

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Кваліфікаційна наукова
праця на правах рукопису

ВОЙЦЕХОВСЬКИЙ АНДРІЙ ВАЛЕРІЙОВИЧ

УДК 004.056

ДИСЕРТАЦІЯ

«Моделі та методи забезпечення кіберфізичної стійкості мереж дронів»

125 Кібербезпека
12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Войцеховський А.В.

Науковий керівник
Новіков Олексій Миколайович
доктор технічних наук, професор,
член-кореспондент НАН України

Київ – 2026

АНОТАЦІЯ

Войцеховський А.В. Моделі та методи забезпечення кіберфізичної стійкості мереж дронів. – Кваліфікаційна праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2026.

Дисертаційна робота присвячена розробці комплексних моделей та методів захисту від кіберфізичних і кібернетичних загроз для безпечного функціонування мереж БпЛА в умовах динамічних ворожих та несприятливих впливів.

В умовах сучасного поля бою мережі рухомих пристроїв БПЛА відіграють критично важливу роль, дозволяючи дистанційно виконувати поставлені завдання та суттєво зменшуючи ризики для життя військовослужбовців, проте їхня ефективність та виживання постійно перебувають під загрозою через комплексний зовнішній вплив та особливості агресивного середовища. Забезпечення безпеки таких мереж є комплексним завданням, оскільки БПЛА наповнені вбудованими системами з датчиками та передавачами, що робить їх вразливими як до кібернетичних атак у вигляді експлуатації вразливостей програмного забезпечення, так і до кіберфізичних впливів, таких як радіоелектронна протидія, підміна сигналу та робота в умовах складного рельєфу.

У наявних наукових працях зазвичай розглядалися питання доступності мережі БпЛА переважно для цивільних місій, де враховувалися лише траєкторія польоту та розташування будівель, проте фактори, притаманні військовим умовам, залишалися поза увагою дослідників. До таких специфічних факторів належать: вплив потужних комплексів радіоелектронної боротьби супротивника, вплив природного рельєфу на затухання сигналу та специфічна топологія мережі БпЛА, що виникає під час реальних операцій. Водночас стрімкий розвиток інтелектуальних функцій БпЛА, включаючи машинне навчання та складну програмну складову, робить

їх потенційною ціллю для атак через бездротові оновлення та використання вразливих драйверів операційних систем, що створює ризик перехоплення керування усім роєм. Критичний приклад реалізації такої загрози був продемонстрований експлойтом UniPwn у прошивках автономних роботів Unitree, які використовують бездротовий зв'язок. Найбільшу небезпеку становить те, що інфікований апарат може сканувати інші пристрої в радіусі дії мережі та автоматично скомпрометувати їх, створюючи самопоширюваний ботнет.

Метою дисертаційної роботи є вирішення науково-технічної задачі підвищення кіберфізичної стійкості мереж БпЛА шляхом розробки комплексу моделей і методів, що забезпечують збереження доступності каналів зв'язку мережі БпЛА, цілісність і конфіденційність польотних завдань, а також розширення можливостей спостережності за динамікою станів мережі в умовах впливу несприятливих та ворожих факторів.

Поставлена мета досягається через розробку та вдосконалення комплексу моделей і методів керування мереж БпЛА, які, на відміну від існуючих, враховують вплив засобів радіоелектронної протидії каналам зв'язку, топологічні перешкоди та вразливості програмного забезпечення, що дозволяє забезпечити надійне керування мережею БпЛА та гарантувати виконання місій у критичних умовах.

Об'єкт: мережі безпілотних літальних апаратів (БпЛА).

Предмет: моделі та методи дослідження мереж БпЛА в контексті їх кібербезпеки та доступності.

Для протидії цим загрозам автором запропоновано комплекс результатів, що включають моделювання стану мережі БпЛА, просторово-часову оптимізацію розміщення БпЛА та автоматизований пошук вразливостей у зразках програмного забезпечення БпЛА. Фундаментальною складовою дослідження є розроблені моделі функціонування мережі БпЛА на основі апарату звичайних та кольорових мереж Петрі, яка комплексно враховує динаміку кіберфізичних загроз, зокрема вплив пристроїв РЕП різної потужності, топологічні перешкоди та згасання сигналу залежно від відстані. Для моделювання окремого БпЛА розроблено загальну мережу Петрі, яка дозволяє відслідковувати зміну рівня якості сигналу, а для множини пристроїв

побудовано кольорову мережу Петрі.

У цій моделі фішки ідентифікують окремі дрони та рівень їхнього сигналу, динамічно відображаючи переходи між критичними станами, такими як стабільне підключення, втрата зв'язку, потрапляння в зону глушіння, перехід в автономний політ або успішний пошук ретранслятора. Це забезпечує можливість прогностичної аналітики станів мережі БПЛА та візуалізації динаміки зміни сигналу в умовах активного придушення. Числові показники ефективності розроблених моделей Петрі підтверджені під час симуляційного моделювання сценаріїв для групи зі 100 пристроїв протягом шести кроків. Проведений порівняльний аналіз показав, що модель здатна адекватно відображати критичну деградацію системи, коли на 4-му кроці через інтенсивний вплив РЕП кількість апаратів із нульовим рівнем сигналу досягла максимуму у 36 одиниць, а 41 пристрій перейшов у режим автономної навігації. Водночас використання цієї моделі підтвердило високу відновлюваність мережі: на фінальному кроці після виходу із зони дії перешкод 93 пристрої (93% рою) успішно відновили стабільне підключення, що підтвердило логічну коректність розроблених механізмів резервних переходів у мережі Петрі.

Для вирішення задачі оптимального позиціонування мережі БПЛА під час його просування від початкової точки розгортання до цілі в умовах кіберфізичних загроз, автором запропоновано метод на основі генетичного алгоритму та багатокомпонентної цільової функції. Цей метод відрізняється від існуючих рішень врахуванням загроз підміни геолокаційних даних, радіолокаційних перешкод та особливостей рельєфу на основі відкритих наборів даних. Запропонована цільова функція ефективно вирішує проблему балансування впливу ключових конкуруючих факторів: вона одночасно забезпечує мінімізацію відстані до цілі, максимізацію зв'язності комунікаційного ланцюга (уникаючи як ізоляції вузлів, так і їх надмірного скупчення), а також стратегічний обхід зон дії ворожих засобів радіоелектронної боротьби.

