. 2022).

However, imposing batch runs, and delayed communications eventually took its toll on both teams. There were many communications between principals. The problems identified seem to be the APIs were not fully compatible, as IQ samples and the simulation omits some phenomena.

Nearing the conclusion of the testing window of opportunity it became evident the full simulation of the ECD required extended effort in the project and due to unforeseen circumstances and scope of the work. In this phase of the project the amount of work was beyond the scope of the project and a full implementation of the ECD mitigation solution was not achieved. Both teams were working frantically to prove the technology, and both left with a positive frustration that ECD was in fact a sustainable and effective countermeasure. The inventor of ECD is interested and is willing to assist in the continued efforts to demonstrate the full potential of the ECD mitigation strategy.

5.14 ECD Simulation Results

Several key finding and results were accomplished and are highlighted below:

1. For Task 4, the researchers have closed out our research and simulation activities out of necessity and schedule of principles. KSU-ERAU jointly have not lost faith or interest in the ECD counter-spoofing technology.
2. Task 1 and Task 2 showed the viability and power of ECD to do three things that other countermeasure technologies cannot do in entirety:
   a. Detect Spoofed communication / navigation signals in four or more false satellite transmitters.
   b. Using ECD (discussed previously) mitigate the false and true signals (eliminating the false and exposing the true)
   c. recover the true signals in all risk conditions – especially beyond visual line of sight flight.
3. A functional GPS simulation model has been created by ERAU which needs to be modified to explicitly prove the ECD validity. Adjustments to certain variables and API's may need to be performed. However, the ERAU model is viable. ERAU has accomplished a great deal with its simulation approach.
4. KSU-ERAU both agree that we are on the verge of a huge success in terms of ECD as a countermeasure to reduce the potentially high-risk or catastrophic effects of spoofing and pre-

jamming of GNSS/GPS/ADS-B navigation signals in air, land, and sea scenarios. This is true for both commercial and military operations.

ECD Simulation Recommendations

In closing, KSU-ERAU jointly recommend:

1. Continuation and completion to success of the ERAU ECD simulation efforts
2. Funding via ASSURE sources
3. Flight testing (perhaps along the lines of the recent NIST 3.3 Cyber Challenge which addressed spoofing and demonstrated it on sUAS)
4. Submission of results as PAR for an FAA or NIST or IEEE standard

6. DEVELOPMENT AND IMPLEMENTATION OF OPTICAL FLOW AND GEOMAGNETIC NAVIGATION

6.1 Data Acquisition

The operation of Uncrewed Aerial Vehicles (UAVs) in GNSS degraded environments faces significant challenges due to various factors such as signal blockage, interference, intentional jamming, and spoofing attacks. These factors can degrade the accuracy and reliability of GNSS signals, especially in urban environments where the demand for UAV services is increasing. To ensure the safe and efficient operation of UAVs in such environments, it is crucial to develop navigation methods and technologies that can compensate for the reduced quality of GNSS signals. This report focuses on Task 4, which involves the description of the data acquisition and analysis process to support the development and implementation of Optical Flow (OF) and Geomagnetic Algorithm (GMA) approaches. These approaches enable UAVs to maintain accurate positioning and navigation capabilities even in situations where GNSS signals are partially compromised or degraded. Specifically, this document outlines the data acquisition process and performance analysis to showcase the capabilities of these two techniques.

To evaluate the performance, safety, and reliability of the systems under investigation, this section of the Task 4 report presents numerical simulations and flight testing that accurately represent conditions in UAV-simulated applications. These evaluations provide valuable insights into the effectiveness of the OF and GMA approaches in compensating for GNSS signal degradation.

5.1.1 Optical Flow Navigation

5.1.1.1 Simulation Data Acquisition

Optical flow can be considered as a valuable visual odometry tool for UAV navigation, providing a means of estimating the vehicle's motion based on the observed changes in the scene's features over time. By analyzing the apparent motion of features in the captured images, optical flow algorithms can estimate the UAV's relative position and velocity, offering an alternative or

complementary source of navigation information. The optical flow algorithms essentially analyze pixel motion between two-dimensional images as a projection of the three-dimensional motion of objects relative to the visual sensor. The navigation information obtainable through optical flow fields includes rotational and translational velocities. Sub-components of the optical flow process were implemented and analyzed including the feature detection and tracking, optical flow vector determination, and velocity estimation through camera models.

ERAU simulation environment was used to acquire the necessary data to analyze the performance of the developed OF algorithm (Figure 36). The simulation environment offers a flexible platform for integrating various sensors to the vehicle model, enabling a comprehensive evaluation of their performance under different conditions. In this case, a monocular camera with a resolution of 752x480 pixels and a focal length of 230 mm was incorporated into the simulation, along with an ultrasound sensor for altitude measurement as shown in Figure 37. These sensors provide the required data for the Optical Flow visual odometry system.

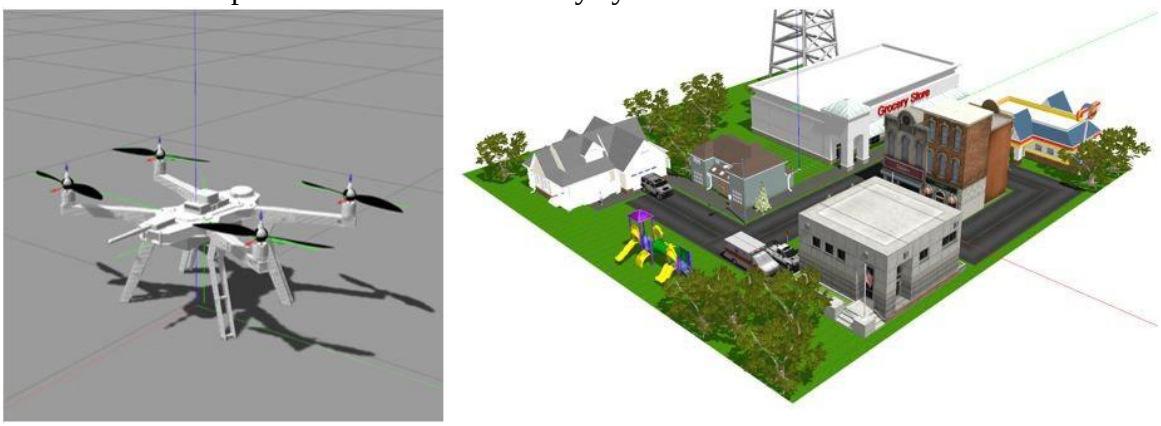


Figure 36. ERAU Virtual Environment Models.

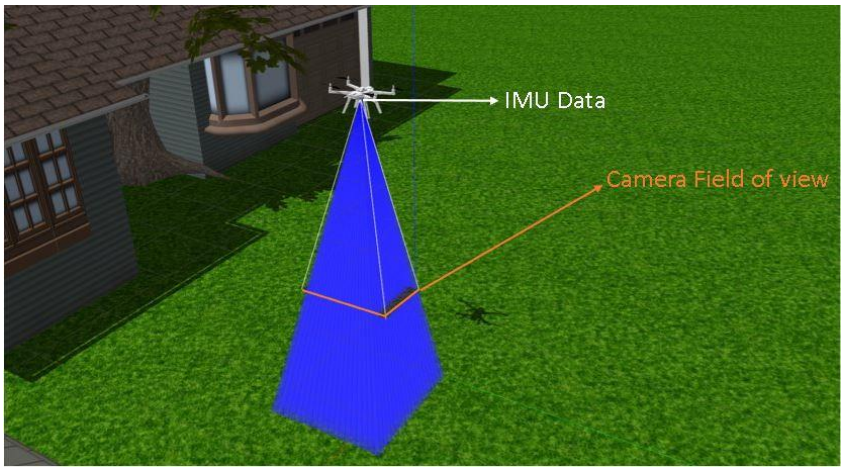


Figure 37. Simulated Camera Field for Optical Flow Assessment.

The simulation environment allowed to capture from the monocular camera, images at a frame rate

of 30 frames per second, as well as Inertial Measurements provided at a rate of 100 Hz. To effectively process the data from the monocular camera, the Shi-Tomasi feature detection algorithm was employed to identify salient visual features in each image frame. The Lucas-Kanade OF algorithm was then used to track the movement of these features between consecutive frames as illustrated in the sequence depicted in the Figure 38, yielding estimates of their 2D displacement in the image plane. By combining this information with the pinhole camera model, the 3D motion of the vehicle could be estimated in the world frame.

