УДК 621.39

СЦЕНАРІЇ ПРОТИДІЇ ВПЛИВУ НАВМИСНИХ ЗАВАД НА КАНАЛИ ЗВ'ЯЗКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Кайденко М.М.
Навчально-науковий інститут телекомунікаційних систем
КПІ ім. Ігоря Сікорського, Україна
E-mail: kkk610@ukr.net

SCENARIOS FOR COUNTERACTING THE INFLUENCE OF INTENTIONAL INTERFERENCE ON COMMUNICATION CHANNELS OF UNMANNED AERIAL VEHICLES

This article presents scenarios for the impact of various types of intentional interference on the UAV communication channel and qualitative estimates of the measured parameters. Based on the presented qualitative assessments, algorithms for detecting and counteracting the influence of intentional interference on the UAV control channel can be built.

Захист каналу передачі даних безпілотного літального апарату (БПЛА) є першочерговим завданням для забезпечення протидії атакам на БПЛА. При цьому треба враховувати, що навіть використання найбільш захищених від впливу навмисних перешкод видів модуляції з розширенням спектру не гарантує захисту такого каналу. У роботах [1-3] було запропоновано архітектурне рішення з використанням двох каналів у різних діапазонах частот для каналу управління БПЛА. При цьому інформація в обох каналах передається одночасно з повним дублюванням, що має підвищити стійкість такого каналу до впливу навмисних перешкод.

В роботі [4] було описано поріг опору заваді (*anti-jam margin*), який визначає стійкість системи до спроб подавлення сигналу. Незважаючи на те, що використання цього терміну не завжди коректне, його можна застосувати у загальному випадку для позначення запасу міцності проти конкретної навмисної завади.

Для традиційного варіанту системи зв'язку, на який впливає навмисна завада anti-jam margin можна описати як:

$$M_{AJ} = \left(\frac{E_b}{(N_0 + J)}\right)_{\text{Received}} - \left(\frac{E_b}{(N_0 + J)}\right)_{\text{Required}} \quad (1)$$

Для варіанту, запропонованого в [1-3] з двома каналами прийому, в яких передається дубльована інформація, *anti-jam margin* можна представити як:

$$M_{AJ} = \max(M_{AJ\_Channel1}, M_{AJ\_Channel2}) \quad (2)$$

Таким чином, у разі впливу навмисних завад тільки на один з каналів, anti-jam margin буде максимальним і обмежуватися лише ненавмисними завадами в діапазоні роботи каналу, в якому відсутні навмисні завади. У разі впливу навмисних завад на обидва канали прийому для забезпечення високої достовірності передачі інформації в каналі управління і, відповідно, «живучості» каналу зв'язку БПЛА і самого БПЛА, достатньо забезпечити

достатній *anti-jam margin*, хоча б в одному з каналів прийому.

Незважаючи на те, що вирази (1,2) досить інформативно описують *anti-jam margin* у разі впливу на канал зв'язку енергетичних завад, запропоноване архітектурне рішення матиме аналогічний ефект і при впливі на канал зв'язку структурованих завад. При цьому наступним дуже важливим завданням тракту прийому є розпізнавання наявності в каналі зв'язку навмисних перешкод. У разі впливу енергетичної завади (як шумової, так і структурованої) це завдання не є особливо актуальним, оскільки навмисна завада призводить тільки до втрати управління БПЛА оператором, при цьому вона легко детектується. Засобом протидії впливу такої завади може бути переведення БПЛА в автономний режим польоту. У разі впливу імітаційної завади типу *replay attacks*, або *false data injection attack* ситуація стає неоднозначною, тому дуже важливо правильно визначити канал, на який впливає навмисна завада і таким чином здійснюється атака на БПЛА.

Для ефективної протидії впливу навмисних завад необхідно детектувати цю заваду та, по можливості, класифікувати її з метою правильного вибору та активації оптимального алгоритму протидії. Сучасний приймач має кілька засобів оцінки стану каналу зв'язку: рівень прийнятого сигналу (RSSI - Received Signal Strength Indication), відношення сигнал шум (SNR - Signal-to-noise ratio), коефіцієнт помилок (BER- Bit Error Rate). Показник рівня прийнятого сигналу RSSI визначає кількісну характеристику прийнятого сигналу в певній смузі частот, при цьому не визначається чи сигнал є корисним, це сигнал завади, або це суміш сигналу та завади. Відношення потужності прийнятого сигналу до потужності шуму SNR визначає якість прийнятого корисного сигналу за умови, що цей сигнал корисний (детектується) і приймається суміш сигналу та перешкоди, при цьому не конкретизуючи тип перешкоди. Вимірювання BER (підрахунок кількості помилок на інтервалі кадру N_{error}) можливе в каналах зв'язку з завадостійким кодуванням з прямою корекцією помилок (FEC - Forward Error Correction) і дозволяє точніше визначати якість прийнятого сигналу в порівнянні з SNR, оскільки визначає якість прийнятої інформації. Зазначене вище вказує на те, що для визначення присутності навмисної завади, її класифікацію та ефективну протидію її впливу, в загальному вигляді необхідно мати ще мінімум один ступінь свободи. Такий ступінь свободи може бути досягнутий додатковими вимірами, або (і) архітектурними рішеннями відносно побудови системи зв'язку. Наявність третього ступеня свободи при використанні запропонованих у [1-3] архітектурних рішень дозволяє будувати алгоритми детектування навмисних завад та алгоритми протидії впливу таких завад на систему зв'язку БПЛА.

