МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет аеронавігації, електроніки та телекомунікацій
Кафедра аеронавігаційних систем

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Ларін В.Ю.

“___”_____2022р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)
ВИПУСКНИКА ОСВІТНЬО–КВАЛІФІКАЦІЙНОГО РІВНЯ
“МАГІСТР ”

Тема: «Навігація безпілотних літальних апаратів в умовах широкого спектру перешкод»

Виконавець: Ключенко І.І.

Керівник: Харченко В.П.

Нормоконтролер: Шмельова Т.Ф.

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації електроніки та телекомунікації
Кафедра аеронавігаційних систем
Спеціальність 272 «Авіаційний транспорт»
Освітньо-професійна програма «Безпілотні авіаційні комплекси»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Ларін В.Ю.
_____
"_____ "_____2022р.

ЗАВДАННЯ

на виконання дипломної роботи

_____Ключенка Івана Ігоровича_____

1. Тема дипломної роботи: «Навігація безпілотних літальних апаратів в умовах широкого спектру перешкод» затверджена наказом ректора від 20.09.2022 №1594/от
2. Термін виконання роботи (проекту): з 05 вересня 2022 року по 30 листопада 2022 року.
3. Вихідні дані до проекту: Навігація безпілотних літальних апаратів в умовах завад широкого спектру перешкод. Представлений аналіз систем навігації БПЛА, дослідження засобів захисту систем навігації БПЛА від перешкод різного спектру. Розробка та впровадження системи попередження завад.
4. Зміст пояснювальної записки:
   - загальна характеристика систем навігації;
   - загальна характеристика радіо-електронної боротьби;
   - формування і запис даних для обробки;

– розробка системи попередження від завад в програмному забезпеченні MissionPlanner.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: дані пояснювальних матеріалів, рисунки результатів проведених досліджень, таблиці, додатки.

6. Календарний план–графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Вибір напрямку дослідження проекта	21.09.21 р. – 22.11.21 р.	Виконав:
2.	Загальна характеристика системи навігації БПЛА. Запис даних.	18.12.21 р. – 21.12.21 р.	Виконав:
3.	Загальна характеристика систем радіолектронної боротьби.	21.12.21р. – 02.01.22 р.	Виконав:
4.	Формування даних для обробки.	02.02.22 р. – 31.05.22 р.	Виконав:
5.	Розробка системи попередження від завад в програмному забезпеченні MissionPlanner.	05.06.22 р. – 10.09.22р.	Виконав:
6.	Оформлення пояснювальної записки та інших документів	10.10.22 р. – 24.10.22 р.	Виконав:
7.	Підготовка документів та презентації	24.10.22 р. – 20.11.22 р.	Виконав:

7. Дата видачі завдання: "____"_____2022р.

Керівник дипломного проекту _____Харченко Володимир Петрович

Завдання прийняв до виконання_____Ключенко Іван Ігорович

РЕФЕРАТ

Пояснювальна записка до дипломного проекту магістра «Навігація БПЛА в умовах завад широкого спектру»: 114 с.,
44 рис., 9 табл., 2 дод., 30 джерел.

Об’єкт дослідження – Навігаційні системи БПЛА; Засоби завад навігаційних систем та методи їх протидії.

Метою дипломного проекту є розробка аппаратно–програмного комплексу для попередження систем навігації БПЛА та захисту їх від завад.

Мета розробки – покращити можливості позиціонування БПЛА для виконання бойових завдань в умовах дії завад широкого спектру;

Наукова новизна проекту полягає у впровадженні системи попередження «anti-jumming» та «anti-spoofing» в програмне забезпечення MissionPlanner, що дозволить безпечніше виконувати польоти на БПЛА в умовах завад.

Дипломний проект завершується зробленими висновками і списком використаної літератури.

АРКУШ ЗАУВАЖЕНЬ

.

ЗМІСТ

УМОВНІ ПОЗНАЧЕННЯ

Абревіатура	Опис англійською мовою	Опис
GNSS	Global Navigation Satellite System	Глобальна навігаційна супутникова система
ICAO	International Civil Aviation Organization	Міжнародна організація цивільної авіації
РЕБ/EW	Electronic Warfare	Радіо-Елктронна Боротьба
IGS	International GNSS Service	Міжнародні GNSS сервіси
GPS	Global Positioning System	Глобальна Система Навігації
ГЛОНАСС		Глобальна Навігаційна Супутникова Система (Російської Федерації)
GELILEO		супутникова система навігації Європейського Союзу та Європейського космічного агентства
FTO	Flight Test Order	Завдання на льотне випробування
BeiDou	China's BeiDou Navigation Satellite System	Китайська навігаційна супутникова система
QZSS	Quasi-Zenith Satellite System	Японська квазізенітна супутникова система
HDO	Head of Design Organization	Керівник організації розробників
HoA	Head of Airworthiness	Керівник відділу льотної придатності
WAAS	Wide Area Augmentation System	Глобальна американська система поширення диференціальних поправок
PtF	Permit to Fly	Дозвіл на польоти
EGNOS	European Geostationary Navigation Overlay Service	Європейська геостаціонарна служба навігаційного покриття
MSAS	Multi-functional Satellite Augmentation System	Багатофункціональна система диференціальної корекції супутникового базування
GSM	Groupe Spécial Mobile	Міжнародний стандарт для мобільного цифрового стільникового зв'язку
ПС/ПК		Повітряне судно/Повытряний корабель
БпЛА		Безпілотний літальний апарат

Абревіатура	Опис англійською мовою	Опис
ІЛВ		Інженер по льотним випробуванням
ВЛВ		Відділ льотних випробувань
GPRS	General Packet Radio Service	Стандарт, який використовує не зайняту голосовим зв'язком смугу частот для передачі інформації
RINEX		це стандартний формат, який дозволяє зберігати та передавати проміжні виміри зроблені приймачем
AutoPP, QC		Обробка даних і оцінка точності на сервері мережі
UGV	Unmanned Ground Vehicle	Безпілотні наземні апарати
AUV	Autonomous Underwater Vehicle	Автономні підводні апарати
ROV	Remotely Operated Vehicle	Автомобіль з дистанційним керуванням
INS/IHC	Inertial Navigation System	Інерціальна система навігації
IMU	Inertial Measurement Unit	Інерціальний вимірювальний блок
AHRS	Attitude and Heading Reference System	Референтні системи положення та курсу
MEMS	Microelectromechanical system	Мікроелектромеханічні системи
SLAM	Simultaneous Localisation And Mapping	Одночасна локалізація та картографування
6DoF	Six degrees of freedom	Орієнтація в 6-ти вимірному просторі
RB	Rao-Blackwellised	Фільтр частинок
EO/IR	Electro-Optical/Infrared	Видимі та інфрачервоні датчики

Абревіатура	Опис англійською мовою	Опис
DTED	Digital Terrain Elevation Data	Карта цифрового рельєфу місцевості
Locata	Alternative Navigation System	Система супутникової навігації, встановлена на серії наземних веж
NAVSOP	NAVigation via Signals of OPportunity	Навігаційні сигнали можливості
РЕВ		Радіоелектронна війна
РЕЗ		Радіоелектронний захист
РЕП		Радіолелектронне подавлення
Hi-Tech	High technology	Висóкі технолóгії
ЗС		Збройні сили
НЗФ		Незаконні збройні формування
VHF	Very High Frequency	Діапазон високочастотних хвиль
CDMA	Code Division Multiple Access	Система множинного доступу із кодовим розділенням
UHF	Ultra high frequency	Діапазон надвисокочастотних хвиль
FPV	First Person View	Вид від першого лиця
PPD	Privacy Protection Devices	Пристрої захисту конфіденційності
IMO	International Maritime Organization	Міжнародна морська організація
ДС		Діаграмма спрямованості
ПЧОС		Просторова часова обробка сигналів
ААКЗ		антенні адаптивні компенсатори завад
SNR	Signal-to-noise ratio	Співвідношення сигнал/шум
LMS	Least Mean Square	Найменший середній квадрат

Абревіатура	Опис англійською мовою	Опис
RLS	Recursive Least Square	Рекурсивний найменший квадрат
MUSIC/ ESPRIT		Алгоритми високого дозволу
C/N_0		Оцінка сигнал/шум
SQM	Signal quality monitoring	Слідкування за якостю сигналу
PRN	Pseudorandom noise	Псевдовипадковий шум
ADS-B	Automatic dependent surveillance-broadcast	Автоматичне залежне спостереження - радіомовне
NEU		Система локальних координат

ВСТУП

Зображення сьогодення спонукає до вирішення питань різних сфер в із застосування мінімуму зусиль та найголовніше часу. На початок повномасштабного вторгнення українські розробники БПЛА не були готові до того, що ці «пташки» будуть літати в таких тяжких умовах. Нажаль, саме війна сприяла вибору даної теми роботи, тому в написаному буде йти мова саме про використання БПЛА у військових цілях, про виконання завдань розвідки, корегування та ураження.

В мирний час, для точної навігації БПЛА, цілком достатньо використати дешевий та простий приймач GNSS, проте, надіятись на стабільних сигнал супутників в зонах дії РЕБ - марно. Як показує практика, GPS в таких зонах взагалі відсутній.

Навігація БПЛА включає в себе комплекс датчиків та приймачів. Використання цих сенсорів та процесорів дозволяє використовувати існуючі архітектури побудови БПЛА різних типів та класів. Більшість БПЛА, що виробляються, мають схожу та просту архітектуру побудови апаратної та програмної частини, що надає їм основну перевагу – дешевизна виготовлення.

Для безпечного виконання польотів заздалегідь запланованих місій потрібні надійні системи захисту каналів зв’язку, навігації, та спостереження.

В дипломній роботі я намагатимусь повністю розкрити та описати ситеми, що використовуються для навігації БПЛА, опишу фактори які можуть впливати на коректну поведінку систем навігації, що таке «jamming» та «spoofing». В даній роботі буде представлений один з варіантів попередження та захисту систем супутникової навігації для виконання польотів в умовах завад.

Метою дипломного проекту є розробка аппаратно–програмного комплексу для попередження систем навігації БПЛА та захисту їх від завад.

Мета розробки – покращити можливості позиціонування БПЛА для виконання бойових завдань в умовах дії завад широкого спектру;

Наукова новизна проекту полягає у впровадженні системи попередження «anti-jumming» та «anti-spoofing» в програмне забезпечення MissionPlanner, що дозволить безпечніше виконувати польоти на БПЛА в умовах завад.

Дипломний проект завершується зробленими висновками і списком використаної літератури.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА НАВІГАЦІЇ БПЛА

1.1 GNSS для навігації БПЛА

GNSS представляє собою систему супутникової навігації, створену з метою позиціонування (визначення місця розташування в просторі – тобто координат) об'єктів. Окрім визначення місця розташування об'єкта сучасні навігаційні системи дозволяють визначити напрямок його руху і швидкість. На даний час близько 200 організацій, що займаються збором GNSS даних з базових станцій по всьому світу, об'єднані в IGS (International GNSS Service), яка, в свою чергу, входить до Міжнародної асоціації геодезії.

GNSS системи складаються з двох складових: космічної та наземної. Якщо не вдаватися в подробиці, то принцип роботи таких систем полягає у вимірюванні відстані від антени на об'єкті до супутників. Знаючи відстані до декількох супутників, положення яких відомо достатньо точно, навігаційні системи за допомогою звичайних геометричних побудов обчислюють місцезнаходження об'єкта.

Основні діючі і перспективні GNSS системи: GPS (США), ГЛОНАСС (Росія), GELILEO (Євросоюз), BeiDou (Китай), QZSS (Японія).

З метою підвищення точності позиціювання з декількох метрів до сантиметрів у багатьох країнах створюються наземні системи радіомаяків, а також інформаційна радіосистема для передачі користувачам диференціальних поправок, що дозволяють значно підвищити точність визначення координат. Диференціальна поправка пересилається або з геостаціонарних супутників (системи WAAS, EGNOS, MSAS і ін.), обо з наземних базових станцій. Найбільша точність досягається при використанні RTK-поправок саме з наземних базових станцій. Саме така мережа під назвою System.NET діє з 2011 р в Україні.

Крім значного підвищення точності мережа System.NET дозволяє значно розширити зону позиціонування: визначення місця розташування стало можливо по всій зоні покриття мобільної мережі, де приймається GSM / GPRS сигнал, а так само в місцях з можливістю підключення до мережі Інтернет за допомогою інших каналів зв'язку.

Також стали можливими: виключення грубих помилок вихідних пунктів; підтримка єдиної міжнародної системи координат; можливість безпосередньої роботи в будь-який необхідної системі координат; скорочення витрат на обладнання; контроль точності безпосередньо під час виконання вимірювань; збільшення продуктивності праці; використання додаткових сервісів – постобработка сирих даних RINEX, використання згенерованої віртуальної базової станції при постобробці кінематичних вимірювань (Virtual Reference Station), автоматична обробка даних і оцінка точності на сервері мережі (AutoPP, QC) і ін.

1.1.2 Приймачі GNSS для БПЛА, дронів і автономних транспортних засобів

Багато безпілотних систем, таких як БПЛА, UGV і AUV, потребують використання GPS/GNSS, щоб забезпечити їм високий ступінь точності позиціонування для таких застосувань, як картографування, геодезія, точне землеробство та пошук і порятунок. Антена GNSS встановлюється десь на транспортному засобі, і супутникові дані зазвичай подаються в авіоніку, автопілот або навігаційні системи.

Окрім навігації, безпілотні транспортні засоби можуть використовувати GNSS для географічної прив'язки зібраних даних, уникнення зіткнень або забезпечення можливостей відстеження. Дані GNSS надають вхідні дані для контуру керування дроном або іншим автономним транспортним засобом, дозволяючи йому підтримувати позицію, повертатися додому або слідувати серії

заданих маршрутних точок. Це особливо важливо для водних роботів, таких як AUV і ROV, на положення яких може суттєво вплинути приливна активність.

Мікросхеми приймача GNSS отримують супутникові дані та обробляють їх, щоб визначити положення, швидкість і час. Цю інформацію можна зберігати локально або відправляти на віддалену станцію моніторингу чи відстеження.

1.1.3 Архітектура GNSS приймача

Багато приймальних модулів GNSS можуть відстежувати кілька сузір'їв GNSS, а також багато супутників одночасно. Зазвичай кожен сигнал від кожного супутника призначається на власний виділений канал у системі приймача. Багаточастотні приймачі можуть обробляти сигнали, що транслюються супутником на кількох частотах, наприклад L1, L2 і L5 для GPS. Приймачі з подвійною антеною забезпечують більшу точність курсу, особливо в ситуаціях із низькою динамікою.

Модулі зазвичай складаються з наступних блоків:

- Антена GNSS – фіксує сигнали L-діапазону (радіочастоти від 1 до 2 ГГц) із супутника;
- Інтерфейс – фільтрує, підсилює та оцифровує вхідні сигнали;
- Обробка сигналів – використовується для отримання та відстеження різних сигналів;
- Обробка додатків – виконує обчислення інформації про сигнал і представляє результати відповідно до конкретного додатка.

1.1.4 Програмно визначені GNSS приймачі

Програмно-визначені приймачі GNSS, доступні як програмно-визначені та спеціальні апаратні модулі, забезпечують більшу гнучкість, оскільки їх легше оновлювати та додавати нові функції до програмного забезпечення. Однак

апаратні модулі, як правило, більш ефективні, оскільки апаратне забезпечення розроблено спеціально для цієї конкретної програми.

Приймачі GNSS є здебільшого пасивними пристроями – винятком буде, коли європейська система Galileo стане повністю функціональною. Приймачі Galileo GNSS будуть оснащені аварійною функцією, яка зможе транслювати інформацію після активації.

GNSS стикається з обмеженнями, пов'язаними з необхідністю перебувати в зоні прямої видимості принаймні чотирьох супутників, щоб забезпечити надійну навігацію. У середовищах із поганим сигналом може бути вигідним поєднання GNSS з інерціальною навігаційною системою (INS), яка використовує інформацію про обертання та прискорення для обчислення відносного положення, яке можна використовувати для навігації під час втрати сигналу GNSS. У свою чергу, GNSS може забезпечити зовнішнє посилання на INS, що допомагає зменшити вплив помилок зсуву.

Приймачі GNSS/INS для БПЛА та безпілотних транспортних засобів особливо корисні для міських чи лісистих середовищ, або для тактичних місій чи промислових інспекцій, коли дрон, ймовірно, пройде через тунелі чи інші перешкоди сигналу GNSS.

1.2 Інерціальна система навігації на базі польотних контролерів

Інерціальна навігаційна система (ІНС) - це автономний пристрій, що складається з інерціального вимірювального блоку / inertial measurement unit (IMU) і обчислювального блоку. IMU зазвичай складається з 3-осьового акселерометра, 3-осьового гіроскопа та іноді 3-осьового магнітометра та вимірює кутову швидкість і прискорення системи. Обчислювальний блок, який використовується для визначення орієнтації, позиції та швидкості системи на основі необроблених вимірювань від IMU з урахуванням початкової початкової позиції та орієнтації.

1.2.1 Інерцій вимірювальний блок як основа ІНС

Інерційний вимірювальний блок (IMU) — це пристрій, який може вимірювати та повідомляти питому вагу та кутову швидкість об’єкта, до якого він прикріплений. IMU зазвичай складається з:

- Гіроскопи: забезпечення вимірювання кутової швидкості;
- Акселерометри: вимірювання питомої сили/прискорення;
- Магнітометри (опціонально): вимірювання магнітного поля, що оточує систему;

Додавання магнітометра та алгоритмів фільтрації для визначення інформації про орієнтацію призводить до створення пристрою, відомого як референтні системи положення та курсу (AHRS).

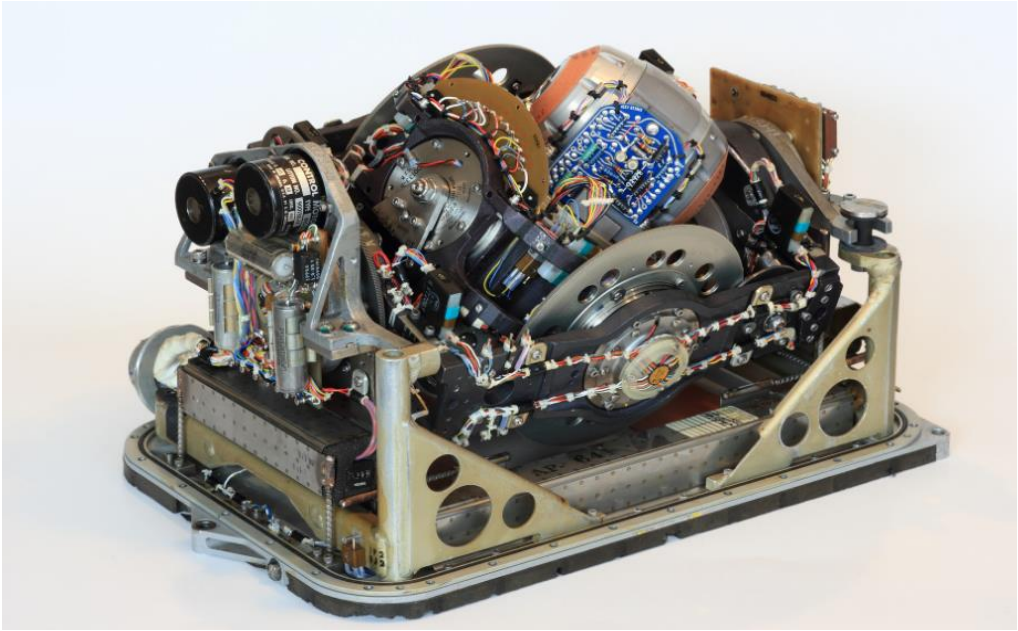


Рисунок 1.1 - Інерційний вимірювальний блок Аполло

IMU доступні в кількох класах продуктивності. Вони поділяються на чотири категорії на основі характеристик акселерометра та гіроскопа:

- Споживча/автомобільна;
- Промислова;
- Тактична;
- Навігаційна.

Ці категорії продуктивності зазвичай визначаються на основі стабільності зсуву датчика під час руху, оскільки стабільність зміщення під час руху відіграє таку важливу роль у визначенні продуктивності інерційної навігації. У наведеній нижче таблиці підсумовано продуктивність різних сортів для цих специфікацій.

Таблиця 1.1 Порівняльна характеристика категорій IMU

Категорія	**ЦІНА, $**	**Стабільність зміщення, °/годину**	**В зоні без GNSS, хв.**	**Застосування**
Споживча	<10**$**	–	–	Смартфони
Промислова	100-1000**$**	<10°/годину	<1 хв.	БПЛА
Тактична	5000-50000**$**	<1°/годину	<10 хв.	Розумні боєприпаси
Навігаційна	<100000**$**	<0.1°/годину	1-3 год.	Військового призначення

Як вже згадували вище, інерціальна навігаційна система (ІНС) використовує інерціальний вимірювальний блок (IMU), що складається з акселерометрів, гіроскопів і іноді магнітометрів.

1.2.2 Акселерометр

Акселерометр є основним датчиком, який відповідає за вимірювання інерційного прискорення або зміни швидкості з часом, і його можна знайти в різних типах, включаючи механічні акселерометри, кварцові акселерометри та акселерометри MEMS. MEMS-акселерометр — це, по суті, маса, підвішена на пружині, як показано на малюнку 2. Маса відома як пробна маса, а напрямок, у якому маса може рухатися, називається віссю чутливості. Коли акселерометр піддається лінійному прискоренню вздовж осі чутливості, це прискорення

спричиняє зміщення пробної маси вбік із величиною відхилення, пропорційною прискоренню.

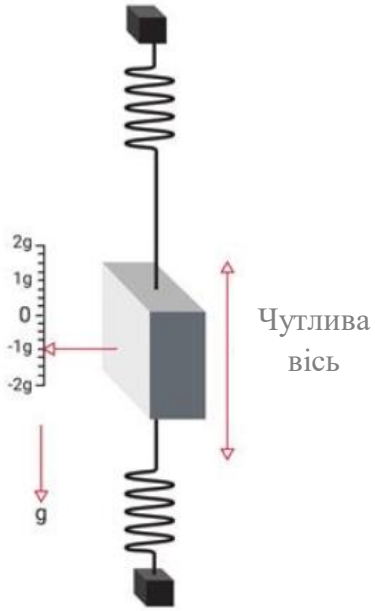


Рисунок 1.2 - Проста модель акселерометра.

1.2.3 Гіроскоп

Гіроскоп — це інерційний датчик, який вимірює кутову швидкість об’єкта відносно інерціальної системи відліку. На ринку доступно багато різних типів гіроскопів, які мають різні рівні продуктивності та включають механічні гіроскопи, волоконно-оптичні гіроскопи, кільцеві лазерні гіроскопи і кварцові/ MEMS гіроскопи. Кварцові та MEMS-гіроскопи зазвичай використовуються на ринках споживчого, промислового та тактичного класів, тоді як волоконно-оптичні гіроскопи охоплюють усі чотири категорії продуктивності. Кільцеві лазерні гіроскопи зазвичай складаються зі стабільності зміщення під час руху в діапазоні від 1 °/год до менше 0,001 °/год, охоплюючи тактичний і навігаційний рівні. Механічні гіроскопи є найефективнішими гіроскопами, доступними на ринку, і можуть досягати стабільності зміщення під час роботи менше 0,0001 °/год.

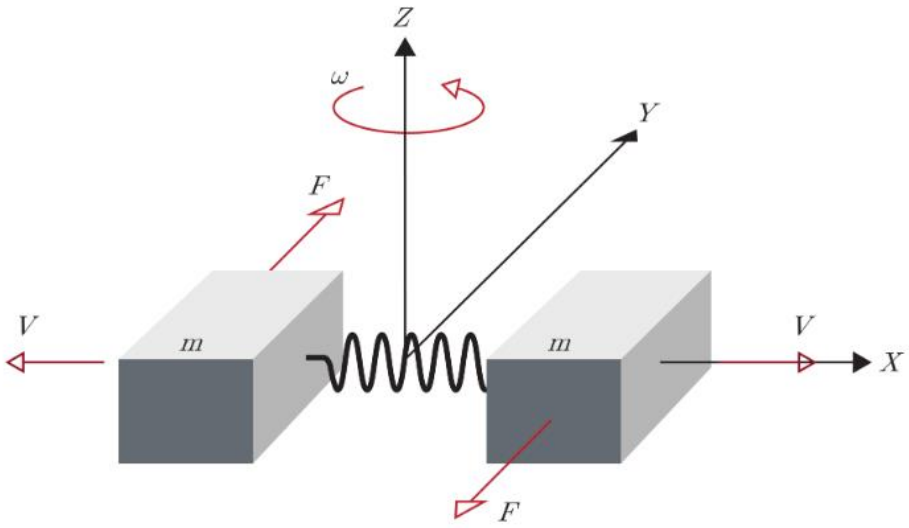


Рисунок 1.3 - Простий приклад гіроскопу

1.2.4 Магнітометр

Магнітометр — це тип датчика, який вимірює силу та напрямок магнітного поля. Хоча існує багато різних типів магнітометрів, більшість магнітометрів MEMS покладаються на магнітоопір для вимірювання навколишнього магнітного поля. Магніторезистивні магнітометри складаються з пермалою, який змінює опір через зміни магнітного поля. Як правило, магнітометри MEMS використовуються для вимірювання локального магнітного поля, яке складається з комбінації магнітного поля Землі, а також будь-яких магнітних полів, створюваних сусідніми об’єктами.

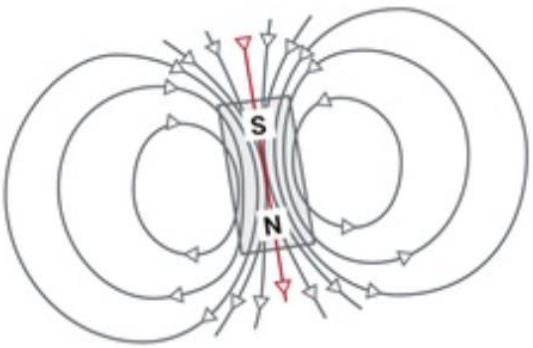


Рисунок 1.4 - Простий дипольний магніт

Гіроскоп і магнітометр надають системі ІНС такий самий внесок, як і AHRS. Вимірювання кутової швидкості гіроскопа інтегровано для рішення високої швидкості оновлення орієнтації, тоді як магнітометр (якщо використовується) забезпечує орієнтир курсу, подібний до магнітного компаса.

Обчислювальний блок відповідає за запис усіх інерційних вимірювань і виконання необхідних обчислень, як правило, за допомогою передової фільтрації Калмана для визначення орієнтації, швидкості та кінцевого положення.

1.3 Відеонавігація

Високоточна навігація та здатність позиціонування БПЛА (безпілотних літальних апаратів) є ключовим фактором, що відображає ступінь його автоматизації. Візуальна навігація на основі зіставлення зображень стала однією з важливих областей досліджень для БПЛА для реалізації автономної навігації через її низьку вартість, потужну здатність запобігати перешкодам і хороший результат визначення місця розташування. Однак на візуальну якість зображень, отриманих БПЛА, серйозно вплинуть деякі фактори, такі як слабке освітлення або недостатня продуктивність його датчиків. Усунення серії погіршень зображень із слабким освітленням може покращити візуальну якість і покращити продуктивність візуальної навігації БПЛА.

Одним із найбільш використовуваних підходів є навігація на основі зору. Цей метод використовує монокулярні відеокамери як головний датчик. Камери дуже підходять для завдань навігації та уникнення перешкод завдяки своїй малій вазі та енергоспоживанню. Крім того, одне зображення може надавати різні типи інформації про навколишнє середовище одночасно. Також можна зменшити витрати, використовуючи камери, а не інші типи датчиків . Підходи до навігації на основі бачення вже є звичайними навігаційними системами для структурованих або напівструктурованих середовищ. Ці системи класифікують зображення з сегментацією доріжок для ідентифікації безпечної навігаційної зони, що призводить до реактивних моделей для керування навігацією. ALVINN

і RALPH були одними з перших, хто застосував нейронні мережі для цього реактивного контролю у зовнішньому середовищі. У Shinzato розробив нейронний класифікатор, складений з ансамблю ШНМ, здатний виявляти та сегментувати судноплавні ділянки дороги через зображення Пізніше цей класифікатор був прийнятий Соузою для реактивного керування на основі відповідності шаблонів. Чисто реактивні моделі не є цілком адекватними для розробки автономної навігаційної системи, оскільки миттєвої реакції на дані датчиків недостатньо, щоб гарантувати правильне керування в складних середовищах. Слід запровадити більш надійну систему, яка надає інформацію про послідовність і контекст, які відсутні в чисто реактивних моделях.

Слід розуміти, що розробка якісної системи автономної відеонавігації потребує серйозного фінансування. Навігація на основі порівнянні зображень та вичислення основних точок позиціонування потребує також серйозною фільтрації та прорахунку. Нажаль не просто впровадити відеонавігацію з ІНС через її нелінійність. Проте, «ROBOTICS And AUTONOMUS LAB» з Австралійського національного університету розробили бортовий інерціальний SLAM - Simultaneous Localisation And Mapping.

Бортовий інерціальний SLAM.

Одночасна локалізація та картографування (SLAM) вперше була розглянута в основоположній статті Сміта та Чізмена та еволюціонувала від внутрішньої робототехніки до відкритих і підводних зон. Та для повітряний апаратів створює додаткові труднощі через високу динаміку, обмежене поле зору та обмежені функції. Ключовим елементом його успіху є надійна система одометрії між основними періодами допомоги. Повна інерціальна навігаційна система 6DoF потрібна для безперервної та повної інформації про стан. Проблема полягає в тому, що будь-яка система INS, заснована на недорогому IMU, має дуже погану навігаційну продуктивність без будь-яких допоміжних сигналів, і IMU слід калібрувати на льоту за допомогою оцінки. Існує багато дослідницьких робіт щодо автоматизованої системи INS, зокрема з використанням GNSS

Інерціальна система, яка не покладається на сигнал GNSS, є відкритою проблемою, а інерціальний SLAM є одним із найбільш потенційних підходів. Домінуючими датчиками, які використовуються, є бачення/лазер, які є самодостатніми сигналами. У всьому світі існують різні дослідницькі групи в цій галузі.

