УДК 003.26.09
Малий О.Ю.[1], Пироженко О.О. [2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] асист. НУ «Запорізька політехніка»

МЕТОД КОДУВАННЯ СИГНАЛУ ДЛЯ ЗАХИСТУ ВІД ПЕРЕХОПЛЕННЯ КЕРУВАННЯ БПЛА

У сучасному світі швидко розвиваються технології безпілотних літальних апаратів (БПЛА). Вони знаходять застосування у сільському господарстві, гірничодобувної промисловості, будівництві, лісничому секторі, сфері розваг, для наукових досліджень та для військових цілей.

Усі апарати керуються з деякого віддаленого пульта управління - це дає можливість перехопити керування, яке здійснюється по радіоканалу і змусити безпілотний літальний апарат виконувати спотворене завдання. Важливою проблемою використання безпілотних літальних апаратів є захист даних.

У БПЛА військового призначення актуальність захисту інформації має найвище значення. Слабо захищені системи є великою загрозою для всієї країни. Вони можуть бути зламані та перепрофільовані для шпигунства, надання недостовірної інформації або навіть нанесенню ударів по своїм об'єктам військової або цивільної інфраструктури.

Прикладом перехоплення керування БПЛА є GPS-спуфінг. Принципом дії GPS-спуфінгу є відправка на GPS датчик завідома спотворених даних для визначення хибного місцеположення.

БПЛА використовує GPS-систему на основі локалізації та синхронізується із супутниками. Зловмисник починає посилати власні сигнали, що змушують жертву синхронізуватися з новими, хибними сигналами. Зловмисник може затримати сигнали або надіслати їх передчасно. Через відсутність механізмів автентифікації він може змінити зміст сигналів GPS, що приймаються, або довільно генерувати імітуючі сигнали з використанням параметрів публічних GPS. Зловмисник не може генерувати діючі сигнали GPS, але може захоплювати та передавати існуючі.

Механізми спуфінгу та антиспуфінгу розглядаються в сучасних додатках GPS як найважливіші аспекти.

Заходи захисту, встановлені у програмному забезпеченні на GPS приймачах, можуть бути згруповані за такими категоріями:

– амплітудна невідповідність;

– невідповідність часу отримання сигналу;

– перехресна перевірка вмісту інерційного вимірювального пристрою (IMU);

– поляризаційна перевірка;

– перевірка кута приходу сигналу;

– криптографічна автентифікація.

Для підвищення захисту від несанкціонованого перехоплення за рахунок відкритого каналу зв'язку БПЛА з пульта управління, розглядається застосування методу перестановочного декодування в каналі зв'язку.

Пропонується метод схожий на метод декодера, коли в блоці прийому перший вихід якого через послідовно включені блок м'яких рішень символів, накопичувач оцінок і блок упорядкування оцінок підключений до першого входу блоку еквівалентного коду, другий вихід якого підключений до іншого входу блоку порівняння та зворотних перестановок, вихід якого підключений до другого входу блоку виправлення стирання, при цьому другий вихід блоку прийому підключений до першого входу виправлення блоку стирання.

Розглянемо на прикладі коду Хеммінга (7, 4, 3) з істиною матрицею, що породжує G виду:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Стовпці істиною матриці G нумеруються від 1 до 7 зліва направо. Нехай передавач передає інформаційний вектор Vінф = 1010, тоді канал зв'язку буде відправлений вектор Vкан = Vінф × G =1010011. Нехай вектор помилок Ve має вигляд Ve =1100100. У ході фіксації вектора прийому Vпр в блоці прийому 1 і вироблення для кожного біта цього вектора м'яких рішень в

блоці м'яких рішень символів 2 в накопичувачі оцінок 3 фіксується послідовність жорстких рішень символів і відповідних цілих МРС виду:

$$V_3 = \begin{matrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 3 & 4 & 5 & 6 & 4 & 7 & 7 \end{matrix}$$

Послідовність МРС у блоці 2 формується за правилом $\lambda_i = \left\lfloor \frac{\lambda_{max}}{p\sqrt{E_в}} \cdot Z \right\rfloor$,

де p – інтервал стирання; $E_в$ – енергія сигналу, що припадає однією інформаційний біт; Z – рівень прийнятого модульованого параметра (сигналу); λ_{max} – фіксована оцінка МРС з максимальним значенням, як правило, що визначається конструктором декодера.

Після цього відбувається об'єднання номерів негативних та позитивних рішень, що ранжуються. Порівнюючи значення з ранжированными позитивними рішеннями, декодер знаходить аналогічну комбінацію в пам'яті і приступає до формування матриці породжувальної матриці еквівалентного коду.

Запропонований метод повною мірою використовує властивість лінійних перетворень матриць і скорочує обсяг пам'яті для зберігання еталонних матриць в $k! \times (n-k)$ разів. При цьому максимально використовується введена в код надмірність і виключаються такі матричні операції як обчислення визначників і подальший пошук матриць еквівалентних кодів, що породжують, і подальшого приведення їх до систематичної форми.

Застосування цього принципа дозволяє створити в пам'яті декодера об'єктивний образ реальних команд, зміст яких вимагатиме додаткових зусиль для розкриття суті команди.

У результаті отримуємо зашифрований канал зв'язку, який забезпечуватиме безпечну роботу БПЛА від GPS-спуфінгу.