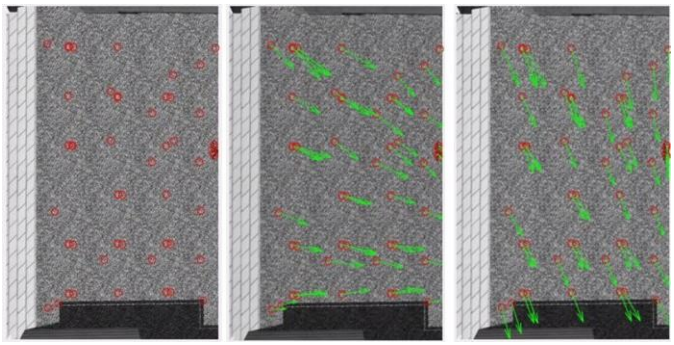


Figure 38. Consecutive Camera Frame Sequence and its Optical Flow Visualization.

5.1.1.2 ***Flight Testing Data Acquisition***

A dataset from a real flight test was provided to the ERAU team by UAF for further testing of the OF algorithm in a real-world implementation. The dataset included Inertial measurements, camera images, and GPS information contained in a Robot Operating System bag file. The OF algorithm was applied to this dataset, following the same sequence of steps as in the simulation environment. Figure 39 presents the OF steps applied over frames of the provided flight test data.

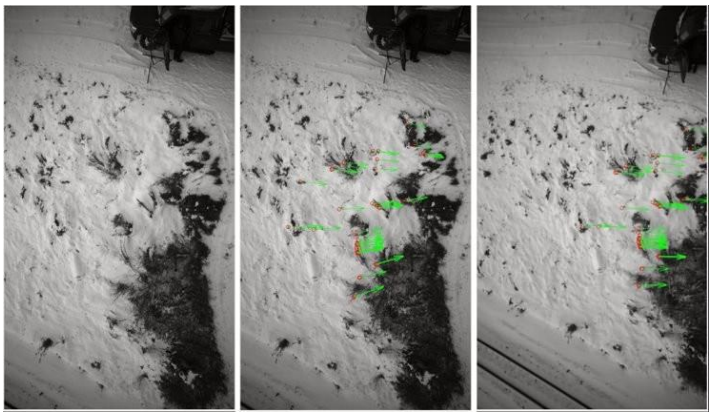


Figure 39. Consecutive Real Camera Frame Sequence and its Optical Flow Visualization.

6.1.2 Geomagnetic Navigation

6.1.2.1 Simulation Data Acquisition

The ERAU team conducted extensive research on geomagnetic localization approaches, primarily focusing on airborne navigation (Cuenca and Moncayo 2021a; 2021b; 2023), which represents a distinct navigation environment. A key consideration in urban environments is the magnetic distortion caused by buildings in the area, which affects the local anomaly field due to man-made disruptions. Consequently, it is contemplated that magnetic mapping of urban areas may be necessary to capture the structural distortions of the field. However, it is important to note that there is no guarantee that these distortions will remain constant over time and cannot work as well as indoor navigation approaches. Therefore, some analyses are presented over this project under several assumptions as it is the existence of a refined magnetic map, and no magnetic disturbances due to motors over the simulation.

A test case is defined for the navigation algorithm assessment using two proposed trajectories shown in blue in Figure 40 with the corresponding anomaly geomagnetic map as the geomagnetic database. These cases simulate the drone flight over a small map with a known magnetic map under perfect conditions, with no external disturbances.

Alongside an Extended Kalman Filter (EKF), the geomagnetic matching algorithm, and a Nearest Contour Point method were integrated as supplementary modules. The results derived from the algorithm, the INS and EKF scenarios are presented concurrently to illustrate the performance of the algorithms graphically. The algorithm, once initialized, needs to build trust in its matching history. The matching method largely depends on a reliable position measurement and aims to correct the drift in the INS.

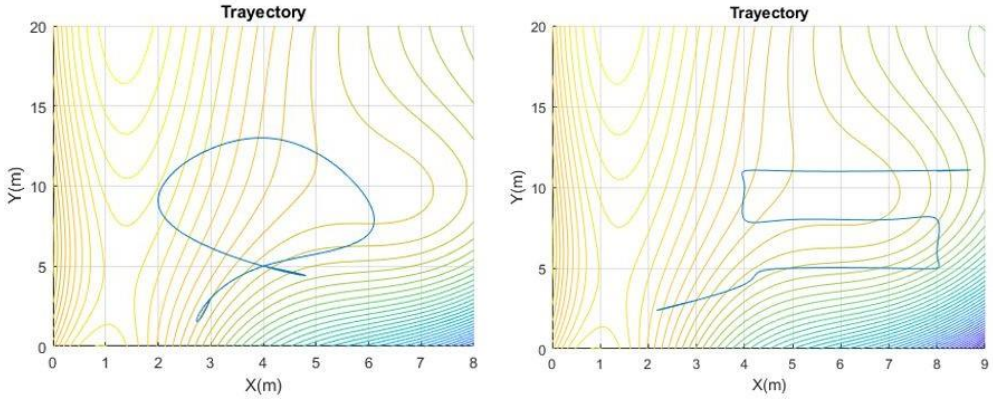


Figure 40. Trajectories proposed as study cases. A) O pattern, b) S pattern.

6.1.1.2 Flight Testing Data Acquisition

A reduced set of flight tests were conducted to gather sensor data from the field and evaluate the impact of the vehicle and its dynamics on the measurements. GPS data was also recorded during all

flights as a position reference value. The recorded data was stored on the PX4 SD card and required post-processing in Matlab to be used as reference data for the GAN architecture implemented. These tests help to better understand the performance of the system under real-world conditions and to refine the algorithms accordingly. Figure 41 illustrates one of the flights during the campaign.

Figure 41. Collection data Flight performed at Embry-Riddle's Softball Field.

6.2 Data Analysis

6.2.1 Optical Flow Navigation

6.2.1.1 Simulation Data Analysis

Figure 42 presents the results of the vehicle velocity estimation derived from only the Optical Flow visual odometry system. The graph illustrates that the velocity estimation is quite accurate when features are available. It is noteworthy that there is some low-level noise present in the estimated velocity, which can be attributed to the vibrations of the vehicle while in motion. These vibrations can cause slight oscillations of the image pixels captured by the camera, subsequently affecting the OF calculations.

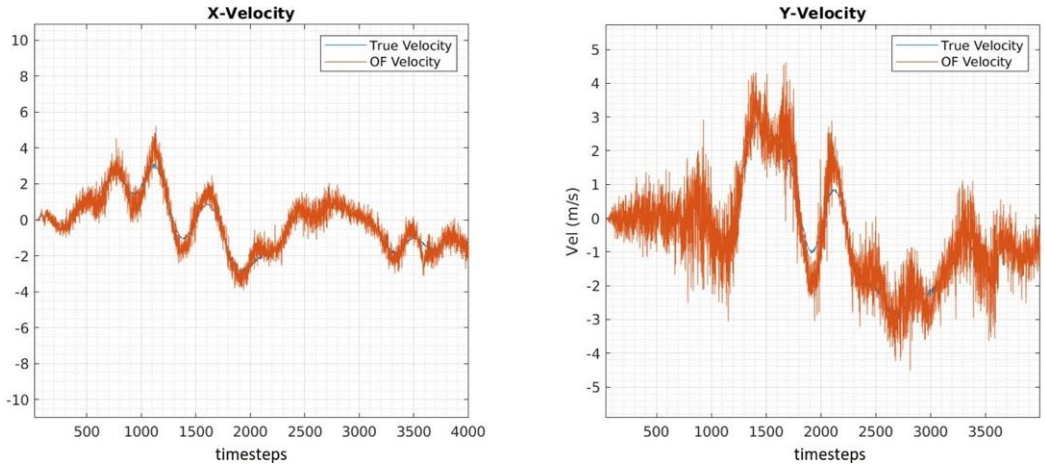


Figure 42. Velocity Measurements by only Optical Flow Odometry.

The OF velocity measurements were subsequently incorporated into the Kalman Filter estimator, without including any geomagnetic algorithms at this stage. Figure 43 demonstrates the filtered velocity estimation, even when integrating degraded GPS signals due to shadowing effects. The integration of OF measurements with the EKF effectively compensates for the reduced accuracy of GPS signals, which can be compromised under certain environmental conditions or in the presence of obstacles.