Структура Airborne SLAM

Загальна структура SLAM — це побудова відносної карти орієнтирів за допомогою відносних спостережень, визначення карти та використання цієї карти для одночасного визначення місця транспортного засобу. Традиційно була навігація за допомогою відомим положенням маяка або аерофотокартування з відомим навігаційним рішенням. Таким чином Airborns SLAM об’єднує ці два методи, значно підвищуючи живучість БПЛА в умовах невідомої місцевості.

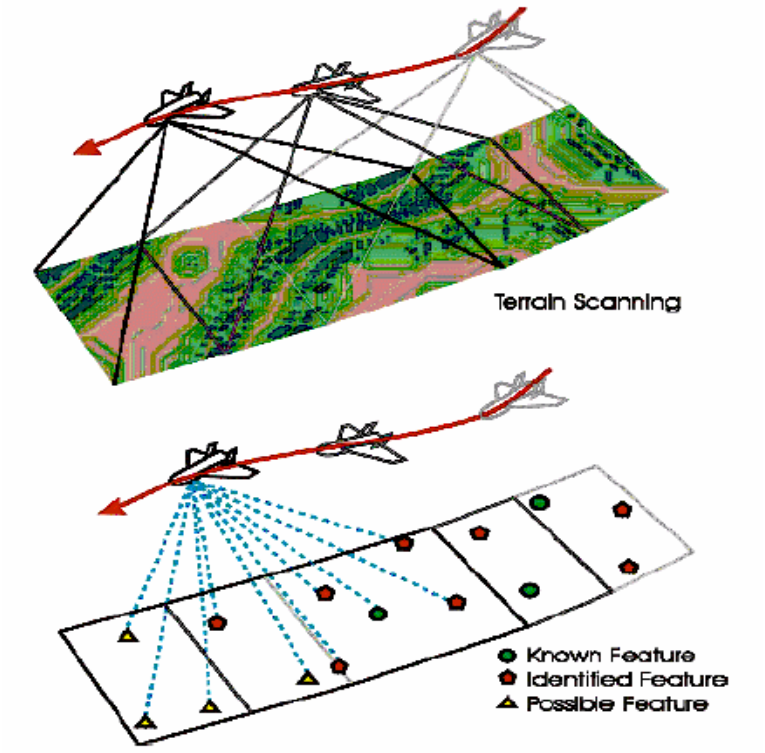


Рисунок 1.5 - Відносно карти орієнтирів

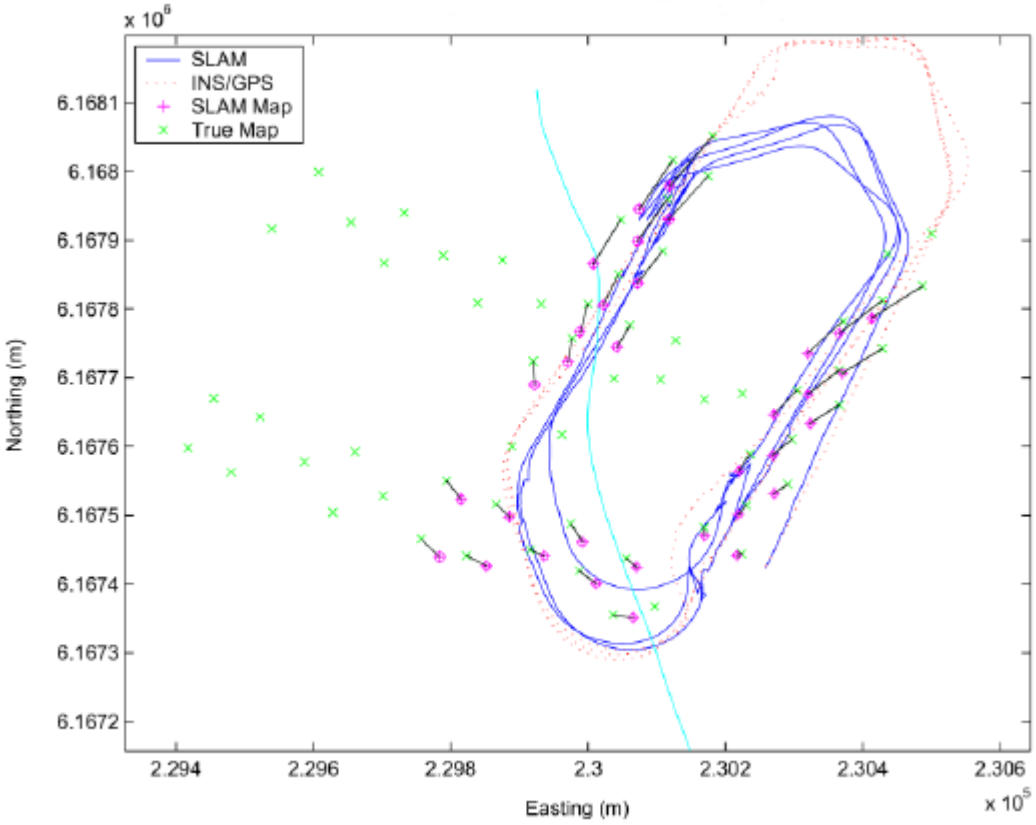
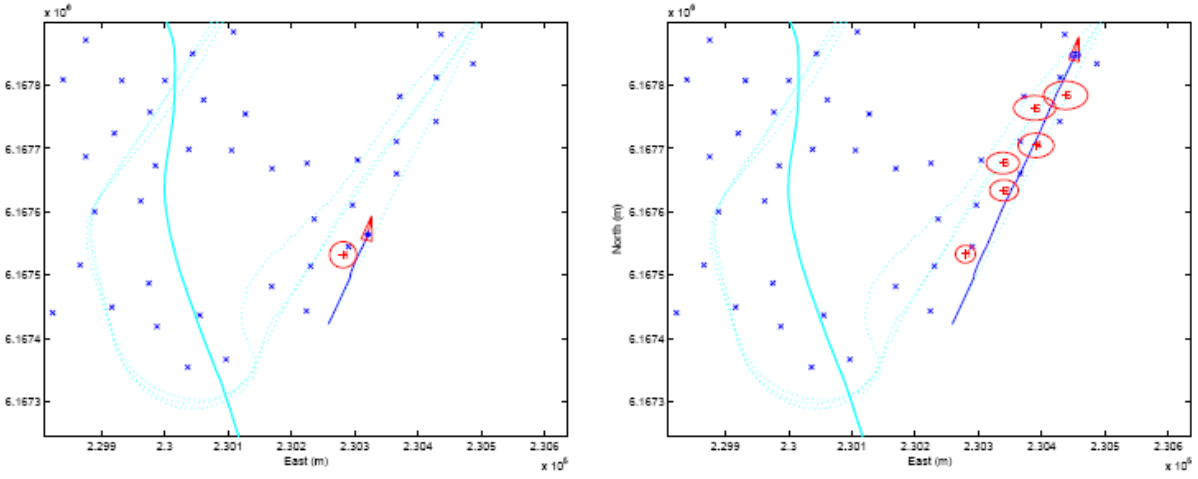


Рисунок 1.6 - Результати Airborne SLAM на реальному польоті БПЛА

Позиції БПЛА та орієнтирів, оцінені за допомогою системи SLAM у реальному часі. GNSS/Інерціальна позиція та орієнтирні позиції наносяться на графік для порівняння, показуючи відповідність наземним істинам.



(a) (b)

Рисунок 1.7 - Перший раунд роботи системи SLAM

Детальний перегляд SLAM у реальному часі під час першого раунду. (a) Система SLAM була активована під час польоту. (b), (c) і (d) представляють поступове створення карти та використовують його для оцінки інерційних похибок одночасно (5σ еліпси були нанесені на орієнтир).

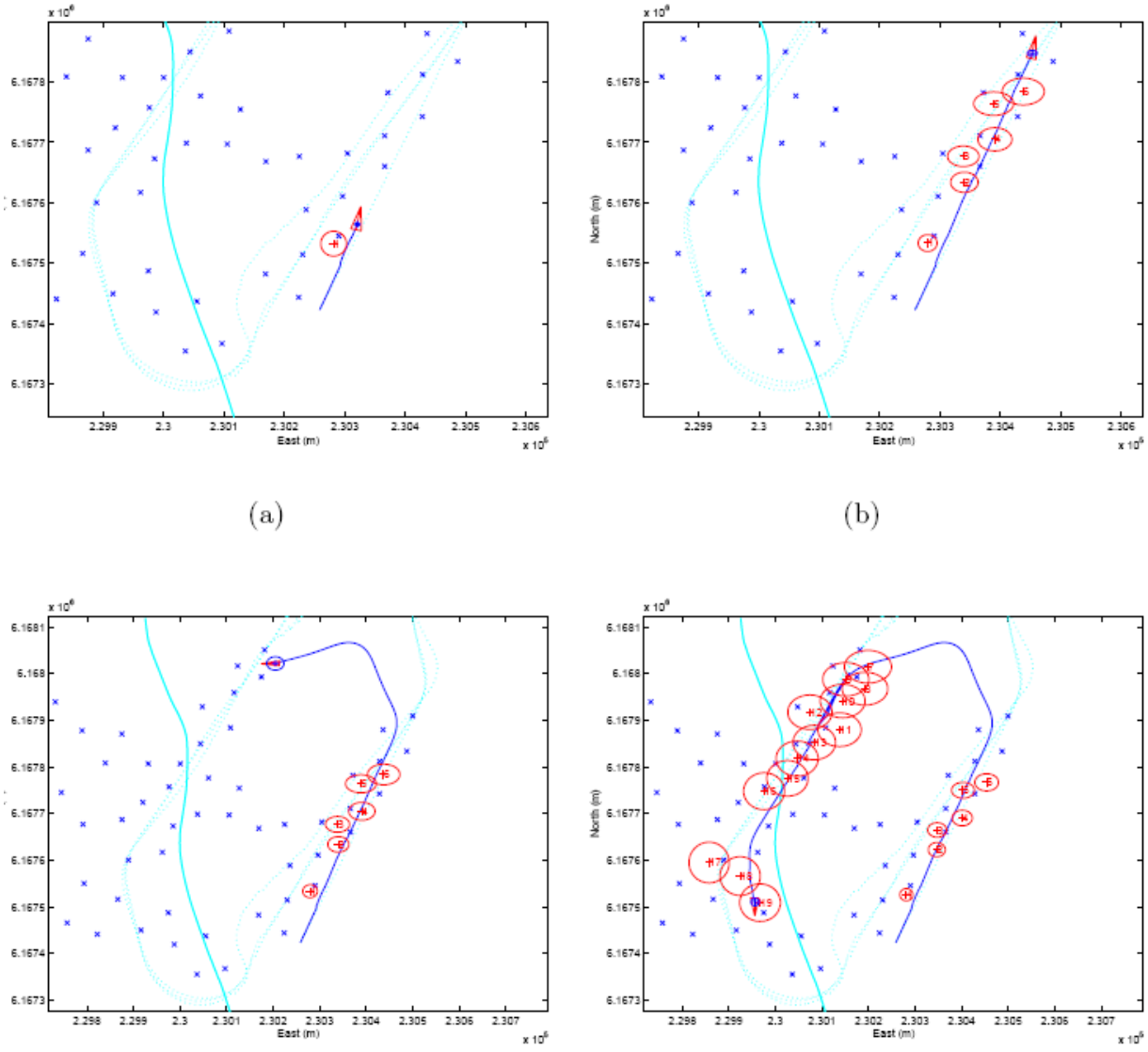


Рисунок 1.8 - Перший раунд роботи системи SLAM

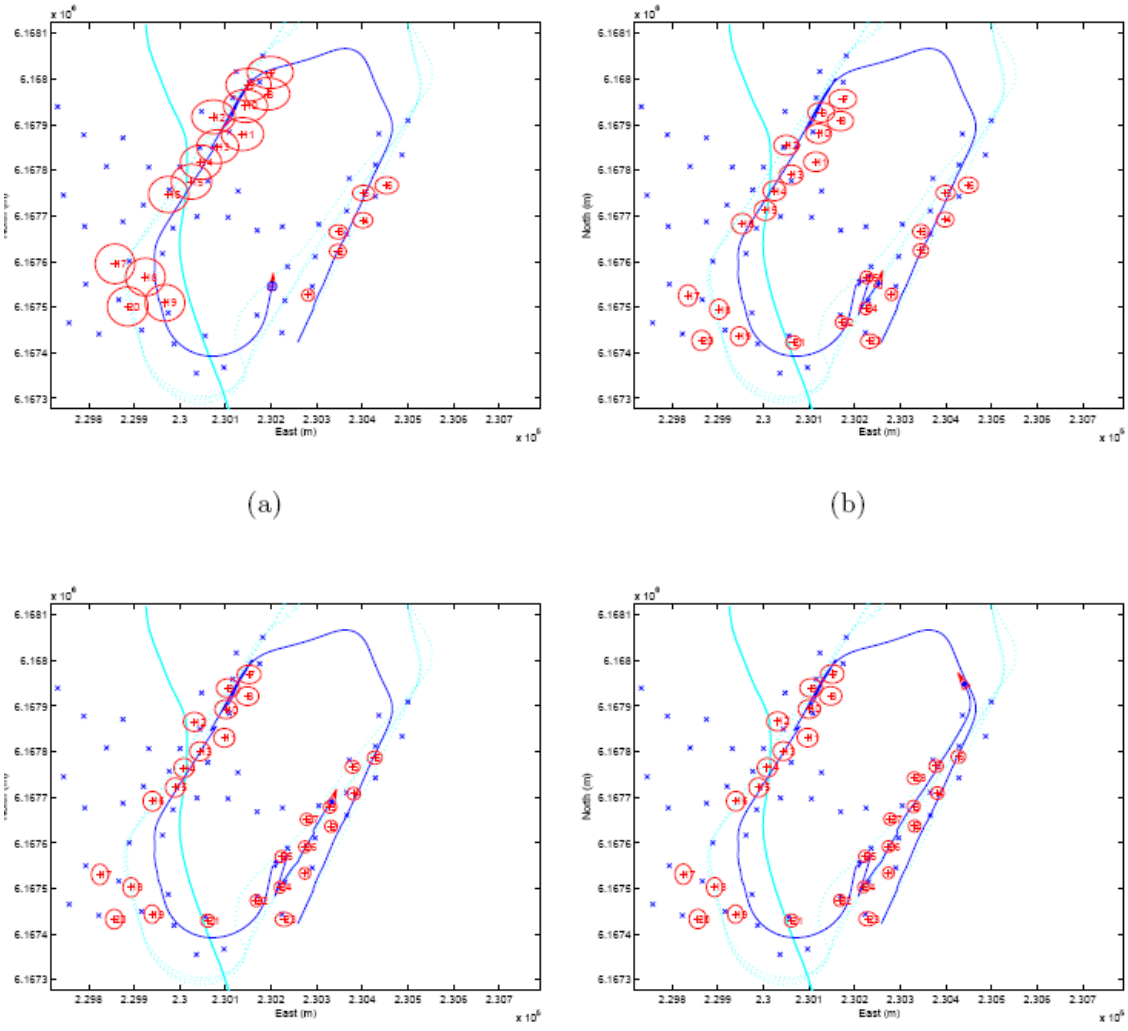


Рисунок 1.9 - Другий раунд роботи системи SLAM

Детальний перегляд SLAM у реальному часі під час раунду. БПЛА знову наближається до початкової позиції та (b) цикл замикається шляхом спостереження за попередніми орієнтирами. Покращено точність карти та разом із станом автомобіля. (c) і (d) показують підвищення точності для послідовних повторних спостережень орієнтирів у межах раунду.

Було досягнуто значного прогресу в байєсівському SLAM (одночасна локалізація та відображення) у додатках мобільних роботів. Однак його застосування з інерційною системою, яка має вирішальне значення для літаючих роботів, все ще зазнає труднощів через нелінійність і високу розмірність у складних умовах польоту. Було показано, що фільтр частинок Rao-blackwellized може ефективно зменшити кількість частинок у проблемі SLAM, і його можна додатково використовувати в інерціальному SLAM, що бореться з нелінійністю

в динаміці положення, одночасно обробляючи лінійні частини за допомогою фільтрації Калмана.

Фільтрація Rao-Blackwellised

Пряме застосування фільтрації частинок для високорозмірної системи не піддається обчисленням і тому не є бажаним. Однак фільтр Rao-Blackwellised (RB) забезпечує ефективний засіб для зменшення простору вибірки шляхом факторизації повної щільності та застосування фільтрації частинок лише для зменшеного підпростору.

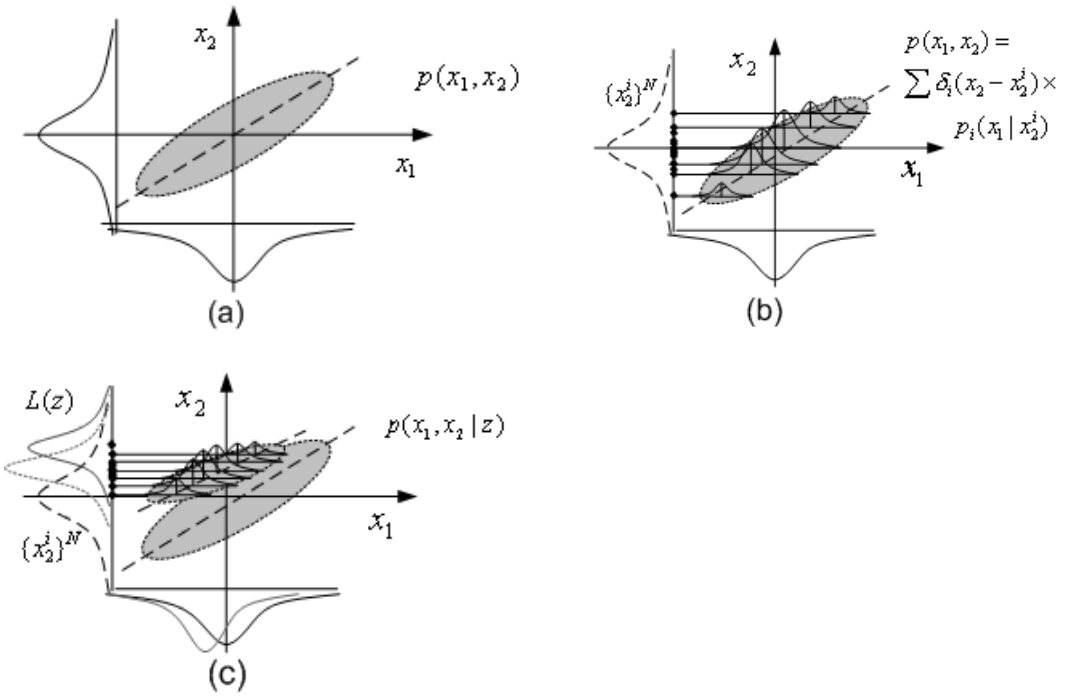


Рисунок 1.10 - RB фільтрація частинок для двовимірної системи стану: а) повна спільна PDF. б) один із його підпросторів (x2) апроксимується набором частинок, кожна з яких несе умовну щільність x1. с) При спостереженні на x2 частинки переміщуються, згодом змінюючи повну спільну та крайову PDF.

Rao-Blackwellised Inertial-SLAM

Ідея полягає в тому, щоб розділити високовимірні стани INS на два підстани: зовнішній стан пози xe, який пов’язаний із відображенням, і внутрішні стани xi для навігації та калібрування інерційного датчика.

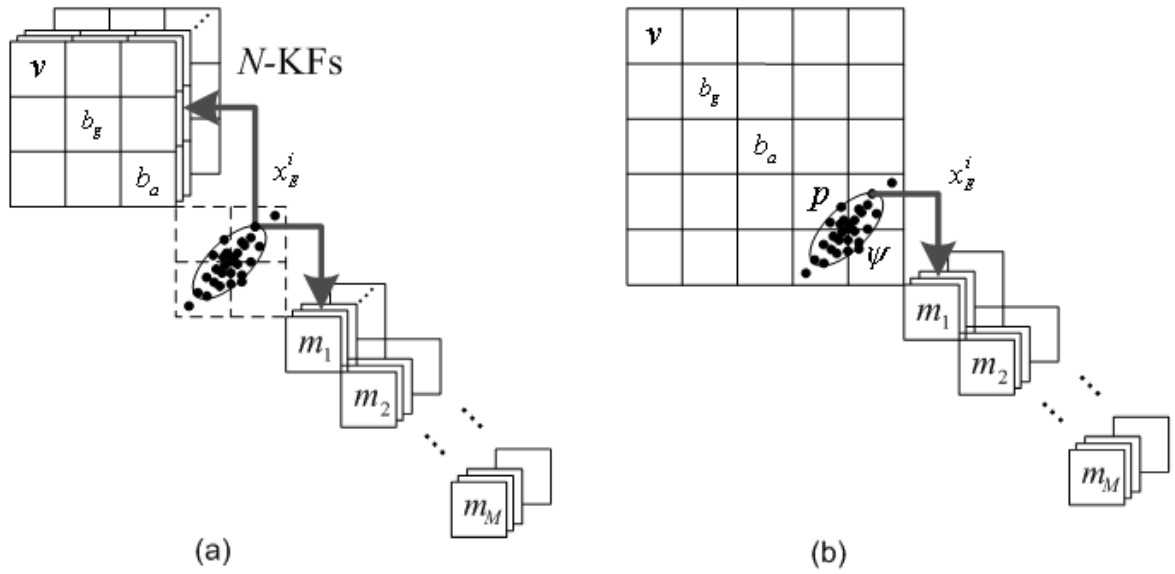


Рисунок 1.11 - a) RB Inertial-SLAM ефективно усуває кореляції між картами, але не кореляції між внутрішніми станами. (b) Hybrid RB Inertial-SLAM, однак, підтримує лише один транспортний засіб EKF.

1.4 Альтернативны системи навігації БПЛА.

В даний час існує багато типів систем, що знаходяться в стадії розробки або виробництва. Навігація за допомогою зображень, відеонавігація, відстеження сонця, відстеження зірок, використання сигналів можливостей і використання дуже точної INS – ось деякі з рішень, які я знайшов у своєму дослідженні. Тепер я хотів би описати, як працюють деякі з цих систем. Тому ми повинні знайти альтернативні навігаційні системи, які є більш надійними та менш чутливими до перешкод. В даний час існує багато типів систем, що знаходяться в стадії розробки або виробництва. Навігація за допомогою зображень, відеонавігація, відстеження сонця, відстеження зірок, використання сигналів можливостей і використання дуже точної INS – ось деякі з рішень, які я знайшов у своєму дослідженні. Тепер я хотів би описати, як працюють деякі з цих систем.

Перш ніж обговорювати альтернативні системи, важливо зазначити, що алгоритми об’єднання даних, такі як фільтр Калмана, можна використовувати з двома або більше датчиками. Різниця між прогнозованим розташуванням об’єкта та фактичним розташуванням об’єкта може бути використана для

усунення зміщень IMU. Як правило, коли кілька оцінок позиції навігаційної системи поєднуються, INS стає основним компонентом. Якщо інші оцінки сенсорної системи точніші, ніж INS, їх можна використовувати для виправлення або оновлення INS.

Навігація за допомогою зображень використовує зображення датчиків для навігації. Вимірювання 3D-зображень місцевості можна отримати за допомогою датчиків EO/IR. Для навігації за допомогою зображень у пам'яті можна зберігати базу даних карт цифрової рельєфу місцевості – digital terrain elevation data (DTED). Зображення датчика можна співвіднести зі збереженою картою DTED і обчислити помилку. Цю помилку можна використати для оновлення INS. Фільтр Калмана може поєднувати зображення та вимірювання INS, використовуючи результати відповідності ознак для виправлення INS. Корекції траєкторії потім повертаються для покращення майбутніх прогнозів. Інший метод використовує зображення для обчислення нової координати. Потім нові координати завантажуються в пам'ять БПЛА та використовуються для навігації.

Інша альтернативна система навігації називається Locata. По суті, це система супутникової навігації, встановлена на серії наземних веж. Це наземна система позиціонування з точністю до сантиметра.

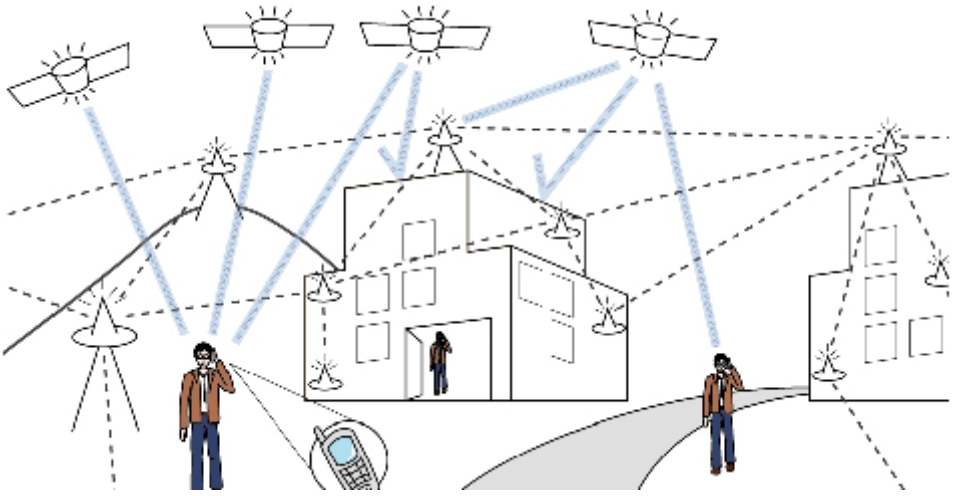


Рисунок 1.12 - Концепт позиціонування Locata

Сигнали в мільйон разів сильніші за сигнал супутникової навігації, а точність була продемонстрована на рівні 18 см на відстані 30 миль. Точність

системи становить близько 3 наносекунд, точніше, ніж атомний годинник, встановлений на супутниках. Ще однією перевагою перед супутниковою навігацією є те, що Locata працюватиме всередині будівель. Приймач Locata також відстежуватиме як супутникові сигнали, так і сигнали Locata. Для корекції часу не потрібні атомні годинники, кабелі та опорна мережа. Locata може синхронізуватися лише за 10 пікосекунд. Компанія BAE нещодавно розробила навігаційну систему БПЛА, яка використовує сигнали можливостей під назвою «Навігаційні сигнали можливості» (NAVSOP). Ця система може використовувати вежі мобільного телефону, радіо вежі, мікрохвильові вежі, телевізійні сигнали та сигнали WiFi. Усі ці типи сигналів, якщо вони доступні, можна використовувати для тріангуляції позиції. Здається, це чудове рішення, однак є деякі проблеми. Одна з проблем полягає в тому, що якщо БПЛА знаходиться дуже близько до однієї вежі стільникового зв'язку, він буде відхиляти сигнали з інших веж, і оцінка тріангуляції буде неможливою.

Висновок: отже, в цьому розділі розглянуто основні та альтернативні види навігації для БПЛА. Головною системою для позиціонування БПЛА залишається GNSS, тому далі будемо вивчати методи впливу на цю систему навігації. Та на майбутнє, слід звернути увагу на альтернативні методи навігації, особливо ті, що пов'язані з машинним зором та системою SLAM, тому що , таким чином можливо досягти повної незалежності БПЛА в сфері навігації.

РОЗДІЛ 2
ЗАВАДИ, ВИДИ ЗАВАД ТА ЇХ КЛАСИФІКАЦІЯ

2.1 Радіоелектронна боротьба

Керівні документи Армії США визначають радіоелектронну війну (РЕВ) як дії військ (сил) з використання електромагнітної енергії і засобів спрямованої енергії з метою здійснення управління (контролю) випромінюваннями електромагнітного спектру частот (у тому числі й використання самого спектру частот) або дії (атаки) на особовий склад, радіоелектронні системи і засоби, об'єкти, озброєння та військову техніку противника. Радіоелектронна війна включає три основних взаємозв'язаних і взаємодоповнюючих один одного елементи: радіоелектронну атаку, радіоелектронний захист і забезпечення ведення РЕВ. Радіоелектронний захист як один з елементів РЕВ одним із напрямків передбачає підсилення захисних якостей об'єктів (цілей), зокрема, створення спеціальних схем, екранів, сховищ, технічних засобів захисту (у першу чергу мова йде про фізичні та технічні засоби захисту від дії електромагнітних випромінювань радіоелектронних засобів (РЕЗ) своїх військ або військ противника). Для забезпечення ведення РЕВ визначені склад сил і засобів – органи управління, розвідки, тилового та технічного забезпечення, – а також напрямки оперативної та бойової підготовки. Підкреслюється, що РЕВ є одним з елементів інформаційних операцій.

У Збройних силах України під терміном радіоелектронна боротьба (РЕБ) розуміють сукупність узгоджених за метою, завданнями, місцем і часом одночасних і послідовних дій з радіоелектронного подавлення систем управління військами та зброєю противника і заходів щодо радіоелектронного захисту РЕЗ своїх систем управління, які спрямовані на забезпечення переваги у використанні електромагнітного спектру. Радіоелектронне подавлення (РЕП) розглядають як сукупність узгоджених за метою, завданнями, місцем і часом радіоелектронних впливів на радіоелектронні системи і засоби управління

військами та зброєю, які здійснюються силами та засобами РЕБ за єдиним замислом і планом відповідно з радіоелектронною обстановкою, що склалася. У свою чергу, радіоелектронний захист (РЕЗах) – це комплекс організаційно-технічних заходів і дій, спрямованих на забезпечення стійкої роботи своїх систем управління військами і зброєю з метою забезпечення переваги у використанні електромагнітного спектру.

