УДК 621.396.1

ПРОЦЕДУРИ АУТЕНТИФІКАЦІЇ ТЕРМІНАЛІВ ТА ПРОМІЖНИХ МОДУЛІВ НА БАЗІ РОЮ БПЛА ЯК ЧАСТИНИ МЕРЕЖІ РАДІОДОСТУПУ 5G

Кравчук С.О., Кравчук І.М.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. І. Сікорського, Україна
E-mail: sakravchuk@ukr.net

PROCEDURES FOR AUTHENTICATION OF TERMINALS AND INTERMEDIATE MODULES BASED ON A SWARM OF UAVS AS PART OF A 5G RADIO ACCESS NETWORK

Authentication is a fundamental property that allows a UAV network to establish secure communication between its core components. This allows for the authentication and identification of UAVs. The purpose of this work is to carry out an analytical review of the possibilities of creating authentication procedures for a swarm of UAVs/drones, taking into account the peculiarities of swarm formation and the requirements for 5G NR.

Широке використання безпілотних літаючих апаратів (БПЛА) для різноманітних цивільних і комерційних застосувань, а також повсюдне безпроводове підключення мереж 5G і 6G можуть вимагати передових заходів безпеки для запобігання несанкціонованому доступу до конфіденційних даних [1-4]. Так само, встановлюючи заходи безпеки для мереж БПЛА, слід враховувати такі характеристики, як висока масштабованість, різноманітність пристроїв і висока мобільність.

Автентифікація (Authentication): автентифікація є фундаментальною властивістю, яка дозволяє мережі БПЛА встановлювати безпечний зв’язок між її основними компонентами. Це дозволяє автентифікувати та ідентифікувати БПЛА, які беруть участь у польоті. Надійність кожного БПЛА перевіряється за допомогою цифрового підпису і лише автентифіковані БПЛА можуть брати участь у польоті. Автентифікація також захищає мережу БПЛА від зловмисників, які видають себе за законні БПЛА.

Аутентифікація БПЛА може додатково захистити канал зв’язку, запобігаючи уособленню та повторним атакам. Розробка схем контролю доступу БПЛА, таких як механізми авторизації та автентифікації, залишається складною проблемою для дослідження в мережах БПЛА. Дійсно, будь-які неавтентифіковані БПЛА не повинні брати участь у польотних місіях для збору даних з інших БПЛА в мережі.

Протокол автентифікації об’єкта — це процес у режимі реального часу, який забезпечує впевненість у тому, що об’єкт, який аутентифікується, працює в той момент, коли цей об’єкт виконав певну дію з початку виконання протоколу.

Відоме рішення для аутентифікації одного БПЛА/дрона з використанням нової 5G радіомережі (NR) вимагає виконання двох кроків. Перший етап

охоплює аутентифікацію між дроном і базовою мережею 5G, а другий етап - аутентифікацію між дроном і станцією управління дроном. Неможливо аутентифікувати кожен дрон у рої за допомогою поточного рішення без затримки. Ключі аутентифікації між базовою станцією (BS) та користувальницьким обладнанням (UE) мають бути передані нової BS під час виконання передачі обслуговування. Зграї дронів дуже мобільні і вимагають кількох перемикань із BS на нову BS.

Важливо також торкнутися тут деяких конкретних аспектів, які тісно пов’язані з моделлю співпраці роїв і впливають на алгоритми, що лежать в основі місій. На додаток до звичайних проблем із шифруванням та автентифікацією (всередині рою та для зв’язку між рою та GCS), ми стикаємося з двома основними додатковими проблемами.

Рій за своєю природою має динамічну структуру, і це піднімає проблему ненадійних кордонів. Рій - це система, що розвивається: БПЛА можуть приєднатися та залишити будь-коли, або з запланованих причин, або через настання несподіваної події. БПЛА може приєднатися до зграї замість того, хто покидає, або додати деяку додаткову потужність до загальної системи. Таким чином, має бути механізм для запобігання вторгненню шкідливого БПЛА. На жаль, оскільки зграї повинні підтримувати стійкість і оскільки вони динамічні, у зграї немає стабільного БПЛА.

Тому метою даної роботи є проведення аналітичного огляду можливостей створення процедур автентифікації для рою БПЛА/дронів з урахуванням особливостей формування рою та вимог до 5G NR.