Проведений обчислювальний експеримент підтвердив, що генетичний алгоритм забезпечує необхідний баланс між просуванням мережі до цілі та збереженням комунікаційного ланцюга, дозволяючи зменшити значення

цільової функції майже в десять разів за сто ітерацій. Проведений порівняльний аналіз показав, що метод градієнтного спуску демонструє найгірші результати через залежність від початкової точки та застрягання в локальних мінімумах складного рельєфу, внаслідок чого значення цільової функції не вдалося істотно зменшити, а дистанційна похибка становила понад сорок один кілометр. Жадібний послідовний алгоритм показав швидший результат спрацювання в середньому в 0.01 секунди, проте він не здатний правильно корегувати позиції вже розміщених дронів, що призводить до посередніх результатів. Найвищу ефективність продемонстрував генетичний алгоритм, який одночасно оптимізує всю конфігурацію рою протягом ста поколінь. Застосування генетичного алгоритму дозволило істотно зменшити значення цільової функції, що за показником точності є в середньому у 16 разів кращим за жадібний алгоритм та майже у 330 разів перевершує результати градієнтного спуску. Крім того, цей метод дозволив скоротити підсумкову дистанцію маршруту у 56 разів порівняно з жадібним алгоритмом та у понад 500 разів порівняно з градієнтним спуском, забезпечуючи оптимальний баланс між просуванням до цілі та збереженням зв'язку за 0.82 секунди обчислень.

Паралельно з цим було вдосконалено алгоритм генерації безпечних траєкторій за допомогою великих мовних моделей. Модель інтерпретує контекст місії, генерує адаптивні рішення та здатна запропонувати альтернативні маршрути з поясненням тактичних компромісів. Використання спеціалізованих структурованих шаблонів запитів, які динамічно заповнюються даними цифрових карт висот Copernicus DEM, характеристиками ворожих засобів РЕП та параметрами місії, дозволяє системі уникати зон виявлення та підтримувати можливість передачі сигналу між вузлами мережі. Результати експериментів із моделлю Claude Sonnet підтвердили здатність таких моделей генерувати маршрути, що успішно оминають населені пункти та висотні перешкоди, мінімізуючи ризики переривання зв'язку.

Окрему увагу в роботі приділено безпеці програмного забезпечення БПЛА через розробку моделі комунікаційної архітектури та методу автоматизованого статичного аналізу бінарних прошивок на наявність

недокументованих можливостей. Запропоноване рішення базується на інтеграції можливостей LLM із професійними інструментами бінарного аналізу, такими як декомпілятори IDA Pro та Binary Ninja, через стандартизований протокол MCR. Розроблена система структурованих шаблонів запитів мінімізує ризики генерації помилкових висновків моделлю та формалізує звітність, що значно знижує вимоги до професійної підготовки експерта. Автоматизований аналіз модулів польотного контролера PX4 та бібліотеки `muparser` продемонстрував високу швидкодію, яка в 4 рази перевищує показники класичних методів динамічного аналізу, при цьому точність істинно позитивних виявлень досягла 94,7%.

Практичне значення отриманих результатів полягає у створенні програмної реалізації розроблених методів, що може бути використана для прогнозування та планування місій БПЛА в умовах воєнних дій, а також для оперативного виявлення вразливостей та генерації виправлень програмного забезпечення. Розроблений інструментарій дозволяє підвищити ситуаційну обізнаність операторів та забезпечити швидке реагування на поширення шкідливого програмного забезпечення в мережах типу mesh.

Розроблені моделі та методи були успішно використані під час виконання грантового проєкту “Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework”, а також впроваджені у навчальний процес в курсах “Методи штучного інтелекту в кібербезпеці”, “Кіберзахист об’єктів критичної інфраструктури”, “Аналіз бінарних вразливостей”.

За матеріалами дисертації опубліковано 10 робіт, з яких 5 - це статті у журналах, що входять до переліку фахових видань затверджених МОН України за спеціальністю дисертації, 1 стаття в виданні Scopus та 4 - публікації у матеріалах конференцій (у тому числі, міжнародних).

КЛЮЧОВІ СЛОВА: Кібербезпека, інформаційна безпека, цілісність, доступність, конфіденційність, кіберфізичні системи, мережі Петрі, пошук вразливостей в ПЗ БпЛА, оптимізація прокладання маршруту, великі мовні моделі, БпЛА роторного типу.

ABSTRACT

Voitsekhovskiy A.V. Models and Methods for Ensuring Cyber-Physical Resilience of Drone Networks. – Qualification work in manuscript form. Dissertation for the degree of Doctor of Philosophy in the field of knowledge 12 – Information Technologies, specialty 125 – Cybersecurity. – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute Kyiv, 2026.

The dissertation is devoted to the development of comprehensive models and methods for protection against cyber-physical and cybernetic threats to ensure the safe operation of UAV networks under conditions of dynamic hostile and adverse influences.

On the modern battlefield, networks of mobile UAV devices play a critically important role, enabling remote mission execution and significantly reducing risks to the lives of military personnel; however, their effectiveness and survivability are constantly threatened by complex external influences and the characteristics of aggressive environments. Ensuring the security of such networks is a complex task, as UAVs are equipped with embedded systems containing sensors and transmitters, making them vulnerable both to cybernetic attacks in the form of software vulnerability exploitation, and to cyber-physical influences such as electronic warfare, signal spoofing, and operation in complex terrain conditions.

Existing scientific works typically addressed UAV network availability primarily for civilian missions, considering only flight trajectories and building locations, while factors inherent to military conditions remained outside the researchers' scope. Such specific factors include: the influence of powerful enemy electronic warfare systems, the effect of natural terrain on signal attenuation, and the specific topology of UAV networks that emerges during real operations. At the same time, the rapid development of intelligent UAV capabilities, including machine learning and complex software components, makes them a potential target for attacks via over-the-air updates and exploitation of vulnerable operating system drivers, creating the risk of an entire swarm being compromised. A critical example of such a threat was demonstrated by the UniPwn exploit in the firmware of Unitree autonomous robots, which use wireless communications. The greatest danger lies in

the fact that an infected device can scan other devices within the network's range and automatically compromise them, creating a self-propagating botnet.