Окремо розглядають радіоподавлення як дії щодо порушення роботи радіо-, радіорелейних, тропосферних і супутникових ліній зв'язку, засобів радіолокації і радіонавігації противника шляхом впливу на них електромагнітними випромінюваннями, застосуванням оманних радіолокаційних цілей і пасток, передачі повідомлень, що дезінформують, у радіомережах противника або своїх військ, демонстрації (помилкової) роботи своїх радіоелектронних засобів або імітація роботи РЕЗ противника, а також зміни умов розповсюдження радіохвиль. Для ведення РЕБ залучають спеціальні сили та засоби – батальйони, вузли РЕБ, індивідуальні і групові засоби РЕБ, у тому числі літальних апаратів, пристрої (прилади) радіоелектронного захисту засобів військ. Аналогічний підхід до тлумачення понять і дій РЕБ прослідкується і в інших джерелах.

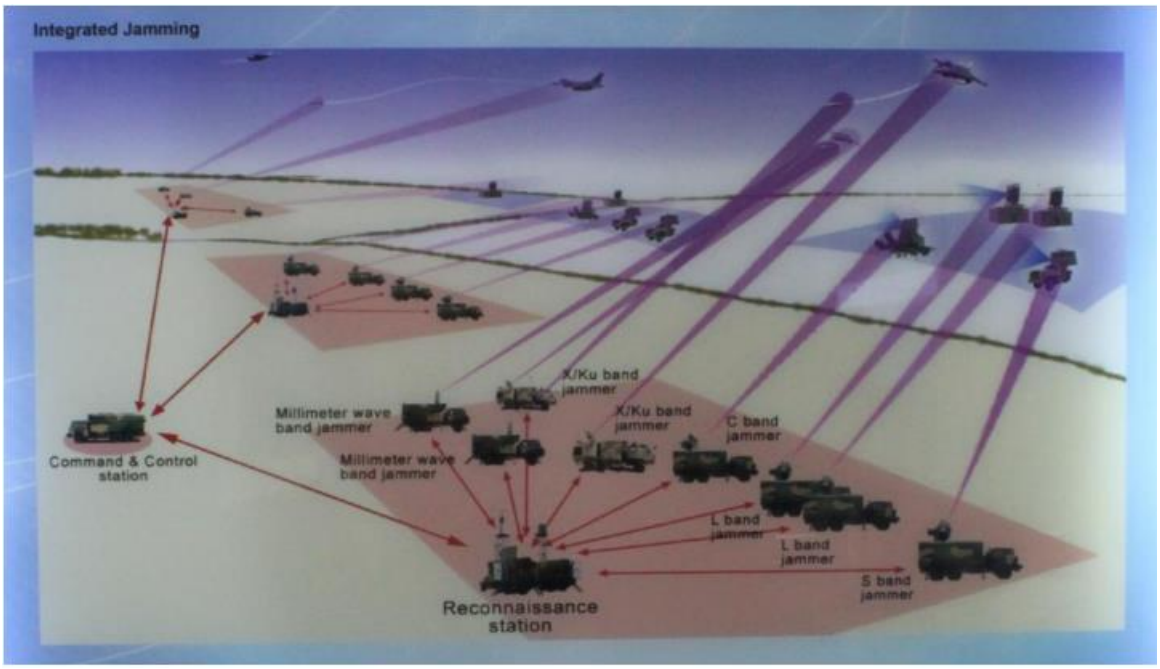


Рисунок 2.1 - Приклад ведення РЕВ китайських військ

Широке застосування в житті суспільства знайшли пристрої Hi-Tech: засоби зв’язку, обробки інформації, навігації, Wi-Fi камери, тепловізори, безпілотні літальні апарати (БПЛА) невеликих розмірів і т.д. Ці пристрої є засобами подвійного призначення і породжують масу проблем збройним силам (ЗС) і силам охорони правопорядку (СОП), до яких відноситься Національна гвардія України (НГУ). Пристрої Hi-Tech використовують терористичні угруповання і незаконні збройні формування (НЗФ) для зв’язку і протидії підрозділам сил охорони правопорядку і ЗС.

Основними доступними засобами зв'язку Hi-Tech у вільному продажу є: аналогові і цифрові портативні і автомобільні радіостанції діапазонів VHF (146-174 МГц), UHF (400-480 МГц), мобільні телефони GSM і CDMA, супутникові телефони, Wi-Fi, скануючі приймачі, вбудовані пристрої GPS-навігації, зв’язок з віддаленим доступом (Internet Radio). До засобів Hi-Tech в останні роки додалися радіокеровані моделі БПЛА, зокрема квадрокоптери, з відеокамерами високої роздільної здатності та професіональними функціями. Їх технології удосконалюються, поліпшуються надійність, безпека, керованість та інші характеристики. У цих “іграшок” з’явились такі функції, як “повернення додому”, системи FPV з відстеженням “положення голови” (спосіб управління БПЛА за допомогою відеокамери на борту – відео реального часу дозволяє оператору управляти апаратом, який знаходитися поза зором оператора), 3D FPV окуляри, режим огинання перешкод, функція “слідуй за мною” та інші. Навіть при невеликому часі польоту (15-30 хвилин) “іграшка” в руках терориста перетворюється на ефективний засіб розвідки і протидії підрозділам СОП, особливо в міських умовах.

2.2 Класифікація завад

Вплив радіозавад може призвести до таких наслідків, як перевантаження приймального пристрою, маскування чи спотворення радіосигналу або його

імітації. На кінцевий результат дії навмисних радіозавад впливають такі фактори:

- співвідношення сигнал/шум на вході радіоприймача, що піддається впливу завади;
- співвідношення ширини спектру корисного радіосигналу до сигнала радіозавади;
- особливості побудови засобу радіозв'язку, параметри його роботи (модуляція, частота роботи, потужність передавача та чутливість приймача) та структури корисного сигналу (використання кодування, методи розширення спектру);
- параметри самих радіозавад.

Класифікація навмисних радіозавад доволі широка, може ділитись по багатьом параметрам. Стисла класифікація наведена на Рис. 2.2

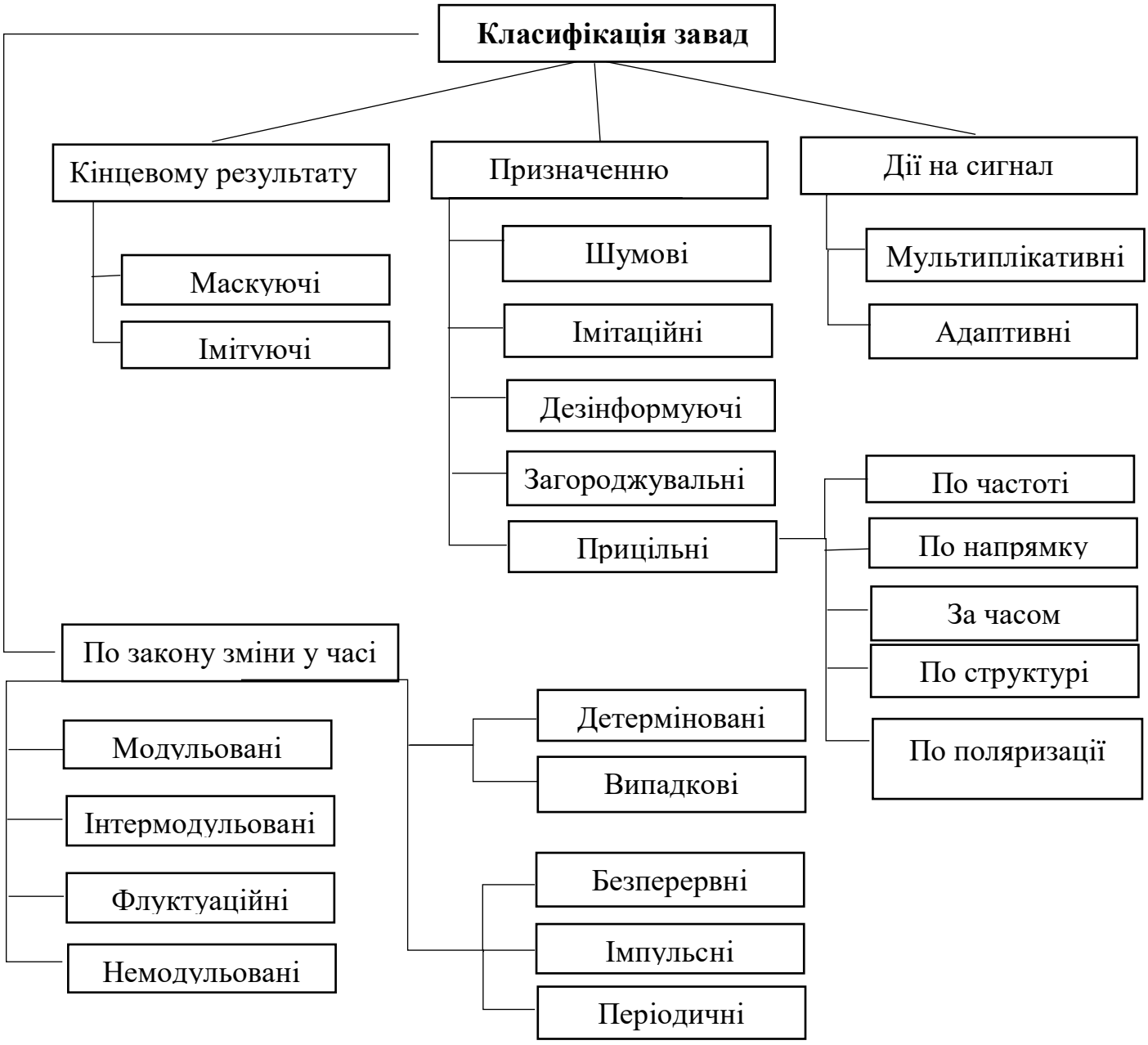


Рисунок 2.2 - Класифікація завад

За параметрами більш детально радіозавади класифікуються за:

– джерелом походження. Розрізняють завади які з’явилися у наслідку природних явищ та штучні – утворені пристроями, що випромінюють енергію електромагнітних хвиль;
– виду випромінюваної енергії. Існують електромагнітні, оптичні та акустичні завади;
– співвідношенню спектрів. Завади, чий спектр значно перевищує спектр корисного сигналу називають загороджувальними. Прицільними називають такі завади, чий спектр порівняний с спектром корисного сигналу, а частота змінюється у діапазоні роботи ЗРЗ;
– структурою випромінювання. Розрізняють імпульсні завади, що являють собою серії модульованих або не модульованих радіоімпульсів, та безперервні, які можуть бути промодульовані по частоті, фазі чи амплітуді;
– характером впливу на ЗРЗ. Розрізняють маскуючи, що ускладнюють виявлення та розпізнавання параметрів прийнятого корисного радіосигналу. Іншим видом є імітуючи радіозавади, мета яких створити помилкові (не вірні) радіосигнали на вході приймача;
– потужності. Слабкі радіозавади, чий рівень не перевищує рівень корисного сигналу та викликає втрату не більше ніж 25% корисної інформації.

Середні радіозавади по рівню потужності можна порівняти з рівнем корисного сигналу, вони можуть викликати втрату не менше 50% корисної інформації. Сильні радіозавади по рівню потужності значно перевищують корисний сигнал, можуть привести до повної втрати корисної інформації. В окремих випадках можуть перевищувати динамічний діапазон радіоприймального пристрою.

Пасивні радіоелектронні завади створюються завдяки відбиттю (розсіюванню) електромагнітного випромінювання, що надходить від інших радіоелектронних пристроїв. Це випромінювання може надходити завдяки

відбиттю від штучних об’єктів, таких як дипольні та кутові відбивачі, лінзи Люнеберка, аерозолі, тощо. Зазвичай, результуючий сигнал утворений відбиттям є сумою елементарних сигналів з випадковими параметрами амплітуди, частоти і фази.

Активні радіоелектронні завади створюються з використанням спеціальних пристроїв – генераторів завад чи станцій постановки завад. Параметри сигналу завади визначаються призначенням, структурою цих генераторів перешкод.

Далі проведено опис основних видів активних радіоперешкод.

Найбільш універсальною за сферами використання є загороджувальна шумова завада, що являє собою білий гаусівський шум з певною спектральною щільністю потужності у обмеженій полосі частот. Як виходить з назви, полоса частот завади перекриває діапазон роботи засобу радіозв’язку. Спектральну щільність потужності можна визначити за формулою (1.1):

$$G_z = \frac{P_Z}{\Delta f_c}$$

де: Pz – потужність радіозавади;

Δf – ширина спектру радіозавади.

Найбільш ефективно загороджувальна радіозавада діє у випадках, коли рівень потужності радіозасобу, що подавлюється нижче або дорівнює рівню самої завади, але такі випадки рідкі. Рис. демонструє ситуацію, де спектр корисного сигналу перекритий завадою, але його рівень потужності значно вищій ніж рівень завади. Світло–сірим показана завада, чорно–сірим корисний сигнал.

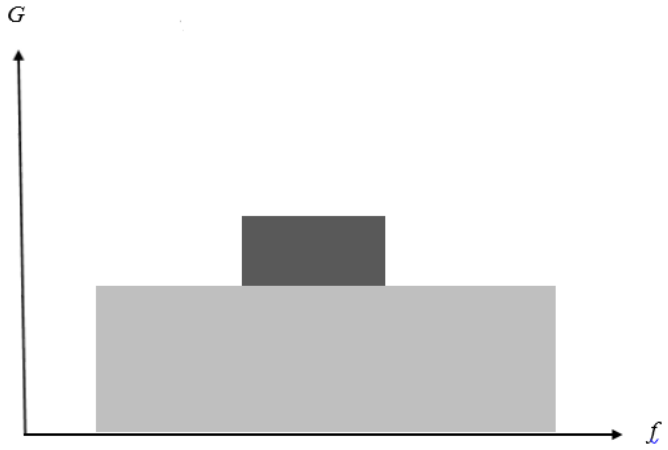


Рисунок 2.3 - Ефективний вплив загороджувальної завади

Різновидом загороджувальної шумової завади є шумова завада у частині смуги. Спектральна щільність потужності цієї завади може бути описана системою рівнянь (1.2):

Перше для завади у смузі $\gamma\Delta f_c$.

Друге відповідно $(1 - \gamma\Delta f_c)$

$$G_z = \begin{cases} \frac{P_z}{\gamma\Delta f_c} \\ 0 \end{cases}$$

де: γ – коефіцієнт, що характеризує частину спектру сигналу, на якій діє завада. Його значення лежить у діапазоні 0 ≤ γ ≤1.

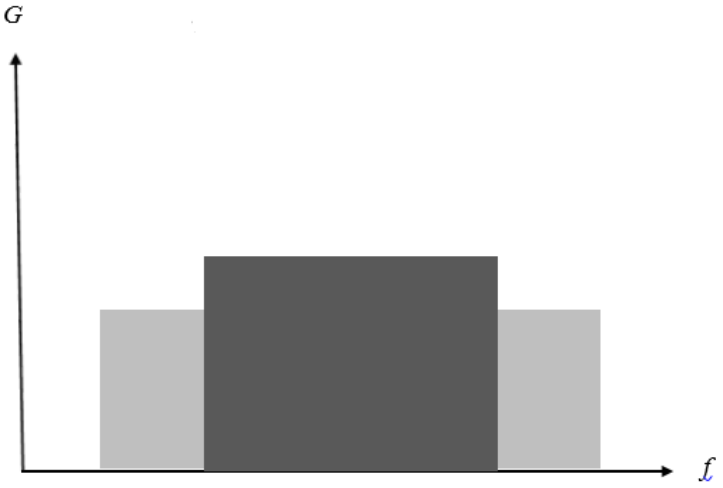


Рисунок 2.4 - Загороджувальна завада у частині смуги

Маскуючи радіозавади мають на меті ускладнення виявлення корисного сигналу (збільшення ймовірності помилкової тривоги) шляхом створення завадового фону на приймальній частині засобу зв'язку. На рівень завданого ускладнення впливають співвідношення частотних, часових та структурних параметрів корисного сигналу та радіозавади.

У якості активних маскуючи радіозавад зазвичай використовуються безперервні шумові завади Прицільні радіоперешкоди характеризуються тим, що їх спектр співвідносний чи повністю збігається зі спектром корисного сигналу ЗРЗ що подавлюється. Імітуючи радіозавади мають на меті внести хибну інформацію на приймальній стороні ЗРЗ що подавлюється. Параметри такої завади зазвичай близькі до значень параметрів корисного сигналу, що імітується. В деяких випадках у якості сигналу, що імітує, може бути використана частина корисного сигналу, яка починає ретранслюватися станцією завад.

Таблиця 2.1 - Загальна аналітика засобів РЕБ які використовуються

Приймачі розвідки радіозв'язку	**Радіостанції зв'язку**	**Антени***	**Радіоукриття***
Радіостанції з функцією сканунування	Передавачі перешкод*	Пеленгаційні	На основі куткової антени
Скануючі приймачі*	Передавачі перешкод з віддаленим доступом	Спрямовані для подавлення	Екрануючий шатер з металізованої тканини
Скануючі приймачі з віддаленим доступом	Передавачі подавлення БПЛА**	З керованою діаграмою	Площинний екран розмірами n λmax·m λmax

*VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

** Передавачі перешкод видимого та IR діапазонів

Таблиця 2.2 - Загальна характеристика антен станцій РЕБ

Завдання	**Діаграма**	**Поляризація**	**Діапазон**
Радіомаскування активне	Секторна*	Вертикальна, горизонтальна	VHF,UHF,3G, Wi-Fi
Радіорозвідка (пеленгація)	Двопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення радіостанцій зв'язку	Секторна, однопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління рухомих командних пунктів	Кругова, секторна*	Вертикальна, кругов	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління і передавання інформації БПЛА	Секторна, однопелюсткова, косекансна	Вертикальна, горизонтальна	VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

* Передавачі перешкод видимого та IR діапазонів

Зазвичай, станції радіоелектронної боротьби працюють в парі, або мають обладннання засобів радіоелектронної розвідки. Для вдалої роботи, станція повинна геренувати завади тих частот, які використовує ворог, та направити цю завати в сектор де він знаходиться. Найбільш ефективні станції РЕБ, які проінформовані частотами на яких працює ворог, тоді для визначення цих частот самостійно не потрібнь витрачати час, а зразу починати працювати для встановлення завади.

Існують ряд частот, які використовуються для навігації та управління БПЛА:

Таблиця 2.3 - Діапазони та смуги частот БПЛА

Діапазон	Смуга	Призначення
WiFi 5.8 ГГц	5.7-5.9 ГГц	Передавання відео
WiFi 2,4 ГГц	2400-2480 МГц	Управління
GPS L1	1575.42 МГц	Навігація
GPS L2	1227.60 МГц	Навігація
433 МГц		Пульт управління
800/900 М, 850-965МГц		Пульт управління

2.3 «Jamming» та «Spoofing» як основні завади для навігації БПЛА

2.3.1 Jumming

Jamming - це акт навмисного спрямування електромагнітної енергії на систему зв'язку (і навігації), щоб порушити або запобігти передачі сигналу. Таким чином, пристрої перешкод GNSS транслюють свій сигнал перешкод у діапазоні частот, який використовується для супутника навігація. Атаку з перешкодами можна класифікувати як відмову в обслуговуванні – GNSS все ще доступна, але потужніть перешкод повністю перекриває сигнали від супутників. Треба розрізняти військові та цивільні перешкоди.

У кризових і не тільки ситуаціях глушіння можуть впроваджувати військові для локальних операцій, чи захисту певних об'єктів. Але, як показує практика, jummer це найбільший ворог насамперед для своїх. Практика показує, під час війні в Україні наші РЕБ станції робили більше лиха ніж ворожі. Джамери зазвичай покривають зону куполом, тому використання нашими бійцями БПЛА навіть далеко на свої території викликало певні питання про силу російського РЕБ, але це все свій РЕБ що стоїть поряд, про існування якого ніхто не знає. Цю проблему вирішує тільки чітка скоординованість груп що виконують завдання в одній зоні.

Джамери активно використовуються також в цивільній сфері, насамперед поблизу критичних інфраструктур, такиз як аеропорти , атомні електростанції,

квартали влади чи різних консульств. Протягом останніх кількох років комерційні перешкоди – так звані пристрої захисту конфіденційності Privacy Protection Devices (PPD) – стають дедалі популярнішими, але також привернули увагу громадськості через кілька випадків зловживання. Ці пристрої PPD можна придбати, напр. через Інтернет, починаючи від 30 євро за звичайний автомобільний із живленням від прикурювача до дуже складних GPS-автодіапазонів (включно з GSM, WiFi) із зовнішніми антенними роз'ємами та настроюваними режимами роботи за кілька сотень євро.

Існує багато різних причин для використання PPD, більшість із яких межує з незаконністю, як-от вимикання протиугінної системи в автомобілі, яка передає дані GPS положення транспортного засобу до центрального блоку, або в обхід читання систем збору проїзду та страхування оплати за те, що ви ведете, або виходу з системи керування автопарком; або вимкнення системи автоматичної ідентифікації суден; або для захисту конфіденційності агентів з доставки посилок від їхніх роботодавців. Незважаючи на те, що деякі з мотивів можуть бути розумними, вплив використання PPD часто незрозумілий для користувачів. Вони не усвідомлюють, що такий крихітний PPD може порушити або спотворити цілісність GNSS на відстані кількох кілометрів.

2.3.2 Spoofing

Spoofing — це навмисна передача фальшивих сигналів GNSS з наміром обдурити приймач GNSS, щоб він надав неправдиву інформацію про місцезнаходження, швидкість і час. Мета підробки полягає в тому, щоб таємно змусити приймач GNSS відстежувати підроблений сигнал (або оманливі сигнали) з метою надання або принаймні спонукання до визначення неправильного визначення місцезнаходження. Використання підробки секретних сигналів захист криптографічного сигналу, як військовий GPS P(Y) або Galileo PRS, практично неможливий. Однак навіть секретні сигнали не є такими захист від атак meaconing: Meaconing означає запис і ретрансляцію

автентичних сигналів GNSS. Якщо приймач відстежує сигнали, створені апаратним забезпеченням без вимірювання, помітивши це, приймач отримає не своє правильне положення, а замість нього положення вимірювального обладнання або його дещо змінену версію.

Незалежно від джерела спуфінгові атаки можна класифікувати таким чином:

– без перекриття;
– перекриваючі;
– за їх відносною потужністю.

Без перекриття - у цьому випадку код і фаза підмінного сигналу не синхронізується зі справжнім сигналами. Піки кореляції підмінного і робочого сигналів не перекриваються. Якщо під час холодного запуску потужність спуфінгового сигналу вище, ніж у справжньому, вхідному тракті пошуку та ідентифікації сигналів навігаційних супутникових приймачів може бути обмануто.

Коли ж супутникові сигнали вже відстежуються приймачем (виповнена ініціалізація), приймач ігнорує всі несинхронізовані сигнали. Отже, спуфінговий сигнал більш високої потужності не пов'язаний з відображенням подовжених супутникових сигналів, якщо затримкі або додаткові частоти не вирівняні.

Перекриваючі - більш складний тип спуфінгової атаки, джерело підмінного сигналу, може синхронізувати свою фазу, код і доплерівську частоту з фазою, кодом і доплеровской частотою справжнього сигналу. Перекриваючі типи спуфінгової атаки, піки кореляції спуфінгових і подовжених сигналів об'єднуються, щоб конструктивно або деструктивно змінити форму піка кореляції.

Цей тип спуфінгової атаки може бути сформований генератором спуфінга на основі приймача, де спуфер знає поточний час, спостережувані супутники, місце розташування та параметри роботи атакуючого приймача. Правильне виявлення спуфінгової атаки з перекриттям є складною задачею, оскільки виявлені, викликані спуфінговими сигналами, схожі на помилки, викликані багатолучевістю.

За відносною потужністю - потужність сигналу атаки спуфінга є важливою складовою при обмані GNSS приймача. Відносний рівень потужності сигналів спуфінгу в порівнянні з рівнем справжніх сигналів може сильно вплинути на ефективність і можливість перешкоди спуфінгу. Виявлення спуфінгової атаки на основі їх відносної потужності більш складно, оскільки для цього потрібна інформація про канал поширення спуфінгу, діаграму посилення антени та її орієнтацію.

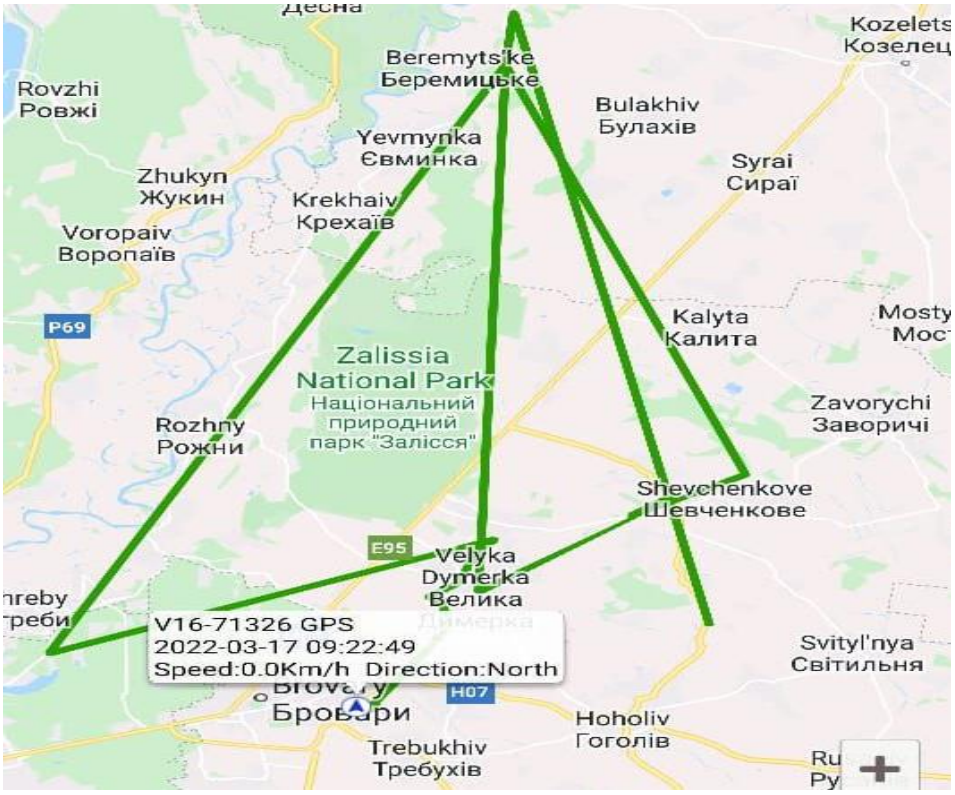


Рисунок 2.5 - Приклад спуфінгової атаки станцією РЕБ ВСРФ.

На Рис. 2.5 бачимо як спуфінгові атаки впливають на положення GPS.

Висновок: у разі відсутності будь-якого захисту приймача, БПЛА буде реагувати на кожну підміну в результаті чого автопілот намагатиметься компенсувати зміни підмінного положення. Таким чином це може призвести до того, що апарат вилетить із контрольованої зони.

РОЗДІЛ 3
МЕТОДИ ЗАХИСТУ БПЛА ВІД ЗАВАД ШИРОКОГО СПЕКТРУ

3.1 Анті-jamming

Анті-jamming – це один з основних напрямків захисту цілісності та доступності GNSS апаратури споживачів. Напрямки по компенсації перешкод даються в документах ICAO і діляться на організаційні заходи та технічні заходи. В даний час світова навігаційна спільнота вже чітко сформулювала напрями анті-jamming. Для повного убезпечення сигналів GNSS потрібно використовувати комплекс засобів захисту. Напрямки засобів по компенсації завад анті-jamming розписані в **ДОДАТОК А**.

Поліпшення якості сигналу ДОДАТОК А:

- *підвищення* рівня сигналу GNSS, як недолік цього напряму потреба в додатковому зовнішньому обладнанні яке буде неефективно при значному великому енергетичному рівні завади;
- *підвищення* завадостійкості сигналу, ці зходи проводяться на передавальній стороні і як недолік це довга і дорога модернізація космічного сегменту GNSS або введення нової системи GNSS (наприклад GALIEO).

Організаційні методи компенсації завад. Проведення організаційних заходів по забезпеченню цілісності та доступності інформації GNSS це вимоги ICAO та IMO, які необхідно виконувати. Для цього необхідно створювати комплекси моніторингу радіонавігаційного поля GNSS і аналізу завадової обстановки (система радіоконтролю) в зоні роботи апаратури споживача. Та організаційні заходи по компенсації завад працюють лише в цивільній сфері та у випадках боротьби зі злочинним використанням глушилок. Для використання GNSS в умовах війни, ставку потрібно робити на удосконалення апаратної частини споживача.

Таблиця 3.1 - Заходи щодо поліпшення апаратури споживача.

№	Заходи завадостійкості	Можливий виграш по відношенню до стандартних приймачів GNSS, дБ	Можливий приріст вартості по відношенню до стандартних приймачів GNSS, %	Примітки
1	Поліпшення діаграми спрямованості антени (ДСА) приймальних антен на малих кутах піднесення	10 – 15	30	Реально, у всіх системахспоживачів
2	Управління ДСА, зменшує чутливість в напрямку джерела перешкод (*beamforming*-антенна)	20 – 25	До 100	Практично ефективнийпо одному постановнику завади, потрібно знання направлення на постано-вник завад
3	Управління ДСА, зменшує чутливість в напрямку джерела перешкод (*nullingng*-антенна)	до 80	До 100	Практично ефективнийпо де кільком постанов-ників завади, не потрібнознання направлення на постановник завад
4	Антенна решітка з поляризацією сигналу	10 – 15	До 50	Діє не в усіх умовах застосування
5	Поліпшення обробки сигналів у приймачі	до 20	5 – 10	Потрібні дослідження з можливими методами реалізації. Не можливо реалізувати в діючих приймачах GNSS
6	Комбінування приймача GNSS з INS	10 – 15	10 – 300	Вартість визначається рівнем INS і має тенденції до зниження
7	Використання двочастоних приймачів L1, L2	5	20 – 30	
8	Використання багато частотних приймачів	8	40 – 50	

Інформація в табл. 1 розкриває напрям по анті- *jamming* при поліпшенні апаратури споживачів, переваги та недоліки недоліки перераховані в примітках.

