UDC 527.161.2.03.111

І.І. Ключенко
(Національний авіаційний університет, Україна)

Навігація БПЛА в умовах завад.

Сучасні проблеми потребують швидких та простих рішень. В цій статті розглянемо актуальну, не тільки на даний момент, проблему навігації Безпілотних літальних апаратів (БПЛА) в умовах завад.

В умовах війни, БПЛА потребують швидкого та простого вирішення проблеми навігації. БПЛА – один з ключових методів ведення бойових дій на сьогодні. Не можна уявити сучасну розвідку, корегування артилерійського вогню, пошуку та моніторингу територій без цих апаратів. В нашій країні багато виробників БПЛА різних класів зіткнулись з проблемою навігації БПЛА у середовищі без GPS.

Якщо з телеметрією та відео-link'ом все більш-менш ясно - використання низькочастотних передавачів для телеметрії, широкий діапазон , змінна частота, шифрування - це відомі методи захисту каналів зв'язку. Для відео - використання двох-канального «стрімкастера» та інші. Але що робити з навігацією, в умовах коли звичний нам GPS взагалі відсутній, або ще гірше, коли нам намагаються «підсунути» свої координати. Інерційна система навігації (ІНС) не справляється з цим завданням на довгу тривалість польоту. На моїй практиці були випадки, коли ІНС мала похибку в декілька десятків кілометрів всього за півтори години у повітрі без GPS. Основна причина такої похибки – вітер. Розробка інерційних систем що можуть розраховувати поправку на вітер потягне за собою величезні витрати часу та грошей. На жаль, у нас не має ні того ні того. Всі пташки, легкого класу, будуються з використанням імпортних та дешевих автопілотів, GPS приймачів та інших модулів радіоелектронного обладнання. Дешева собівартість БПЛА та їх простота - це основа їх масовості а, отже, ефективності.

Впровадження альтернативної комплексної системи для позиціонування в середовищі без GPS.

Спуфінг GPS - це термін, що використовується для атак, при яких хакери передають сигнали, подібні до GPS, і кодують їх таким чином, що одержувачі обманом змушують їх думати, що вони знаходяться в іншому місці, ніж вони є насправді. Хтось, проводячи спуфінгову атаку, намагається обдурити GPS-приймач за допомогою передачі невірних сигналів, замаскованих під типові. Також можна провести спуфінгову атаку, транслюючи справжні сигнали з неправильною позначкою часу або сигнали, захоплені в іншому місці. Потім спуфер модифікує ці сигнали, щоб змусити одержувача повірити, що він знаходиться в іншому місці або потрібному місці в неправильний час.

У той час як спуфінг GPS – це, перш за все, робота військових операцій, **джамінг (глушення) GPS** – це те, що кожен може зробити з відносною легкістю. Джамер - це пристрій, який збиває з пантелику приймач,

випромінюючи радіосигнали на тій же частоті, що і GPS. Ці перешкоди перешкоджають здатності пристрою GPS визначати своє правильне положення.

Приймачі GPS, такі як U-Blocks чи NovAtel, мають реалізовану функцію детектування спуфінгу та джамінгу. Це дозволяє нам виявити завади на стадії їх формування.

На рисунку 1 та рисунку 2 зображено як GPS приймач U-Block реагує на симульовану заваду та виводить інформацію про статус спуфінгу та джамінгу.

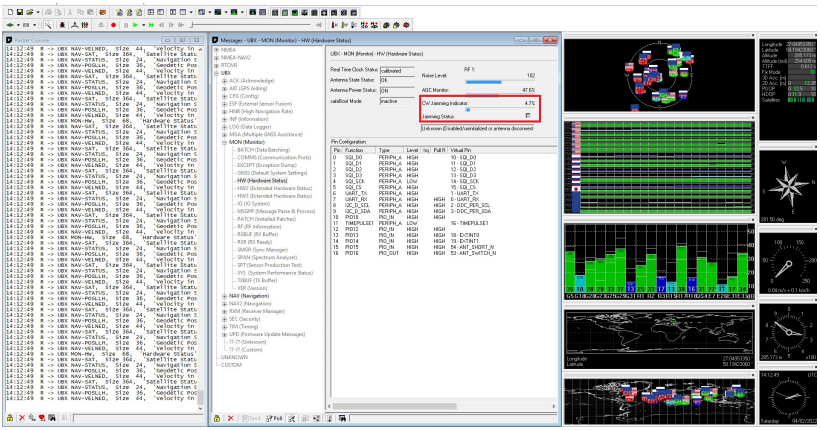

Рисунок 1 Індикація джамінгу в U-Center.

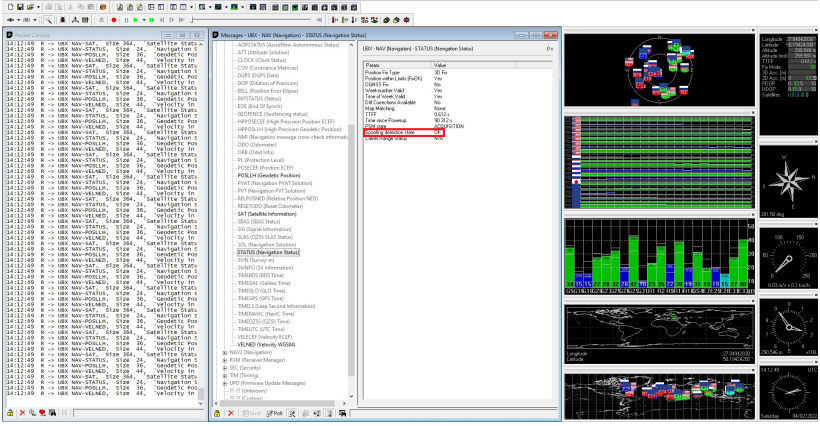

Рисунок 2 Індикація спуфунгу в U-Center.

Для інформування оператора БПЛА ці індикатори потрібно продублювати в програмному забезпеченні для виконання польотів типу

Mission Planner, або, реалізувати режим автоматичного реагування автопілота на ці індикатори.

Найефективнішим способом вберегтись від завади - це своєчасне відключення GPS (фізичним способом або на програмному рівні). Після відключення GPS автопілот буде використовувати інерційні сенсори та інші датчики (приймач повітряного тиску, бародатчик, лазерний висотомір і т.д) для подальшого позиціонування. Нажаль, ІНС має накопичувальну помилку, але рішення - це використання відеокамери для візуального орієнтування та встановлення нової точки відліку для ІНС. Якщо оператор корисного навантаження спостерігає, що позиція БПЛА суттєво відрізняється від положення його іконки на карті, то оператор, використовуючи орієнтири, встановлює йому координати, тим самим скидає похибку ІНС та починає новий цикл накопичення похибки. Такі маніпуляції потрібно проводити поки індикації «спуфінгу» та «джамінгу» не прийдуть в норму, щоб знову використовувати GPS.

Про реалізацію такої системи та її успішне використання в реальних умовах детально розповім у своєму дипломному проекті.

Список літератури

1. Nobody’s Fool. Spoofing Detection in a High-Precision Receiver» Inside GNSS, July/August 2020

2. INFORMATION THREATS TO THE GLOBAL NAVIGATION SATELLITE SYSTEM AND HOW TO ELIMINATE THEM Sciences of Europe # 35, (2019)

3. https://content.u-blox.com/sites/default/files/NEO-M9N_Integrationmanual_UBX-19014286.pdf