The aim of the dissertation is to solve the scientific and technical problem of increasing the cyber-physical resilience of UAV networks through the development of a set of models and methods that ensure the preservation of UAV network communication channel availability, the integrity and confidentiality of flight missions, as well as expanded observability of network state dynamics under the influence of adverse and hostile factors. The stated goal is achieved through the development and improvement of a set of UAV network management models and methods which, unlike existing ones, account for the influence of electronic warfare means on communication channels, topological obstacles, and software vulnerabilities, thereby enabling reliable UAV network management and guaranteeing mission completion under critical conditions.

Object of research: unmanned aerial vehicle (UAV) networks.

Subject of research: models and methods for studying UAV networks in the context of their cybersecurity and availability.

To counter these threats, the author proposes a set of results encompassing UAV network state modeling, spatio-temporal optimization of UAV placement, and automated vulnerability discovery in UAV software samples. The fundamental component of the research is the developed UAV network operation models based on ordinary and colored Petri nets, which comprehensively account for the dynamics of cyber-physical threats, including the influence of electronic warfare devices of varying power, topological obstacles, and signal attenuation as a function of distance. A general Petri net was developed to model an individual UAV, enabling tracking of signal quality level changes, while a colored Petri net was constructed for a set of devices.

In this model, tokens identify individual drones and their signal levels, dynamically reflecting transitions between critical states such as stable connection, loss of communication, entry into a jamming zone, transition to autonomous flight, or successful relay discovery. This enables predictive analytics of UAV network states and visualization of signal dynamics under active suppression. The numerical performance indicators of the developed Petri net models were confirmed during simulation of scenarios for a group of 100 devices over six steps. The comparative

analysis conducted showed that the model is capable of adequately reflecting critical system degradation: at step 4, due to intense electronic warfare influence, the number of devices with zero signal level reached a maximum of 36 units, while 41 devices transitioned to autonomous navigation mode. At the same time, application of this model confirmed high network recoverability: at the final step, after exiting the interference zone, 93 devices (93% of the swarm) successfully restored stable connectivity, which confirmed the logical correctness of the developed fallback transition mechanisms in the Petri net.

To solve the problem of optimal UAV network positioning during its advance from the initial deployment point to the target under cyber-physical threat conditions, the author proposes a method based on a genetic algorithm and a multi-component objective function. This method differs from existing solutions by accounting for geolocation data spoofing threats, radar interference, and terrain characteristics based on open datasets. The proposed objective function effectively addresses the problem of balancing the influence of key competing factors: it simultaneously ensures minimization of the distance to the target, maximization of communication chain connectivity (avoiding both node isolation and excessive clustering), and strategic avoidance of enemy electronic warfare zones.

The computational experiment conducted confirmed that the genetic algorithm provides the necessary balance between advancing the network toward the target and preserving the communication chain, reducing the objective function value by nearly ten times over one hundred iterations. The comparative analysis showed that the gradient descent method demonstrates the worst results due to its dependence on the starting point and entrapment in local minima of complex terrain, resulting in a failure to substantially reduce the objective function value, with a distance error exceeding forty-one kilometers. The greedy sequential algorithm showed a faster execution time, averaging 0.01 seconds, but it is unable to correctly adjust the positions of already-placed drones, leading to mediocre results. The highest effectiveness was demonstrated by the genetic algorithm, which simultaneously optimizes the entire swarm configuration over one hundred generations. Application of the genetic algorithm substantially reduced the objective function value, which in terms of accuracy is on average 16 times better than the greedy algorithm and nearly 330 times superior to gradient descent results.

Furthermore, this method reduced the final route distance by 56 times compared to the greedy algorithm and by over 500 times compared to gradient descent, providing an optimal balance between advancing toward the target and maintaining communication in 0.82 seconds of computation. In parallel, an algorithm for generating safe trajectories using large language models was improved. The model interprets the mission context, generates adaptive solutions, and is capable of proposing alternative routes with explanations of tactical trade-offs. The use of specialized structured prompt templates, dynamically populated with data from Copernicus DEM digital elevation maps, enemy electronic warfare system characteristics, and mission parameters, enables the system to avoid detection zones and maintain signal transmission capability between network nodes. Experimental results with the Claude Sonnet model confirmed the ability of such models to generate routes that successfully bypass populated areas and elevated obstacles, minimizing the risk of communication interruption.

Separate attention in the work is devoted to UAV software security through the development of a communication architecture model and a method for automated static analysis of binary firmware for undocumented capabilities. The proposed solution is based on integrating LLM capabilities with professional binary analysis tools, such as IDA Pro and Binary Ninja decompilers, via the standardized MCP protocol. The developed system of structured prompt templates minimizes the risk of the model generating false conclusions and formalizes reporting, significantly reducing the requirements for expert professional training. Automated analysis of PX4 flight controller modules and the muparser library demonstrated high performance speed, exceeding that of classical dynamic analysis methods by a factor of 4, while the true positive detection accuracy reached 94.7%.

The practical significance of the obtained results lies in the creation of software implementations of the developed methods, which can be used for predicting and planning UAV missions under wartime conditions, as well as for rapid vulnerability detection and software patch generation.

The developed toolset enables increased situational awareness for operators and ensures rapid response to malware propagation in mesh-type networks. The developed models and methods were successfully applied during the execution of the grant project “Towards Networked Airborne Computing in Uncertain Airspace:

A Control and Networking Facilitated Distributed Computing Framework”, and were also incorporated into the educational process in the courses “Artificial Intelligence Methods in Cybersecurity”, “Cyber Protection of Critical Infrastructure Objects”, and “Binary Vulnerability Analysis”.