3.1.2 Beamforming-антени

Оцінюючи можливий виграш у стійкості апаратури споживачі GNSS до завад, найбільш перспективним методом є управління діаграмою спрямованості (ДС) приймальної антени (зменшення чутливості або встановлення "0" ДС в напрямку джерела завад), тобто просторова часова обробка сигналів (ПЧОС), яка реалізується в антенних адаптивних компенсаторах завад (ААКЗ). Перевага ПЧОС в наступному:

− виграш в завадостійкості може бути вельми істотним;

− не потрібне коригування самого приймача супутникової навігації.

Адаптивні компенсатори завад будуються на основі антенних решіток і адаптивних методах управління ДС.

Основні напрямки розробки ААКЗ це радіолокаційні системи та системи радіозв'язку, т. к. в основному вирішувалися завдання підвищення завадостійкого прийому по боковим пелюсткам.

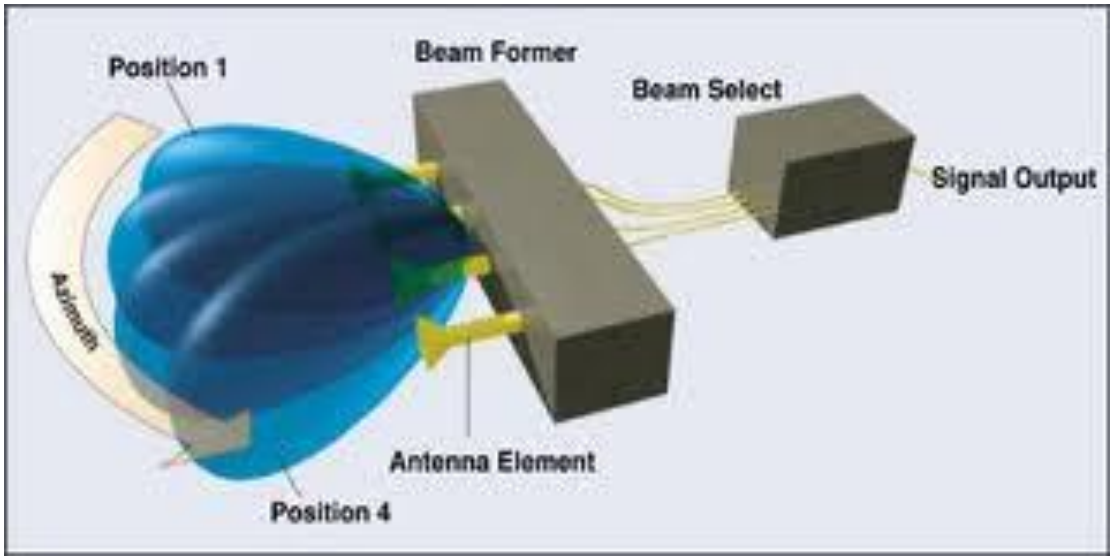


Рисунок 3.1 - Приклад beamforning-антени

Формування променя (від сл. *Beam*-промінь) в інтелектуальній антенній решітці використовує кілька окремих антен і відповідних сигнальних процесорів для створення бажаної діаграми випромінювання.

Основні переваги використання інтелектуальної системи активної антени походять від зменшення загальної потужності системи, зменшення перешкод у зв'язку, збільшення пропускної здатності системи та підвищення енергоефективності.

Найпростішою реалізацією є лінійна решітка щонайменше від 4 до 8 незалежних антен. Це дозволяє охопити загальне кутове покриття. Більш ефективний масив будується в матричній конфігурації. Два поширених підходи використовують або матрицю Батлера, або матрицю Бласса. Хоча технічні деталі виходять за рамки цієї статті, ми надаємо дуже короткий опис кожного: Батлер використовує комбінацію з 64 антен у діаграмі 8 на 8, зі зсувом розміщення на 45 градусів для реалізації фазових зрушень у передачі. сигнал. Матриця Blass також може бути реалізована з 64 антенами. Вони розташовані ортогонально та вздовж осі z.

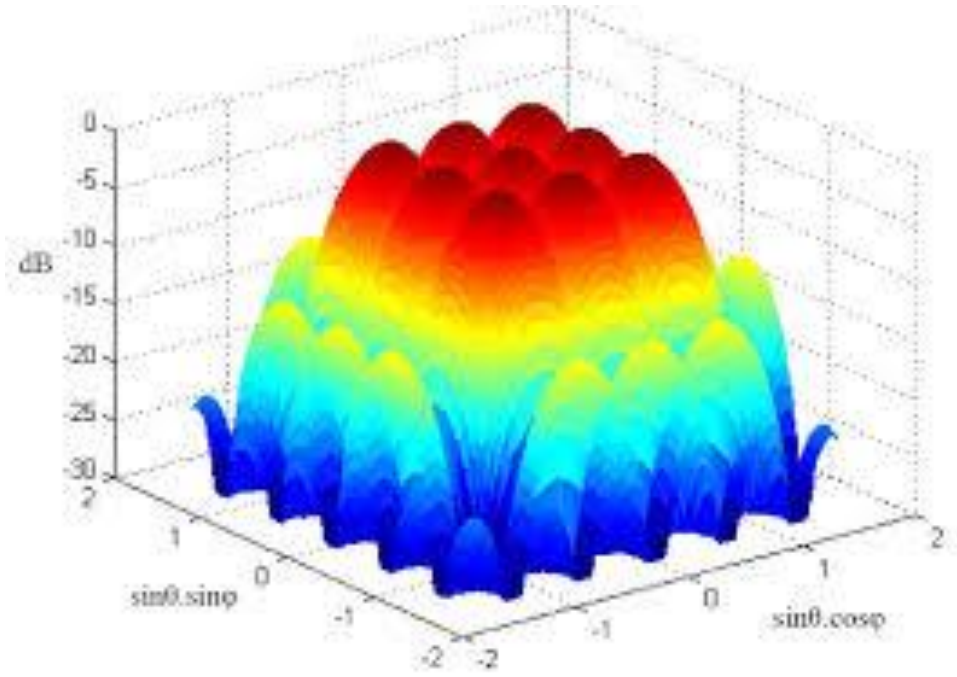


Рисунок 3.2 - Приклад антени Батлера з антенною решіткою 4x4

Для передачі алгоритми обробки сигналу використовуються для обчислення векторів формування променя шляхом одночасної активації однієї або кількох антен у решітці. Як випливає з назви, формування променя створює сигнал передачі з просторовою сигнатурою, щоб максимізувати прийом сигналу в приймачі. Якщо існує двосторонній зв'язок від приймача до передавача, це також може дозволити місцезнаходження та відстеження приймача. Це робиться шляхом конструктивного додавання фаз сигналів передачі в потрібному напрямку з одночасним обнуленням шаблонів, де є завади.

Більш складні антенні решітки є адаптивними, що дозволяє отримати набагато більшу можливу кількість діаграм спрямованості, які можна постійно змінювати. Однією з суттєвих переваг є те, що за допомогою складних алгоритмів оцінки напрямку прибуття і високошвидкісного процесора промінь передачі може ефективно спрямовуватися будь - якому напрямку.

Використовуючи цей метод формування променя, також можна звести нанівець будь-які заважаючі сигнали. Адаптивне формування променя також забезпечує схему передачі, яка може відстежувати рухомий об'єкт, щоб підтримувати постійну потужність сигналу для приймача.

Спираючись на цю концепцію, розширена версія матриць з комутацією променів використовує «Методи комбінування різноманітності» для покращення продуктивності в шумних або несправних каналах зв'язку. У найпростішому вигляді, використовуючи зворотний зв'язок із приймачем, можна контролювати відношення сигнал/шум переданого сигналу для кожного елемента антени в решітці. Через періодичні проміжки часу вибирається елемент із найкращим SNR. Комбінування різноманітності робить цей крок далі, миттєво оцінюючи кожен елемент і призначаючи зважене значення його SNR. Потім сигнальний процесор на передавачі екстраполює оптимальну схему променя та створює її за допомогою передачі із затримкою часу через вибрані елементи. Хоча це вимагає великих обчислень.

До недоліків beamforme*r*-антени можна віднести повільну збіжність LMS або RLS адаптивних алгоритмів, повільний перехідний процес, значне звуження

основного пелюстка ДС і можлива втрата сигналу від де яких супутників, а також необхідність апріорних даних про направлення на за- ваду і прийнятому сигналі, тому beamforme*r*-антени працюють в два етапи:

− оцінка напрямку (кута) на джерело завади, з використанням алгоритмів високого дозволу MUSIC або ESPRIT;

− за вимірюваним кутом обчислення вагових коефіцієнтів і формування ДС.

На жаль, максимальний коефіцієнт придушення завади у таких систем не перевищує 25 − 30 дБ (табл. 1). Однак розробка *beamformer*-антен ведеться в наш час з-за їх основної переваги – простота реалізації, можливість використання АР з великою апертурою, кроком між поодинокими елеме- нтами АР від λ/2 до 3λ/4 (збільшується коефіцієнт підсилення АР підвищується роздільна здатність по куту) і лінійними розмірами одиничного елемента АР від λ/2 та невисокою обчислювальною складністю.

3.1.3 Nulling-антени

Nulling-антени тісно пов’язані з beamforming-антенами за будовою та дещо за принципом роботи. Beamforming-антена зменшує коефіцієнт посилення сигналу перешкод і збільшує коефіцієнт посилення сигналу супут- никового зв'язку GNSS, тоді як nulling-антена зменшує коефіцієнт посилення в напрямку сигналу перешкод, але без додаткового посилення сигналу супутникового зв'язку GNSS.

На перший погляд beamforming-антена виконує ту ж саму функцію, та ще й підсилює сигнал у вибраному напрямку, та це не зовсім так. beamformer-антени не використовують можливості розв'язання рівняння Вінера-Хопфа, та переваги адаптивної обробки сигналів, яке передбачає, що вся інформація про джерела завад, а саме його кутове положення в просторі знаходиться в кореляційній матриці завади:

$$W = R^{-1}S; \quad (2)$$

де **W –** вектор вагових коефіцієнтів (розмірні-стю *N*);

$\mathbf{R}^{-1}$ – обернена кореляційна матриця завади (розмірністю $N \times N$);

S – вектор комплексних амплітуд корисного сигналу (розмірністю N).

Для обчислення вагового вектору за виразом необхідно провести операцію безпосереднього звернення кореляційної матриці. Однак на практиці кореляційна матриця невідома. Тому обчислюють максимально правдоподібну оцінку кореляційної матриці L часовими вибірками випадкових амплітуд вхідного процесу. Якщо ваговий вектор оцінюється за формулою (2), виникають дві проблеми. По-перше при $L<N$ (коротка вибірка) кореляційна матриця є виродженою і, отже, не має зворотної матриці, а при $L \geq N$ є погано обумовленої, де N – кількість елементів в АР, L – об'єм вибірки.

На основі рівняння (2) працює *nulling*-антенна, в якої формується нуль в ДС на джерело завади (Рис. 3.3).

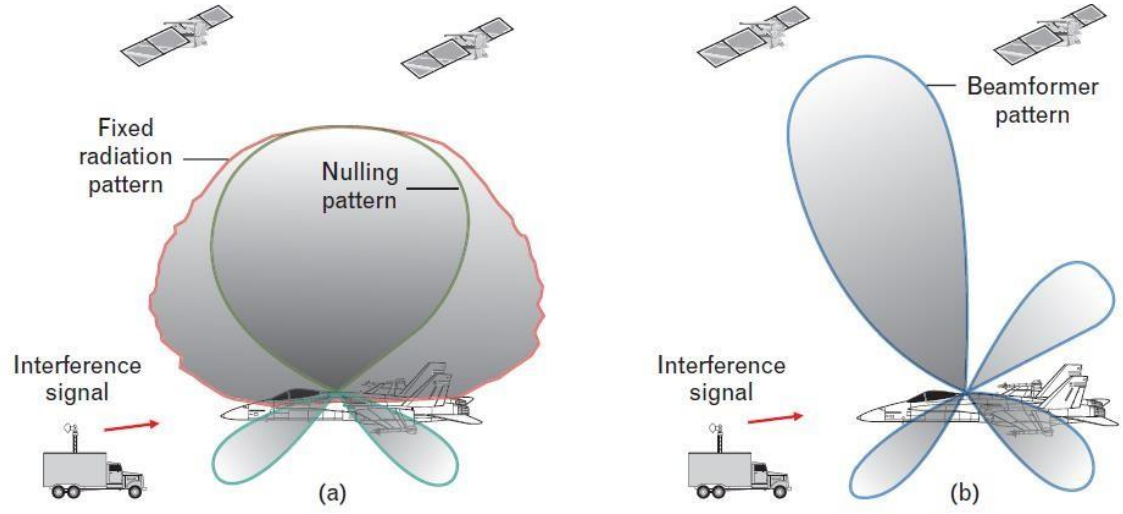


Рисунок 3.3. Принцип роботи nulling-антени і beamformer-антени.

Використовуючи вираз (2) надається можливість в отриманні простий реалізації обчислення вагового вектору, необхідно тільки обчислити оцінку оберненої кореляційної матриці завади $\mathbf{R}^{-1}$ тобто використовувати прямий метод обчислення обер- неної кореляційної матриці завади $\mathbf{R}^{-1}$ і знахо- дження оцінки вагового вектору **W**.

Прямі методи обчислення оберненої кореляційної матриці завади $\mathbf{R}^{-1}$ дають ряд важливих переваг:

– малий час для отримання оцінки вагового вектору;

– високий коефіцієнт придушення завади;

– відпадає необхідність у апріорних даних.

Таблиця 3.2 - Порівняння за основними параметрами beamformer і nulling антен в ААКЗ

Параметри ААКЗ	*beamformer*-антена	*nulling*-антена
коефіцієнт придушення завади	до 35 дБ	до 90 дБ
апріорні данні про просторове розташування джерела корисного сигналу	+	–
апріорні данні про просторове розташування джерела завади	+	–
апріорна інформація про корисний сигнал	+	–
аналогова реалізація	+	–
цифрова реалізація	+	+
крок АР	від λ/4 до λ	від λ/4 до λ/2
тип АР:		
лінійна	+	+
пласка	+	+
перехідний процес	+	–
рівень бічних пелюсток	-40 ÷ -20 дБ	-100 ÷ - 80 дБ
звуження основного пелюстка	+	–
підвищення коефіцієнта підсилення в напряму корисного сигналу	+	–

Проведений аналіз дав підстави виділити найбільш дієві методи забезпечення цілісності і доступності інформації GNSS при дії організованих завад серед котрих є застосування ААКЗ з використанням beamformer і nulling антен.

Серед beamformer і nulling антен найкращим є ААКЗ з nulling-антеною (табл.3.2). Тому актуальним на даний час є дослідження, розробка і впровадження ААКЗ на базі nulling-антен.

3.2 Анті-spoofing.

Методи анті-spoofing призначені для вичислення навмисних сигналів завад. Вони можуть визначатись за декількома способами:

– аналіз вхідної потужності;

– структурний аналіз потужності;

– оцінка сигнал/шум (**C/N_0**);

– слідкування за якостю сигналу (SQM);

– слідкування за часом;

Аналіз вхідної потужності - один із методів спуфінгу – спочатку заглушити приймач, а потім подати хибні сигнали. Користувачі повинні контролювати вхідну потужність, щоб виявити цей вид атаки, пов'язаний із збільшенням потужності, оскільки сигнали перешкод мають більш високу потужність. Це можна зробити, відстежуючи коефіцієнт підсилення модуля автоматичного регулювання підсилення.

Структурний аналіз потужності - цей метод використовує властивість циклостаціонарності сигналів GNSS, виявлення надмірного збільшення потужності структурованого сигналу (наприклад, коди розширення) в отриманому наборі вибірок. Отримані вибірки основної смуги частот спочатку фільтруються в межах смуги пропускання GNSS-сигналу, а потім множаться на їхню версію із затримкою для усунення ефекту Доплера.

В результаті множення циклостаціонарних складових спектр у результуючого сигналу стає лінійним. На наступному етапі спектри сигналу та шуму фільтруються гребневими фільтрами відповідної форми. Статистика тесту виявлення розраховується з урахуванням порівняння вихідних даних фільтра з пороговим значенням виявлення атаки.

Оцінка сигнал/шум (C/N_0) - Ця загальна метрика моніторингу GNSS-сигналів доступна у більшості комерційних приймачів. Верхній рівень

потужності GNSS-сигналу відомий для заданих тестових налаштувань. Для кожного приймача може бути визначено верхню межу значення C/N0. Аномально високе значення C/N0 може вказувати на атаку спуфінгову. Однак важливо відзначити, що сигнали глушення можуть впливати на ефективні значення C/N0, збільшуючи мінімальний рівень шуму.

Слідкування за якостю сигналу (SQM) - інтерференція між справжніми та хибними сигналами під час атак з перекриттям викликає спотворення форми піку кореляції. Моніторинг якості сигналу зосереджується на цьому моменті з метою виявлення будь-яких асиметричних, аномально різких або підвищених піків кореляції.

Метрики SQM спочатку були розроблені для моніторингу якості кореляції піків, оскільки це давало змогу ідентифікувати багатопроменеві сигнали. Ці метрики знайшли широке застосування у додатках, що потребують високого ступеня цілісності. Застосовуючи ці методи, розробники досягли великих успіхів при виявленні атак спуфінга.

Слідкування за часом - ця метрика виявляє помилкові сигнали від спуфінгового джерела з однією антеною на основі рішення про місцезнаходження приймача, що рухається. У сценарії спуфінгу з однією антеною всі підроблені PRN передаються з однієї антени. В результаті у всіх сигналів однакова затримка, яка пов'язана з відстанню між антеною спуфера і антеною/приймачем, що атакується. Зміна відстані між антенами спуфера і атакованого приймача створює змінне зміщення годинника приймача, яке можна використовувати для ідентифікації спуфінгової атаки.

3.3 Тестування блоку анті-spoofing на базі GNSS-приймача NovAtel OEM7 та симулятора Spirent GSS 7700.

У цьому тесті використовувався апаратний симулятор, який генерував два радіочастотні вихідні сигнали GPS L1 C/A у двох різних місцях. Моделювалися

справжній і хибний сигнали. Виходи RF output1 і RF output2 були призначені для справжніх та хибних сигналів, відповідно. Для цього тесту приймач був налаштований на відстеження лише GPS L1 C/A. Блок-схема сценарію представлена на рис. 3.4.

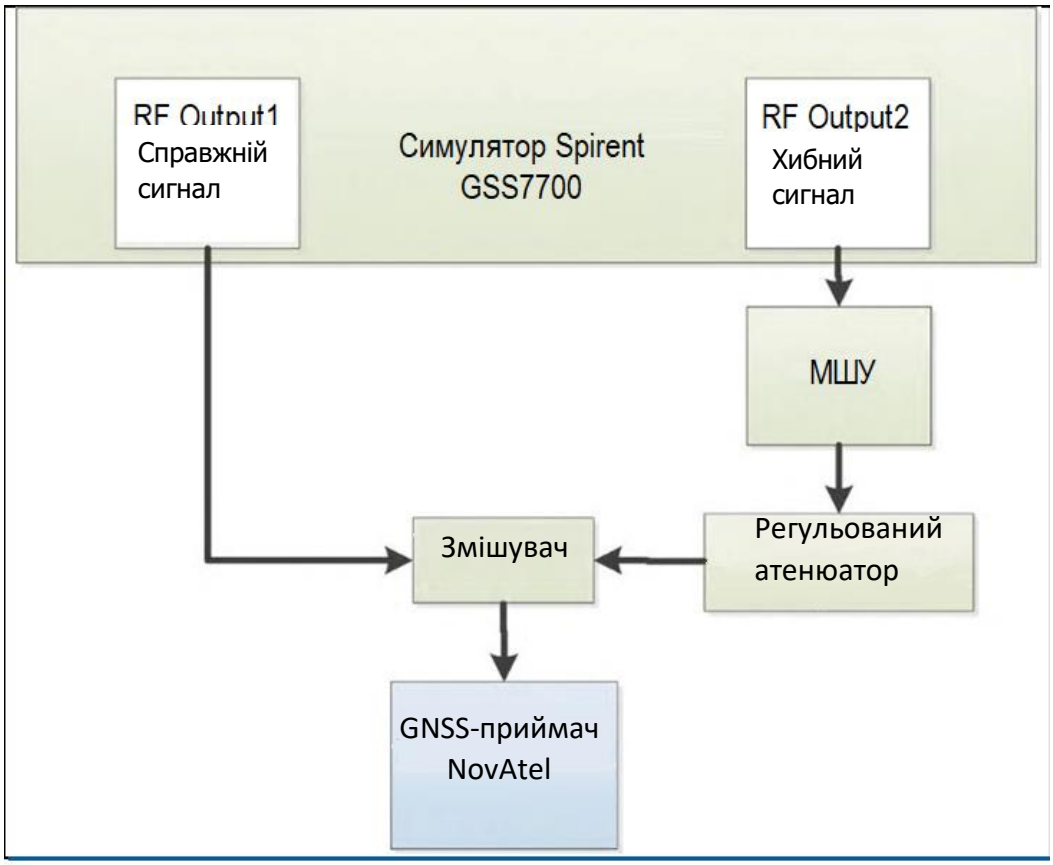


Рисунок 3.4 - Схема симулятора атаки GSS7700 та приймача NovAtel

Справжні сигнали безпосередньо підключалися до змішувача на RF вході приймача, в той час як спуфінгові сигнали, генеровані симулятором, проходили через малошумний підсилювач і регульований атенюатор, що регулює рівень потужності щодо справжнього. Обидва виходи RF генерували однакові PRN.

За допомогою цього симулятора користувач може регулювати зміщення тактової частоти та дрейф тактової частоти кожного RF-виходу, що дозволяє генерувати два синхронізованих сигнали, що відносяться до одного і того ж положення, з різним зсувом смуги та дрейфом. Зміщення смуги та дрейф для всіх PRN кожного RF-виходу однакові.

Це дозволило згенерувати атаки як без перекриття, так і з перекриттям. Для випадку без перекриття (заміна розташування) зміщення тактової частоти сигналів спуфінгу було встановлено на 6 мкс. Піки кореляції справжніх сигналів та сигналів спуфінгу були розділені приблизно 6 чіпами GPS L1 C/A і не перекривалися.

Зміщення годинника і дрейф сигналів спуфінгу були змінені, щоб імітувати атаку спуфінгу (атака з заміною часу і позиції). Для простоти порівняння статичні та динамічні позиції були віднесені до справжніх випадків та випадків спуфінгу відповідно. Підроблена позиція переміщалася по колу, а справжнє розташування було встановлено у центрі кола.

3.3.1 Тест з перекриттям

Цей тест включав атаку узгодженої потужності, при якій потужність сигналу спуфінга перевищувала потужність справжнього в межах двох дБ. Протягом перших 50 секунд приймач відстежував лише справжні сигнали. Потім до сценарію було додано спуфінгові сигнали з трохи більшою потужністю. Величина усунення тактового сигналу спуфінгу щодо справжніх сигналів було встановлено 6 мкс, дрейф якого — 0,007 мкс.

Піки кореляції спочатку не перекривалися. Однак дрейф годинника призвів до того, що всі заміни PRN пройшли через справжні сигнали і захопили корелятори відстеження приймача і, в кінцевому підсумку, підробили положення приймача. Нагадаємо, що в даному тесті приймач відстежував лише сигнали GPS L1 C/A.

На рис. 3.5 показана відносна вхідна потужність (щодо справжнього сигналу), відносне середнє C/N0 (щодо C/N0 на початку тесту) і кількість сигналів, що відстежуються для цього тесту. На рис. 3.5а показані результати виявлення спуфінгу у міру розвитку атаки.

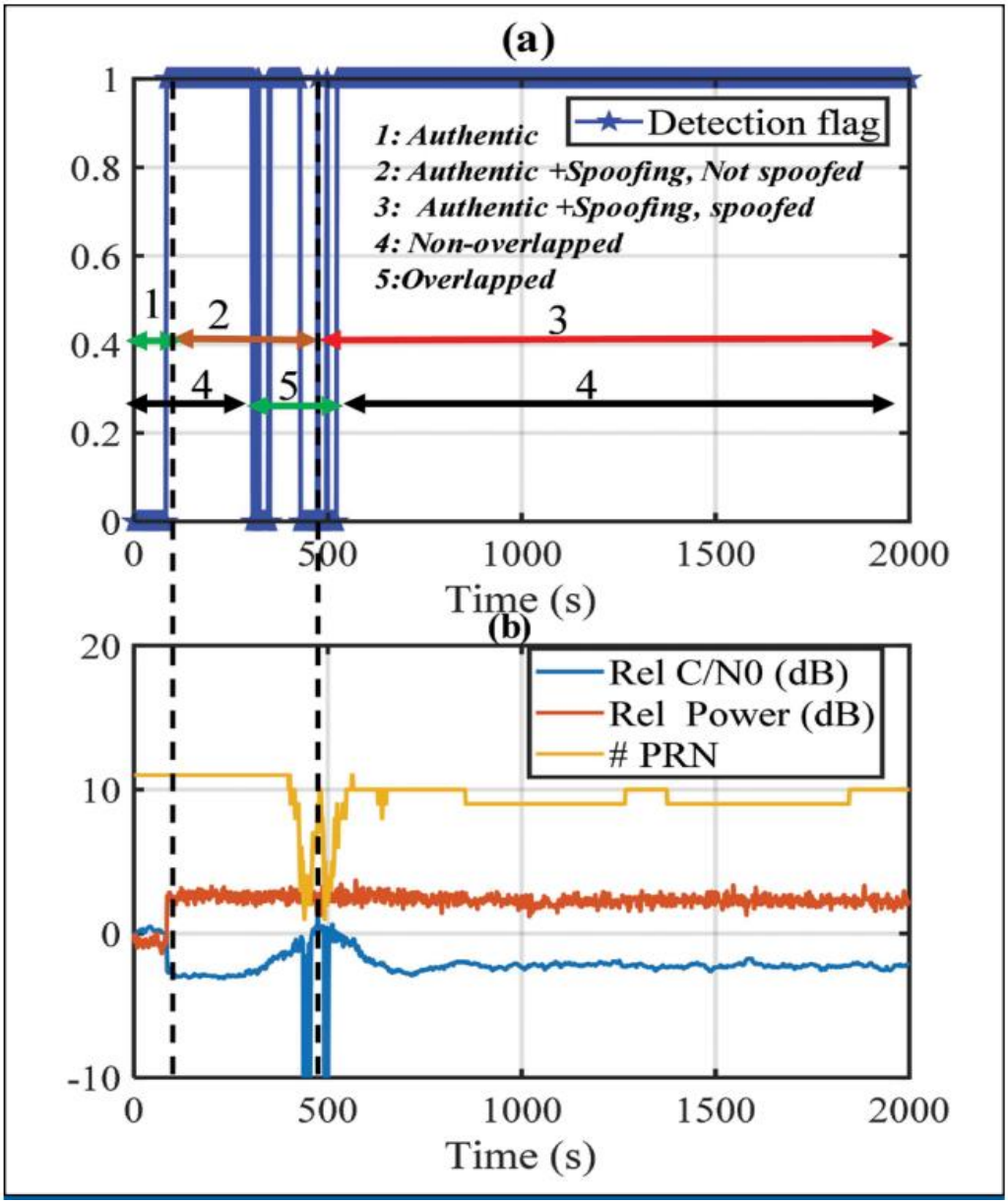


Рисунок 3.5 - Метрики виявлення та моніторингу для тесту за допомогою апаратного симулятора

Через 50 секунд після початку сценарію було запущено спуфінгову атаку. Атака виявляється відразу після появи сигналів спуфінга (50 с). На Рис. (a) графік займає значення 0, коли приймач відслідковує справжні сигнали, та значення 1 – виявляє спуфінгову атаку. Атака викликала стрибок вхідної потужності на 3 дБ та, як наслідок, зниження середнього відношення C/N0 (рис. 2b). Між 50 і 450 секунд спуфінгова атака діяла як широкосмуговий глушник. У

цей час приймач відстежував справжні сигнали, і обчислене положення було справжнім.

По відносним C/N0 і кількості PRN, що відстежуються, на Рис. 3.5 b видно, що справжні та хибні сигнали почали взаємодіяти на позначці часу 450-550 секунд. Під час інтерференції спуфінгу та справжнього сигналу (470–530 с) прапор виявлення вмикався та вимикався. У цей час відстеження сигналів приймачем було втрачено і кількість спостережень стала недостатньою для виявлення спуфінгу, хоча вона залишалася включеною до кінця тесту (Рис. 3.5 a).

На Рис. 3.6 показано просторове (схід, північ, висота) та планове (горизонтальне) положення приймача під час проведення тесту. Приблизно через 500 секунд після початку тесту позиція приймача була спотворена і він почав рухатися по колу. В результаті атака спуфінгу, під час якої потужність сигналу спуфінгу була вищою за потужність справжнього сигналу на кілька дБ, була надійно виявлена.