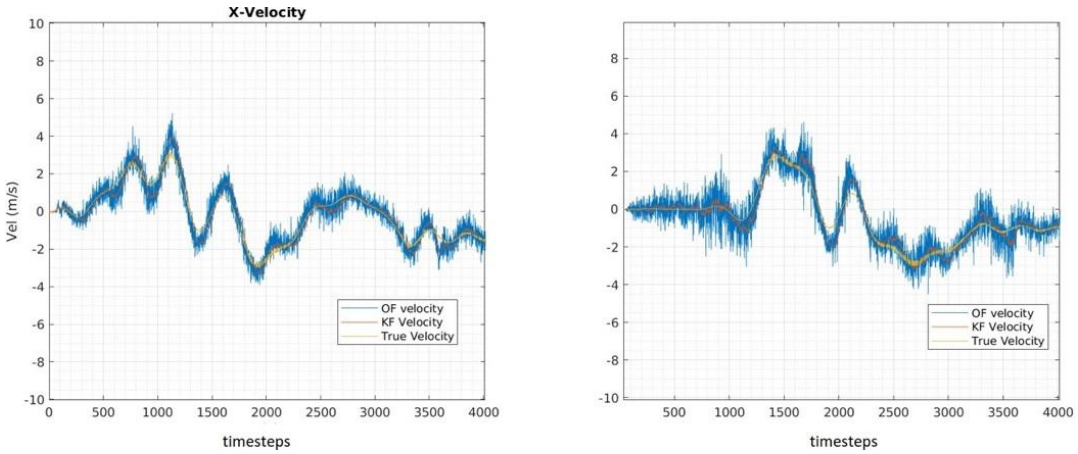


Figure 43. Velocity Estimation integrating OF Velocity Measurements.

Furthermore, the position estimation from the EKF is also computed using velocity estimations from the OF odometry as measurement source, in conjunction with GPS positional measurements. This results in a significant improvement in the position estimation, as shown in Figure 44. This improvement can be attributed to the increased measurement update rate obtained from the OF odometry compared to the GPS update rate. Additionally, the OF measurements are independent of satellite distribution, which represents an additional source of information to correct the noise from GPS measurements in areas where GPS signals might be degraded.

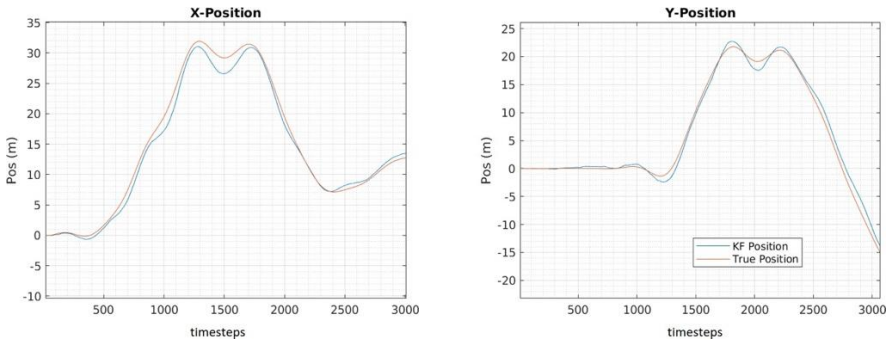


Figure 44. Position Estimation integrating OF Velocity Measurements.

By incorporating the OF odometry, the navigation system is more robust against GPS signal

degradation and can provide more accurate position estimates in a wider range of environments. This demonstrates the effectiveness of using a multi-sensor approach to enhance the overall accuracy and reliability of the navigation system for UAV operations, especially in challenging environments where the performance of standalone GPS systems may be compromised.

6.2.1.2 Flight Testing Data Analysis

The successful application of the OF algorithm to real flight test data demonstrates the robustness and adaptability of the proposed approach. By combining the OF odometry with the sensor data, it is possible to estimate the vehicle velocity using both the INS/GNSS loosely coupled integration as illustrated in the Figure 45 and separately, the visual odometry through OF as depicted in Figure 46.

The INS/GNSS integration combined the IMU data with the GPS information to generate an initial velocity estimation, while the visual odometry through OF was applied to the flight video provided by UAF to obtain an independent velocity measurement. These results were then compared to assess the performance of the OF algorithm in real-world environments.

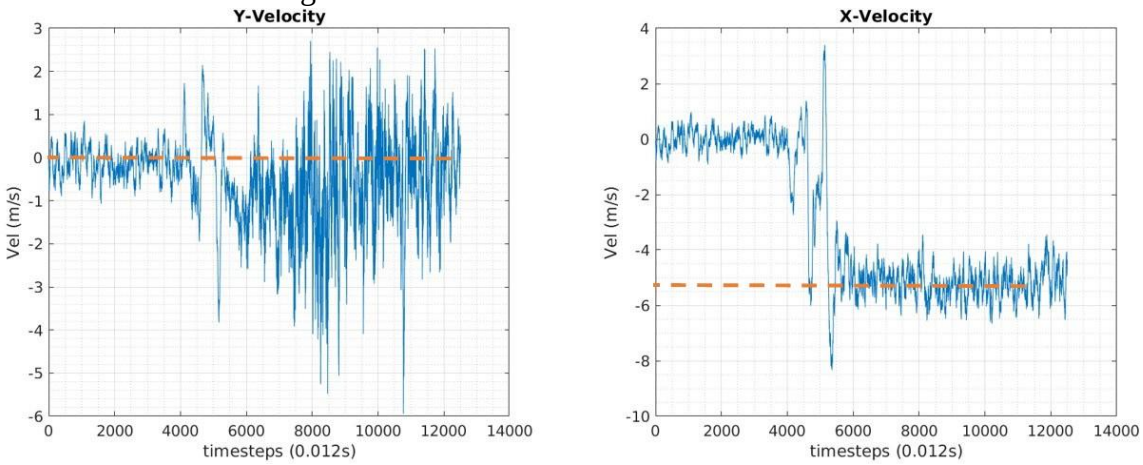


Figure 45. Vehicle Kalman Filter Velocity Estimation INS/GNSS Loosely Coupled integration.

The velocity estimations highlight the effectiveness of the OF algorithm in providing accurate velocity estimates, even when used independently from the other sensor data. It also emphasizes the importance of using a multi-sensor approach for enhancing the overall accuracy and reliability of the navigation system.

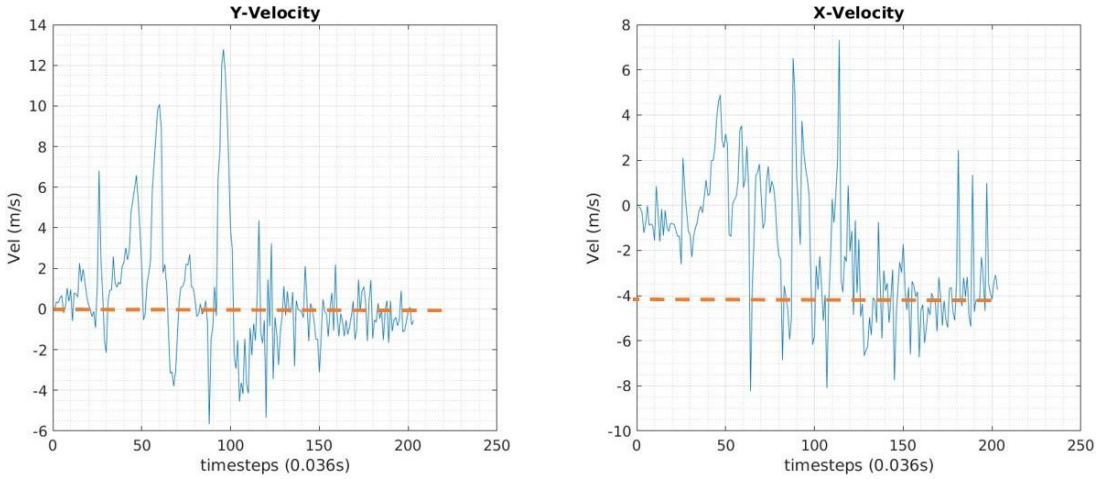


Figure 46. Velocity Measurements by only Optical Flow Odometry in real data.

Maintaining constant altitude measurements and stable camera orientation is crucial for optimal performance of optical flow algorithms. However, it is worth noting that using high-resolution cameras may introduce challenges due to the increased computational demands associated with processing more pixels for feature detection.

6.2.1 Geomagnetic Navigation

6.2.2.1 Simulation Data Analysis

The results from both the S and O trajectories proposed, as demonstrated in Figure 47 and Figure 48, reveal that the GMA algorithm converges to the INS estimation point, which is at the center of the uncertainty area. This can be observed at 11s in Figure 47 and at 13s in Figure 48,where a jump in position estimation occurs.