Based on the dissertation materials, 10 works have been published, of which 5 are articles in journals included in the list of professional publications approved by the Ministry of Education and Science of Ukraine in the dissertation’s specialty, 1 article in a Scopus-indexed publication, and 4 publications in conference proceedings (including international conferences).

KEYWORDS: Cybersecurity, information security, integrity, availability, confidentiality, cyber-physical systems, Petri nets, UAV software vulnerability analysis, optimization route planning, LLM, rotary-wing UAVs.

List of principal publications of the applicant:

1. Stopochkina I., Novikov O., Voitsekhovskiy A., Ilin M., Ovcharuk M. Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability. Theoretical and Applied CyberSecurity. 2024. Vol. 6, no. 2. P. 66 – 76. URL: <https://doi.org/10.20535/tacs.2664-29132024.2.318182> (date of access: 07.03.2026).

У роботі здобувачем запропоновано метод оптимізації позиціонування рою безпілотних літальних апаратів, що ґрунтується на багатокомпонентній цільовій функції. Проведено обчислювальний експеримент, що візуалізує диспозицію апаратів залежно від рельєфу та характеристик засобів РЕБ противника. І. Стъопочкіна - підготовка тексту статті та методика реалізації експерименту, М. Ільїн, М. Овчарук - робота з вихідними даними та пошук актуальних моделей пристроїв РЕП, аналіз та розробка методів забезпечення доступності, О. Новіков - загальне керівництво роботою.

2. Novikov O., Ilin M., Stopochkina I., Ovcharuk M., Voitsekhovskiy A. Application of LLM in UAV route planning tasks to prevent data exchange availability violations. Cybersecurity: Education, Science, Technique. 2025. No. 1(29). P. 419 – 431. URL: <https://doi.org/10.28925/2663-4023.2025.29.892> (date of access: 07.03.2026).

У роботі здобувачем наведено розроблений метод планування маршрутів

БПЛА в умовах кіберфізичних загроз із використанням великих мовних моделей (LLM). Описано модульну архітектуру системи, яка інтегрує геопросторові дані (карти висот) та характеристики засобів РЕБ для генерації безпечних траєкторій. Представлено шаблони запитів для врахування контексту місії та результати експерименту з моделлю Claude Sonnet 4.0, що підтверджують здатність LLM мінімізувати ризики переривання зв'язку та кібератак. М. Ільїн, М. Овчарук - розробка програмного забезпечення для обробки даних датасету, участь в розробці методу планування, аналіз можливих атак на доступність БпЛА, І. Стьопочкіна - обробка різних гілок сценарію роботи методу планування, підготовка тексту статті, керування експериментом, О. Новіков - загальне керування роботою.

3. Skorobahatko M., Voitsekhovskiy A. Lightweight Cryptography in UAV systems. Theoretical and Applied Cybersecurity. 2025. Vol. 7, no. 1. P. 20-29 URL: <https://doi.org/10.20535/tacs.2664-29132025.1.326898> (date of access: 07.03.2026). *У роботі здобувачем взято участь в тестуванні алгоритмів Ascon, Elephant, GIFT-COFB та Xoodyak. Проведено аналіз властивостей цілісності та конфіденційності у системах БпЛА, які забезпечуються криптографічними засобами. М. Скоробагатько - розробка експериментальної установки, реалізація методики випробовувань.*

4. Novikov O., Ilin M., Ovcharuk M., Stopochkina I., Voitsekhovskiy A. Determination of Cyberattack Parameters on the Measurements System of Critical Infrastructure. Theoretical and Applied Cybersecurity. 2025. Vol. 7, no. 2. P. 38 – 43. URL: <https://doi.org/10.20535/tacs.2664-29132025.2.339005> (date of access: 07.03.2026).

У роботі здобувачем виконано обчислювальні експерименти щодо динаміки атак, які можуть бути перенесені на вимірювальні системи БпЛА, випробувано методику виявлення втручань в дані та потенційно ПЗ БпЛА. М. Ільїн, О. Новіков, І. Стьопочкіна - алгоритм детектування прихованих (stealth) атак на вимірювальні системи об'єктів критичної інфраструктури, підготовка тексту статті. М. Овчарук - розроблено математичні співвідношення для виявлення складних втручань, які обходять системи діагностики.

5. Novikov O., Voitsekhovskiy A., Stopochkina I., Ilin M., Ovcharuk M. Petri Net-Based Analysis of UAV Networks Availability Issues in Conditions of Adversary Counteraction. Theoretical and Applied Cybersecurity. 2025. Vol. 7, no. 3. P. 67-73. URL: <https://doi.org/10.20535/tacs.2664-29132025.3.346322> (date of access: 07.03.2026).

У роботі здобувачем запропоновано моделі мережі пристроїв, що ґрунтується на використанні узагальненої мережі Петрі. Реалізовано алгоритми імітації втрати сигналу через рельєф або завади та сценарії відновлення зв'язку через пошук ретрансляторів. Проведено комп'ютерне моделювання в середовищі Python, що дозволило оцінити ймовірність виконання місії в умовах активного придушення сигналу та візуалізувати динаміку станів мережі. М. Ільїн, І. Стъопочкіна - участь в розробці моделей, постановка експерименту, підготовка тексту статті, М. Овчарук - відпрацювання сценаріїв доступності та спостережності БпЛА з використанням розроблених моделей, О. Новіков - керівництво роботою.

6. Voitsekhovskiy A., Sun P., Xie J., Stopochkina I., Ilin M., Novikov O. Detection of vulnerabilities in software for unmanned aerial vehicles by using large language models Eastern-European Journal of Enterprise Technologies. 2026. No. 1(139). P. 36–47. URL: <https://doi.org/10.15587/1729-4061.2026.352029> (date of access: 07.03.2026).

У роботі здобувачем розроблено метод та архітектурну модель автоматизованого виявлення вразливостей у бінарному програмному забезпеченні БпЛА з використанням великих мовних моделей (LLM). Проведено серію експериментів на реальних і синтетичних зразках (PX4, ArduPilot, BdApiUtil.sys). І. Стъопочкіна, М. Ільїн - концепція побудови центру безпеки з використанням даної архітектури, підготовка шаблонів інструкцій, участь в експериментальних випробуваннях методу. P.Sun - порівняльний аналіз роботи методу на хмарних реалізаціях моделей, J.Xie - підготовка тексту статті та керівництво експериментом. О. Novikov - керівництво роботою.