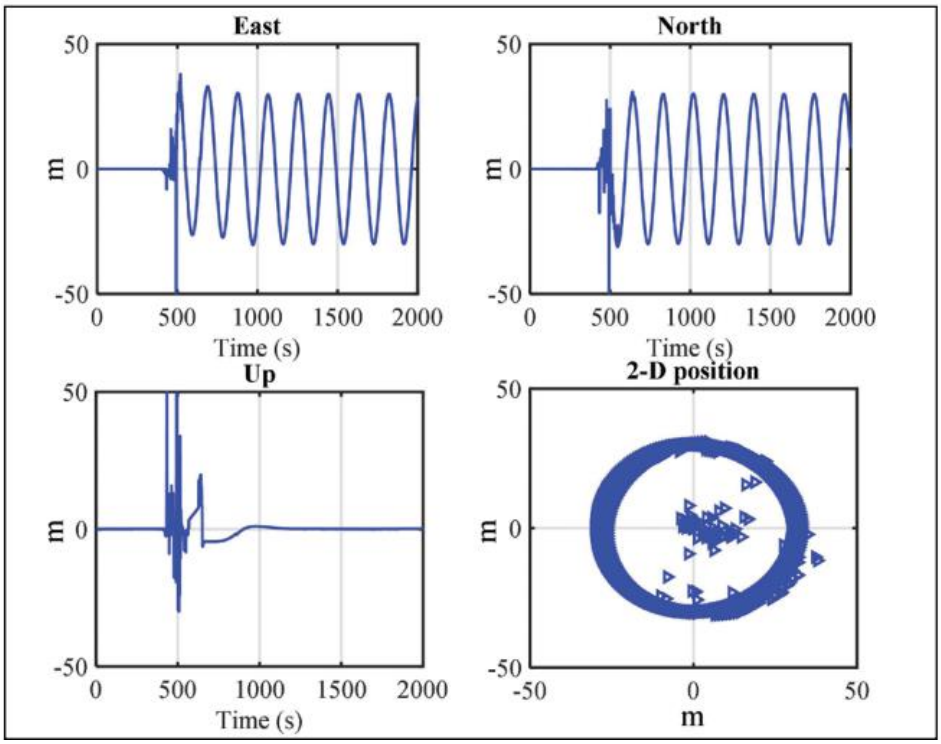


Рис. 3.6 - Результати позиціонування для тесту за допомогою апаратного симулятора

3.3.2 Спуфінг із змінною потужністю

У наступному тесті симулятор змусив приймач припинити відстеження справжніх сигналів. Цей варіант моделює сценарій потужного спуфера. Зміщення тактової частоти сигналів спуфінгу було встановлено на 6 мкс, а дрейф тактової частоти на 0. Це гарантує, що піки кореляції не перекриваються, так що єдиний спосіб атакувати приймач спочатку заглушити його, а потім атакувати спуфінгом.

На рис. 3.7c показані відносна вхідна потужність, відносне середнє C/N0 і кількість сигналів, що відстежуються під час тесту.

На рис. 3.7 b показаний прапор виявлення спуфінгу для цього сценарію.

Атака спуфінгу була виявлена, як тільки потужність спуфінгу почала впливати на рівень шуму приблизно через 500 секунд, до того, як позиція приймача була спотворена через 750 секунд, і тривала, поки приймач не перестав відстежувати сигнали спуфінгу.

Нагадаємо, що у цьому тесті використовувалися лише сигнали GPS L1 C/A. Приймач почав відстежувати справжні сигнали, тоді як потужність спуфінгу поступово збільшувалася приблизно на 30 дБ, а потім зменшувалась. Спуфінгова атака почала помітно впливати на відношення C/N0 і вхідну потужність через 500 секунд.

З 500 до 750 секунд потужність спуфінгу була збільшена приблизно на 20 дБ і зрештою замаскувала справжні сигнали. У цей час спуфер діяв як широкосмуговий глушник. Приблизно через 770 секунд приймач перестав відстежувати всі справжні PRN і незабаром почав відстежувати сигнали спуфінгу, тоді як потужність спуфінгу збільшувалася.

Як показано на рис. 3.7 a, позиція приймача змінилася приблизно через 780 секунд, коли він почав рухатися по колу з радіусом 100 м. Між 780 і 1250 секунд потужність спуфінгу збільшувалася і зменшувалася, але середнє значення C/N0

залишалося постійним. Ця картина тривала приблизно 1250 секунд, коли середнє значення C/N0 почало падати.

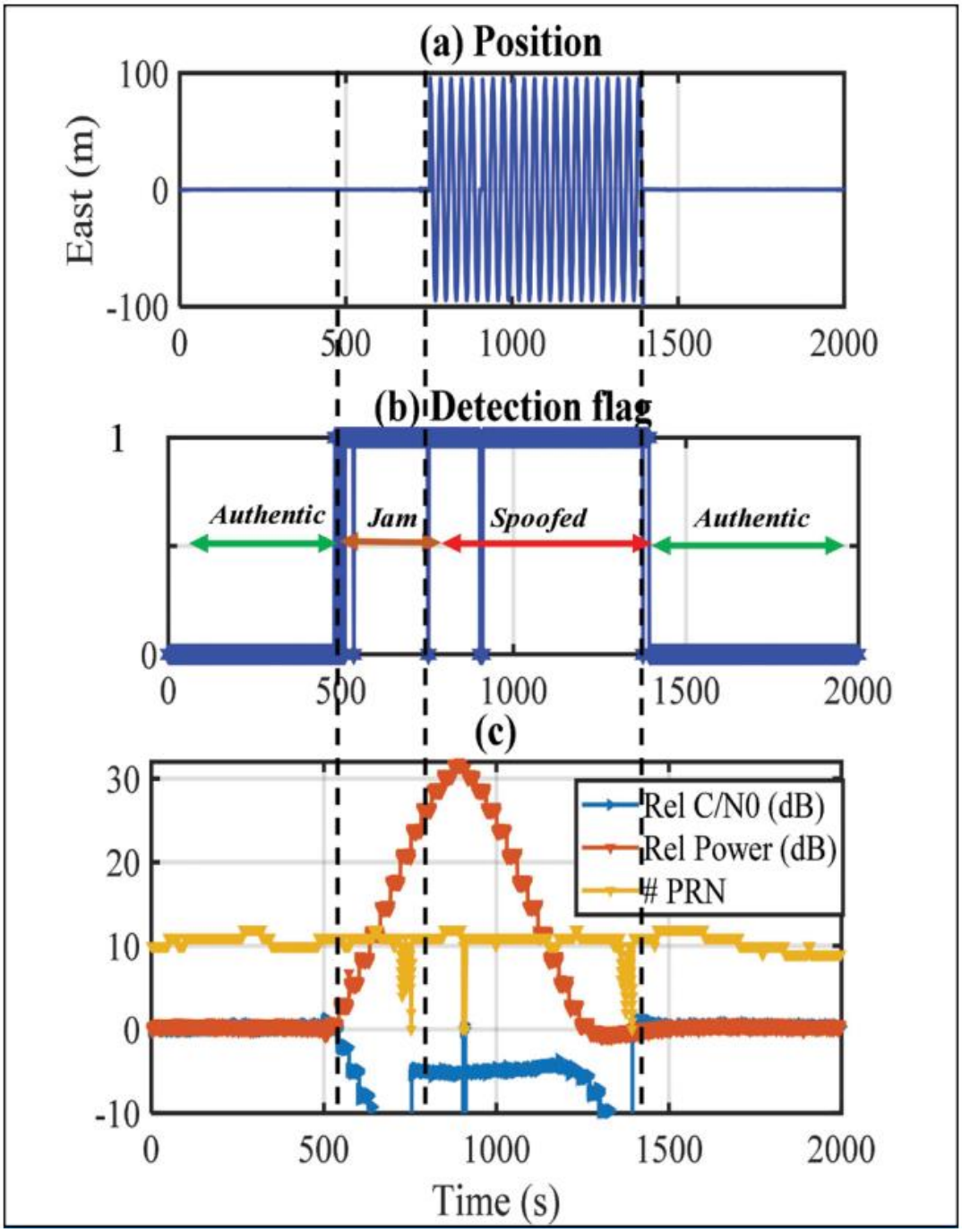


Рисунок 3.7 - Результати позиціонування після спуфінгу зі змінною потужністю

У цей момент потужність сигналу починала впливати на рівень шуму приймача. З 1250 до 1450 секунд приймач відстежував сигнали спуфінгу, тоді як потужність спуфінгу було зменшено. Приблизно через 1450 секунд приймач втратив хибні сигнали і знову почав відстежувати справжні сигнали.

3.3.3 Ретранслятори спуфінгу

У цьому розділі наведено результати атаки ретранслятора перешкод. Для цієї мети на даху будівлі були встановлені дві антени на відстані приблизно 30 м один від одного, які використовувалися як джерела справжніх і помилкових сигналів. Тестова конфігурація показано на рис. 5.

Антена із справжнім сигналом була безпосередньо підключена до RF-змішувача. Сигнали спуфінгу проходили через активний модуль, в якому відбувалася затримка та фільтр сигналів. Спуфінг використовує лише сигнали GPS L1/L2 та затримує їх приблизно на 150 мкс. Потім сигнали надходять на малошумний підсилювач 40 дБ, а потім на аттенюатор, що регулюється, після чого подаються на змішувач.

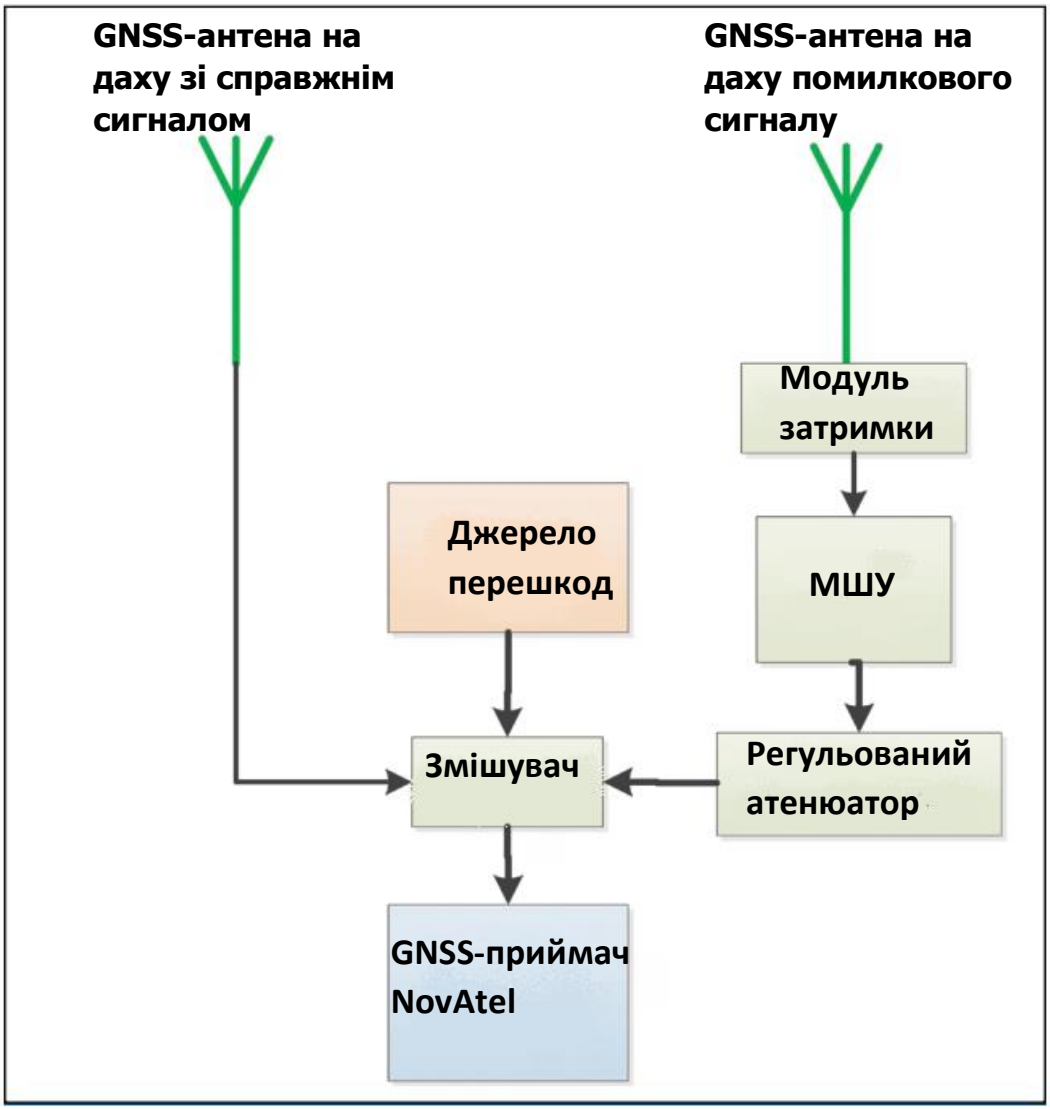


Рисунок 3.8 - Схема атаки із заміною репітера

До виходу змішувача було підключено два приймачі: один із конфігурацією GPS L1 C/A, а інший – мультичастотний та мультисистемний, що відстежує всі доступні сигнали із супутників GPS, ГЛОНАСС, Galileo та BeiDou. Цей варіант

був розроблений для перевірки можливостей мультисистемності та мультичастотності у відображенні атак спуфінга.

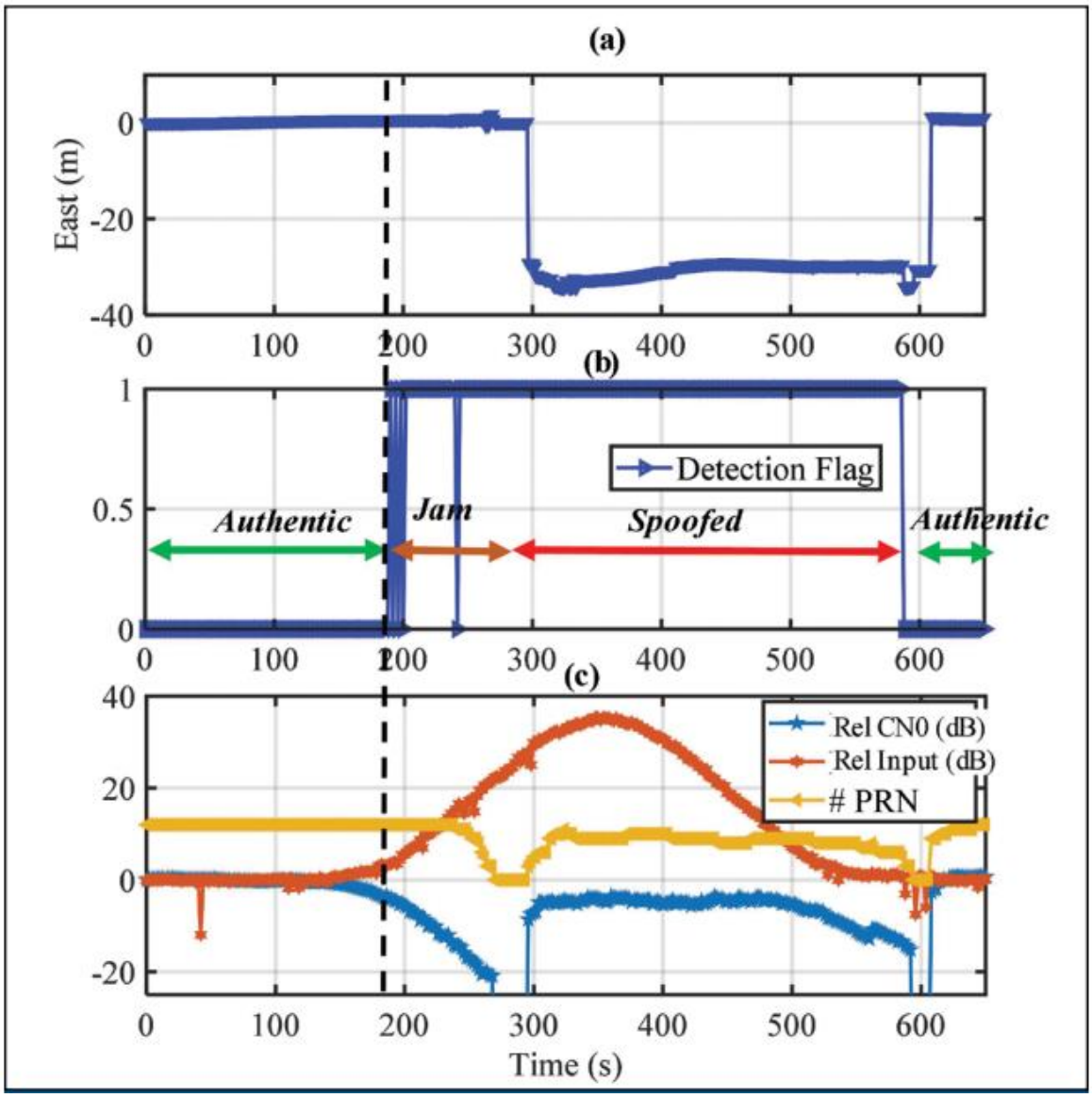


Рисунок 3.9 - Робота приймача GPS L1 C/A при атаці ретранслятора перешкод: a) усунення позиції у східному напрямку; b) метрики виявлення впливу спуфінгу; c) моніторинг атак у конфігурації репітера GPS L1 C/A

На рис. 3.9 показано результати роботи приймача GPS L1 C/A. Протягом приблизно 180 секунд на приймач подавалися справжні сигнали, а потім підключили спуфінг, поступово збільшуючи його потужність. Відносна вхідна потужність, відношення C/N0 і кількість сигналів GPS L1 C/A, що відстежуються, показані на рис. 3.9c.

Потужність сигналу спуфінгу поступово збільшувалася, що призвело до збільшення рівня шуму приблизно на 35 дБ, а потім зменшився шум. На рис. 6b

показаний прапор виявлення спуфінгу. Модуль виявлення спуфінгу розпізнав активність спуфінгу приблизно через 190 секунд, як тільки почав змінюватися мінімальний рівень шуму (до того, як положення приймача було спотворено), і залишався включеним до закінчення атаки приблизно протягом 600 секунд.

Приймач перестав відстежувати всі канали приблизно через 280 секунд і почав відстежувати сигнали спуфінга приблизно через 300 секунд. Під час відсутності сигналу (280-300 с), коли даних спостереження було недостатньо для вирішення навігаційного завдання, приймач безперервно видавав останній розрахунковий час та місцезнаходження.

Через 300 секунд положення приймача було спотворено (рис. 3.9а), доки через 600 секунд приймач не перестав відстежувати спуфінгові сигнали і почав відстежувати справжні сигнали, приблизно через 610 секунд. Результати зміщення у східному напрямку показано на рис. 6а.

3.3.4 Мультисистемний мультичастотний приймач

На рис. 3.10 показано результати аналогічного тесту з мультичастотним мультисистемним приймачем NovAtel OEM7. Потужність сигналу спуфінгу почала впливати на рівень шуму приймача приблизно через 120 секунд. Через 300 секунд приймач перестав відстежувати всі справжні сигнали GPS L1 C/A (також було заглушено інші сигнали в смузі частот GPS L1, включаючи Galileo E1), а мінімальний рівень шуму був збільшений на 20 дБ.

Під час атаки приймач постійно відстежував справжні сигнали інших частотах і сузір'їв, включаючи GPS L5 і Galileo E5. Таким чином, відстеження справжніх сигналів інших супутникових систем та частот спрацювало як перевірка цілісності та дозволило приймачеві заблокувати спуфінговісигнали.

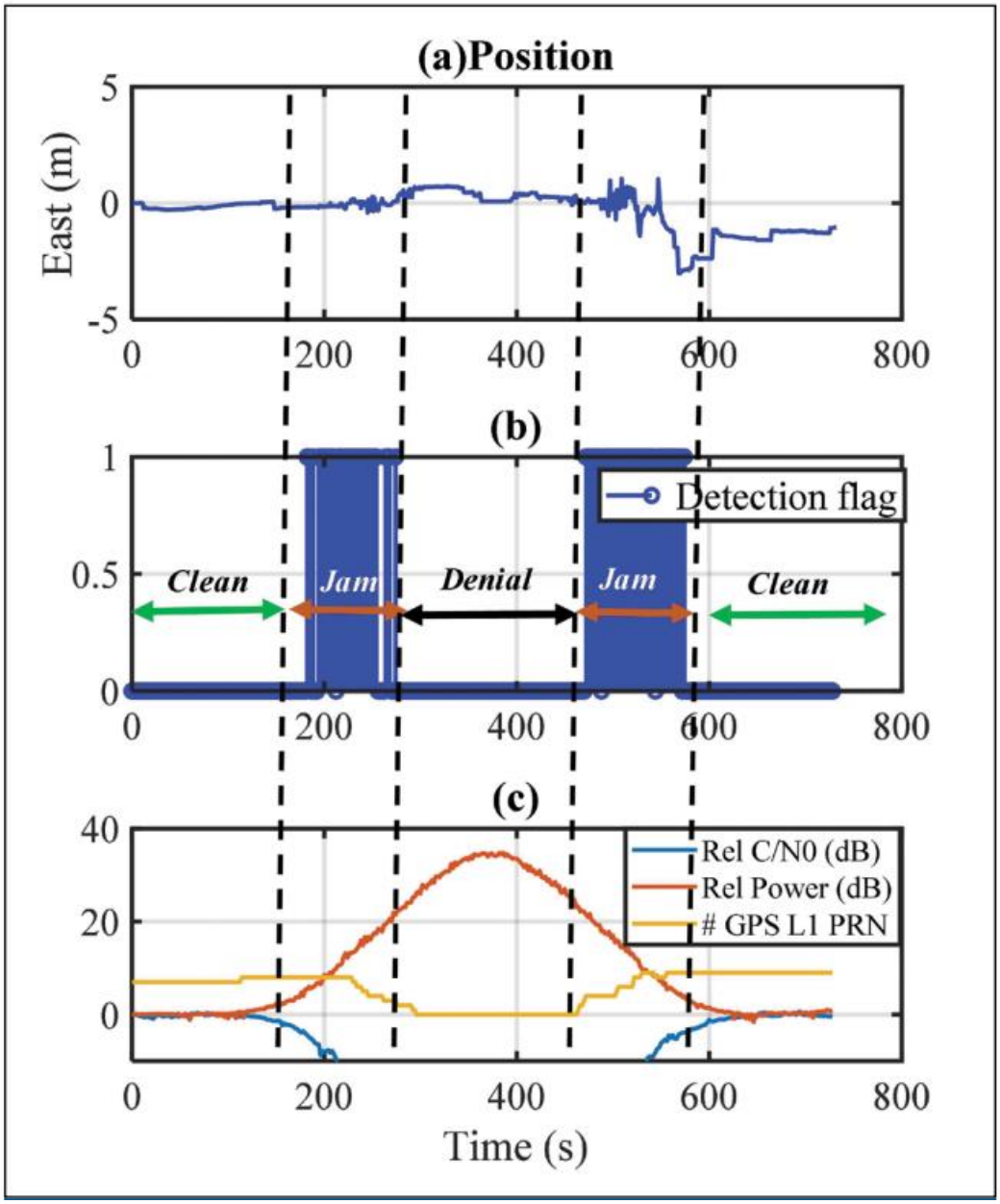


Рисунок 3.10 - Робота мультисистемного мультичастотного приймача при атаці ретранслятора перешкод: a) спотворення позиції у східному напрямку; b) метрики виявлення впливу спуфінгу; c) моніторинг атак з репітера приймача

Отже, як показано на рис. 3.10 c, під час спуфінгової атаки (300-500 с) вимірювань та розрахунків по GPS L1 C/A не проводилося, тобто атака викликала блокування сигналів GPS L1 C/A. Під час атаки положення приймача не було спотворене, і він забезпечував безперервне справжнє розв'язання навігаційного завдання (рис. 3.10a). На рис. 3.10b показано прапор виявлення атаки.

Блок виявлення активний протягом 180-280 секунд і 500-560 секунд, коли були доступні вимірювання GPS L1 C/A, і успішно виявляє атаку, оскільки доступні сигнали інших навігаційних систем та інших частот.

Відносна вхідна потужність та відношення C/N0 у порівнянні з справжнім сценарієм наведено на рис. 8c. Протягом перших 120 секунд потужність сигналу спуфінгу залишалася постійною і була на 20 дБ вище за потужність справжнього сигналу. Потім потужність поступово зменшувалась.

Приблизно через 280 секунд приймач перестав відстежувати хибні сигнали. Через 300 секунд приймач почав відстежувати справжні PRN. Прапор виявлення спуфінгу показано на рис. 8b. Атаку було успішно виявлено та відстежено протягом усього тесту.

На рис. 8a показано зміщення приймача під час атаки у східному напрямку. Видно, що позиція приймача спочатку була спотворена, потім приймач визначив справжню позицію коли через 300 секунд атака спуфінгу припинилася.

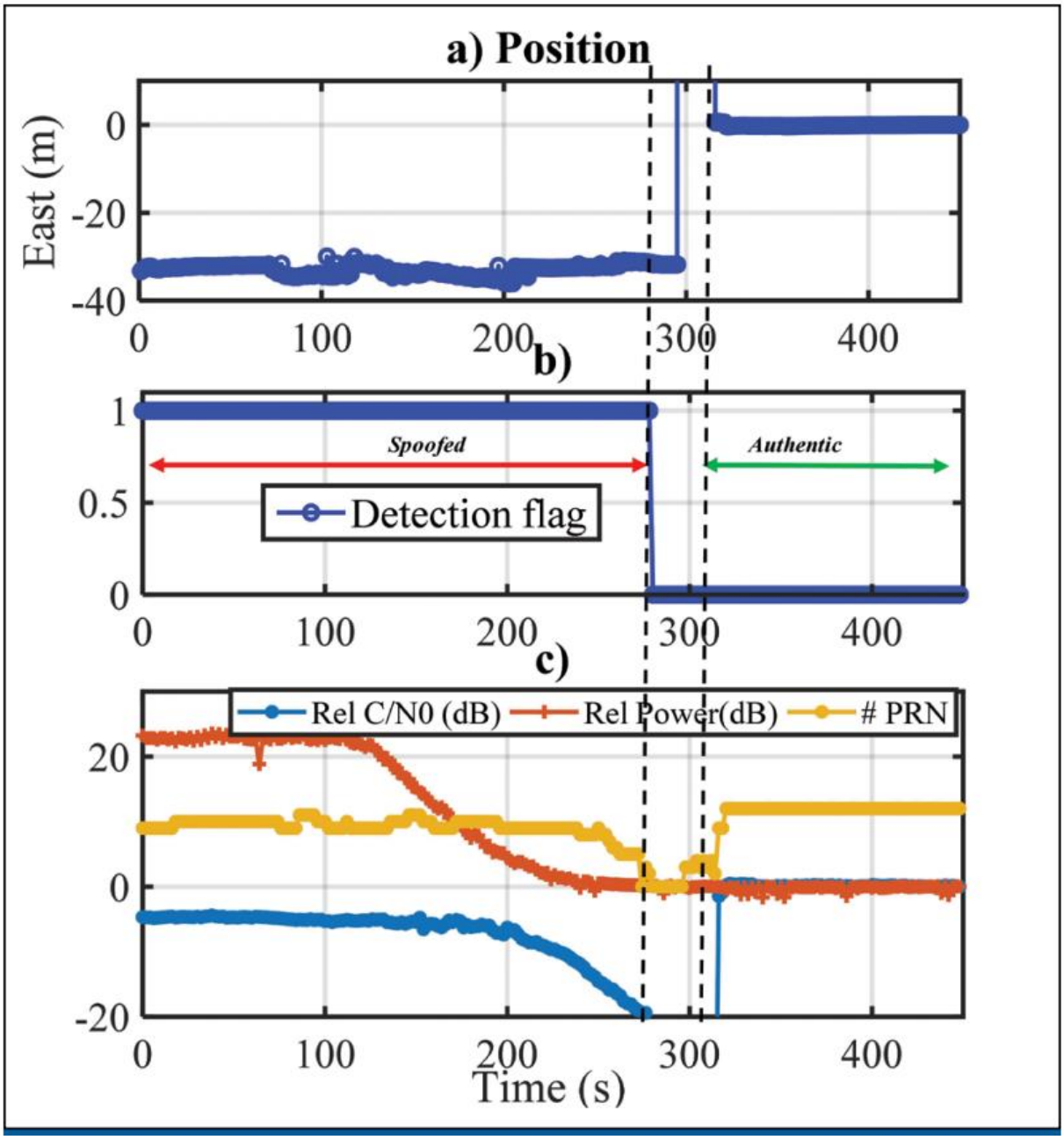


Рисунок 3.11 - Запуск приймача в конфігурації GPS L1 C/A під час атаки спуфінга: a) зміщення позиції приймача в східному напрямку; b) метрики виявлення спуфінгу; c) моніторинг атаки спуфінгу під час запуску приймача.

3.3.5 Результати обробки та висновки.

Результати обробки показують:

— на скільки ефективними є метрики виявлення впливу спуфінгу при ідентифікації спуфінгових сигналів з різними сценаріями;

— атака може бути ідентифікована відразу після появи спуфінгових сигналів і навіть до того, як буде підмінена позиція приймача;

- атаки на частоти L1 і L2 GPS з використанням різних конфігурацій приймача показали, що визначення положення та час мультичастотного і мультисистемного приймача несприйнятливе до атаки, тоді як положення приймача GPS L1 уразливе при дії спуфінгу. Проте в обох випадках блок виявлення зміг успішно ідентифікувати атаку.

Експериментальні результати в умовах перешкод, високої багатопроменеві, при статичних та кінематичних вимірах були використані для аналізу ймовірності помилкової тривоги блоку виявлення. Під час тестів за умов відсутності впливу спуфінгу хибних виявлень не спостерігалося.

Надійне та своєчасне виявлення спуфінгу – це перший крок до безпечної та ефективної протидії загрозам, будь то дії користувача або програма приймача.

РОЗДІЛ4. РЕАЛІЗАЦІЯ СИСТЕМИ ПОПЕРЕДЖЕННЯ БПЛА ВІД ЗАСОБІВ РЕБ

4.1 Система виявлення завад сигналів GNSS на платформі U-blox M9

Розділом вище ми провели аналіз та тестування роботи модуля детектування спуфінгової атаки на приймач NovAtel OEM7, дійшли до висновку що система працює і її потрібно впроваджувати.