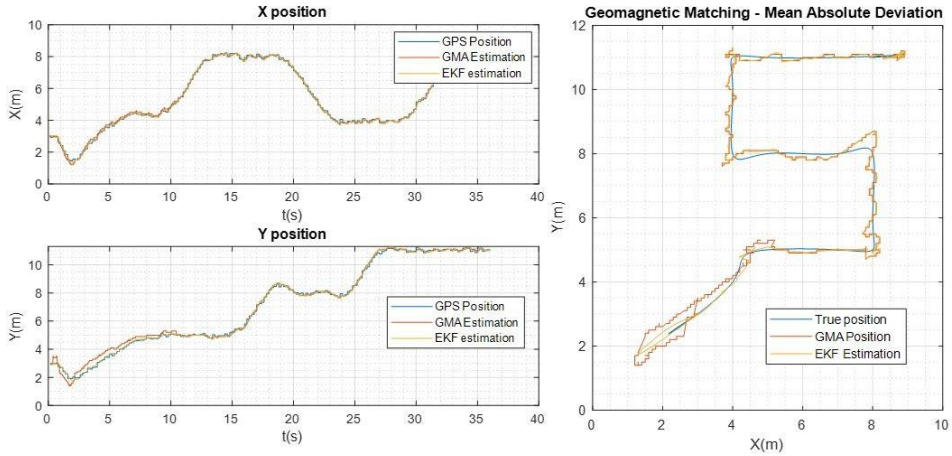


Figure 47. Trajectory S - Geomagnetic Matching Position estimation.

These findings suggest that the GMA algorithm places considerable trust in the INS estimation, which is primarily guided by the GPS measurements.

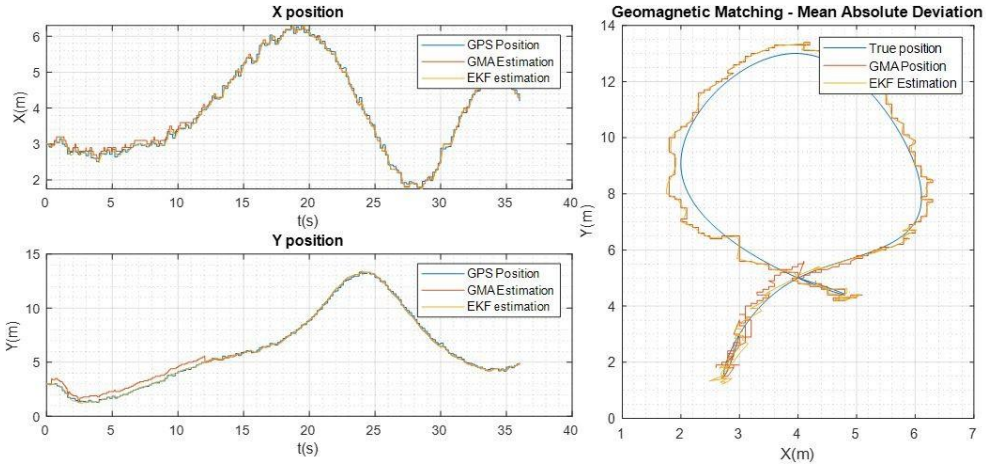


Figure 48. Trajectory O - Geomagnetic Matching Position estimation.

The simulation environment provides visual information of all the elements that structures the GMA architecture as presented in Figure 49 and Figure 50. When calculating the positions with the closest magnetic value as the measurement, a tolerance in the comparison can be defined. Depending on the field's features, a high tolerance can be wise to use when the surface has a distinctive slope, while a low tolerance helps to prevent drifting when the surface is even.

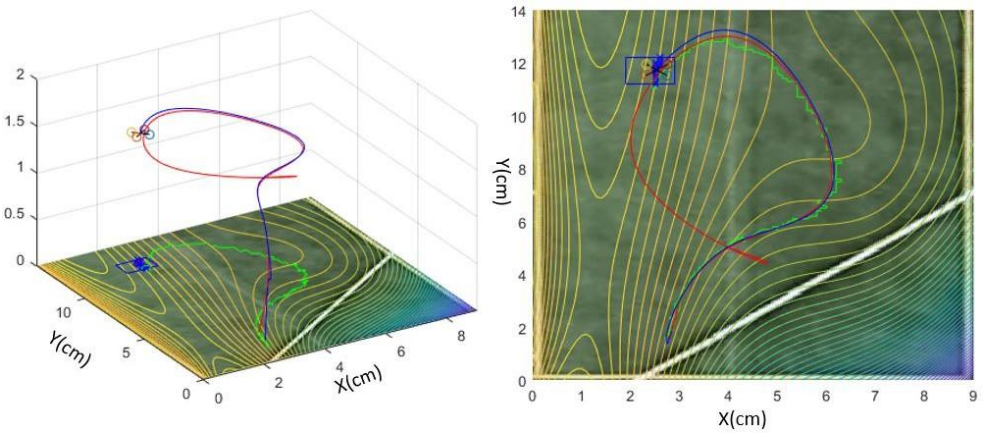


Figure 49. Trajectory O - 3D Visualization of GAN Path estimation.

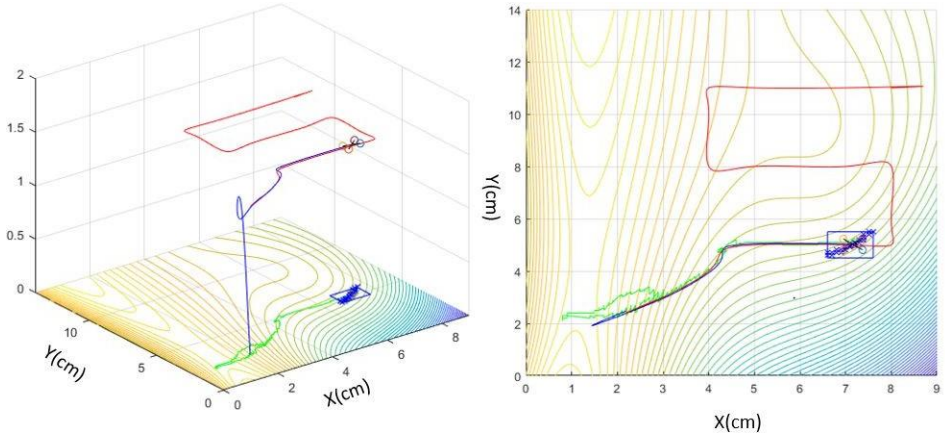


Figure 50. Trajectory S - 3D Visualization of GAN Path estimation.

A non-continuous pattern in the GMA estimation is observed since it depends on the resolution of the map grid. However, the information from the GMA algorithm is handled by the EKF estimation by smoothing the estimation. Again, the algorithm performs an enhancement of the position estimation with Geomagnetic referencing while still using GPS as main position measurement.

*6.2.2.2.**Flight Testing Data Analysis***

During the post-processing of flight test data gathered from various flights, several factors were identified that had a significant impact on the GMA algorithm. The most critical of these factors was the magnetic distortion of the field caused by the motors spinning. The motors, consisting of magnets with high currents flowing through them, generate magnetic fields that are still detected by the sensors. This introduces a large noise, which affects the magnetic measurements.

The magnetic distortion phenomenon is evident in Figure 51 when the motors are activated, and the flight starts. The generated noise magnitude is significantly greater than the expected value derived from the map, emphasizing the considerable influence of this distortion on the system's performance.

Finally, the ERAU team is concurrently studying the MagNav.jl suite, a toolset developed by MIT in collaboration with the Air Force. The suite offers a comprehensive set of tools tailored for airborne Magnetic Anomaly Navigation (MagNav), encompassing features such as flight path and INS data import or simulation, mapping, aeromagnetic compensation, and navigation. The dataset provided within this suite was collected during a geo-survey in Canada at various altitudes, and it includes readings from five scalar magnetometers with different noise levels. Additionally, data from vector magnetometers are included, allowing for extensive testing of various geomagnetic algorithms.