7. Novikov O., Stopochkina I., Ilin M., Rybak O., Ovcharuk M., Voitsekhovskiy A. Security Level of Critical Infrastructure Facility in the Simulation of Cyberattack Cascading Effects. 2024 IEEE 5th International

Conference on Advanced Trends in Information Theory (ATIT): Conference Proceedings (Kyiv, May 20–22, 2024). Kyiv, 2024. P. 112 – 116.

А. Войцеховський - аналіз топологій мережних структур, обчислення показників, які використовуються для аналізу доступності та стійкості в мережах, на основі пропускної здатності та центральності вузла. М. Ільїн, І. Стьопочкіна - метод моделювання каскадних збоїв у мережах критичної інфраструктури, що враховує рівень кіберзахисту кожного об'єкта. О. Рибак - ілюстрація роботи методу, М. Овчарук - розрахунок показників відмов. О. Новіков - керівництво, робота з нормативною та законодавчою базою.

8. Войцеховський А. В. Методи відновлення файлової системи у атаках шифрувальників на основі динамічного аналізу шаблонів шифрування. Теоретичні і прикладні проблеми фізики, математики та інформатики: Матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (11 – 12 травня 2023 р., м. Київ). Київ, 2023. С. 45 – 48.

У роботі здобувачем розроблено метод динамічного аналізу програм-вимагачів на основі шаблонів операцій у файлових системах Linux та Windows. Метод актуальний для ПЗ центрів керування БнЛА. Реалізовано тестове середовище з використанням інтерфейсу FUSE для фіксації активності шкідливого ПЗ та обчислення ентропії файлів для раннього виявлення шифрування. Проведено дослідження зразків сучасних шифрувальників, що дозволило сформулювати патерни їхньої поведінки та підтвердити можливість повного відновлення даних за допомогою механізму миттєвих знімків (snapshots) LVM.

9. Novikov O., Ilin M., Stopochkina I., Voitsekhovskyi A. Attack models for industrial control system elements based on graph approach and countermeasures. ITS-2024: Information Technologies and Security: Workshop Proceedings (Kyiv, Ukraine, December 19, 2024). CEUR Workshop Proceedings, 2024. Vol. 4068. URL: <https://ceur-ws.org/Vol-4068/paper6.pdf> (date of access: 07.03.2026).

У роботі здобувачем запропоновано методику аналізу кібератак в мережних системах, реалізовано експеримент. М.Ільїн, І.Стьопочкіна: моделі атак у графовій формі. О.Новіков: постановка експеримента та керування роботою.

10. Войцеховський А. Методи раннього виявлення атак шифрувальників на рівні мережевого сховища. Theoretical and Applied Cybersecurity. 2023. Vol. 5, no. 2. С. 49. URL: <https://is.ipt.kpi.ua/pdf/TACS-23.pdf> (date of access: 07.03.2026). *У роботі здобувачем розроблено програмний інтерфейс файлової системи, що забезпечує логування підозрілих операцій у середовищах Linux та Windows, включаючи аналіз ентропії та послідовності запису байтів. Проведено динамічний аналіз шкідливих зразків, спрямованих на гіпервізори (зокрема VMware ESXi).*

ЗМІСТ

АНОТАЦІЯ	2
ABSTRACT	7
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ	18
ВСТУП	19
РОЗДІЛ 1 ІСНУЮЧІ РІШЕННЯ В ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРФІЗИЧНОЇ СТІЙКОСТІ МЕРЕЖ БПЛА	26
1.1 Аналіз сучасного стану моделювання мереж БпЛА	26
1.2 Моделі з використанням мережі Петрі	27
1.3 Моделі з використанням клітинкового автомату	29
1.4 Методи оптимізації мереж БпЛА	30
1.5 Проблеми безпеки безпілотних літальних апаратів	33
1.6 Моделі та показники для аналізу продуктивності на основі апарату комплексних мереж	34
1.7 Аналіз безпеки та вразливостей ПЗ	37
Висновки до розділу 1	41
РОЗДІЛ 2 ПОБУДОВА МОДЕЛЕЙ ТА СЦЕНАРІЇВ РОБОТИ БЕСПЛОТНИХ ЛІТАЮЧИХ ПРИСТРОЇВ З УРАХУВАННЯМ СПЕЦИФІКИ АТАК КІБЕРФІЗИЧНОГО ТИПУ	42
2.1 Дані пристроїв радіоелектронної протидії як основа побудови моделей	42
2.1.1 Обчислення пропускної здатності та продуктивності передачі сигналу в мережах БпЛА	45
2.2 Моделі в формі мереж Петрі	47
2.2.1 Маршрути дронів для моделювання мереж Петрі	47
2.2.2 Загальна мережа Петрі для кожного дрона	48
2.2.3 Кольорова мережа Петрі для множини дронів	54
2.3 Методи оптимізації	57
2.3.1 Розробка методів оптимізації для розподіленої мережі об'єктів	57
2.3.2 Прокладання маршрутів за допомогою LLM	64