Система виявлення завад працює також на приймачі фірми «U-blox» та моделі «NEO-M9N». NEO-M9N це стандартний GNSS приймач що працюэ на частотах L1, але він має свої переваги.

Приймач NEO-M9N GNSS оснащений стандартною прецизійною платформою GNSS u-blox M9 і забезпечує виняткову чутливість і час збору для всіх систем L1 GNSS. Приймачі u-blox M9 доступні в різних варіантах для використання в автомобільних і промислових додатках відстеження, таких як навігації, телематики та БПЛА.

Стандартна прецизійна GNSS-платформа u-blox M9, яка забезпечує метрову точність, є наступником добре відомий асортимент продукції u-blox M8.

Приймачі u-blox M9 підтримують одночасний прийом чотирьох GNSS. Велика кількість видимих супутників дозволяє приймачу вибирати найкращі сигнали. Це, зокрема, максимізує точність позиціонування у складних умовах, таких як глибокі міські каньйони.

Приймачі u-blox M9 виявляють події перешкод і спуфінгу та повідомляють про них хосту, що дозволяє системі реагувати на такі події. Розширені алгоритми фільтрації пом’якшують вплив радіо-завад і глушіння, що дозволяє виробу працювати належним чином.

Приймач також забезпечує вищу швидкість навігації та покращені функції безпеки порівняно попередні покоління u-blox GNSS.

Спуфінг – це процес локальної передачі підробленого сигналу GNSS, щоб запобігти використанню справжнього сигналу та створити помилкове місцезнаходження та/або час.

Алгоритм виявлення спуфінгу відстежує численні спостережувані параметри сигналу на наявність підозрілих змін, щоб визначити зовнішні маніпуляції. Прапорець у повідомленні UBX-NAV-STATUS (flags2 - spoofDetState) попереджає користувача про потенційний спуфінг.

Виявлення вважається успішним, коли спостерігається перехід сигналу від початково справжньої до підробленої версії. Отже, виявлення неможливо, якщо приймач запускається в умовах підробки.

Алгоритми виявлення покладаються на доступність сигналів від кількох сузір'їв GNSS – алгоритм виявлення не працює в режимі одного GNSS.

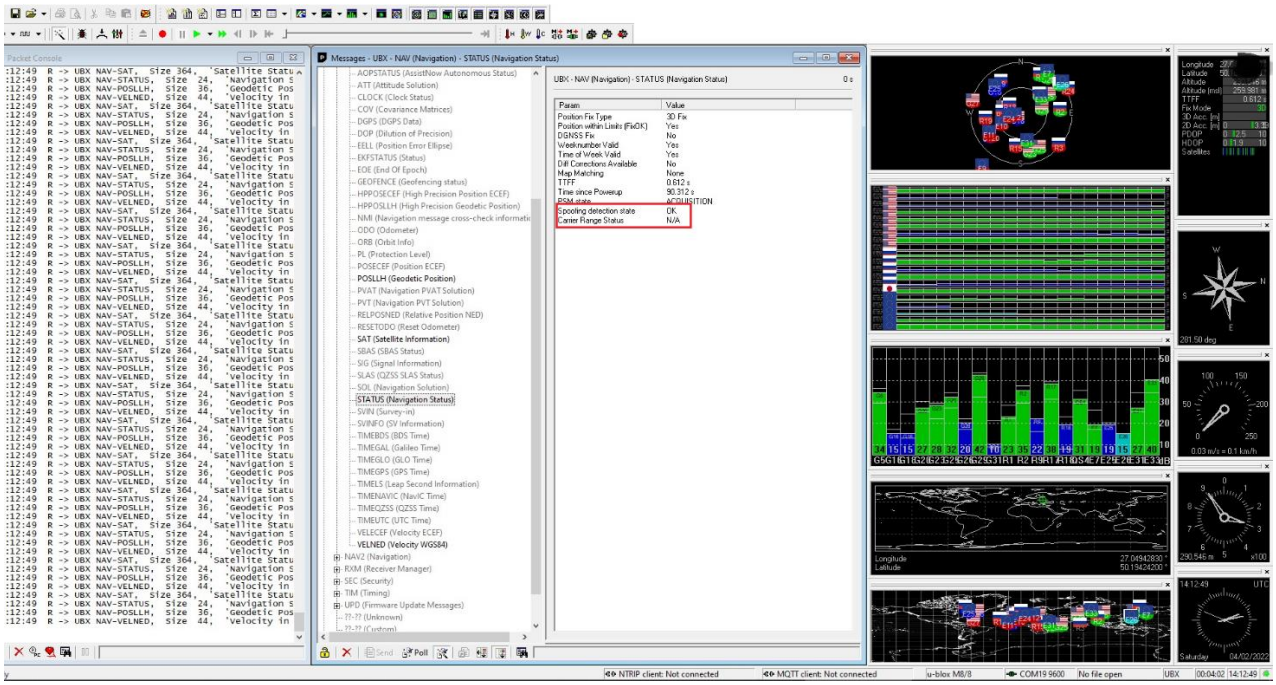


Рисунок 4.1 - Попередження про потенційний спуфінг в програмі U-Center

Приймач також реагує про виявлення джамінгу. Поле jamInd повідомлення UBX-MON-RF можна використовувати як індикатор лише для безперервних (вузькосмугових) перешкод. Інтерпретація значення залежить від програми. Необхідно запустити приймач у середовищі без перешкод, щоб визначити відповідний поріг для випадку без перешкод. Якщо значення значно

підвищується вище цього порогу, це вказує на те, що присутні безперервні хвильові завади. Ця функція моніторингу завжди ввімкнена.

Індикатор повідомляє про будь-які поточні виявлені вузькосмугові перешкоди (Рис. 4.2) для всіх поточних налаштованих смуг сигналу.

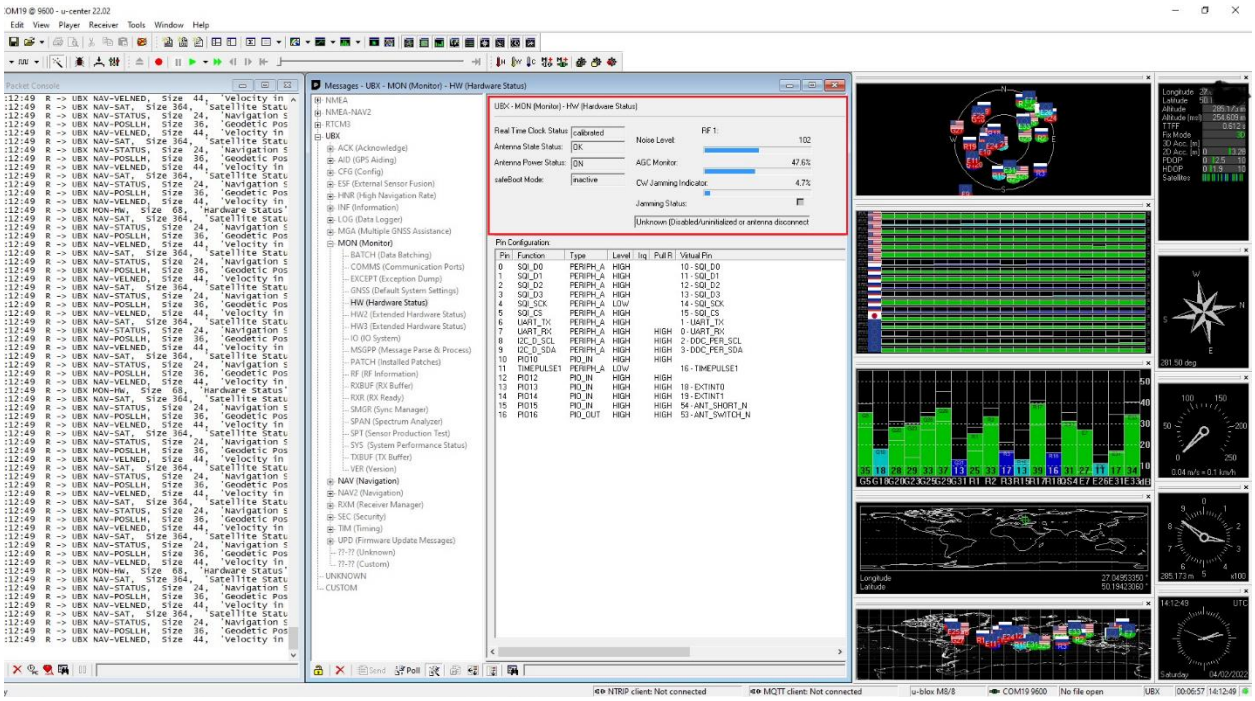


Рисунок 4.2 - Функція моніторингу jamming в U-Center

Цей моніторинг повідомляє, чи приймач виявив або підозрює перешкоди. Приймач контролює фоновий шум і шукає значні зміни. Зазвичай, якщо перешкод не виявлено, він повідомляє «OK». Якщо приймач виявляє, що рівень шуму перевищив попередньо встановлений поріг, приймач повідомляє "Попередження". Крім того, якщо поточного дійсного виправлення немає, приймач повідомляє «Критичний».

За замовчуванням монітор вимкнено. Монітор увімкнеться налаштуванням елемента конфігурації CFG-ITFM-ENABLE. У цьому повідомленні також можна вказати порогові значення, за яких повідомляються про широкосмугові та CW перешкоди. Ці порогові значення слід інтерпретувати як рівень дБ вище "нормального". Також можна вказати, чи очікує приймач активну чи пасивну антену.

Алгоритм моніторингу ґрунтується на порівнянні поточного виміряного спектру з еталонним, з якого було отримано хороше виправлення. Таким чином, монітор працюватиме лише тоді, коли приймач отримав принаймні одне (хороше) перше виправлення, і повідомлятиме «Невідомо» до цього часу.

4.2 Впровадження системи попередження в програмне забезпечення для виконання польотів

Осноновним програмним забезпеченням для виконання польотів БПЛА вже більше як десять років є MissionPlanner. MissionPlanner є вагомою частиною пакету програмного забезпечення ArduPilot. ArduPilot спочатку був розроблений любителями для керування моделями літальних апаратів і марсоходів і перетворився на повнофункціональний і надійний автопілот, який використовується промисловістю, дослідницькими організаціями та аматорами.

Основною перевагою цього програмного забезпечення є його відкритий код, тому всі організації використовують цей софт для інтеграціїіпрограмного забезпечення під свої наративи.

Впровадження системи попередження завад на мою думку важливе питання для вирішення проблем навігації. Для того щоб інтегрувати дані з U-blox, та вивести його на дисплеї MissionPlanner для інформування зовнішнього пілота. Ідея полягає в тому, щоб декодувати повідомлення UBX-MON (Monitor)-HW(Hardware status) в ArduPilot та передвати це через MavLink в MissionPlanner для відображення Jamming Indicator. Теж саме робимо з Spoofing detection state бітом в повідомленні UBX – NAV(Navigation) –STATUS (Navigation Status). В результаті ми отримуємо індикацію в головному вікні моніторингу за польотом Рис. 4.3.

Рисунок 4.3 - Spoofing/Jamming indicator в програмному забезпеченіі MissionPlanner

Для перевірки працездатності даної системи попередження використовували глушник GNSS частот L1 та L2 невеликої потужності.

Рисунок 4.4 - Глушник частот L1 та L2.

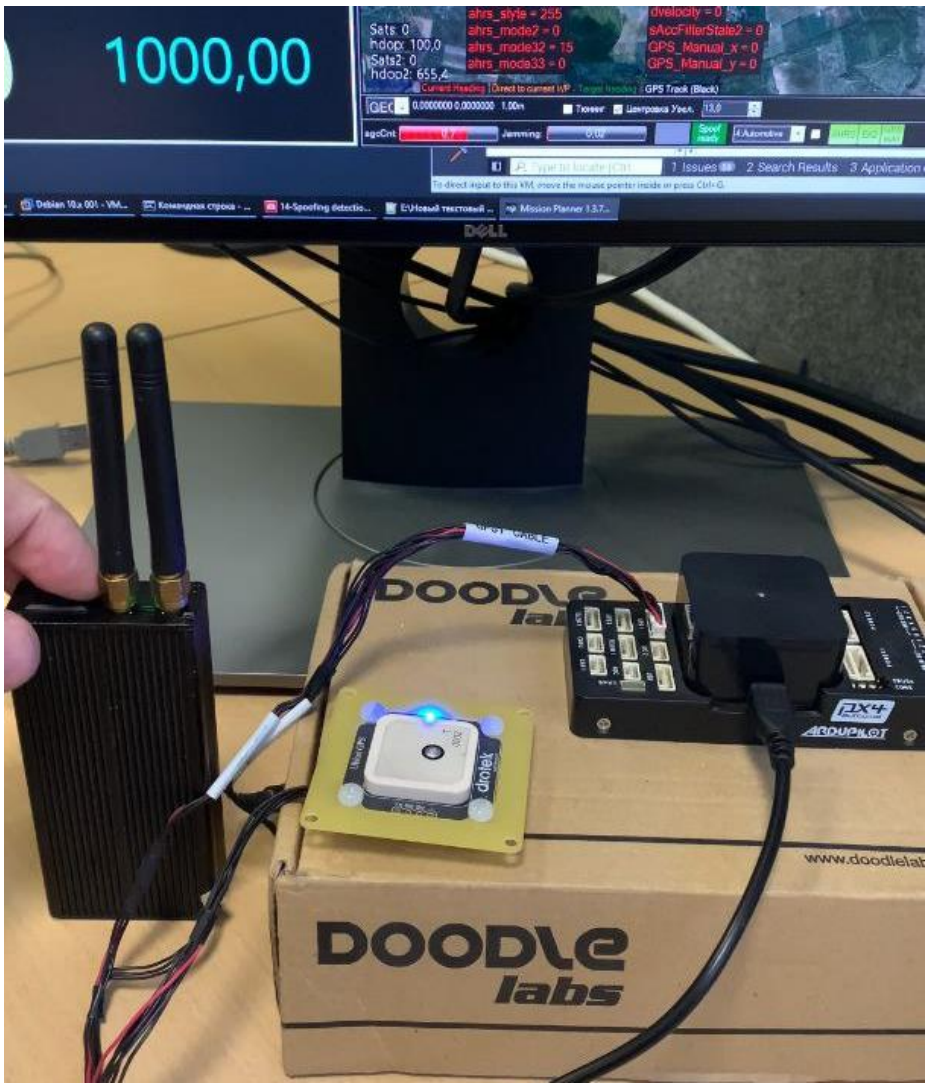


Рисунок 4.5 - Апаратна частина для перевірки попереджувальної системи.

На Рис.4.5 зображено конфігурацію для перевірки працездатності попереджувальної системи, вона складається з:

– Автопілот PixHawk CUBE;
– GNSS приймач U-Blox NEO-M9N;
– GNSS глушник частот L1 та L2 малої потужності.

На Рис. 4.6 бачимо, що індикатор AgcCnt змінюється на 1, що означає виявлення системою сигналів завади, що генерується глушилкою.

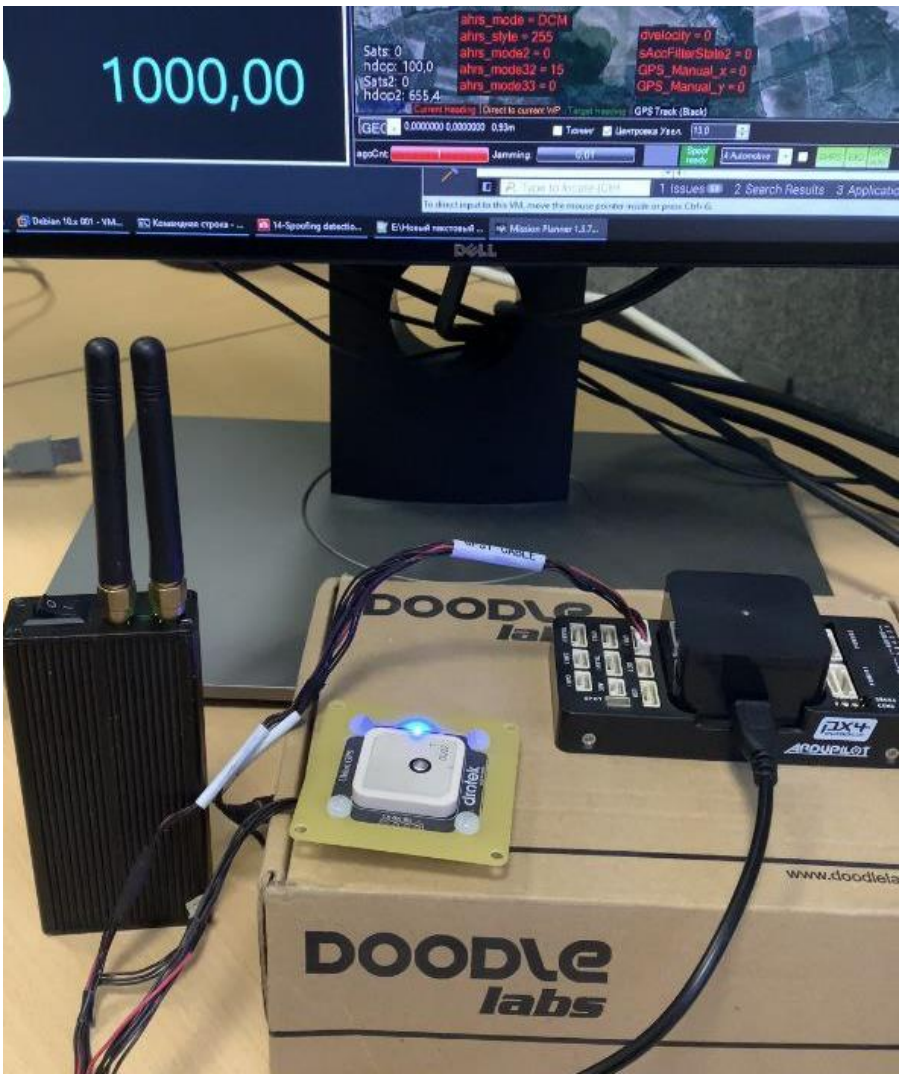


Рисунок 4.6 - Індикація попереджувальної системи з увімкненим спуфером

Далі уже є 2 варіанта розвитку подій. Перший – це залишити за оператором вирішення реакції на ту чи іншу заваду. Другий – це розробка алгоритму автоматичної реакції на певні сигнали попередження. Для цього потрібно провести дослідження, які завади стають критичними, та як БПЛА краще реагувати в тій чи іншій ситуації.

Висновок: на даний момент, основним вирішенням завдання навігації в умовах широкого спектру перешкод, це вимкнення GNSS приймача, коли зовнішній пілот побачив хоча б якісь підозри на створення примусової завади. Процедуру відключення приймача можливо реалізувати як в ручному режимі, так і в автоматі. В цьому розділі розроблено та реалізовану систему попередження GNSS в програмному забезпеченні виконанні польотів.

РОЗДІЛ 5. АВТОМАТИЗОВАНА ОБРОБКА АЕРОНАВІГАЦІЙНИХ ДАНИХ ВЕЛИКОЇ РОЗМІРНОСТІ

Автоматизована обробка даних є типовою задачею що вирішується сучасними аеронавігаційними системами. Обробка аеронавігаційних даних забезпечується як на борту у певних блоках авіоніки так і у наземних обчислювальних комплексах. Навігаційні параметри у сучасних системах вимірюються за допомогою значної кількості різних сенсорів, що забезпечують створення архіву даних, обробка яких потребує застосування спеціалізованих алгоритмів статистичної обробки. Кожен сенсор виконує вимірювання з певною величиною похибки, дію якої не можна виключили, проте її можна зменшити до прийнятного рівня. Отже сумісна обробка даних у аеронавігаційній системі виконується з врахуванням дії похибок кожного з сенсорів. Для цього використовують довірчі інтервали, що гарантують знаходження певного інтервалу у проміжку з певною ймовірністю. Найбільш застосовуваними довірчими інтервалами є подвійне середньоквадратичне значення, що забезпечує 95% локалізації виміряних значень, виходячи з припущення про нормальний закон розподілу похибок.

Кожен блок авіоніки у своїй структурі більш схожий до архітектури персонального комп’ютера з відповідними елементами: процесор, пам'ять, аналого-цифрові /цифро-аналогові перетворювачі, що дозволяє виконувати обробку виміряних даних на програмному рівні. Дані сенсорів переводяться до цифрового вигляду за допомогою дискретизації аналогових значень. Результати вимірювань у цифровому вигляді зберігаються у відповідних регістрах, змінних, матрицях чи архівах даних.

Визначення точного місцеположення повітряного корабля (ПК) є однією з найважливіших задач цивільної авіації. Зростаючі обсяги авіаперевезень вимагають постійного перегляду норм ешелонування для задоволення росту потреб авіаційного транспорту. Норми ешелонування ПК визначають максимально допустимі межі розділення ПК у просторі у вертикальній площині,

боковому та повздовжньому відхиленнях. Єдиним можливим шляхом вирішенням питання перевантаженості повітряного простору є збільшення пропускної здатності певної частини повітряного простору за рахунок зменшення безпечних відстаней між ПК. На практиці це реалізується шляхом введення більш точних вимог до визначення місцеположення ПК у просторі. Введення більш точних вимог до позиціонування ПК можливе лише за умови наявності відповідних систем здатних задовільнити їх. Функціонування систем позиціонування ПК цивільної авіації забезпечується полем аеронавігаційних сигналів, що створюється у просторі різними системами.

У якості прикладу обробки даних великої розмірності розглянемо траєкторію руху літального апарату та виконаємо її розрахунок за допомогою програмного забезпечення MATLAB.

5.1. Вхідні дані

Сучасний літак цивільної авіації обладнаний цілою групою різноманітних датчиків, що забезпечують визначення координат місцеположення ПК у просторі. Відповідно до концепції автоматичного залежного спостереження (ADS-B) користувачі повітряного простору повинні періодично повідомляти своє місцеположення у просторі в автоматичному режимі. Найбільш поширеним бортовим обладнанням ADS-B є літаковий відповідач режиму 1090ES. Літаковий відповідач виконує функції автоматичного генерування цифрових повідомлень відповідно до налаштувань системи (стандартні налаштування забезпечує випромінювання сигналу з частотою у 1 Гц) та виконує їх випромінювання через всеспрямовоні антені системи [6, 7]. Поширене цифрове повідомлення містить ідентифікацію літака, координати місцеположення, барометричну висоту та інші дані. Координати ПК отримуються з обчислювальної системи літаководіння після вибору оптимальної системи позиціонування для певного повітряного простору виходячи з точності, що забезпечується системою та специфікаційних вимог які діють у повітряному просторі де знаходиться літак.

Наземна мережа програмно керованих приймачів приймає і декодує дані передані за концепцією ADS-B. Зокрема, ідентифікаційний код літака з координатами місцеположення та барометричною висотою архівується у глобальних базах даних [8, 9]. Зокрема, обчислювальний кластери компаній Flightradar24 та Flightaware забезпечує одночасну обробку даних від більше ніж 30 тис програмно-керованих приймачів [10] сигналів ADS-B розміщених по всій планеті (рис. 5.1).

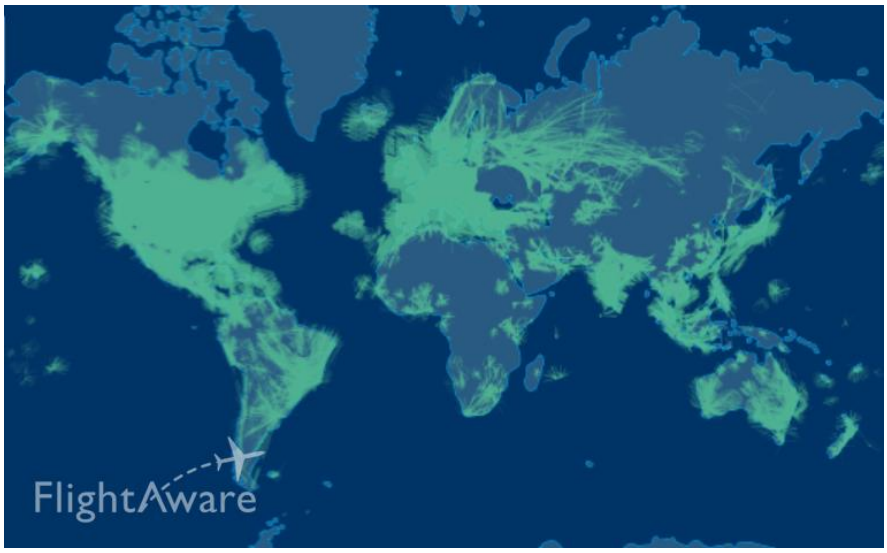


Рисунок 5.1 - Мапа глобального трафіку

Доступ до глобальних баз даних траєкторної інформації є відкритим і забезпечується на комерційній основі. Програмно керований інтерфейс дозволяє отримати будь-який сегмент траєкторних даних для подальшого аналізу.

У якості вхідних даних я використаю дані траєкторії польоту ALL146/ AA146 (American Airlines 146), що забезпечуються авіакомпанією American Airlines зі сполученням NEW YORK (JFK) та TEL AVIV, ISRAEL (TLV). Дата вильоту 11 листопада 2022 о 11;47 PM (EST). Дата посадки 12 листопада о 05:35AM (IST). Політ затримався на 35 хв від запланованого часу посадки. Політ виконувався на Boeing 777-200 (B772).

У таблиці 5.1 наведено перші та останні 15 рядків даних траєкторії польоту.

Таблиця 5 .1 - Траєкторні дані рейсу ALL146 від 11 листопада 2022

Час (EEST)	**Широта**	**Довгота**	**Курс**	**Швидкість (kts)**	**Швидкість (mph)**	**Висота (фут)**
Sat 12:14:21 AM	40.6233	-73.7850	↙ 213°	175	201	800
Sat 12:14:37 AM	40.6138	-73.7935	↙ 215°	159	183	1,900
Sat 12:14:53 AM	40.6046	-73.8019	↙ 214°	161	185	2,425
Sat 12:15:09 AM	40.5918	-73.8070	↓ 179°	180	207	2,725
Sat 12:15:25 AM	40.5788	-73.8008	↘ 144°	223	257	2,850
Sat 12:15:41 AM	40.5680	-73.7824	↘ 115°	255	293	3,325
Sat 12:15:59 AM	40.5650	-73.7498	→ 83°	298	343	3,900
Sat 12:16:16 AM	40.5724	-73.7222	↗ 61°	320	368	4,475
Sat 12:16:33 AM	40.5889	-73.6975	↗ 39°	334	384	5,050
Sat 12:16:52 AM	40.6118	-73.6796	↗ 27°	335	386	5,875
Sat 12:17:22 AM	40.6551	-73.6510	↗ 26°	337	388	7,025
Sat 12:17:52 AM	40.6990	-73.6213	↗ 28°	340	391	8,200

Продовження таблиці 5.1

Sat 12:18:22 AM	40.7394	-73.5941	↗ 27°	345	397	9,300
Sat 12:19:07 AM	40.8045	-73.5486	↗ 29°	353	406	10,875
Sat 12:19:37 AM	40.8494	-73.5164	↗ 28°	386	444	11,175
…						
Sat 10:22:41 AM	32.1625	34.5779	↘ 122°	225	259	4,950
Sat 10:23:11 AM	32.1473	34.6084	↘ 121°	225	259	4,400
Sat 10:23:38 AM	32.1328	34.6384	↘ 120°	225	259	3,675
Sat 10:23:54 AM	32.1244	34.6547	↘ 122°	221	254	3,350
Sat 10:24:10 AM	32.1164	34.6699	↘ 122°	202	232	3,200
Sat 10:24:45 AM	32.1026	34.6965	↘ 122°	180	207	3,075
Sat 10:25:46 AM	32.1010	34.6996	↘ 122°	180	207	3,360
Sat 10:26:02 AM	32.0744	34.7509	↘ 121°	179	206	2,200
Sat 10:26:19 AM	32.0673	34.7647	↘ 121°	177	204	1,950
Sat 10:26:35 AM	32.0604	34.7779	↘ 122°	172	198	1,675

Продовження таблиці 5.1

Sat 10:26:35 AM	32.0539	34.7903	↘ 121°	160	184	1,450
Sat 10:26:52 AM	32.0478	34.8022	↘ 121°	143	165	1,225
Sat 10:26:57 AM	32.0462	34.8051	↘ 122°	139	160	1,385
Sat 10:28:12 AM	32.0212	34.8535	↘ 121°	142	163	275
Sat 10:28:28 AM	32.0153	34.8649	↘ 122°	143	165	50

5.2. Візуалізація траєкторних даних у програмному забезпечені

Виконаємо імпорт траєкторних даних рейсу ALL146 від 11 листопада 2022 у програмне забезпечення MATLAB [11]. Результати візуалізації даних траєкторії польоту наведені на рис.5.2., а вертикальний профіль представлено на рис. 5.3.