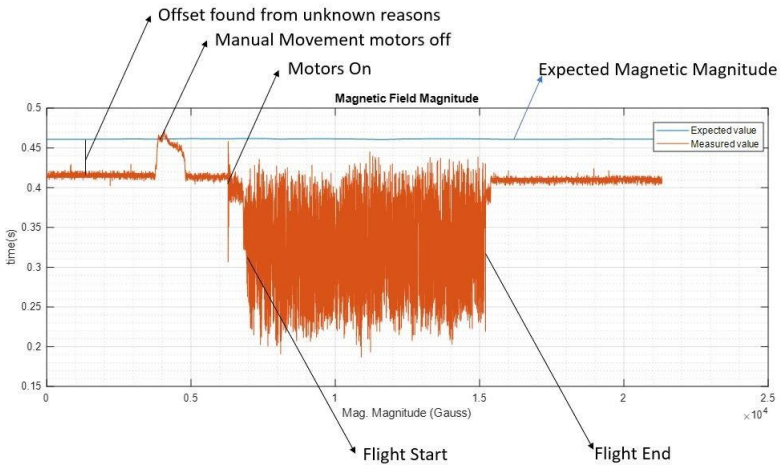


Figure 51. Flight test Magnetic Data.

6.3 Optical Flow and Geomagnetic Navigation Summary and Recommendations

This Task 4 report provides a comprehensive overview of the design, development, and testing of two alternative methods, OF and GNAV, with the aim of enhancing autonomous navigation systems. These algorithms have demonstrated significant potential in improving the accuracy and robustness of navigation systems, as supported by the results obtained from numerical simulations and flight test data.

OF, which relies on vision-based velocity vectors, proved to be particularly valuable in urban environments. Its ability to detect a wide range of features and provide high-rate velocity measurements greatly enhanced estimation accuracy. On the other hand, GNAV, utilizing Earth magnetic anomalies, served as a corrective measure against the inherent drift in inertial navigation systems. Although GNAV alone does not provide position estimation, when combined with a sensor fusion algorithm, it can significantly enhance position estimation, especially over long distances and in environments with minimal magnetic electronic interference.

However, it is important to acknowledge that several challenges and limitations persist in the application of these navigation techniques. These limitations serve as a valid rationale for further research in these areas. Therefore, future work should focus on addressing these challenges and refining the proposed algorithms to achieve improved performance and continuously enhance navigation accuracy in GPS-denied environments.

6.3.1 Geomagnetic Navigation

When magnetic distortions are present, the Earth's magnetic field measurements used by GNAV can be corrupted, leading to erroneous position estimates. This limitation becomes particularly problematic in environments with a high level of magnetic interference, such as industrial areas or regions with extensive underground infrastructure.

To improve the performance of GNAV in the presence of magnetic distortions, several recommendations can be considered:

1. Calibration and Magnetic Field Mapping: Prior to navigation, a calibration procedure can be conducted to characterize and compensate for magnetic distortions in the environment. This involves mapping the magnetic field anomalies in the area of operation and developing correction algorithms to account for the distortions during position estimation.
2. Sensor Fusion with Redundant Sensors: Integrating GNAV with other complementary sensors, such as IMUs, barometers, or optical sensors, can enhance the accuracy and robustness of the navigation system. By fusing the measurements from multiple sensors, it becomes possible to mitigate the effects of magnetic distortions and improve position estimation in challenging environments.
3. Machine Learning-based Approaches: Machine learning techniques can be employed to learn and model the complex relationship between the magnetic field measurements and the corresponding position errors caused by distortions. By training algorithms on datasets that capture different magnetic distortion scenarios, the navigation system can better adapt and compensate for distortions in real-time.
4. Environmental Mapping and Prior Knowledge: Creating a database or map of magnetic anomalies in the environment can provide prior knowledge that assists in navigation. By incorporating this information into the GNAV algorithm, the system can make informed decisions and adjust position estimates accordingly.
5. Dynamic Magnetic Field Monitoring: Continuously monitoring the magnetic field during navigation can help detect and mitigate sudden changes or variations caused by nearby sources of interference. This real-time monitoring can trigger recalibration or adaptive algorithms to account for dynamic magnetic distortions.

By implementing these recommendations, the limitations posed by magnetic distortions in GNAV can be addressed, leading to improved accuracy and reliability of position estimation, even in environments with significant magnetic interference.

6.3.2 Optical Flow based Nav

One limitation of OF navigation is its sensitivity to environmental factors such as lighting conditions, texture variations, and occlusions. These factors can affect the accuracy and robustness of OF-based position estimation.

In challenging lighting conditions, such as low-light or high-contrast environments, the quality of image acquisition may deteriorate, resulting in noisy or unreliable velocity measurements. Similarly, textureless or repetitive surfaces can hinder the accurate detection and tracking of features, leading to decreased estimation accuracy. Additionally, occlusions, where objects obstruct the field of view, can cause discontinuities in the optical flow, making it challenging to track and estimate the vehicle's motion accurately.

To address these limitations and improve the performance of OF navigation, the following recommendations can be considered:

1. Robust Feature Selection and Tracking: Developing more advanced feature selection and tracking algorithms can enhance the reliability and accuracy of OF-based estimation. These algorithms should be designed to handle various environmental conditions, including low-light or high-contrast scenarios, textureless regions, and occlusions. Utilizing robust feature descriptors and incorporating temporal information can aid in maintaining accurate feature tracking and estimation.
2. Multiple Sensor Fusion: Integrating OF with other sensors, such as IMUs or LiDAR, can provide complementary information and improve the overall navigation system's robustness. Sensor fusion techniques can combine the strengths of different sensors, compensating for the limitations of OF and enhancing estimation accuracy, especially in challenging environments.
3. Adaptive Parameter Tuning: Designing adaptive algorithms that can dynamically adjust OF parameters based on the environmental conditions can improve performance. For example, adapting the feature detection threshold, flow regularization parameters, or outlier rejection criteria based on the quality of the image, or the presence of occlusions can enhance the accuracy and reliability of OF-based estimation.
4. Machine Learning-based Approaches: Leveraging machine learning techniques can aid in addressing the limitations of OF navigation. Training deep learning models to detect and track features robustly in various environmental conditions can enhance the accuracy of OF-based estimation. Additionally, using machine learning algorithms to predict and compensate for OF errors caused by challenging scenarios can further improve navigation performance.
5. Environmental Mapping and Prior Knowledge: Creating maps or models of the environment, including information about lighting conditions, texture variations, and potential occlusions, can assist OF navigation. Incorporating this prior knowledge into the algorithm can help anticipate and handle challenging situations, leading to more accurate position estimation.

By implementing these recommendations, the limitations associated with OF navigation can be mitigated, leading to improved accuracy and robustness in a wide range of environmental conditions.

Finally, both GNAV and OF techniques rely on accurate sensor measurements for optimal performance within the navigation architecture. GNAV heavily depends on precise Earth magnetic field measurements, making it susceptible to errors caused by magnetic distortions or variations in the environment. To mitigate these limitations, high accuracy magnetometers are required, which can be expensive and may pose challenges in terms of calibration and maintaining consistent performance. Similarly, OF navigation relies on accurate and reliable visual input for velocity estimation. This necessitates high-quality cameras or sensors capable of capturing detailed and clear images, which may be costly or limited in certain applications. The need for high accuracy sensors within the navigation architecture highlights a critical aspect that must be considered when

implementing GNAV or OF, as suboptimal sensor quality can significantly impact the accuracy and robustness of these navigation techniques.

Although significant successes have been achieved in this project, it is important to acknowledge that there is still ample room for further refinement and development in the field of autonomous navigation. Real-world environments, especially in urban settings, present ongoing complexities that demand innovative solutions. However, the insights and knowledge gained from this research serve as a strong groundwork for future endeavors in this domain. The researchers maintain a sense of confidence in the potential of these methodologies to drive substantial advancements in autonomous navigation capabilities.

7. TASK 4 SUMMARY

The A44 team has completed the testing and demonstration of mitigations report which fulfills Task 4 for the A44 ASSURE project. Select mitigation strategies and test plans were chosen from previous reports. This report prioritizes the mitigations in Task 2 for further analysis based on those that show the most promise for reducing risks while remaining cost effective and implementable whose test plans were developed in the Task 3 report. It places particular emphasis on prioritizing mitigations that support sUAS operations that were tested in Task 4. The use of simulated flight data is a significant source of the test data used for evaluation.