2.4 Контрольний приклад моніторингу стану пристроїв з використанням моделей Петрі	69
2.5 Контрольний приклад моделей і методів оптимізації маршрутів БпЛА	72
Висновки до розділу 2	80
РОЗДІЛ 3 МЕТОДИ ВИЯВЛЕННЯ НЕДОКУМЕНТОВАНИХ МОЖЛИВОСТЕЙ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ БЕСПЛОТНИХ ЛІТАЮЧИХ ПРИСТРОЇВ	82
3.1 Зворотна розробка прошивок за допомогою LLM	82
3.2 Пошук вразливостей в прошивках за допомогою LLM	83
3.2.1 Виявлення вразливостей в бінарних зразках БпЛА	83
3.2.2 Побудова шаблону запитів для бінарного аналізу та пошуку вразливостей	85
3.2.3 Метод виявлення вразливостей за допомогою LLM та нова архітектурна модель пошуку вразливостей	85
3.3 Контрольний приклад експериментальної перевірки запропонованого методу та архітектури для виявлення вразливостей	91
Висновки до розділу 3	96
РОЗДІЛ 4 ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ ТА МЕТОДІВ	97
4.1 Моніторинг станів вузлів мережі БпЛА засобами апарату мереж Петрі	98
4.2 Прокладання маршрутів за допомогою LLM	102
4.3 Розрахунок продуктивності та пропускну здатності БпЛА	107
4.4 Оптимізація позиціонування мережі БпЛА	110
4.5 Пошук вразливостей в зразках прошивок пристроїв	116
Висновки до розділу 4	121
ВИСНОВКИ	122
ПЕРЕЛІК ПОСИЛАНЬ	125
ДОДАТОК А ВЕЛИКІ РИСУНКИ І ТАБЛИЦІ	135
ДОДАТОК Б АКТИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ	137

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БпЛА - Безпілотний Літальний Апарат
UAV - Unmanned Aerial Vehicle
FANET - Flying Ad-Hoc Networks
MANET - Mobile Ad-Hoc Networks
VANET - Vehicular Ad-Hoc Networks
GCS - Ground Control Station
РЕБ - Радіоелектронна Боротьба
РЕП - Радіоелектронна Протидія
SAST - Static Application Security Testing
CVE - Common Vulnerabilities and Exposures
CVSS - Common Vulnerability Scoring System
MITM - Man-in-the-Middle
BLE - Bluetooth Low Energy
OTA - Over-The-Air
ПЗ - Програмне Забезпечення
LLM - Large Language Model
MCP - Model Context Protocol
КА - Клітинковий Автомат
MAC - Мультиагентна Система
GA - Genetic Algorithm
ACO - Ant Colony Optimization
PSO - Particle Swarm Optimization
RRT - Rapidly Exploring Random Tree
A* - A Star
GERT - Graphical Evaluation and Review Technique
FTA - Fault Tree Analysis
MILP - Mixed Integer Linear Programming
TP - True Positive Result
FP - False Positive Result

ВСТУП

Актуальність роботи

В умовах сучасного поля бою БпЛА відіграють критично важливу роль, дозволяючи дистанційно виконувати поставлені завдання та зменшуючи ризик для життя військовослужбовців. Водночас, їхня ефективність та виживання перебувають під постійною загрозою через зовнішній вплив та особливості середовища. [1].

Забезпечення кібербезпеки мереж БпЛА є важливим завданням, оскільки вони наповнені вбудованими системами з датчиками, передавачами та іншими компонентами, що робить їх вразливими до кібернетичних та кіберфізичних загроз [2].

Існуючі дослідження з моделювання систем моніторингу та прогнозування можливих помилок у їхній роботі, зокрема, на основі апарату мереж Петрі [3, 4], вже розглядають подібні проблеми. Однак, дослідження з врахуванням функціонування БпЛА в умовах, притаманних сучасному полю бою, практично відсутні.

Актуальність роботи визначається необхідністю підвищення цілісності, конфіденційності та доступності функціонування цих пристроїв в умовах активної протидії, що включає два основні вектори впливу:

1. Кіберфізичний вплив [5]: Це загрози, які критично впливають на доступність пристроїв, включаючи засоби радіоелектронної протидії (РЕП) та спуфінг, які можуть призводити до втрати керування, а також вплив несприятливих форм рельєфу та топологічні перешкоди, що спричиняють втрату прямого радіозв'язку. Ворог застосовує потужні комплекси РЕП, як-от Р-330Ж "Житель" Шиповник-Аеро" та "Поле-21 здатні придушувати GPS, GSM та інші канали зв'язку. Додатковою загрозою є використання мобільних мереж противника. Сучасні пристрої об'єднують в сітчасті мережі використовуючи SIM карти. Необхідно розробити удосконалений алгоритм прокладання маршруту, який відрізняється від існуючих, враховуючи топологічні перешкоди, загроза втрати та підміни сигналу.

2. Кібернетичний вплив присутній через вразливості в прошивках

пристроїв, що загрожує конфіденційності та цілісності [6]: мережі БпЛА є складними системами, з широкою поверхнею атаки, використовуючи недокументовані можливостями, бінарні вразливості у їхньому програмному забезпеченні. Критичний приклад такої загрози був продемонстрований експлойтом UniPwn у прошивках роботів Unitree (Go2, B2, G1, H1), який використовує бездротовий зв'язок (BLE/Wi-Fi). Ця вразливість, що використовує жорстко закодовані ключі шифрування та дозволяє введення довільного коду, може призвести до привілейованого захоплення пристрою. Інфікований робот може сканувати інші пристрої Unitree в радіусі BLE та автоматично скомпрометувати їх, створюючи робот-ботнет, який поширюється автоматично. Цей прецедент підкреслює критичну важливість аналізу прошивок БпЛА на наявність недокументованих можливостей.

Мета і задачі наукового дослідження Метою дисертаційної роботи є вирішення науково-технічної задачі підвищення кіберфізичної стійкості мереж БпЛА шляхом розробки комплексу моделей і методів, що забезпечують збереження доступності каналів зв'язку мережі БпЛА, цілісність і конфіденційність польотних завдань, а також розширення можливостей спостережності за динамікою станів мережі в умовах впливу несприятливих та ворожих факторів.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

1. Провести аналіз сучасного стану проблем забезпечення кіберфізичної стійкості мереж БпЛА, методів маршрутизації та виявлення вразливостей, а також визначити специфіку впливу засобів радіоелектронної боротьби (РЕП) і рельєфу на функціонування мереж дронів.

2. Розробити моделі функціонування мережі, які дозволяють врахувати динаміку зміни станів пристроїв під впливом кіберфізичних загроз (втрата зв'язку, дія РЕП, автономний режим) та забезпечити прогнозування поведінки мережі.

3. Розробити алгоритм прокладання маршруту БпЛА шляхом врахування факторів загасання сигналу, топологічних перешкод (рельєфу) та зон дії ворожих засобів РЕП, що дозволить підвищити доступність та цілісність пристроїв під час виконання місій.