Спільне використання ключів автентифікації для кожного БПЛА, як описано в 5G NR, не масштабується для груп БПЛА. У [5] була змодельована схема групової аутентифікації для нового БПЛА та аутентифікація БПЛА 5G NR. БПЛА у зграї утворюють три підгрупи, які мають різні обов'язки. Охоронні БПЛА/дрони (guard drones) - це дрони, в обов'язки яких входить відстеження догляду та приєднання дронів, а також аутентифікація нових учасників у зграях. Мережеві операції виконуються сітковими дронами (network drones). Основний сервіс надають сервісні дрони (service drones). Основні переваги запропонованого методу можна резюмувати так: 1) груповий ключ розподіляється між дронами в рої, щоб забезпечити безпечний канал зв'язку, і пропонується рішення поділитися груповим ключем із новими учасниками; 2) аутентифікація нового дрона, що бере участь у рої, вимагає двох кроків, якщо використовується рішення 5G NR. Першим кроком є підтвердження нового дрона базовою мережею, а наступним кроком є аутентифікація через станцію керування дронами. Пропонований метод пропонує рішення для групової аутентифікації, яке має кращі тимчасові та комунікаційні складності, ніж 5G NR.

У [6] представлена безпечна та спрощена схема аутентифікації для повітряної мережі з кількох БПЛА. Запропонований підхід заснований на фізичній, неклонуємої функції, яка надійно вбудована на згадку про вузли БПЛА. Запропонований підхід забезпечує безпечну роботу мережі БПЛА,

споживаючи при цьому менше бортових ресурсів, таких як заряд батареї, обчислювальна потужність та пам'ять.

В [7] запропоновано новий підхід для віддаленої ідентифікації роїв дронів. Для ефективного процесу ідентифікації між зграєю дронів та GCS кожен дрон Reader у регіоні збирає ідентифікаційну інформацію рою дронів та передає її до наземної станції для перевірки. Пропонований протокол ідентифікації скорочує час перевірки рою дронів за рахунок використання пакетної перевірки для одночасної перевірки множини дронів у рої дронів.

Можна використовувати протокол аутентифікації та узгодження ключів для встановлення безпечного зв'язку між дронами та ZSP (Zone Service Provider: IoT та IoD) у незахищеному середовищі. Проте одночасна аутентифікація великої групи дронів за допомогою ZSP призведе до серйозного навантаження сигналів аутентифікації, що неминуче погіршує якість обслуговування (QoS) систем IoD. Для правильного вирішення вищезгаданих проблем у [8] пропонується полегшений протокол групової автентифікації, який називається liteGAP (Lightweight Group Authentication Protocol).

Література

1. Swarm of UAVs for Network Management in 6G: A Technical Review / M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywiołek, I. Ullah // IEEE Transactions on Network and Service Management, 20(1), p. 741-761 (2023), http://dx.doi.org/10.1109/TNSM.2022.3213370
2. Kravchuk S., Afanasieva L. Formation of a wireless communication system based on a swarm of unmanned aerial vehicles // Information and Telecommunication Sciences. - 2019. - No 1. - 11-18 p. DOI: https://doi.org/10.20535/2411-2976.12019.11-18
3. Kaidenko M., Kravchuk S. 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. pp. 289-302 (2019), https://doi.org/10.1007/978-3-030-58359-0_16
4. Kaidenko M., Kravchuk S. Protection against the effect of different classes of attacks on UAV control channels // Information and Telecommunication Sciences. – No. 1 (2022) . – p. 35-43, DOI: https://doi.org/10.20535/2411-2976.12022.35-43
5. Authentication and Handover Challenges and Methods for Drone Swarms / Y. Aydin, G. K. Kurt, E. Ozdemir, H. Yanikomeroglu // IEEE Journal of Radio Frequency Identification, Vol. 6, p. 220 – 228 (2022). https://doi.org/10.1109/JRFID.2022.3158392
6. A Lightweight Authentication Scheme for a Network of Unmanned Aerial Vehicles (UAVs) by Using Physical Unclonable Functions / Alkatheiri, M.S., Saleem, S., Alqarni, M.A., Aseeri, A.O., Chauhdary, S.H., Zhuang, Y. A. // Electronics 2022, 11, 2921. https://doi.org/10.3390/electronics11182921
7. Efficient Remote Identification for Drone Swarms / K.-M. Seo, J. Kim, S. Lee, J.-W. Kwon, S.-H. Seo // Computers, Materials & Continua 2023, *76*(3), 2937-2958, http://dx.doi.org/10.32604/cmc.2023.039459
8. liteGAP: Lightweight Group Authentication Protocol for Internet of Drones Systems / C. Pu, C. Warner, K.-K. R. Choo, S. Lim, I. Ahmed // IEEE Transactions on Vehicular Technology (2023) https://doi.org/10.1109/tvt.2023.3335839