The Task 4 report contains summaries of the testing and demonstration of mitigations of UAS navigation anomalies including dropouts and erroneous data, GPS and ADS-B signal jamming, and GPS and ADS-B signal spoofing. The UAS anomalies section focused on using ADS-B data sets to identify ADS-B anomalies that would result in ceasing operations and identify the scenarios that are most common. The data analyzed was collected by using flight test operations at UAF as well as from a unique case study of public use ADS-B data from the Dallas Fort Worth airport where ADS-B data was unavailable for an extended length of time over a large area. Additional metrics are recommended for ADS-B reception quality and the distance and altitudes of the ADS-B receiver and transmitting aircraft should be tracked. The DFW case illustrated that extended loss of ADS-B signals may occur, and mitigation strategies are critical for aerospace safety. In Section 3, flight tests were developed to record and utilize nearby LTE/4G cellular signals to inform a GNSS-independent positioning solution from a UAS-based receiver. Based on the findings from the cellular navigation study, precise cellular signal positioning approaches show strong potential for mitigating risk in UAS operations and should be further considered as a supporting or backup navigation source in the case of GNSS signal dropout or jamming. For the spoofing chapter, the ECD method was studied in a simulation environment to produce preliminary data to assess its effectiveness. The research efforts have shown the viability and power of ECD to do three things that other countermeasure technologies cannot do. The ability to detect spoofed signals in four or more false satellite transmitters, mitigate the false and true signals, and recover the true signals. A functional GPS simulation model has been

created by ERAU which needs to be modified to explicitly prove the ECD validity. All parties agree that the researchers are on the verge of a huge success in terms of ECD as a countermeasure to reduce the potentially high-risk or catastrophic effects of spoofing and pre-jamming of GNSS/GPS/ADS-B navigation signals in air, land, and sea scenarios. In Section 6, the evaluation of the capabilities, advantages, and limitations of OF and GNAV techniques were tested using both flight and simulated data. These algorithms have demonstrated significant potential in improving the accuracy and robustness of navigation systems. Several challenges and limitations persist and serve as a valid rationale for further research in these areas.

The A44 team Task 4 report on the testing and demonstration of mitigations report provides in depth studies of several navigational mitigation techniques and events that help better inform the FAA and standards bodies detailed information to create appropriate regulations and operational guidelines. The A44 Final Report will provide further recommendations based on the data and the preliminary recommendations presented.

8. REFERENCES

Adamy, David. 2001. *EW 101: A First Course in Electronic Warfare*. Artech House. https://us.artechhouse.com/EW-101-A-First-Course-in-Electronic-Warfare-P451.aspx.

Alan Bensky. 2008. *Wireless Positioning Technologies and Applications*. Artech House.

ALI, BUSYAIRAH S Y D. 2019. *AIRCRAFT SURVEILLANCE SYSTEMS: Radar Limitations and the Advent of the Automatic Dependent... Surveillance Broadcast.* ROUTLEDGE.

AXELRAD, PENINA, BEN K. BRADLEY, JAMES DONNA, MEGAN MITCHELL, and SHAN MOHIUDDIN. 2011. "Collective Detection and Direct Positioning Using Multiple GNSS Satellites." *NAVIGATION* 58 (4): 305–21. https://doi.org/10.1002/j.2161-4296.2011.tb02588.x.

Bissig, Pascal, Manuel Eichelberger, and Roger Wattenhofer. 2017a. "Fast and Robust GPS Fix Using One Millisecond of Data." www.disco.ethz.ch.

———. 2017b. "Fast and Robust GPS Fix Using One Millisecond of Data." In *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 223–33.

Bloomberg.Com. 2022. "FAA Warns Airline Pilots as GPS Signals Disrupted Around Dallas," October 18, 2022. https://www.bloomberg.com/news/articles/2022-10-18/faa-warns-airline-pilots-as-gps-signals-disrupted-around-dallas.

Burgees, M. 2017. "When a Tanker Vanishes, All the Evidence Points to Russia | WIRED UK." Wired.Co. September 21, 2017. https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

"CDDIS |." n.d. Accessed May 21, 2023. https://cddis.nasa.gov/.

"CelesTrak." n.d. Accessed May 21, 2023. http://celestrak.org/.

Cheong, Joon Wayn, Jinghui Wu, Andrew G Dempster, and Chris Rizos. n.d. "Efficient Implementation of Collective Detection."

Cuenca, Andrei, and Hever Moncayo. 2021a. “A Geomagnetic-Based Integrated Architecture for Dead-Reckoning Navigation.” In *AIAA Scitech 2021 Forum*. AIAA SciTech Forum. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2021-1227.

———. 2021b. “Machine Learning Application to Estimation of Magnetospheric Contributions for Geomagnetic-Based Navigation.” In *AIAA SCITECH 2022 Forum*. AIAA SciTech Forum. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2022-1714.

———. 2023. “Geomagnetic Aided Navigation Using Rao Blackwellized Particle Filter.” In . https://doi.org/10.2514/6.2023-1452.

Department of Defense. 2008. “GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD 4th Edition.” DoD. https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

Eichelberger, Manuel. 2019. “ETH Library Robust Global Localization Using GPS and Aircraft Signals.” https://doi.org/10.3929/ethz-b-000379990.

EUROCONTROL. 2013. “EUROCONTROL Specification for Surveillance Data Exchange - Part 1 All Purpose Structured EUROCONTROL Surveillance Information Exchange (ASTERIX).” SPEC-0149. 2.1. Brussels, Belgium: EUROCONTROL.

Goodin, Dan. 2022. “GPS Interference Caused the FAA to Reroute Texas Air Traffic. Experts Stumped.” Ars Technica. October 19, 2022. https://arstechnica.com/information-technology/2022/10/cause-is-unknown-for-mysterious-gps-outage-that-rerouted-texas-air-traffic/.

Haider, Zeeshan, and Shehzad Khalid. 2016. “Survey on Effective GPS Spoofing Countermeasures.” In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 573–77. IEEE.

Hata, M. 1980. “Empirical Formula for Propagation Loss in Land Mobile Radio Services.” *IEEE Transactions on Vehicular Technology* 29 (3): 317–25. https://doi.org/10.1109/T-VT.1980.23859.

Humphreys, Todd E, Mark L Psiaki, Brady W O’hanlon, and Paul M Kintner. n.d. “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.” http://philosecurity.org/2008/09/07/gps-spoofing.

———. n.d. “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer.” http://philosecurity.org/2008/09/07/gps-spoofing.

ICAO. 2021. “ATM Security Manual 9985.” http://www.aviationchief.com/: http://www.aviationchief.com/uploads/9/2/0/9/92098238/icao_doc_9985_-_atm_security_manual_-_restricted_and_unedited_-_not_published_1.pdf.

IS-GPS-200G, Navstar. 2013. “IS-GPS-200H, GLOBAL POSITIONING SYSTEMS DIRECTORATE SYSTEMS ENGINEERING & INTEGRATION: INTERFACE SPECIFICATION IS-GPS-200 - NAVSTAR GPS SPACE SEGMENT/NAVIGATION USER INTERFACES (24-SEP-2013).” http://everyspec.com/MISC/IS-GPS-200H_53530/.

Jafarnia-Jahromi, Ali, Tao Lin, Ali Broumandan, John Nielsen, and Gérard Lachapelle. 2012. “Detection and Mitigation of Spoofing Attacks on a Vector Based Tracking GPS Receiver.” In *Proceedings of the 2012 International Technical Meeting of the Institute of Navigation*, 790–800.

Khalife, Joe J., Souradeep Bhattacharya, and Zak M. Kassas. 2018. “Centimeter-Accurate UAV Navigation With Cellular Signals.” In , 2321–31. Miami, Florida. https://doi.org/10.33012/2018.16105.

Liu, Jie, Bodhi Priyantha, Ted Hart, Heitor S. Ramos, Antonio A. F. Loureiro, and Qiang Wang. 2012. “Energy Efficient GPS Sensing with Cloud Offloading.” In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, 85–98. SenSys ’12. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2426656.2426666.

López-Risueño, Gustavo, and Gonzalo Seco-Granados. 2005. “CN/Sub 0/Estimation and near-Far Mitigation for GNSS Indoor Receivers.” In *2005 IEEE 61st Vehicular Technology Conference*, 4:2624–28. IEEE.

Madhani, Premala H, Penina Axelrad, Kent Krumvieda, and John Thomas. 2003. “Application of Successive Interference Cancellation to the GPS Pseudolite Near-Far Problem.” *IEEE Transactions on Aerospace and Electronic Systems* 39 (2): 481–88.

“MARBEN ASN.1 Solutions: 3GPP LTE Messages Decoder.” n.d. Marben Products. Accessed May 22, 2023. https://www.marben-products.com/decoder-asn1-lte/.

McCallie, Donald, Jonathan Butts, and Robert Mills. 2011. “Security Analysis of the ADS-B Implementation in the next Generation Air Transportation System.” *International Journal of Critical Infrastructure Protection* 4 (2): 78–87. https://doi.org/10.1016/j.ijcip.2011.06.001.

