

Секція 1

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ЛІТАЮЧОЇ МЕРЕЖІ З БПЛА

Сіроклин О. В.

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»

Науковий керівник: Ключніков І. М.

Актуальність. Розвиток безпілотних літальних апаратів (БПЛА) відкриває нові можливості для їхнього використання в різних сферах, таких як моніторинг навколишнього середовища, рятувальні операції та військові місії. Одним із перспективних напрямів є застосування літаючих бездротових мереж (англ. Flying Ad Hoc Network - FANET) як методу для розгортання безперервної передачі інформації між двома об'єктами [1, 2]. Це дозволяє створювати ефективні комунікаційні мережі, які здатні адаптуватися до змінних умов експлуатації, забезпечуючи надійний зв'язок між різними пристроями [3]. Однак, з розширенням застосування БПЛА та FANET виникають нові виклики, пов'язані з безпекою [4]. Кіберзагрози, такі як перехоплення, модифікація або блокування інформації, можуть суттєво зашкодити функціонуванню мережі [5]. Відсутність належних заходів безпеки може призвести до критичних наслідків, включаючи втрату даних, порушення координації дій та небезпеку для людей.

Метою даної роботи є дослідження загроз безпеки для мереж FANET.

Це включає:

- аналіз критичних ресурсів FANET;
- розробку моделей загроз для визначення потенційних вразливостей та методів їх подолання;
- опис моделі порушника, яка включає типи можливих зловмисників, їхні наміри, кваліфікаційні рівні та фізичні можливості.

Основні положення. Було проведено огляд технологій для роботи літаючих мереж, що включає аналіз структурних особливостей і можливостей FANET. Розглянуто різні види підтримки заряду БПЛА, можливі типи зв'язку, вибір яких визначає швидкість і надійність передачі даних, а також вплив мережевих топологій на продуктивність FANET. Було розроблено моделі загроз і порушника, які дозволяють ідентифікувати вразливі елементи мережі. Модель загроз визначає можливі цілі та методи атак, тоді як модель порушника описує потенційних зловмисників, їхні можливості та мотиви. Результати аналізу підкреслюють необхідність використання комплексних заходів безпеки, зокрема технологічних та організаційних, для підвищення захищеності FANET.

Висновки. Результати дослідження підкреслюють важливість комплексного підходу до аналізу загроз безпеки для FANET. Розроблені моделі загроз і порушника допомагають виявити вразливі елементи мережі та прогнозувати можливі сценарії атак. Визначення критичних ресурсів, таких як конфіденційність і цілісність даних, є ключовим для розробки адекватних заходів захисту. Необхідно впроваджувати як технологічні, так і організаційні рішення, що підвищують захищеність FANET та забезпечать надійність його функціонування в умовах зростаючих кіберзагроз.

Список літератури

1. Morgenthaler S., Braun T., Zhao Z., Staub T., Anwander M. UAVNet: A mobile wireless mesh network using Unmanned Aerial Vehicles. Proceedings of the IEEE Global Communications Conference (GLOBECOM). 2012. DOI: <https://doi.org/10.1109/GLOCOMW.2012.6477825>.
2. Ullah H., McClean S., Nixon P., Parr G., Luo C. An Optimal UAV Deployment Algorithm for Bridging Communication. In: 2017 IEEE International Conference on Intelligent Transportation Systems (ITST). 2017. DOI: <https://doi.org/10.1109/ITST.2017.7972194>.
3. I. M. Kliushnikov, H. V. Fesenko, V. S. Kharchenko. Scheduling UAV fleets for the persistent operation of UAV-enabled wireless networks during NPP monitoring. Radioelectronic and computer systems. 2020. No.1 DOI: <https://doi.org/10.32620/reks.2020.1.03>.
4. Ozlem Ceviz, Pinar Sadioglu, Sevil Sen. A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions. arXiv:2306.14281v3, 2023. DOI: <https://doi.org/10.48550/arXiv.2306.14281>.
5. Emmanuel Asituha. A comprehensive overview of privacy, security and performance issues in flying Ad Hoc Networks. World Journal of Advanced Research and Reviews, 2024. DOI: <https://doi.org/10.30574/wjarr.2024.23.1.2166>.

Відомості про авторів

Сіроклин Олександр Віталійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.v.siroklyn@student.csn.khai.edu
 Ключніков Ігор Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., с.н.с, i.kliushnikov@csn.khai.edu