УДК 621.396.96:623.746-519

МЕТОДИ ВИЯВЛЕННЯ АТАК НА СИСТЕМУ НАВІГАЦІЇ БПЛА. Частина 1

Головко М. А.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки, каф. МІРЕС
м. Харків, Україна
e-mail: maksym.holovko@nure.ua

This paper discusses the implementation of methods for protecting unmanned aerial vehicles from global positioning system spoofing attacks. A new self-diagnosis method is proposed, which allows the UAV to independently assess the presence of changes in its subsystems and identify signs of a cyber attack.

Проблема виявлення атак на систему навігації БПЛА є актуальною, оскільки подібні атаки безпосередньо впливають на виконання функцій БПЛА. Незважаючи на те, що для реалізації захисту запропоновано ряд методів на основі перед- та пост- кореляційної обробки сигналів, в наш час актуальною є розробка алгоритмів машинного навчання для виявлення атак подавлення навігаційного сигналу та/або спуфінгу навігайціної системи.

В роботі [1] автори пропонують використовувати метод на основі опорних векторів (SVM) на етапі прийому сигналу, бо тут присутній ряд змін сигналу, які можна проаналізувати. Можна встановити співвідношення між опорними вимірами та поточними, і, відповідно, детектувати аномалії. Додавання реальних наборів даних спуфінгу та подавлення до опорних наборів даних на етапі навчання SVM дозволяє підвищити точність детектування. Порівняльний аналіз усіх чотирьох експериментів, представлених у цій статті, показує, що авторам вдалося досягти досить добрих результатів завдяки наступним аспектам: 1) доповнений навчальний набір даних є актуальним для виявлення спроб маніпулювання сигналами ГНСС; 2) метод SVM є ефективним для виявлення спроб маніпуляції сигналами ГНСС.

В роботі [2] пропонується метод виявлення спуфінгу GPS, на основі використання системи орієнтації та визначення курсу (AHRS), а також акселерометра для порівняння різниці значень прискорення, отриманих від GPS-приймача, та від інерційної системи навігації, що забезпечує виявлення помилки значення прискорення. Прискорення, отримане від GPS-приймача, оцінюється за допомогою фільтра Калмана. Різницю, що було виявлено між значеннями прискорення від приймача GPS і акселерометра, використовують для виявлення спуфінгу.

Якщо немає можливості використовувати GPS, БПЛА для координації польоту можуть використовувати інерційні датчики. При цьому, як прави-

ло, виникають помилки у визначенні просторового розташування за допомогою інерційних датчиків, що може призвести до аварійної ситуації. Щоб уникнути неприпустимої помилки датчиків у разі атак із заміною GPS, автори статті [3] пропонують методику управління з обмеженнями безпеки. Детектор атак використовується для виявлення атак з заміною GPS і забезпечує перемикання між режимами надійного та аварійного керування. Система відстеження розташування зловмисника (ALT) оцінює вихідну потужність пристрою спуфінгу за допомогою фільтра Калмана. Використовуючи оцінки від ALT, автори пропонують використовувати контролер евакуації на основі моделі прогнозуючого контролера, щоб БПЛА дислокувався із зони дії пристрою зловмисника протягом допустимого часу.

Інші методи запобігання спуфінгу GPS, такі як моніторинг справності приймача в автономному режимі, вимірювання відношення сигнал/шум і виявлення доплерівського зсуву, розглянуто в роботі [4]. В роботі [5] запропоновано метод, що дозволяє БПЛА виявляти джерело спуфінгу GPS за допомогою незалежної наземної інфраструктури, яка безперервно аналізує зміст та час надходження інформації про передбачуване місцезнаходження БПЛА. Показано, що запропонований метод ефективний при виявленні атак спуфінгу: час виявлення менше 2 с і точність визначення розташування джерела підробленого сигналу – до 150 м. В роботі 6 для виявлення та оповіщення про потенційні атаки використовується аналіз автоматичного регулювання посилення сигналу GPS у приймачі GPS.

В роботах [7-9] досліджено можливість використання кількох приймачів для виявлення атак спуфінгу GPS. В роботі [8] пропонується використовувати кілька незалежних приймачів GPS для виявлення атак. Пропонований метод аналізує відстань між приймачами та наступним виміром відстані між зазначеними розташуваннями приймачів. При однакових сигналах GPS виміряні відстані будуть аналогічні раніше зафіксованим відстаням. Однак при атаці з заміною GPS результати вимірювання відстані будуть дуже близькі до нуля, оскільки всі приймачі передають інформацію, де вказано те саме місце розташування, тобто різниці між приймачами спостерігатися не буде. Автор роботи [7] продемонстрував можливість використання приймача з двома антенами для виявлення атак із заміною GPS. Пропонований метод ґрунтується на аналізі різниці фаз сигналів, отриманих антенами. Автори роботи [9] пропонують використовувати кілька приймачів для підтвердження справжності сигналів GPS на основі співставлення з сигналом GPS від військових супутників без необхідності його розшифровки. Запропонована методика показала високу ефективність.

В роботі [10] наведено підхід до виявлення атаки спуфінгу GPS на БПЛА на основі аналізу оцінки його стану з використанням методу SVM. В роботі запропоновані рішення для виявлення та середовище моделювання атак з підробкою GPS для оцінки функціональності та продуктивності

методу. Підхід не потребує додаткового обладнання, тому його можна використовувати для невеликого БПЛА. Також було показано, що у разі точного знання зловмисником про позиціювання та траєкторію БПЛА, він зможе залишитися непоміченим системою, викликаючи при цьому часті помилкові спрацьовування. Але в реальних сценаріях зловмисник не знає фактичну траєкторію БПЛА, отже, ризик помилкових спрацьовувань малий і запропонована система може виявити будь-яку атаку спуфінгу.

Автори роботи [11] пропонують захисний механізм, заснований на концепції спільної локалізації [12], що дозволяє БПЛА визначати своє реальне розташування в двовимірній системі координат, використовуючи розташування трьох інших БПЛА. Передбачається, що кожен БПЛА має засоби вимірювання відносних відстаней до інших сусідніх БПЛА. При спільній локалізації БПЛА вибирає будь-які три сусідні БПЛА для оновлення свого місця розташування, враховуючи, що вибрані БПЛА не лежать на одній прямій. Після цього БПЛА може точно визначити своє місце розташування у двовимірній системі координат. Однак цей механізм не може використовуватися безпосередньо при атаці спуфінгу GPS, бо БПЛА не може довіряти своєму місцезнаходження за GPS або за місцезнаходженням інших БПЛА. Для подолання цього обмеження автори [11] виходять з припущення, що зловмисник, який використовує спуфінг GPS, може атакувати тільки один БПЛА. У запропонованому механізмі для визначення свого реального розташування БПЛА враховує місце розташування чотирьох сусідніх апаратів замість трьох. Після ідентифікації БПЛА, що під впливом атаки, останній виключається з розрахунків. Таким чином, необхідно відзначити, що даний метод накладає велику кількість обмежень на його застосування. У роботі [13] представлений метод протидії атакам на GPS, заснований на використанні системи технічного зору, яка дозволяє додатково обчислювати швидкість БПЛА та деякі інші показники та корелювати їх із даними отриманими від GPS.