4. Розробити метод визначення оптимальної конфігурації мережі БпЛА,

що враховує пропускну здатність каналів зв'язку, зон дії РЕП та топологічних перешкод.

5. Розробити модель архітектури та метод статичного аналізу бінарних прошивок БпЛА, для автоматизованого виявлення недокументованих можливостей програмного забезпечення.

6. Перевірити працездатність запропонованих моделей і методів шляхом програмної реалізації та симуляції сценаріїв роботи мережі БпЛА в умовах протидії, а також пошуку вразливостей на реальних зразках прошивок.

Об'єкт: Мережа безпілотних літальних апаратів.

Предмет дослідження: моделі та методи дослідження мереж безпілотних літальних пристроїв в контексті їх кібербезпеки та доступності.

Наукова новизна

1. Запропоновано моделі на основі апарату мереж Петрі, які відрізняються врахуванням комплексу кіберфізичних загроз у вигляді пристроїв радіоелектронної боротьби, поширення шкідливого програмного впливу, несприятливих форм рельєфу, та ведуть до підвищення спостережності мережі БпЛА, забезпечуючи прогнозну аналітику її станів та зниження загроз доступності і цілісності.

2. Запропоновано метод для визначення оптимальної конфігурації мережі БпЛА, який відрізняється використанням цільової функції з урахуванням топологічних перешкод, сили сигналу, появи радіолокаційних перешкод та досягнення цілі місії, та веде до забезпечення безперервності комунікаційної мережі в умовах активного ворожого впливу.

3. Запропоновано метод прокладання маршруту БпЛА, який відрізняється від існуючих комплексним врахуванням кіберфізичних загроз, та веде до генерування безпечних адаптивних траєкторій, що мінімізують ризики переривання зв'язку і гарантують зниження загроз доступності під час виконання місій.

4. Запропоновано метод та модель архітектури для реалізації статичного аналізу бінарних зразків програмного забезпечення безпілотних літальних пристроїв на наявність вразливостей, які відрізняються використанням інтеграції великих мовних моделей у поєднанні з інструментами аналізу за допомогою протоколу MCR, та ведуть до прискорення процесу виявлення

вразливостей та можливості швидкого виправлення.

Обґрунтованість і достовірність наукових результатів забезпечується коректним застосуванням математичного апарату та відповідних обчислювальних експериментів із використанням сучасного програмного забезпечення.

Практичне значення отриманих результатів. Практичне значення розроблених методів та моделей полягає в тому, що вони реалізовані у програмному виді і можуть бути використані для завдань прогнозу та планування різноманітних місій БпЛА в несприятливих умовах, а також підвищення ситуаційної обізнаності операторів. В тому числі, дані програмні моделі є корисними в умовах військових задач, або цивільних задач з використанням БПЛА в районах військових дій.

Всі теоретичні і практичні результати дисертаційної роботи у повній мірі висвітлено у статтях, опублікованих у фахових вітчизняних наукових виданнях, що входять до відповідного встановленого переліку; виконано їх належну апробацію на міжнародних та всеукраїнських наукових конференціях.

Особистий внесок здобувача.

Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. Всі фахові публікації написані автором дисертації у співавторстві. Належна апробація результатів була проведена на конференціях та наведена в 4 тезах конференцій. Здобувачеві належать такі наукові та практичні результати:

У роботі [1] здобувачем розроблено моделі на основі звичайних та кольорових мереж Петрі для аналізу стійкості БПЛА до засобів РЕБ. Реалізовано алгоритми імітації втрати сигналу через рельєф або завади та сценарії відновлення зв'язку через пошук ретрансляторів. Проведено комп'ютерне моделювання в середовищі Python, що дозволило оцінити ймовірність виконання місії в умовах активного придушення сигналу та візуалізувати динаміку станів мережі.

У роботі [2] здобувачем розроблено метод автоматизованого планування маршрутів БпЛА з використанням великих мовних моделей (LLM) для запобігання порушенням доступності обміну даними. Реалізовано модульну

архітектуру та систему адаптивних запитів, що інтегрують геопросторові дані про рельєф місцевості. Проведено експериментальну перевірку, яка підтвердила ефективність обходу зон РЕП при збереженні прямої видимості між вузлами мережі.

У роботі [3] здобувачем запропоновано метод оптимізації позиціонування рою безпілотних літальних апаратів із застосуванням критерію. Проведено обчислювальний експеримент, що дозволив візуалізувати позицію апаратів на полі бою з урахуванням рельєфу та потужності джерел завад.

У роботі [4] здобувачем розроблено модель архітектури та метод автоматизованого виявлення вразливостей у бінарному програмному забезпеченні БпЛА за допомогою LLM. Реалізовано механізм взаємодії мовної моделі з інструментами декомпіляції через протокол MCP та створено універсальний шаблон інструкцій для пошуку недокументованих можливостей. Проведено порівняльний аналіз, який показав підвищення точності детектування вразливостей до 94,7% при скороченні часу аналізу в 4 рази.

Апробація результатів дисертації. Результати та основні положення роботи подавалися та обговорювалися на:

1 Novikov O., Voitsekhovskiy A., Stopochkina I., Ilin M., Ovcharuk M. Petri Net-Based Analysis of UAV Networks Availability Issues in Conditions of Adversary Counteraction. Theoretical and Applied Cybersecurity. 2025. Vol. 7, no. 3. P. 67-73. URL: <https://doi.org/10.20535/tacs.2664-29132025.3.346322> (date of access: 07.03.2026).

2 Novikov O., Ilin M., Stopochkina I., Ovcharuk M., Voitsekhovskiy A. Application of LLM in UAV route planning tasks to prevent data exchange availability violations. Cybersecurity: Education, Science, Technique. 2025. No. 1(29). P. 420 – 431. URL: <https://doi.org/10.28925/2663-4023.2025.29.892> (date of access: 07.03.2026).