Microsemi. 2014. “Timing & Synchronization for LTE-TDD & LTE-Advanced Mobile Networks.” Microsemi. https://www.microsemi.com/document-portal/doc_download/133615-timing-sync-for-lte-tdd-lte-a-mobile-networks.

“NAVSTAR GLOBAL POSITIONING SYSTEM INTERFACE SPECIFICATION IS-GPS-200 Revision D Navstar GPS Space Segment/Navigation User Interfaces.” 2006.

Ng, Yuting, and Grace Xingxin Gao. 2016. “Mitigating Jamming and Meaconing Attacks Using Direct GPS Positioning.” In *2016 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, 1021–26. https://doi.org/10.1109/PLANS.2016.7479804.

Nichols, R K, M. Carter Candice, John Hood, Mark ; Jackson, M.J. Johnson Siny, Haley Larson, Wayne D. Lonstein, et al. 2022. *Space Systems: Emerging Technologies and Operations*.

Nichols, Randall K, and Panos C Lekkas. 2002. *Wireless Security : Models, Threats, and Solutions*. McGraw-Hill.

Nichols, Randall K, Hans C Mumm, Wayne D Lonstein, Julie JCH Ryan, Candice Carter, and Julie Jch. 2019. “Unmanned Aircraft Systems in the Cyber Domain.” https://newprairiepress.org/ebooks.

Psiaki, Mark L, and Todd E Humphreys. 2016. “GNSS Spoofing and Detection.” *Proceedings of the IEEE* 104 (6): 1258–70.

Ranganathan, Aanjhan, Hildur Ólafsdóttir, and Srdjan Capkun. 2016. “SPREE: A Spoofing Resistant GPS Receiver.” In *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, 0:348–60. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2973750.2973753.

“Runway Now Open at DFW Airport after Faulty GPS Signal Prompts Temporary Closure.” 2022. Fort Worth Star-Telegram. October 20, 2022. https://www.star-telegram.com/news/business/article267622887.html.

Schäfer, Matthias, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. 2014. “Bringing up OpenSky: A Large-Scale ADS-B Sensor Network for Research.” In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, 83–94. https://doi.org/10.1109/IPSN.2014.6846743.

Seyed A. Zekavat and R. Michael Buehrer. 2012. *Handbook of Position Location: Theory, Practice, and Advances*. IEEE Press.

Shamaei, Kimia, and Zaher M. Kassas. 2019. “Sub-Meter Accurate UAV Navigation and Cycle Slip Detection with LTE Carrier Phase Measurements.” In , 2469–79. Miami, Florida. https://doi.org/10.33012/2019.17051.

Shaukat, S A, K Munawar, M Arif, … A I Bhatti - … on Intelligent, and undefined 2016. n.d. “Robust Vehicle Localization with GPS Dropouts.” *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/7824135/?casa_token=djhUQWz2sLEAAAAA:1UMcMFX4zz0OvIDvI0psy6Cc6uhKL-nBnYkb5_wbBErRvIHrE4Z5iidym0xTvK4FYVp0PadghA.

Spilker, JJ, and BW Parkinson. 1996. “Fundamentals of Signal Tracking Theory.” *Progress in Astronautics and Aeronautics* 163: 245–328.

Strohmeier, Martin, Vincent Lenders, and Ivan Martinovic. 2014. “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol.” *IEEE Communications Surveys & Tutorials* 17 (2): 1066–87.

“The 1090MHz Riddle.” n.d. Accessed May 18, 2023. https://mode-s.org/decode/content/ads-b/1-basics.html.

The Royal Academy of Engineering. 2011. “Global Navigation Space Systems: Reliance and Vulnerabilities.” The Royal Academy of Engineering. https://raeng.org.uk/media/5shgtv4t/global-navigation-space-systems.pdf.

Tippenhauer, Nils Ole, Christina Pöpper, Kasper B. Rasmussen, and Srdjan Čapkun. 2011. “On the Requirements for Successful GPS Spoofing Attacks.” In , 75–85. New York, New York, USA: ACM Press. https://doi.org/10.1145/2046707.2046719.

Tsui, James Bao-Yen. 2005. *Fundamentals of Global Positioning System Receivers: A Software Approach*. John Wiley & Sons.

USGPO. 2021. “What Is GPS,” June.

Van Diggelen, Frank Stephen Tromp. 2009. *A-GPS : Assisted GPS, GNSS, and SBAS*. Artech House.

Warner, J S, and R Johnston. 2003. “GPS Spoofing Countermeasures.”

Wesson, Kyle D. 2014. “Secure Navigation and Timing without Local Storage of Secret Keys.” PhD Thesis.

“What Is a NOTAM? | AIRPORTS AUTHORITY OF INDIA.” n.d. https://www.aai.aero/en/content/what-notam.

Wikipedia. 2023. “Global Positioning System.” https://en.wikipedia.org/wiki/Global_Positioning_System.

Zhengxuan, JIA. 2016. “A Type of Collective Detection Scheme with Improved Pigeon-Inspired Optimization.” *International Journal of Intelligent Computing and Cybernetics* 9 (1): 105–23.

9. APPENDIX

ECD Magic[1]

Collective Detection

CD builds upon the observation that detecting peaks in the correlation functions of individual satellites might yield inconsistent pseudo ranges. ECD builds a correct solution by searching in space and time directly. The problem then consists of finding the location given the received signal. From a given hypothetical location and time (hypothesis) in the following, the corresponding ranges of the satellites and therefore, the ToFs can be inferred. Recall the CTN and CD definitions and satellite correlation relationship:

Circular Cross-Correlation (CCC) – In a GPS classical receiver, the circular cross-correlation is a similarity measure between two vectors of length N, circularly shifted by a given displacement d:

$$\text{Cxcorr}(a, b, d) = \sum_{I=0}^{N-1} a_i \text{ dot } b_I + d \bmod N$$

The two vectors are most similar at the displacement d where the sum (CCC value) is maximum. The vector of CCC values with all N displacements can be efficiently computed by a fast Fourier transform (FFT) in Ó (N log N) time [2] (Eichelberger 2019).

Coarse-Time Navigation (CTN) is a snapshot receiver localization technique measuring sub-millisecond satellite ranges from correlation peaks, like classical GPS receivers (IS-GPS-200G 2013) [See also expanded definition above.].

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combine all the available information and decide only at the end of the computation. This technique is critical to the (Eichelberger 2019) invention to mitigate spoofing attacks on GPS or ADS-B.

(Eichelberger 2019) Figure 5.2 page 47 shows how the correlation functions of the received signal with PRN codes of the different satellites on the top (5.2a – original not shifted). On the bottom (5.2b – shifted circularly according to the distance from the receiver to the corresponding satellite), the same correlation functions are circularly shifted by the expected ToF at the correct location. That makes the correlation peaks of all four satellites align.

A receiver can exploit this by combining corresponding correlation values from all the satellites to compute a likelihood measure. This is what the ECD snapshot receiver does. Erroneous peaks (**spoofed signals)** in the correlation function never align which improves noise resistance.

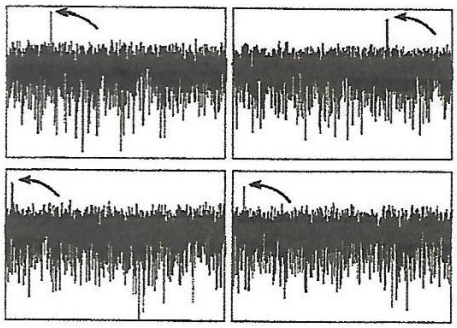
[1] ECD = Dr. Manuel Eichelberger's magic with the Collective Detection Algorithm to detect, mitigate and recovery spoofed GPS signals. The author has named his invention after him.

[2] Ó = Order of magnitude; dot = dot product for vectors

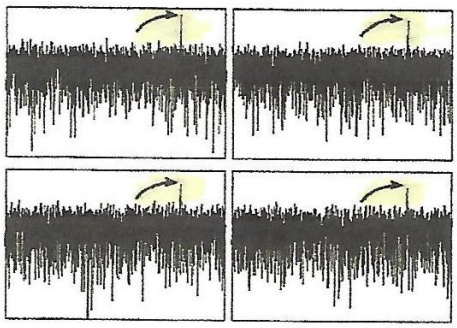
Commonly, the hypothesis pseudo-likelihoods, is defined as the sum of the satellite pseudo-likelihoods.