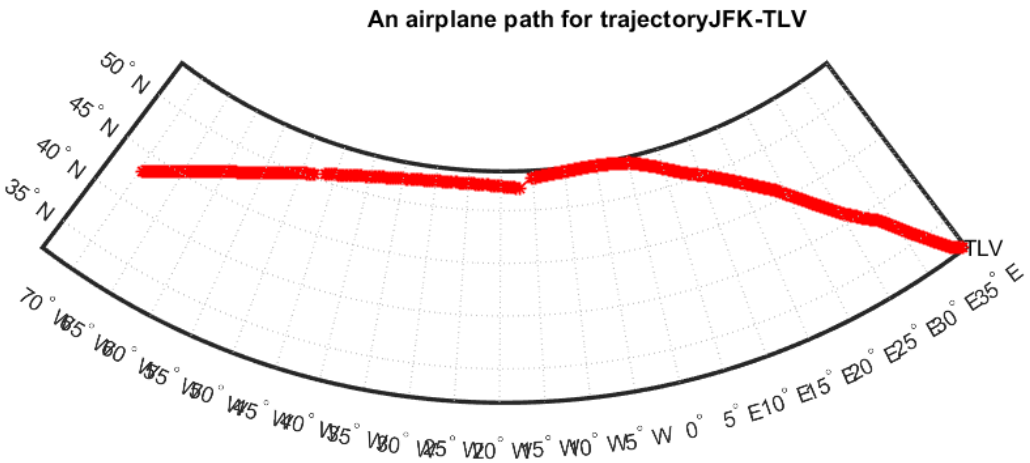


Рисунок 5.2 – Траєкторія руху рейсу ALL146 від 11 листопада 2022

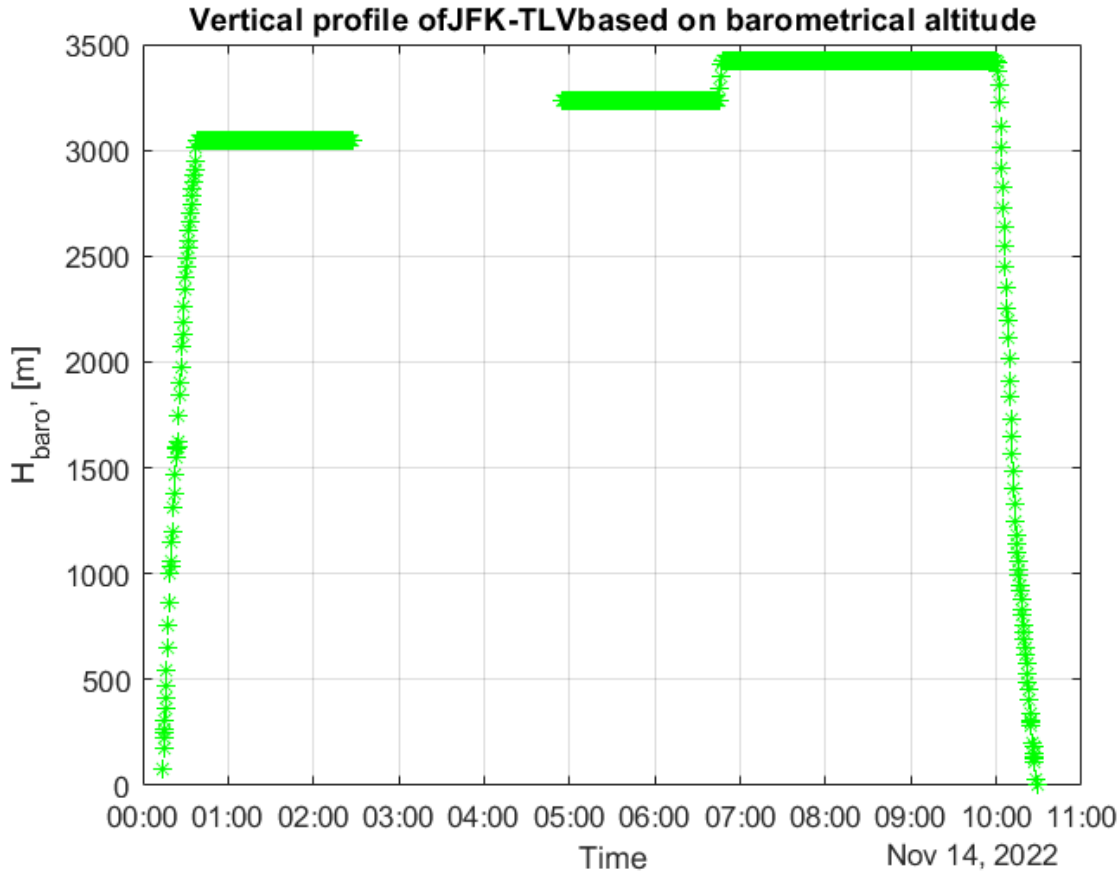


Рисунок 5.3 – Вертикальний профіль рейсу ALL146 від 11 листопада 2022

5.3. Інтерполяція траєкторних даних

Цифрові повідомлення передані за концепцією ADS-B є несинхронізованими за часом. Кожин передавач може бути налаштований на свою частоту видачі цифрових повідомлень. Крім того слід відмітити що частота 1090МГц є доволі завантаженою, оскільки на ній працюють вторинні радіолокатори, системи попередження зближень літаків та ADS-B. Це призводить до того, що певні цифрові повідомлення можуть накладатися однин на одне спотворюючись. Тож траєкторні дані є несинхронізовані з багатьма «битими» повідомленнями. Для вирішення цієї проблеми застосовують методи інтерполяції даних. У якості інтерполюючої функції можуть виступати поліноми чи сплайн-функції. Результати інтерполяції вхідних даних на частоту 1 Гц

наведені на рис. 5.4 - 5.6. Усі наступні обчислення будемо виконувати з інтерпольованими даними. Відобразимо дані у локальній системі NEU. У якості центра системи використаємо координати першої точки траєкторії. Результати візуалізації траєкторії у локальній системі показано на рис. 5.7 та рис. 5.8.

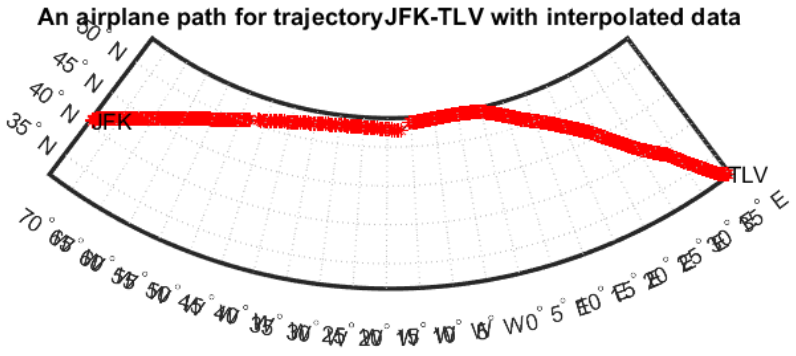


Рисунок 5.4 – Інтерпольована траєкторія руху ПК рейсу ALL146 від 11 листопада 2022

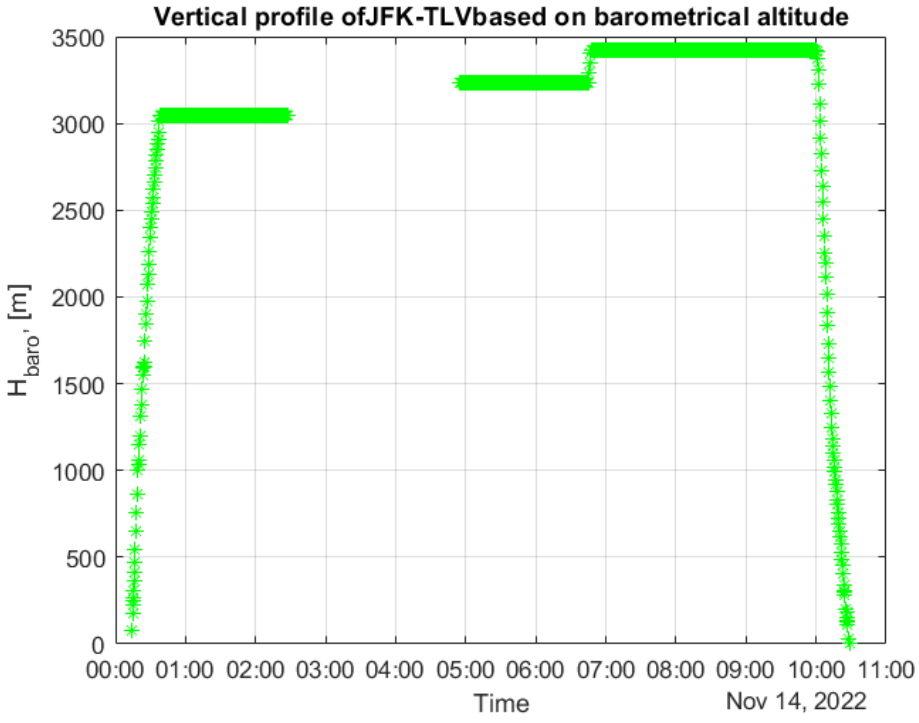


Рисунок 5.5 – Інтерпольований вертикальний профіль ПК рейсу ALL146 від 11 листопада 2022.

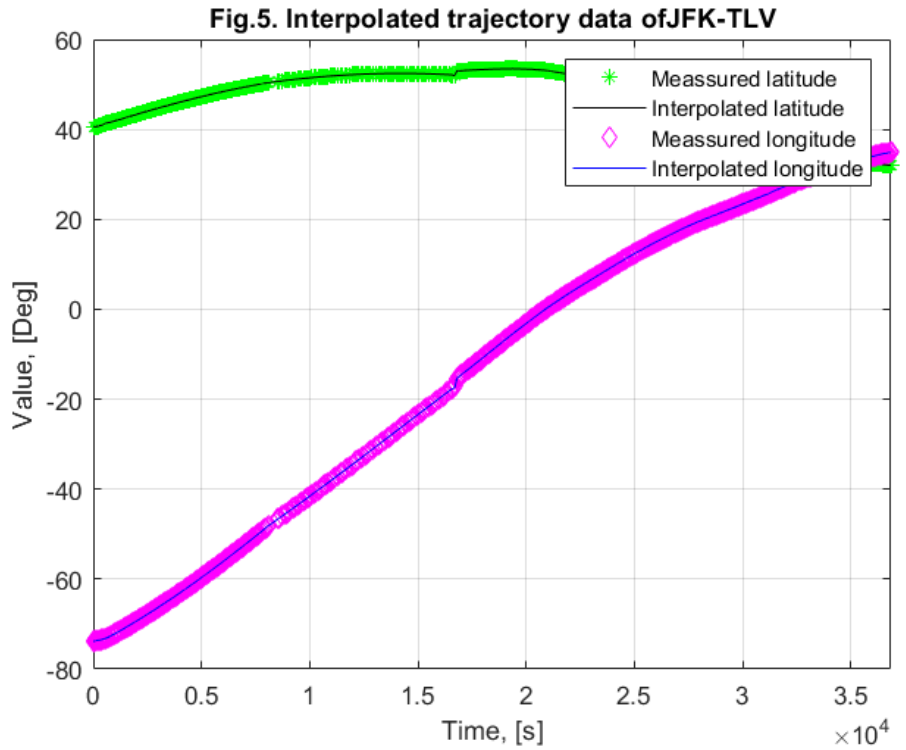


Рисунок 5.6 – Інтерпольовані траєкторні дані на частоту 1 Гц рейсу ALL146 від 11 листопада 2022

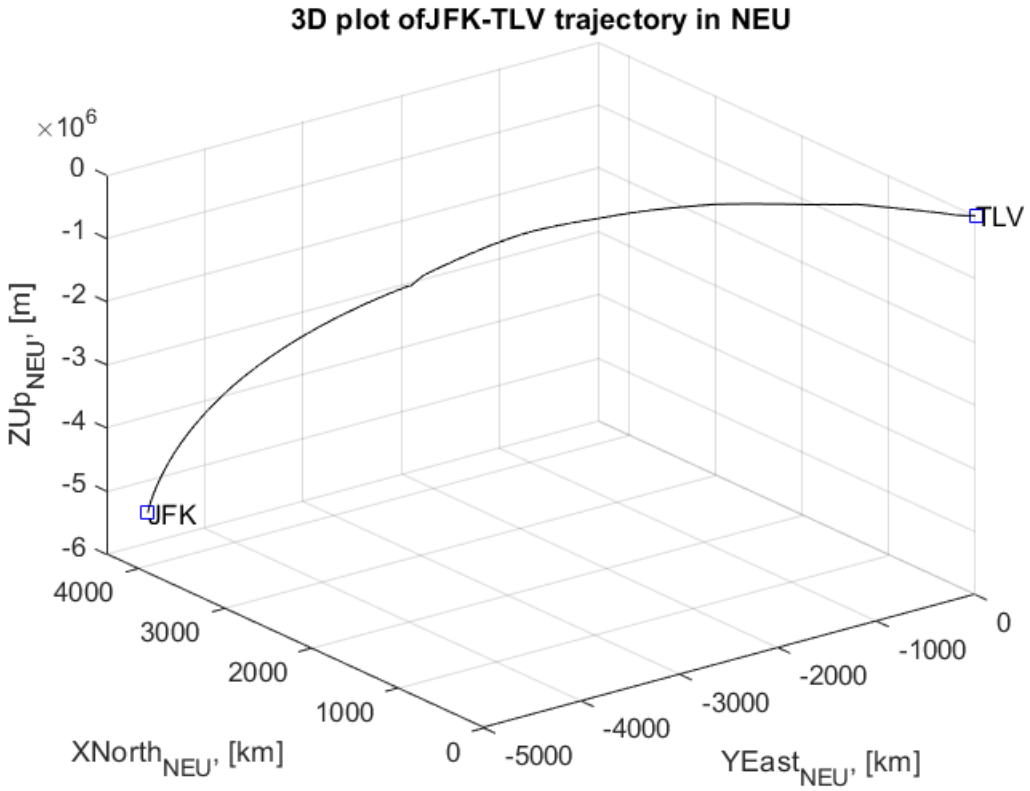


Рисунок 5.7 – Траєкторія руху рейсу ALL146 у локальній системі координат.

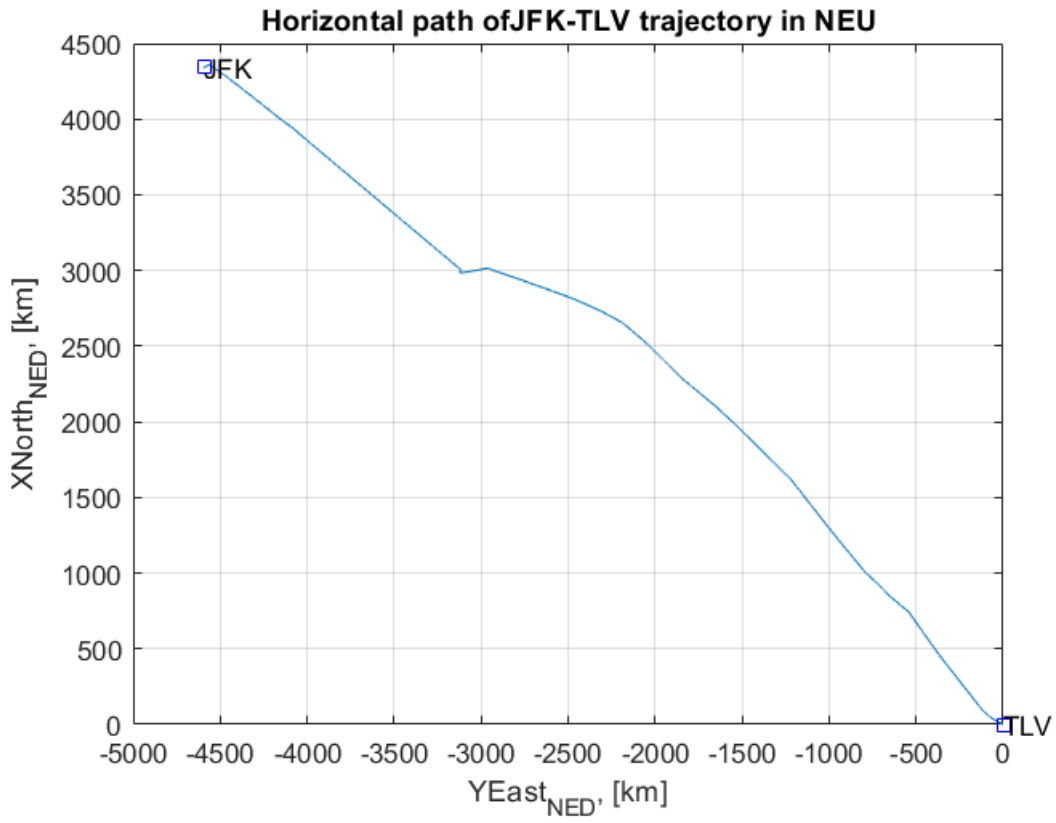


Рисунок 5.8 – Шлях руху рейсу ALL146 у локальній системі координат .

5.4. Розрахунок параметрів траєкторії

За набором даних тривимірної траєкторії руху виконаємо розрахунок компонентів швидкості, зокрема розрахуємо повну швидкість ПК, вертикальний та горизонтальний компонент. Результати розрахунку швидкості наведено на рис. 5.9., а оцінений курс літака на рис. 5.10. Також підрахуємо загальний час польоту, та довжину маршруту та траєкторії.

Загальний час польоту рейсу ALL146 від 11 листопада 2022 склав 10 години 48 хв. Довжина траєкторії – 9227.979км, а довжина маршруту (горизонтальної проекції) – 9126.590км.

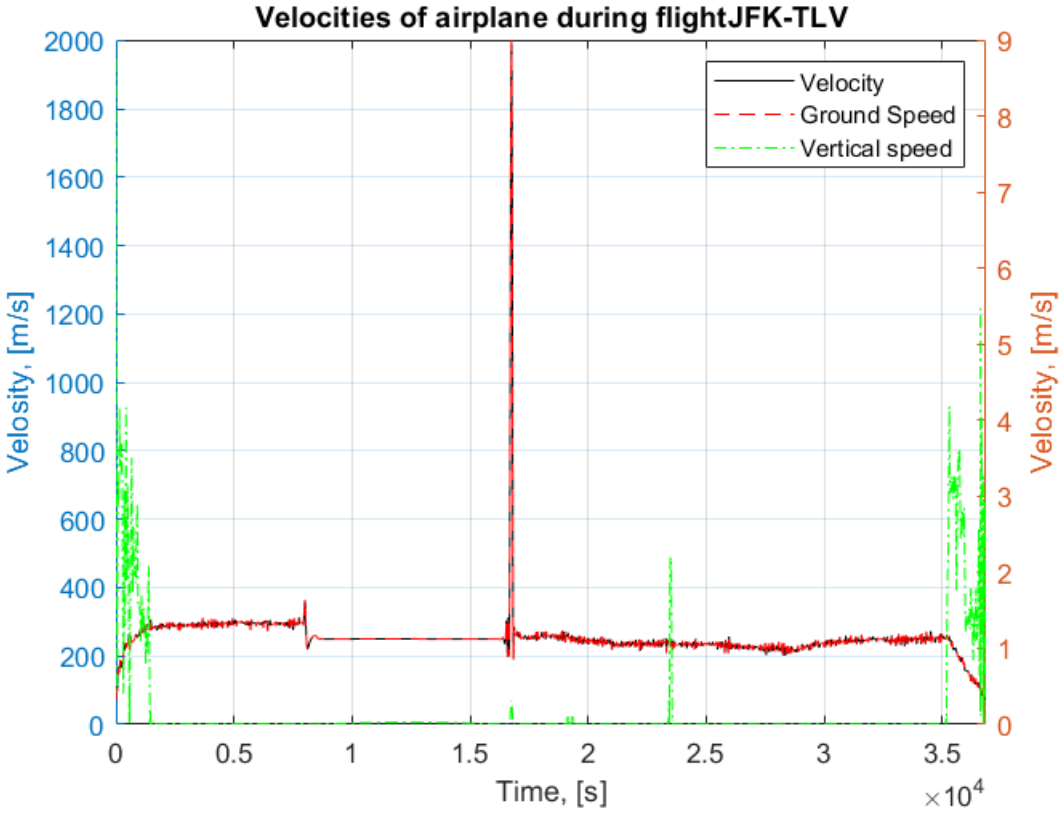


Рисунок 5.9 – Результати розрахунку швидкості польоту для рейсу ALL146 від 11 листопада 2022

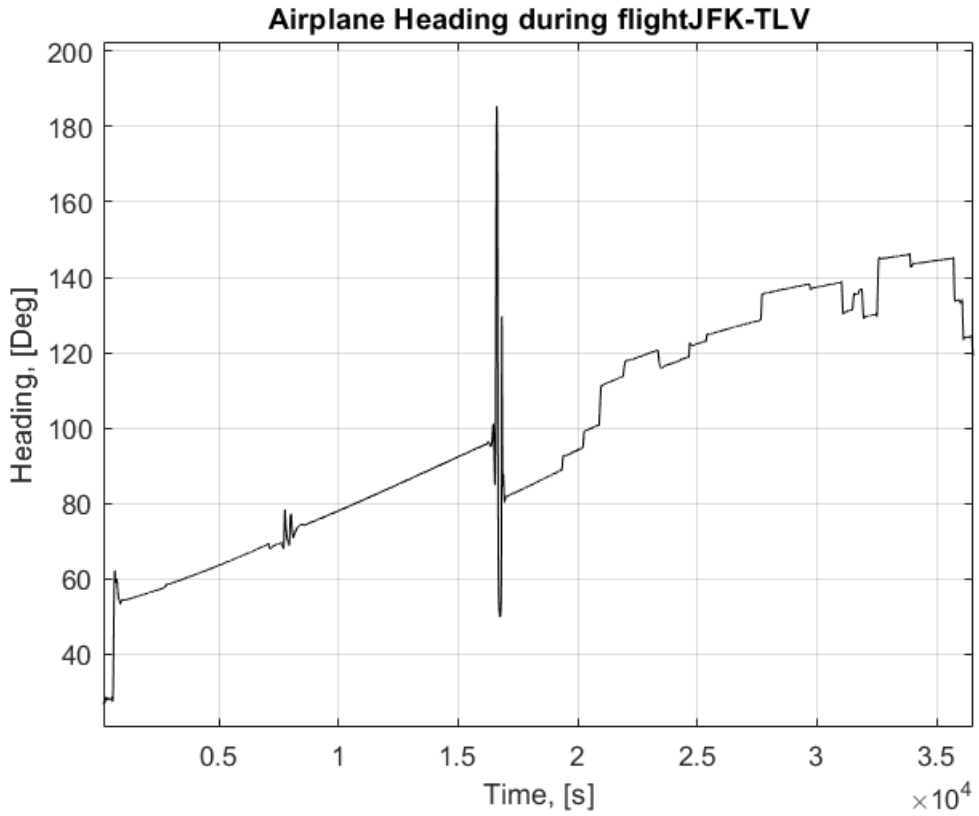


Рисунок 5.10 – Результати розрахунку курсу для рейсу ALL146 від 11 листопада 2022

Висновок: у цьому розділі виконано основну розрахункову частину дипломної роботи. В середовищі MATLAB було розроблено програмний код, який на основі масиву інформації будує графіки про курс, траєкторію, висоту літака у вибраних системах координат. Автоматизація обробки таких даних значно спростовує та пришвидшує процес обрахунку данних отриманих за допомогою ADS-B.

РОЗДІЛ 6. ОХОРОНА ПРАЦІ ПРИ ВИКОНАННІ ЛЬОТНИХ ВИПРОБУВАНЬ БПЛА

6.1 Персонал що допускається до виконання льотних вибробувань

6.1.1 Керівник відділу льотних випробувань

Обов'язки:

- відповідальний за дотримання всіх процедур льотних випробувань;
- керує процесом льотних випробувань, координує кожний крок процесу;
- визначає персонал, необхідний виконання завдань;
- перевіряє правову основу до виконання льотних випробувань;
- ініціює процес отримання PtF;
- схвалює оцінку ризику;
- затверджує польотний лист;
- здійснює комунікації з HoA та HoA.

Кваліфікаційні вимоги:

- Вища освіта в авіаційній сфері або еквівалентна;
- Мінімум 5 років досвіду в експлуатації льотної техніки;
- Мінімум 3 роки досвіду в галузі випробувань льотної техніки;
- Досвід участі щонайменше в одному проекті сертифікації льотної техніки;
- Знання організації та її структури;
- Знання цього посібника та керівництва організації-розробника;
- Знання нормативно-правових документів та законодавства для організації льотних випробувань тієї країни, де здійснюються польоти.

6.1.2 Менеджер з безпеки

Обов'язки:

- Допомагає в ідентифікації небезпеки, аналізі та управлінні ризику;
- Допомагає визначати шляхи та послідовність пом'якшення ризиків;
- Слідкує за дотриманням послідовних кроків пом'якшення ризику;
- Веде звітність щодо забезпечення безпеки;
- Слідкує за веденням записів з управління безпекою;
- Проводить навчання та консультує щодо забезпечення безпеки;
- Ініціює та проводить аналіз внутрішніх подій.

Кваліфікаційні вимоги:

- Вища освіта в авіаційній сфері чи еквівалентна;
- Мінімум 5 років досвіду експлуатації льотної техніки;
- Мінімум 3 роки досвіду у галузі випробувань льотної техніки;
- Знання компанії та її організації;
- Знання даного керівництва та керівництва організації-розробника;
- Знання АПУ-21 (Part 21).
- У разі відсутності менеджера з безпеки його функції виконує керівник відділу льотних випробувань.

6.2 Кваліфікація екіпажу

6.2.1 Кваліфікація провідного інженера

Відповідно до обсягу схвалення Організації-розробника провідні інженери повинні відповідати рівню компетенції для виконання льотних випробувань категорії III та IV.

Для випробувань категорії III:

- відповідає компетенції 1 або 2; або
- Отримав значний досвід польотів відповідно до завдань;
- Брав участь у всіх польотах для кожного класу або типу повітряного судна, є частиною програми для видання індивідуального сертифіката льотної придатності принаймні для п'яти повітряних суден.

Для випробувань категорії IV:

- Повинні мати досвід виконання польотів за програмами льотних випробувань та перевірок для підтвердження відповідності вимогам льотної придатності;
- Брав участь у польотах для видачі сертифікатів льотної придатності ПС;
- Пройшов підготовку в організації з особливостей виконання польотів за програмами льотних випробувань та перевірок;

Кваліфікаційні вимоги:

- Вища освіта за фахом.
- Досвід роботи не менше 1 року в галузі проектування та виробництва авіаційної техніки.

Інші вимоги:

- Наявність діючого медичного сертифіката не нижче 2-го класу
- Наявність повноважень (дозволу) виданих Організацією-розробником включають щонайменше таку інформацію:
    - Ім'я;
    - дата народження;
    - досвід та підготовка;
    - Посаду в організації;
    - Обсяг дозволених робіт;
    - дата видання першого дозволу;
    - дата закінчення терміну дії дозволу, якщо це доречно;
    - Ідентифікаційний номер дозволу.

6.2.2 Кваліфікація пілота

Для виконання льотного випробування Категорії I та II:

1) Для виконання випробувальних польотів категорії I та II обов'язкова наявність рейтингу на право виконання льотних випробувань за винятком:

– Літаків категорії CS-23 злітною вагою менше 2000 кг (FCL 820. b.2.(ii));

– ліцензія, що діє, та відповідний рейтинг, прийнятний для виконання польотів цієї складності.

Крім цього:

• повне та детальне розуміння процесу льотних випробувань та порядку документообігу в межах Організації-розробника;

• знання вимог цього посібника.

Кожен пілот, залучений у процес льотних випробувань, перед тим, як виконувати випробування, має бути оцінений і номінований, як пілот випробувач для виконання польотів у межах програми льотних випробувань.

Дані про пілот, що зберігаються в організації-розробнику, повинні містити, як мінімум:

- копія ліцензії;

- відомості про діяльність у галузі льотних випробувань (за останній рік);

- Інша прийнятна інформація.

6.2.3 Квалифікація оператора БпЛА

Кваліфікаційні вимоги:

– Наявність повноважень (дозвіл) виданих Організацією-розробником після проходження відповідної підготовки в організації.

– Підготовка в Організації-розробнику може проводитись із кандидатами за Програмою підготовки розробленою організацією. Така програма має включати:

• 100 годин теоретичної підготовки з наступних предметів:

- Повітряне право;
- експлуатація повітряних суден;
- аеродинаміка польоту ПС;
- літні характеристики ПС та планування польотів;
- авіаційна метеорологія;
- Експлуатаційні процедури;
- повітряна навігація;
- можливості та обмеження людини в льотній діяльності;
- радіотелефонія;

• Практична підготовка в обсязі не менше 40 годин для виконання польотів БПЛА.

Обсяг підготовки навчання залежить від кваліфікації оператора. За наявності чинного посвідчення оператора проводиться лише практична підготовка обсягом щонайменше 40 годин з виконання польотів БПЛА.

Кваліфікаційні вимоги:

– Середня освіта
– Вік не молодший 18 років
– Фізична та психічна придатність для безпечного виконання покладених на них обов'язків та повноважень. Не мати захворювань та травм, що зумовлюють тимчасову чи постійну втрату працездатності, та таких, що можуть призвести до раптової неможливості керувати БПЛА;

Крім цього:

– повне та детальне розуміння процесу льотних випробувань та порядку документообігу в межах Організації-розробника;
– знання вимог цього посібника.

Дані про оператора, що зберігаються в організації-розробнику, повинні містити, як мінімум:

- копія посвідчення;
- Результати медичного обстеження (за останній рік);
- відомості про діяльність у галузі льотних випробувань (за останній рік);
- Інша прийнятна інформація.

6.2.4 Кваліфікація інженера з льотних випробувань

Кваліфікаційні вимоги:

- Вища освіта в авіаційній сфері чи еквівалентна;
- Мінімум 3 роки досвіду в експлуатації льотної техніки;
- Мінімум 1 рік досвіду у галузі випробувань льотної техніки;
- Знання компанії та її організації;

6.2.5 Категорія льотних випробувань

Льотні випробування, залежно від характеру польоту та рівня ризику, поділяються на дві категорії, що потребує відповідного рівня кваліфікації пілота випробувача/оператора БпЛА.

Табалиця 6.1 - Категорії ризику льотних випробувань

Категорія I (ризик: «високий»)	Категорія II (ризик: "низький", "середній")
- первинний політ на новому типі ПС; - політ, пов'язаний із дослідженням меж області експлуатації; - політ, що виконується у граничних умовах експлуатації; - політ, у якому є ймовірність виникнення небезпечної ситуації (визначення характеристик звалювання, випробування на штопор нового ПС…).	- політ, який потребує високого рівня пілота/оператора, і за якого не очікується появи ненавмисних небезпечних умов польоту; - політ у межах відомих меж області польоту; - політ, що стосується випробування модифікованого ПС, який уже мав сертифікат типу.

