

АНАЛІЗ АРХІТЕКТУРИ, ТЕХНОЛОГІЙ І ВИКЛИКІВ ЛІТАЛЬНИХ AD HOC МЕРЕЖ

Валуйський С.В., Пономаренко О.М.

*Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна*

E-mail: ponomarenko.alexandra@lil.kpi.ua, valuiskyi.stanislav@lil.kpi.ua

ANALYSIS OF THE ARCHITECTURE, TECHNOLOGIES AND FUTURE CHALLENGES OF FLYING AD HOC NETWORKS

This work is focused on analyzing the architecture, technologies, and challenges of Flying Ad Hoc Networks (FANETs). The study involves a detailed examination of the network structure, routing protocols, wireless communication technologies, and the main technical and security challenges faced by FANETs. The research also explores potential solutions to improve the efficiency and reliability of these networks.

Літальні Ad Hoc мережі (FANETs) є динамічними мережами, що складаються з безпілотних літальних апаратів (БПЛА), які можуть самоорганізовуватися для виконання різноманітних завдань. Вони знаходять застосування у військовій, цивільній та комерційній сферах, зокрема для моніторингу, пошуково-рятувальних операцій, доставки вантажів та інших задач. Основною перевагою FANETs є їхня здатність працювати в умовах, де традиційні мережі недоступні або неефективні.

Мета роботи. Основна мета роботи полягає в аналізі архітектури, технологій та викликів літальних Ad Hoc мереж. Для цього використовуються дослідження архітектурних рішень, протоколів маршрутизації, технологій бездротового зв'язку та основних проблем, пов'язаних із функціонуванням FANETs.

Огляд архітектури, технологій та викликів FANETs [1-6].

1. Архітектура FANETs. FANETs можуть мати різні типи архітектур, включаючи централізовану, децентралізовану та гібридну. Централізована архітектура передбачає наявність головного вузла, який керує всіма іншими БПЛА. Децентралізована архітектура дозволяє кожному вузлу приймати самостійні рішення, що підвищує гнучкість мережі. Гібридна архітектура поєднує переваги обох підходів.

2. Технології бездротового зв'язку. Для зв'язку між БПЛА

використовуються Wi-Fi, Bluetooth, Zigbee, LTE/5G, LoRaWAN та спеціалізовані радіопротоколи. LPWAN (Low Power Wide Area Network) є перспективним варіантом для енергоефективного зв'язку дронів, особливо у віддалених районах, оскільки забезпечує зв'язок на великі відстані з низьким енергоспоживанням.

3. Протоколи маршрутизації. Ефективна маршрутизація є ключовим аспектом функціонування FANETs. Використовуються:

- Проактивні протоколи (OLSR, DSDV) – швидке реагування, але високе використання смуги пропускання через постійне оновлення таблиць маршрутів.
- Реактивні протоколи (AODV, DSR) – економія ресурсів, оскільки маршрути встановлюються лише за потреби, однак може збільшуватися затримка через необхідність їхнього пошуку.
- Гібридні протоколи (ZRP, HWMP) – поєднують переваги обох підходів, наприклад, використовують проактивний метод для локальних вузлів і реактивний – для віддалених.

4. Технічні виклики. FANETs стикаються з низкою технічних викликів, таких як обмежена енергоемність БПЛА, висока мобільність вузлів та нестабільність зв'язку. Для подолання цих проблем використовуються методи оптимізації енергоспоживання, динамічного маршрутизації та покращення якості зв'язку.

5. Забезпечення безпеки. Оскільки FANETs часто використовуються для передачі конфіденційних даних, питання безпеки є критичним. Методи шифрування, аутентифікація вузлів і захист від атак відіграють ключову роль у надійності мережі. Зокрема, розглядається використання блокчейн-технологій (Aerial Blockchain) для захисту зв'язку між дронами, що дозволяє створювати децентралізовану та стійку до атак систему автентифікації та перевірки цілісності даних.

6. Інтеграція з іншими мережами. FANETs можуть бути інтегровані з іншими типами мереж, такими як IoT (Internet of Things) та VANETs (Vehicular Ad Hoc Networks). Це дозволяє створювати комплексні системи, здатні вирішувати складніші завдання, такі як моніторинг великих територій або управління транспортними потоками. Інтеграція з IoT дозволяє використовувати дані з різних джерел для покращення ефективності роботи мережі.

Висновок. Робота спрямована на аналіз архітектури, технологій та викликів літальних Ad Hoc мереж. Дослідження показало, що FANETs мають великий потенціал для використання у різних сферах, однак їх ефективне функціонування вимагає подолання низки технічних та організаційних проблем. Аналіз показав, що гібридна архітектура є оптимальним варіантом, оскільки вона поєднує централізоване управління та автономність вузлів, що підвищує гнучкість та масштабованість FANETs. Гібридні протоколи маршрутизації демонструють найкращу ефективність в умовах динамічної топології мережі.

Для забезпечення стабільного зв'язку в умовах високої мобільності FANETs найбільш перспективними є LTE/5G та спеціалізовані радіопротоколи. Додатково, використання Wi-Fi, Bluetooth 5 та LPWAN дозволяє покращити ефективність енергоспоживання.

Важливим напрямком є безпека FANETs, де сучасні криптографічні методи, аутентифікація вузлів та технологія Aerial Blockchain дозволяють підвищити рівень захищеності переданих даних.

Перспективи подальших досліджень включають:

- Інтеграцію FANETs з IoT та VANETs для створення більш комплексних систем.
- Використання штучного інтелекту для автономного управління мережею.
- Впровадження квантових технологій шифрування для підвищення рівня безпеки.

Література

1. İlker Bekmezci, Ozgur Koray Sahingoz, Şamil Temel. Flying Ad-Hoc Networks (FANETs): A survey. *Ad Hoc Networks*. 11(3):1254-1270, 2013.
2. Jennifer S. Raj. A Novel Hybrid Secure Routing for Flying Ad-hoc Networks. *Journal of Trends in Computer Science and Smart Technology (TCSST)*, Vol. 02, No. 03, 155-164, 2020.
3. Sunil Kr Maakar, Yudhvir Singh, Rajeshwar Singh. Considerations and Open Issues in Flying Ad Hoc Network. *International Journal of Scientific Engineering and Research (IJSER)*, Vol. 5, Issue 7, 2017.
4. Yixin He, Xiao Tang, Ruonan Zhang, Xiaojiang Du, Deyun Zhou, Mohsen Guizani. A Course-Aware Opportunistic Routing Protocol for FANETs. *IEEE Access*, 7, 144303-144312, 2019.
5. Macaw Publications. Blockchain-Enhanced Secure Routing in FANETs: Integrating ABC Algorithms and Neural Networks for Attack Mitigation. *Smart Mobile Review Journal*, 2022. URL: <https://www.macawpublications.com/Journals/index.php/SMRJ/article/view/55>