Correlation functions for four satellites[3] [4]

Courtesy of (Eichelberger 2019)



(a) Original (not shifted).



(b) Shifted (circularly) according to the distance from the receiver to the corresponding satellite.

Figure 5.2: Correlation functions for four satellites. Above are the correlations of the received signal with the PRN sequences of four different satellites. The spikes indicating the beginning of the PRN codes in the received signal are marked with arrows. If we shift the correlation vectors according to the true distance to the satellites, we see below that the peaks all align. (SEE YELLOW HIGHLIGHTED PEAKS)

Localization Method (Position Fix)

The ECD method assesses the quality of many hypothetical receiver states $h = (h^p, h^t)$ which consist of receiver location (h^p) and time (h^t). The quality of the hypothesis is determined through a likelihood function which assigns a pseudo-likelihood to the hypothesis given external information

[3] Figure 5.2a/b shows the correlation of the received signal with PRN sequences of four different satellites. The spikes indicating the beginning of the PRN codes in the received signal are marked with arrows. If we shift the correlation vectors according to the true distance to the satellites, we see below the peaks all align.

[4] Chapter 3 in (Eichelberger, Robust Global Localization using GPS and Aircraft Signals 2019) gives sample code logic for classical and snapshot receivers.

and the observed signal. This likelihood Ł(h) is a measure of how well the observed signal matches the signal expected at a hypothesis h. (Eichelberger 2019).

Likelihood

Given the hypothesis h, we can use the knowledge about the satellites' signal transmission times and orbits from the navigation data, to compute the expected signal phase $Ø_i$ (h) arriving at the receiver from the I^{th} satellite. For any hypothesis h, we can expect a C/A code with phase $Ø_i$ (h) from satellite I in the arriving signal. It is possible to check how well the received signal r(t) matches the expectation by computing a single correlation value with satellite $_{I's}$ C/A code ca_i (t). Therefore, in a snapshot receiver: 1ms

$$Ci\ (h) = \sum_{T=0} [\ r(T)\ dot\ ca_i\ (T - Ø_i\ (h))]$$

If hypothesis h is correct, we expect large correlation values c_i for satellites whose signal can be received, because the C/A code phase in the received signal match the expected code phase $Ø_i$ (h). For satellites that are heavily attenuated or reflected, c_i will be random.

The likelihood function is defined as the sum of the correlation values for a ***given hypothesis over all visible satellites,*** whose indices are denoted by the set V. [5] (Eichelberger 2019)

$$Ł\ (h) = \sum_{I\ €\ V} c_i\ (h)$$

The receiver location and time are estimated by selecting the hypothesis h* which maximizes the likelihood measure:

$$h^* = \arg\max_{h\ €\ F} Ł\ (h)$$

Computing the C/A Code Phase

To compute the likelihood of a hypothesis h, the C/A code phase $Ø_i$ (h) of the visible satellites, V must be known. The signal ToF d_i (h) is determined by the distance between receiver and satellite. The maximum ToF to a receiver on Earth is 87 ms. (Tsui 2005). During this short time, a receiver's movement does not have a significant effect on the signal ToF. However, the fast satellite movement has. Therefore, the ToF is computed at the transmission time t_i of a signal even though the receiver may travel for an additional 87 ms. The code phase $Ø_i$ (h) relates to the transmission time, t_i (h) of the receiver signal as follows:

$$Ø_i = t_i\ (h) \bmod 1\ ms$$

[5] This is fundamental to successful implementation of ECD.

The transmission time, t_i (h) of the received signal at time h^t are related by the ToF d_i (h) between the hypothetical location and the satellite location.

$$t_i (h) = h^t - d_i (h)$$

The ToF can be found by dividing the special distance between the hypothetical location h^p and the satellite location p_i by the speed of light C:

$$d_i (h) = \underline{[[h^p - p_i (t_i (h))]]} / C$$

The ToF d_i (h) depends on the distance between the satellite location p_i at the transmission time t_i (h) and the hypothetical location h^p. The satellite location p_i (t_i (h)) at a given time can be computed from the ephemeris. [6] (Eichelberger 2019).

Search Region

The last task is to guarantee that the solution is unique. The search region in which the set F of feasible hypotheses is contained. As GPS signals travel at the speed of light C, the C/A code phase of a satellite are the same for two hypotheses if their distances to the satellite differ by k dot C dot 1ms ~ 300 km for integer values of k. The search region is bound in which the set F of feasible hypotheses is contained to a diameter of 300 km [7]. For bounding the solution domain, the antenna location of the cellular network can be used as a reference. When the signal of the satellite is strong enough, we can also find the approximate receiver location with an idea presented by Liu, et al. (Liu et al. 2012) (Eichelberger 2019).

Supplemental computations for simulation

(Eichelberger 2019) discusses the set V, of visible satellites, space discretization, time discretization, averaging over likely hypotheses, efficient implementation with branch and bound, local oscillator frequency bias, and evaluation tests. These subjects are fascinating but outside the scope of this appendix. The purpose of Appendix A was to give a flavor and key points behind the ECD algorithm. [8]

DEFINITIONS

Acquisition – Acquisition is the process in a GPS receiver that finds the visible satellite signals and detects the delays of the PRN sequences and the Doppler shifts of the signals.

---

[6] The signal ToF from a satellite to a receiver on Earth range between 67 and 86 ms. (Tsui 2005)The ECD satellite location estimation worse case error is 9.5 ms dot 929 m/s = 8.33 m. The ToF estimation error is at most 8.83 m /C = 19.4 ns. The satellite location estimate that can be achieved using this ToF estimate has a negligible error of 19.4 ns dot 929 m/s = 18 micrometers (um).

[7] The correspondence between time error and range error is given by the maximum relative satellite speed against a receiver, which is less than 1 km/s on the Earth surface.(Tsui 2005) A location range of 100km and a time range of 50 km / 1 km/s = 50 s and are guaranteed to deliver a unique solution.

[8] Readers interested in these supplemental subjects for programming purposes should consult Sections 5.3 – 5.4 on pages 50-66 of the primary reference (Eichelberger, Robust Global Localization using GPS and Aircraft Signals 2019)

Circular Cross-Correlation (CCC) – In a GPS classical receiver, the circular cross-correlation is a similarity measure between two vectors of length N, circularly shifted by a given displacement d:

$$\text{Cxcorr}(\mathbf{a}, \mathbf{b}, d) = \sum_{I=0}^{N-1} a_i \text{ dot } b_I + d \bmod N$$

The two vectors are most similar at the displacement d where the sum (CCC value) is maximum. The vector of CCC values with all N displacements can be efficiently computed by a fast Fourier transform (FFT) in Ó (N log N) time. [i] (Eichelberger, Robust Global Localization using GPS and Aircraft Signals, 2019)

Coarse-Time Navigation (CTN) is a snapshot receiver localization technique measuring sub-millisecond satellite ranges from correlation peaks, like classical GPS receivers. (IS-GPS-200G, 2013) [See also expanded definition above.]

Collective Detection (CD) is a maximum likelihood snapshot receiver localization method, which does not determine the arrival time for each satellite, but rather combine all the available information and decide only at the end of the computation. This technique is critical to the invention to mitigate spoofing attacks on GPS or ADS-B.

Coordinate System – A coordinate system uses an ordered list of coordinates, to uniquely describe the location of points in space. The meaning of the coordinates is defined with respect to some anchor points. The point with all coordinates being zero is called the origin. [Examples: terrestrial, Earth-centered, Earth - fixed, poles, ellipsoid, equator, meridian longitude, latitude, geodetic latitude, geocentric latitude, and geoid. [ii]

Localization – Process of determining an object's place with respect to some reference, usually coordinate systems [aka Positioning or Position Fix].

Navigation Data is the data transmitted from satellites, which includes orbit parameters to determine the satellite locations, timestamps of signal transmission, atmospheric delay estimations and status information of the satellites and GPS as a whole, such as accuracy and validity of the data (IS-GPS-200G, 2013).

Pseudo – Random Noise (PRN) sequences are pseudo – random bit strings. Each GPS satellite uses a unique PRN sequence with a length of 1023 bits for its signal transmissions. aka as Gold codes, they have a low cross correlation with each other (IS-GPS-200G, 2013) .

Snapshot GPS Receiver- A snapshot receiver is a GPS receiver that captures one or a few milliseconds of raw GPS signal for a location fix (Diggelen, 2009).

---

i Ó = Order of magnitude; dot = dot product for vectors

ii All these systems are discussed in Chapter 2 of (Eichelberger, 2019)