

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ МРТСП ДЛЯ ПІДВИЩЕННЯ ЖИВУЧОСТІ WIFI КАНАЛІВ УПРАВЛІННЯ БПЛА В УМОВАХ ВПЛИВУ НАВМИСНИХ ТА НЕНАВМИСНИХ ЗАВАД

Гетьман О.В., Кайдено М.М., Роскошний Д.В.

Навчально-науковий інститут телекомунікаційних

систем КПІ ім. Ігоря Сікорського, Україна

E-mail: kkk610@ukr.net

USING MPTCP TECHNOLOGY TO INCREASE THE SURVIVABILITY OF WIFI UAV CONTROL CHANNELS UNDER THE INFLUENCE OF INTENTIONAL AND UNINTENTIONAL INTERFERENCE

This paper proposes the use of MPTCP technology to create UAV control and communication channels. Such control channels will be protected from the influence of various kinds of attacks on the UAV. Features of technology and flow control mechanisms in MPTCP are considered. The proposed solution was tested in laboratory conditions on a test stand using the appropriate software.

В останні роки безпілотні літальні апарати (БПЛА) все більше використовуються для різних застосувань як у військових цілях, так і в цивільних. Однак все більше поширення застосування БПЛА збільшує й проблеми безпеки. Особливо це стосується вразливості каналів управління БПЛА до впливу різноманітних типів атак на них. В роботах [1-4] було запропоновано комплекс рішень по підвищенню стійкості каналів управління та зв'язку БПЛА до впливу на них навмисних та ненавмисних завад, які базуються на побудові каналів управління з використанням двох каналів зв'язку в двох діапазонах частот.

Існує цілий клас безпілотних літальних апаратів, які використовують технології WiFi для організації каналів управління, телеметрії та передачі даних. Для цих БПЛА також можливе використання запропонованих в [1-4] рішень з одночасною роботою в двох діапазонах частот - 2,4 ГГц та 5 ГГц. В таких безпілотних апаратах для здешевлення використовуються стандартні WiFi модулі та програмне забезпечення управління на базі Embedded Linux. Однак застосування вискоєфективних алгоритмів протидії впливу навмисних завад має істотні недоліки в силу існуючого обмеження на кількість доступних параметрів каналу зв'язку, якими визначається стан каналу. По суті використання стандартних WiFi модулів, що побудовані на недорогих чіпсетах, одночасно з використанням стандартних драйверів Linux обмежує можливості цих алгоритмів внаслідок невеликої кількості доступних параметрів для аналізу стану каналу зв'язку [5]. Так, доступними параметрами про стан каналу для інтерфейсу *Interface wlp2s0*, який виводиться командою *iw dev* після введення команди *iw dev wlp2s0 link* є: рівень прийнятого сигналу та швидкість передачі в каналі. Введення команди *iw dev wlp2s0 station dump* дозволяє додатково визначити середній рівень прийнятого сигналу, кількість повторних запитів на передачу пакетів: та кількість втрачених пакетів при передачі. Цих параметрів

достатньо буде лише для того, щоб визначити характеристику прийнятого сигналу за рівнем прийнятого сигналу, а якість сигналу визначається тільки за кількістю втрачених пакетів. Таким чином використання обмеженої кількості параметрів буде достатнім лише для протидії впливу завад глушення каналу. Для протидії впливу іншим видам завад потрібні інші алгоритмічні рішення. Найбільш ефективним є використання технології багатомаршрутного TSP (Multipath TSP).

Технологія MPTSP — одне з найважливіших розширень TSP, що дозволяє використання кількох шляхів передачі для TSP-з'єднання. У MPTSP кінцеві хости передають дані з кількох підпотоків TSP одночасно по одному з'єднанню. MPTSP може досить ефективно використовувати ресурси смуги пропускання для підвищення ефективності передачі. Також ця технологія забезпечує стійкість організованого таким чином каналу зв'язку завдяки багатоканальній передачі даних. У додатках та рішеннях, де важлива швидкість передачі даних та надійність, MPTSP може бути найбільш перспективним підходом до вирішення цих проблем у випадку, коли інші методи є недоступними.

MPTSP розроблено з урахуванням таких моментів: підвищення пропускної спроможності; не створення негативного впливу на звичайний TSP; балансування навантаження і підвищення відмовостійкості за рахунок зміщення потоків з перевантаженого, або несправного шляху, на найменший перевантажений шлях.