Продовження таблиці 6.1

Категорія III (ризик «низький»)	Категорія IV (ризик «низький»)
Польоти для видачі декларації щодо відповідності нового повітряного судна, для чого не потрібно виконувати польоти, що перевищують обмеження .	Польоти, які не класифікуються як категорія 1 або категорія 2 на вже сертифікованому типі літака у разі не затверджених змін у конструкції.

6.3 Проведення льотних випробувань

6.3.1 Літовий склад

Кожне льотне випробування має проводитися з мінімальним необхідним льотним складом.

Літні випробування категорії I виконуються лише одним пілотом/оператором (дослідження характеристик звалювання, перевірка на штопор…). Як виняток, допускається залучення другого пілота або інженера з льотних випробувань, якщо другий пілот необхідний для підстрахування першого пілота (дослідження в області польотів за правилами польоту за приладами) або ведення записів та контролю обладнання. У цьому випадку дозвіл на такий політ затверджує HoA за допомогою внесення відповідного запису до FTO.

Допускається присутність додаткових осіб у кабіні при виконанні льотного випробування категорії II з ризиком «низький» (оператор, який навчається пілот-випробувач…). При цьому робиться відповідний запис складу екіпажу в FTO.

6.3.2 Обмеження льотного часу

6.3.2.1 Загальне

Виконання льотних випробувань пілоту-випробувачу (екіпажу) дозволяється у межах стартового часу.

Стартовий час для льотного складу та учасників випробувань у польоті не повинен перевищувати 8 годин, крім випадків, коли за завданням виконуються тривалі безпосадкові польоти.

За виробничою потребою керівник відділу льотних випробувань має право збільшувати стартовий час для аеродромних польотів до 10 годин з наданням льотного складу у цей період не менше двох годин для відпочинку (сну).

При виконанні неманеврених польотів загальний наліт екіпажу має становити не більше 12 годин, за стартовим часом не більше 14 годин на добу.

У ніч, що передує льотному дню (ночі), особи льотного складу, заплановані на польоти, повинні мати для сна щонайменше 8 годин.

Перерва між польотами, що виконуються у попередній та черговій льотних змінах, має становити не менше 12 годин.

Перед нічними та змішаними польотами льотному складу має бути надано додатковий відпочинок не менше 4 годин, а перед польотами у другій половині дня – не менше 2 годин.

6.3.2.2 Спеціальні обмеження

Таблиця 6.2 - Спеціальне обмеження

Ступінь ризику «високий»	Обмеження безперервного льотного часу без урахування передпольотної підготовки
Дослідження меж області експлуатації ПС	Не більше 1 години
Політ у граничних умовах області експлуатації ПС	Не більше 2 години
Дослідження характеристик звалювання	Не більше 2 години
Розширення галузі експлуатації	Не більше 4 години

6.3.3 Розташування та обладнання

Наземні випробування, дослідні та сертифікаційні польоти, як правило, виконуються на аеродромі Бородянка та/або Київ (Бузова).

Також можуть бути аеродроми України, допущені до виконання на них польотів.

У разі необхідності використання аеродромів із спеціальним обладнанням, організація виконує аналіз та вибір таких аеродромів для виконання специфічних льотних випробувань.

Вимоги до аеродромного та аеродромного обладнання, як правило, визначають DE по льотним випробуванням та/або DE у напрямку. Процес аналізу та вибору місця проведення випробувань координує керівник відділу льотних випробувань.

6.3.4 Обслуговування випробувального ПС

Якщо ПС (як експериментальне) здійснює польоти з PtF, призначеним для льотних випробувань (дослідницьких або сертифікаційних), відповідальність за обслуговування ПС несе керівник відділу льотних випробувань. У цьому випадку немає необхідності залучати сертифікованих фахівців або організацій (Part M, Part 66…). Проте, якщо це зручно, такі фахівці та/або організації можуть залучатись. Як правило, обслуговування ПС виконується персоналом відділу льотних випробувань із залученням інженерного персоналу організації-розробника, а також фахівців організації-виробника. Взаємодія між розробником та виробником здійснюється у рамках правил, визначених DOH.

Записи про виконання обслуговування та/або зміни конфігурації випробувального ЗС вносяться у відповідні документи та форми.

6.3.5 Випробувальне та приладове обладнання

Як правило, кожне ПС обладнано приладами, які передбачені існуючим сертифікатом типу або які передбачені специфікацією продукту (вимогою до продукту), який ще не має сертифіката типу. Тим не менш, програма льотних випробувань у відповідному розділі містить опис приладового обладнання випробувального ПС безпосередньо або за допомогою посилання (специфікація продукту, сертифікат типу, умови польоту для льотних випробувань).

Якщо встановлюється специфічне випробувальне обладнання (вимірювальні прилади, прилади вимірювання та запису параметрів польоту, прилади, що визначають точність заходу на посадку…), таке обладнання визначається програмою льотних випробувань.

Відповідальність за калібрування та обслуговування обладнання, власником якого є організація-розробник, несе відділ льотних випробувань, зокрема інженер з льотних випробувань.

За необхідності використання спеціального обладнання залучаються підрядники. Відповідальність за калібрування та обслуговування такого обладнання несе сам підрядник.

Проте, кожне обладнання від підрядника перевіряється щодо наявності свідоцтва про калібрування (перевірці) устаткування.

Інженер з льотних випробувань несе відповідальність за те, що все приладове та випробувальне обладнання, що застосовується, відкаліброване, повірене та придатне для використання.

Порядок взаємодії із затвердженими та незатвердженими підрядниками визначено у керівництві організації-розробника.

6.4. Управління ризиком та безпекою

Під час виконання польотів необхідно дотримуватись загальних вимог забезпечення безпеки, визначених нормативними та законодавчими документами країни, на території якої виконуються польоти.

Цей розділ лише вказує на основні ключові аспекти правил безпеки.

Забороняється розводити відкритий вогонь або курити поблизу ПС, за винятком необхідності проведення специфічних робіт.

Двигун.

Робота двигуна землі:

- ПС на гальмах (на пусковому пристрої), надійно закріплено на землі;

- персонал у кабіні надійно закріплений ременями (якщо застосовно);

- Перед пуском двигуна вимовити команду: "Від гвинта" і тільки після відкликання: "є від гвинта" здійснювати запуск двигуна;

- ПС знаходиться осторонь перехожої частини, доріжки для наземного персоналу;

- Поточний струмінь від гвинта не повинен бути спрямований у бік ангару;

- на майданчику для газівки не повинно бути сторонніх предметів, які потенційно можуть потрапити під вплив повітряного гвинта;

Підготовка ПС до льотного випробування.

- Не втрачати та не забувати інструмент (предмети) після виконання робіт. Не допускати запуск двигуна доти, доки втрачений інструмент (предмет) не буде знайдений та переміщений у належне місце;

- стежити за станом погоди та умовами атмосфери на рівні аеродрому;

- Проводити ретельну передпольотну перевірку та інструктаж.

Виконання польотів.

- стежити за погодними умовами та умовами видимості;

- дотримуватись зазначених обмежень;

- дотримуватися мінімальної необхідної висоти;

- стежити за станом та самопочуттям льотного складу;

- Припиняти льотне випробування у разі виникнення ненавмисних та неочікуваних ускладнень.

Висновки: у цьому розділі виконано роботу про охороні праці , на етапах виконання льотних випробувань, вказано на умови виконання, персонал що залучається, права, обов'язки та кваліфікаційні можливості кожного з членів екіпажу.

ВИСНОВКИ

При виконанні дипломної роботи було розглянено териоретичну частину, створено апаратну та виконано маметатично-розрахункову частину.

В першому розділі стисло розповідається про GNSS, про те яку важливу роль GNSS відіграє для позиціонування , зокрема для БПЛА. Дізнались які саме системи можливо використовувати для навігації БПЛА окрім супутникової системи навігації. Розглянули сучасну будову ІНС для БПЛА, що таке акселерометри, гіроскопи, магнітометри та їх принципи роботи. Також описано про альтернативні системи навігації. Ці системи – це майбутнє для незалежної, внутрішньої системи навігації. Саме ці системи в майбутньому дадуть стовідсотковий захист БПЛА, але вони потребують більше досліджень та розробок.

В другому розділі піднято питання про навмисні завади направленні на стабільну роботу системи навігації БПЛА. На сьогодні політ в умовах навмисних завад необхідний для вирішення тактичних завдань порятунку та знищення заради життів та незалежності нашої держави. Це підтверджує актуальність даної дипломної роботи.

В наступному, третьому розділі, розглядаються можливоті захисту GNSS-приймачів від дії засобів РЕБ. Виконується аналіз та дослідження працездатності анті-spoofing системи на базі приймача NovAtel OEM7 та симулятора завад.

Четвертий розділ займає практична частина, в ній реалізується система попередження спуфінговим атакам. Ця система набула практичного використання на БПЛА в компанії в якій я працюю, та отримала гарні відгуки від експлуатантів. Вказано методи навігації в умовах без GPS.

У п'ятому розділі виконано обов'язкову частиу математично-розрахункової роботи. Реалізовано код в середовищі MATLAB що виконує обробку навігаційних даних великої розмірності. Для вхідних даних використовуються ADS-B дані, що надаються у вільний доступ компанією Flightaware. Виконано розрахунково-графічну роботу, де візуалізовано графіками окремі параметри польоту.

В останньому розділі описано також обо’язкову частину - охорону праці. На свій розсуд я вибрав саме охорону праці при виконанні льотних випробувань. В цьому розділі акцентував увагу на умови виконання льотних випробувань що відповідають нормам Повітряного Кодексу України.

Дипломну роботу виконано з урахуванням усіх методичних рекомендацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ostroumov I.V., Kuzmenko N.S. Outliers detection in Unmanned Aerial System data. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). 2021. P. 591-594..
2. Харченко В.П., Остроумов І.В. Авіоніка. Київ: НАУ, 2013. 281с. ISBN: 978-966-598-573-0.
3. Ostroumov I.V., Kuzmenko N.S. Performance Modeling of Aircraft Positioning System. Conference on Integrated Computer Technologies in Mechanical Engineering–Synergetic Engineering – ICTM 2021. ICTM 2021. Lecture Notes in Networks and Systems. 2022. № 367. P. 297-310 DOI: 10.1007/978-3-030-94259-5_26.
4. Ostroumov I.V., Marais K., Kuzmenko N.S. Aircraft positioning using multiple distance measurements and spline prediction. Aviation. 2022. № 26(1). P. 1-10 DOI: 10.3846/aviation.2022.16589.
5. Ostroumov I.V., Kharchenko V.P., Kuzmenko N.S. An airspace analysis according to area navigation requirements. Aviation. 2019. № 23(2). P. 36-42 DOI: 10.3846/aviation.2019.10302 .
6. Ostroumov I.V., Kuzmenko N.S. Statistical Analysis and Flight Route Extraction from Automatic Dependent Surveillance-Broadcast Data. 2022 Integrated Communications Navigation and Surveillance Conference (ICNS). 2022. P. 1-9. DOI: 10.1109/ICNS54818.2022.9771515.
7. Ostroumov I.V., Ivashchuk O. Risk of mid-air collision estimation using minimum spanning tree of air traffic graph. Paper presented at the CEUR Workshop Proceedings of the 2st International Workshop on Computational & Information Technologies for Risk-Informed Systems CITRisk-2021. 2022. № 3101. P. 322-334.
8. Ostroumov I.V., Kuzmenko N.S. A Probability Estimation of Aircraft Departures and Arrivals Delays. Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. Lecture Notes in Computer Science. 2021. № 12950. P. 363-377 DOI: 10.1007/978-3-030-86960-1_26 .

9. Ostroumov I.V., Kuzmenko N.S. Incident detection systems, airplanes. In Vickerman, Roger. International Encyclopedia of Transportation. vol. 2. 4569 p. . UK: Elsevier Ltd., 2021. 351-357p. DOI: 10.1016/B978-0-08-102671-7.10150-2. ISBN: 9780081026717.

10. Flightaware. Офіційний веб сайт компанії. [Електронний ресурс]. URL : https://flightaware.com/adsb/

11. Software for Air Navigation analysis. Visualization of airplane trajectory based on ADS-B data messages. [Електронний ресурс]. URL :https://www.ostroumov.sciary.com/codes_airplane-trajectory-visualization

12. Суходоля, О. (2016). Зелена книга з питань захисту критичної інфраструктури в Україні. Упо-ряд. Д. Бірюков & С. Кондратов. за заг. ред. О. Су-ходолі К.:НІСД. Режим доступу: http://www.niss.gov.ua/public/File/2016_book/ Syxodolya_ost.pdf.

13. Конин, В. & Харченко, В. (2010). Системыспутниковой радионавигации. Киев: ХОЛТЕХ.

14. Ward, P. (1994). GPS Receiver RF Interfer-ence Monitoring, Mitigation, and Analysis Techniques, Navigation, 41(4), pp. 367–392. doi: 10.1002/j.2161-4296.1994.tb01886.x

15. Parkinson, B. W. and Spilker, J. J. (1996). Pro- gress In Astronautics and Aeronautics: Global Position-ing System: Theory and Applications. American Insti-tute of Aeronautics & Astronautics. Available at: http://books.google.com.ua/books?id=t0eGFpSwN0w C (Accessed: 3 February 2014).

16. Corrigan, T. M. et al. (1999). GPS Risk As-sessment Study. Final report. Washington. Available at: http://www.rvs.uni-bielefeld.de/publications/ Inci-dents/DOCS/Research/Other/Article/gps-risk-ass.pdf (Accessed 3 February 2014).

17. Vulnerability Assessment of the Transporta- tion Infrastructure Relying on the Global Positioning System (2001). Final Report. Washington. Available at: https://www.navcen.uscg.gov/pdf/vulnerability_as- sess_2001.pdf (Accessed 3 February 2014).

18. M. Powe, J. I. R. O. (1999). European Organ- isation for the Safety of Eurocontrol Experimental Cen- tre GNSS Frequency Protection Requirements. Availa- ble at: https://www.eurocontrol.int/gnss-frequency- protection-requirements (Accessed 3 February 2014).

19. Corbell, P. M. (2000). Design and validation of an accurate gps signal and receiver truth model for comparing advanced receiver processing techniques, AIR FORCE INSTITUTE OF TECHNOLOGY. Avail-able at: http://www.dtic.mil/dtic/tr/fulltext/u2/a380760.pdf (Accessed 3 February 2014).

20. RTCA Inc. (2008). Assessment of Radio Fre-quency Interference Relevant to the GNSS L1 Fre-quency Band. Washington. Available at: http://books.google.com.ua/books/about/Assess- ment_of_Radio_Frequency_Inter-feInt.html?id=w6NWewAACAAJ&redir_esc=y (Ac-cessed 5 February 2014).

21. Wildemeersch, M. and Fortuny-Guasch, J. (2010). Radio Frequency Interference Impact Assess- ment on Global Navigation Satellite Systems. Ispra (VA), Italy. doi: 10.2788/6033.

22. Wildemeersch, M. et al. (2010). Impact Study of Unintentional Interference on GNSS Receivers, Tech. Rep. EUR-24742-EN, Publications Office of the European Union. Luxembourg. doi: 10.2788/57794.

23. Bauernfeind, R. et al. (2012) Analysis, detec- tion and mitigation of incar gnss jammer interference in intelligent transport systems, Deutscher Luft- und Raumfahrtkongress, pp. 1–10. Available at: http://www.dglr.de/publikationen/ 2013/281260.pdf (Accessed: 17 July 2014).

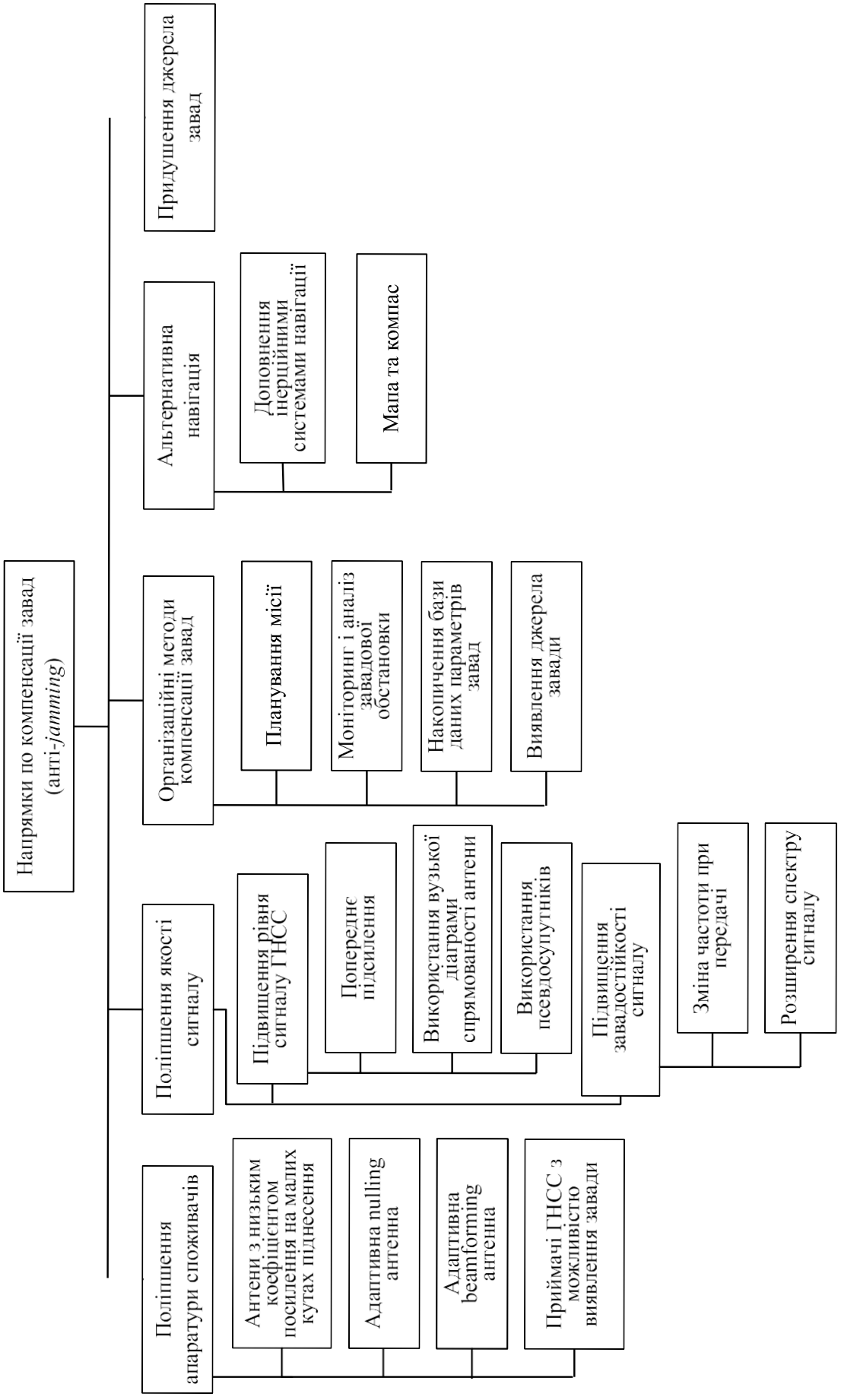
24. Rügamer, A., Iis, F. and Kowalewski, D. (2015). Jamming and Spoofing of GNSS Signals-An Underestimated Risk?! Motivation Applications of GNSS Motivation Applications of GNSS Content Jam-ming and Spoofing of GNSS Signals-An Underesti- mated Risk?! Available at: https://www.fig.net/re- sources/proceedings/ fig_proceed- ings/fig2015/ppt/TS05G/TS05G_ruegamer_kowalews ki_7486_ppt.pdf (Accessed: 19 July 2014).

25. Rügamer, A. and Kowalewski, D. (2015). Jamming and Spoofing of GNSS Signals-An Underes-timated Risk?!, in From the Wisdom of the Ages to the Challenges

of the Modern World. Sofia, Bulgaria,: In-ternational Federation of Surveyors, pp. 1–24. Availa-ble at: https://www.fig.net/resources/proceed-ings/fig_proceedings/ fig2015/pa-pers/ts05g/TS05G_ruegamer_kowalewski_7486.pdf (Accessed: 19 July 2014).

26. Curran, J. et al. (2017). A look at Threat ofSystematic Jamming of GNSS, InsideGNSS, 5, pp. 46–

Додаток А (Напрямки компенсації GNSS)



Додаток Б (код програми MATLAB)

```
% Calculation and Visualization of airplane trajectory based
on non synchronous ADS-B data messages
% Calculation and Visualization of airplane trajectory based
on non synchronous ADS-B data messages (Aircraft Trajectory)
% A code uses airplane trajectory defined by non-synchronize
dataset of points of airplane location measured by GNSS and
barometrical altimeter in various visualization figures.
% Input dataset obtained from decoded messages of airplane
transponder of 1090ES received by Software Defined Radio.

% v 1.0 available on  Jul 10, 2022
% 2022 Ivan Ostroumov
% https://www.ostroumov.sciary.com/codes_airplane-trajectory-
visualization

clc
clearvars
close all

%-----------------------------------------------------------
------------

% Input data
load('AAL146.mat');
alt=alt*0.3040; % ft to meter conversion
airports={'JFK','TLV'};

% lat=   [in Deg]
% lon=   [in Deg]
% alt=   [in m]
% t is datetime

%-----------------------------------------------------------
------------

folder=strcat(pwd,'\', strcat(airports{1},'-
',airports{2},'/'));
if ~exist(folder, 'dir')
    mkdir(folder);
end
% Measuring a time of each data point from start tracking
time
for i=2:numel(lat)
    time(i)=etime(datevec(t(i)), datevec(t(1)));
end
% Increasing a number of data in ten times.
time1=linspace(0,max(time),max(time))
```

```
% Data interpolation for new time serie
latitude = interp1(time,lat,time1,'spline');
longitude = interp1(time,lon,time1,'spline');
altitude = interp1(time,alt,time1,'spline');
%% Plot the data in Geodedic reference frame
% Compute the latitude and longitude limits for investigated
dataset.
 latlim = [min(latitude)-0.2 max(latitude)+0.2];
 lonlim = [min(longitude)-0.2 max(longitude)+0.2];

figure('Color','white','Name',strcat('Fig.1. An airplane path
for trajectory ', airports{1},'-',airports{2}));
usamap(latlim, lonlim);
geoshow(lat, lon, 'Color', 'Red','Marker', '*',
'DisplayType', 'line','LineWidth',1);
textm(lat(1),lon(1), airports{1});
textm(lat(end),lon(end), airports{2});
title(strcat('An airplane path for trajectory ',
airports{1},'-',airports{2}));
savefig(strcat(folder, 'fig_01.fig'));
saveas(gcf,strcat(folder, 'fig_01.jpg'));

figure('Color','white','Name', strcat('Fig.2. Vertical
profile of ', airports{1},'-',airports{2}, 'based on
barometrical altitude'));
plot(t,alt, '*g');
title(strcat('Vertical profile of ', airports{1},'-
',airports{2}, 'based on barometrical altitude'));
xlabel('Time');ylabel('H_{baro}, [m]'); grid on;
savefig(strcat(folder, 'fig_02.fig'));
saveas(gcf,strcat(folder, 'fig_02.jpg'));

figure('Color','white','Name', strcat('Fig.3. An airplane
path for trajectory ', airports{1},'-',airports{2}, 'with
interpolated data'));
usamap(latlim, lonlim);
geoshow(latitude, longitude, 'Color', 'Black','LineWidth',1);
geoshow(lat, lon, 'Color', 'Red','Marker', '*',
'DisplayType', 'point');
textm(lat(1),lon(1), airports{1});
textm(lat(end),lon(end), airports{2});
title(strcat('An airplane path for trajectory ',
airports{1},'-',airports{2}, ' with interpolated data'));
savefig(strcat(folder, 'fig_03.fig'));
saveas(gcf,strcat(folder, 'fig_03.jpg'));

figure('Color','white','Name',strcat('Fig.4. Vertical profile
of ', airports{1},'-',airports{2}, 'based on barometrical
altitude', 'with interpolated data'));
```

```
plot(time,alt, '*g', time1,altitude, '-k');
title(strcat('Fig.4. Vertical profile of ', airports{1},'-
',airports{2}, 'based on barometrical altitude', 'with
interpolated data'));
xlabel('Time, [s]');ylabel('H_{baro}, [m]');legend('Meassured
Data', 'Interpolated data'); grid on; xlim([0,time1(end)]);
savefig(strcat(folder, 'fig_04.fig'));
saveas(gcf,strcat(folder, 'fig_04.jpg'));

figure('Color','white','Name',strcat('Fig.5. Interpolated
trajectory data of ', airports{1},'-',airports{2}));
plot(time,lat, '*g', time1,latitude, '-k',time,lon, 'dm',
time1,longitude, '-b');
title(strcat('Fig.5. Interpolated trajectory data of ',
airports{1},'-',airports{2}));
xlabel('Time, [s]');ylabel('Value, [Deg]');legend('Meassured
latitude', 'Interpolated latitude','Meassured longitude',
'Interpolated longitude'); grid on; xlim([0,time1(end)]);
savefig(strcat(folder, 'fig_05.fig'));
saveas(gcf,strcat(folder, 'fig_05.jpg'));

% visualization of airplane trajectory in NED coordinate
system with
% reference point at first data point
p = lla2ecef([latitude', longitude', altitude'], 'WGS84');
x=p(:,1);
y=p(:,2);
z=p(:,3);
wgs84 = wgs84Ellipsoid('meters');
[xNorth,yEast,zDown] = ecef2ned(x,y,z,latitude(end),
longitude(end), altitude(end),wgs84);

figure('Color','white','Name',strcat('Fig.6. 3D plot of ',
airports{1},'-',airports{2}, ' trajectory in NEU'));
plot3(yEast*1e-3,xNorth*1e-3,-zDown, '-k');
hold on
plot3([yEast(1)*1e-3, yEast(end)*1e-3],[xNorth(1)*1e-
3,xNorth(end)*1e-3],[-zDown(1), -zDown(end)], 'sb');
text(yEast(1)*1e-3,xNorth(1)*1e-3,-zDown(1), airports{1});
text(yEast(end)*1e-3,xNorth(end)*1e-3,-zDown(end),
airports{2});grid on;
title(strcat('3D plot of ', airports{1},'-',airports{2}, '
trajectory in NEU'));
xlabel('YEast_{NEU}, [km]');ylabel('XNorth_{NEU},
[km]');zlabel('ZUp_{NEU}, [m]');
hold off
savefig(strcat(folder, 'fig_06.fig'));
saveas(gcf,strcat(folder, 'fig_06.jpg'));
```

```
figure('Color','white','Name', strcat('Fig.7. Horizontal path
of ', airports{1},'-',airports{2}, ' trajectory in NEU'));
plot(yEast*1e-3,xNorth*1e-3,'-',[yEast(1)*1e-3,
yEast(end)*1e-3],[xNorth(1)*1e-3,xNorth(end)*1e-3], 'sb');
text(yEast(1)*1e-3,xNorth(1)*1e-3, airports{1});
text(yEast(end)*1e-3,xNorth(end)*1e-3, airports{2});grid on;
title(strcat('Horizontal path of ', airports{1},'-
',airports{2}, ' trajectory in NEU'));
xlabel('YEast_{NED}, [km]');ylabel('XNorth_{NED}, [km]');
savefig(strcat(folder, 'fig_07.fig'));
saveas(gcf,strcat(folder, 'fig_07.jpg'));

%% Velocity estimation
for i=1:numel(x)-1
    d(i)=sqrt(power(x(i)-x(i+1),2)+power(y(i)-
y(i+1),2)+power(z(i)-z(i+1),2));
    timed(i)=time1(i+1)-time1(i);
    [x1,y1,z1] = ecef2ned(x(i+1),y(i+1),z(i+1),latitude(i),
longitude(i), altitude(i),wgs84);
    dh(i)=sqrt(power(x1,2)+power(y1,2));
    dv(i)=abs(z1);
    if x1>0 & y1>0 % 1
        H(i)=abs(atand(y1/x1));
    elseif x1<0 & y1>0 % 4
        H(i)=180-abs(atand(y1/abs(x1)));
    elseif x1<0 & y1<0 %3
        H(i)=180+abs(atand(y1/x1));
    else %2
        H(i)=360-abs(atand(y1/x1));
    end

end
v=d./timed;
vh=dh./timed;
vv=abs(dv./timed);

figure('Color','white','Name',strcat('Fig.8. Velocities of
airplane during flight ', airports{1},'-',airports{2}));
yyaxis left
plot(time1(2:end),v, '-k',time1(2:end),vh, '--r');
ylabel('Velosity, [m/s]');
yyaxis right
plot(time1(2:end),vv, '-.g');xlim([0,time1(end)]);
ylabel('Velosity, [m/s]');
title(strcat('Velocities of airplane during flight ',
airports{1},'-',airports{2}));
xlabel('Time, [s]');ylabel('Velosity,
[m/s]');legend('Velocity','Ground Speed', 'Vertical speed');
grid on;
```

```
savefig(strcat(folder, 'fig_08.fig'));
saveas(gcf,strcat(folder, 'fig_08.jpg'));

figure('Color','white','Name',strcat('Fig.9. Airplane Heading
during flight ', airports{1},'-',airports{2}));
plot(time1(2:end),H, '-k');
title(strcat('Airplane Heading during flight ',
airports{1},'-',airports{2}));
xlabel('Time, [s]');ylabel('Heading, [Deg]'); grid on;
savefig(strcat(folder, 'fig_09.fig'));
saveas(gcf,strcat(folder, 'fig_09.jpg'));

%% Total data
disp(['Total trajectory length is ', num2str(sum(d)*1e-3),
'km']);
disp(['Flight path length is ', num2str(sum(dh)*1e-3),
'km']);
disp(['Total flight time is',cellstr(between(t(1),t(end)))]);
save(strcat(folder, 'data.mat'));
```