У таблиці 1 наведено сценарії з якісними оцінками, на основі яких можуть будуватися алгоритми детектування навмисних завад та алгоритми протидії впливу таких завад на канал управління БПЛА. Передбачається, що для роботи алгоритмів використовуються усереднені параметри, при цьому довжина інтервалу усереднення вибирається кратною довжиною одного кадру даних, що дозволяє виключити з розгляду швидкі завмирання в каналі зв'язку, що виникають у випадку наявності частотно-селективних завмирань. Крім того,

потужності в каналах зв'язку повинні бути обрані таким чином, щоб забезпечити однаковий енергетичний потенціал в обох каналах, що буде використано як один із критеріїв при детектуванні навмисної завади.

Сценарії визначені за умови, що потенційний вплив навмисної завади на канал управління виявлено. Найточнішою первинною ознакою виявлення є контроль відмінності інформаційних повідомлень у двох каналах зв'язку:

$$Jam\_d = XOR\left(Message_{Channel1}, Message_{Channel2}\right) \quad (3)$$

Якщо Jam_d=1, то ймовірно, що на один із каналів зв'язку в каналі управління може здійснюватися навмисна атака.

Таблиця 1. Сценарії впливу навмисних завад, їх характеристика та ознаки для детектування.

Сценарій	Тип завади	Опис ознаки завади
1	Енергетична шумова завада, широкосмугова	В одному з каналів N_{error} >>1; $RSSI_{Chan\_error}$ > $RSSI_{Chan\_correct}$; SNR_{Chan_error}< $SNR_{Chan\_correct}$; $RSSI_{Chan\_error+-BW}$~$RSSI_{Chan\_error}$
2	Енергетична шумова завада, вузькокосмугова	В одному з каналів N_{error} >>1; $RSSI_{Chan\_error}$ > $RSSI_{Chan\_correct}$; SNR_{Chan_error}< $SNR_{Chan\_correct}$; $RSSI_{Chan\_error+-BW}$<<$RSSI_{Chan\_error}$
3	Енергетична структурована завада	В одному з каналів N_{error} >>1; $RSSI_{Chan\_error}$ >= $RSSI_{Chan\_correct}$; SNR_{Chan_error}<=$SNR_{Chan\_correct}$; Відсутність синхронізації кадрів (пакетів)
4	Імітаційна завада типу атаки повторення (replay attack)	N_{error_Chan1} ~ N_{error_Chan2}; $RSSI_{Chan1}$>> $RSSI_{Chan2}$; SNR_{Chan1}>= SNR_{Chan2} ; Неправильність порядку слідування імітаційних вставок.
5	Імітаційна завада заміщення (false data injection attack)	N_{error_Chan1} ~ N_{error_Chan2}; $RSSI_{Chan1}$>> $RSSI_{Chan2}$; SNR_{Chan1}>= SNR_{Chan2} ; Спостереження змін на довгому інтервалі часу.

Література

1. Kaidenko M., Kravchuk S. (2021) Autonomous Unmanned Aerial Vehicles Communications on the Base of Software-Defined Radio. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_16
2. M. M. Kaidenko and S. O. Kravchuk, "Anti-Jamming System for Small Unmanned Aerial Vehicles," *2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD)*, 2021, pp. 1-4, doi: 10.1109/APUAVD53804.2021.9615403.
3. M. Kaidenko and S. Kravchuk, "Creation of communication system for unmanned aerial vehicles using SDR and SOC technologies," *2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, Ukraine, 2019, pp. 1-4, doi: 10.1109/UkrMiCo47782.2019.9165422.
4. B. Sklar, Digital Communications: Fundamentals and Applications, Second Edition, Prentice-Hall, Upper Saddle River, NJ, 2001