Застосуванню MPTSP для організації зв'язку в рухомих засобах присвячено велику кількість досліджень, при цьому велика увага присвячується саме автомобільним мережам. Відзначається, що вибір правильних шляхів передачі дуже важливий. Дослідження щодо багатошляхової маршрутизації [6] проводилися для забезпечення ефективності і надійності шляхів передачі. Закордонні дослідники також проводять дослідження, відносно застосування MPTSP технологій в безпілотних літальних апаратах. В роботі [7] було запропоновано безпілотну літальну систему, яка використовує кілька взаємодіючих БПЛА.

MPTSP має два важливі механізми керування потоком, а саме контроль перевантаження і планувальник пакетів. Контроль перевантаження відповідає за контроль викликаного навантаження на мережу щоб уникнути перевантаження мережі. Традиційний TSP з одним маршрутом використовує алгоритм уникнення перевантажень, який включає схему повільного запуску та схему адитивного збільшення/мультиплікативного зменшення (AIMD — additive increase/multiplicative decrease).

Механізм контролю перевантаження MPTSP був розроблений і стандартизований [8]. З іншого боку, планувальник відповідає за розповсюдження даних кількома шляхами. Належний планувальник може покращити хорошу пропускну здатність (пропускна здатність на рівні програми), або забезпечити високу надійність передачі інформації навіть в умовах впливу на канал навмисних завад. Однак, на відміну від контролю перевантаження MPTSP, планувальник ще не стандартизований. Найбільш

часто використовуваними планувальниками є циклічний планувальник (RR - round robin) і найкоротший згладжений (RTT -Round Trip Time), чи (SRTT - Shortest Smoothed RTT). Планувальник реалізації MPTCP ядра Linux [9] базується на SRTT. Останніми роками було проведено багато досліджень щодо контролю перевантажень і планувальника MPTCP, є також деякі дослідження, які поєднують контроль перевантаження MPTCP і планувальник разом для покращення продуктивності та якості передачі.

Для каналу зв'язку та управління БПЛА, який реалізується на базі двох модулів WiFi для діапазонів частот 2,4 та 5 ГГц, що працюють під управлінням операційної системи на базі Linux один з варіантів MPTCP може бути реалізований як в розроблений в відкритому проекті [10].

Процес створення та реалізації MPTCP було перевірено та реалізовано в лабораторних умовах з використанням тестового стенду. Для перевірки було встановлено відповідну версії Linux, яка використовується в якості Embedded Linux, версію MultiPath TCP. Встановлена версія Linux відповідала також версії для Raspberry PI, яка дуже часто використовується в малогабаритних БПЛА. В якості робочої станції в стенді було використано ноутбук, в якому було встановлено два модулі WiFi для діапазонів частот 2,4 та 5 ГГц.

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. Mykola M. Kaidenko, Serhii O. Kravchuk "PROTECTION AGAINST THE EFFECT OF DIFFERENT CLASSES OF ATTACKS ON UAV CONTROL CHANNELS" Information and Telecommunication Sciences, No.1, pp. 35-43, 2022. <https://doi.org/10.20535/2411-2976.12022.35-43>
4. Kaidenko, M., Kravchuk, S. (2023). Principles of Constructing Communication and Control Systems Protected from the Effects of Jamming Attacks for Small-Sized Unmanned Aerial Vehicles. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. https://doi.org/10.1007/978-3-031-16368-5_20
5. Network configuration - Режим доступу: https://wiki.archlinux.org/title/Network_configuration
6. Zhang, T.G.; Zhao, S.; Cheng, B. Multipath Routing and MPTCP-Based Data Delivery over MANETs. IEEE Access 2020, 8, 32652–32673.
7. Chirwa, R.M.N.; Lauf, A.P. Performance improvement of transmission in Unmanned Aerial Systems using multipath TCP. In Proceeding of the 2014 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Noida, India, 15–17 December 2014; pp. 19–24.
8. Raiciu, C.; Handley, M.; Wischik, D. Coupled Congestion Control for Multipath Transport Protocols; RFC6356; IETF: Fremont, CA, USA, 2011.
9. Multipath TCP in the Linux Kernel. Available online: <https://www.multipath-tcp.org/> (accessed on 3 October 2020).
10. MultiPath TCP - Linux Kernel implementation - Режим доступу: <https://multipath-tcp.org/pmwiki.php/Main/HomePage>