3 Stopochkina I., Novikov O., Voitsekhovskiy A., Ilin M., Ovcharuk M. Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability. Theoretical and Applied Cyber Security. 2024. Vol. 6, no. 2. P. 66 – 76. URL:

<https://doi.org/10.20535/tacs.2664-29132024.2.318182> (date of access: 07.03.2026).

4 Voitsekhovskiy A., Sun P., Xie J., Stopochkina I., Ilin M., Novikov O. Detection of vulnerabilities in software for unmanned aerial vehicles by using large language models. *Eastern-European Journal of Enterprise Technologies*. 2026. No. 1(139). URL: <https://doi.org/10.15587/1729-4061.2026.352029> (date of access: 07.03.2026).

5 Skorobahatko M., Voitsekhovskiy A. Lightweight Cryptography in UAV systems. *Theoretical and Applied Cybersecurity*. 2025. Vol. 7, no. 1. P. 20-29 URL: <https://doi.org/10.20535/tacs.2664-29132025.1.326898> (date of access: 07.03.2026).

6 Novikov O., Ilin M., Ovcharuk M., Stopochkina I., Voitsekhovskiy A. Determination of Cyberattack Parameters on the Measurements System of Critical Infrastructure. *Theoretical and Applied Cybersecurity*. 2025. Vol. 7, no. 2. P. 38 – 43. URL: <https://doi.org/10.20535/tacs.2664-29132025.2.339005> (date of access: 07.03.2026).

7 Novikov O., Stopochkina I., Ilin M., Rybak O., Ovcharuk M., Voitsekhovskiy A. Security Level of Critical Infrastructure Facility in the Simulation of Cyberattack Cascading Effects. 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT): Conference Proceedings (Kyiv, May 20–22, 2024). Kyiv, 2024. P. 112 – 116.

8 Войцеховський А. В. Методи відновлення файлової системи у атаках шифрувальників на основі динамічного аналізу шаблонів шифрування. Теоретичні і прикладні проблеми фізики, математики та інформатики: Матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (11 – 12 травня 2023., м. Київ). Київ, 2023. С. 244-246.

9 Novikov O., Ilin M., Stopochkina I., Voitsekhovskiy A. Attack models for industrial control system elements based on graph approach and countermeasures. *ITS-2024: Information Technologies and Security: Workshop Proceedings* (Kyiv, Ukraine, December 19, 2024). *CEUR Workshop Proceedings*, 2024. Vol. 4068. P. 67-82 URL: <https://ceur-ws.org/Vol-4068/paper6.pdf> (date of access: 07.03.2026).

10 Войцеховський А. Методи раннього виявлення атак шифрувальників на рівні мережевого сховища. *Theoretical and Applied Cybersecurity*. 2023. Vol. 5,

no. 2. С. 49. URL: <https://is.ipt.kpi.ua/pdf/TACS-23.pdf> (date of access: 07.03.2026).

Публікації. За матеріалами дисертації опубліковано 10 робіт, 6 з яких – статті у журналах і збірниках наукових праць, що входять до переліку фахових видань, затверджених МОН України за спеціальністю дисертації, 1 стаття в виданні Scopus та 4 тез науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається із анотації, вступу, чотирьох розділів, висновків, списку використаних джерел. Робота містить 137 сторінок, у тому числі: 124 сторінок основного тексту, 52 рисунок, 11 таблиць, список використаних джерел із 62 найменувань 10 сторінках, 2 додатків.

РОЗДІЛ 1

ІСНУЮЧІ РІШЕННЯ В ОБЛАСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРФІЗИЧНОЇ СТІЙКОСТІ МЕРЕЖ БПЛА

У цьому розділі розглядається сучасний стан проблеми моделювання роботи мереж БПЛА в умовах впливу численних зовнішніх факторів та агресивного середовища. Наводяться результати аналізу існуючих підходів до прогнозування станів та оцінки загальної стійкості рою дронів з використанням апарату мереж Петрі, клітинкових автоматів та комплексних мереж. Також наводяться огляди існуючих методів оптимізації (включаючи класичні алгоритми маршрутизації та машинне навчання) і детальний аналіз ключових проблем забезпечення кібербезпеки БПЛА щодо загроз конфіденційності, цілісності та доступності.

1.1 Аналіз сучасного стану моделювання мереж БПЛА

БПЛА відіграють важливу роль в сучасному полі бою, адже за допомогою них можна дистанційно виконувати поставленні завдання, зменшуючи ризик для життя [7].

Проте, вони є досить вразливими до втрати керування, під дією систем РЕП, природних перешкод, та інших особливостей середовища [8].

Важливим завданням є моделювання станів БПЛА під впливом численних факторів та їх об'єднання у комплексну мережу для визначення загальної стійкості системи [9].

Тому, актуальним представляється визначення найкращої з точки зору стабільності сигналу позиції кожного окремого пристрою, та подальше переміщення дронів, зменшуючи при цьому кількість ймовірних втрат самих літаючих пристроїв.

Проблема моделювання рою дронів уже розглядалась в роботах дослідників. Зокрема, в роботах [10, 11] надано моделі на основі мереж Петрі, щодо прогнозування можливих помилок та небажаних дій в роботі дронів, для забезпечення безпеки людей та навколишнього середовища, метою є завчасно

моделювати та визначати події, що призводять до невдалої та критичної роботи під час польоту БПЛА, адже це набагато безпечніше та практичніше, аніж збирати статистику та виявляти помилки вже під час невдалих польотів в реальному часі. Відкритим завданням є визначити чи станеться критична подія, чи буде можливість вжити заходи для вирішення проблеми та чи буде можливість власне вирішити саму проблему та досягнути бажаного стабільного результату.

Також, існує ряд робіт [12, 13], які показують перспективність використання апарату комплексних мереж для встановлення ознак стійкості при визначеній будові графа зв'язків між елементами мережі. Разом із цим, умови функціонування літаючих пристроїв, притаманні вітчизняній ситуації, практично відсутні у існуючих виданнях. Необхідно враховувати специфіку літаючих пристроїв, які беруть участь у сучасних військових операціях на полі бою.

Отримані результати є значущими з точки зору кібербезпеки безпілотних літальних апаратів (БПЛА), оскільки їхня фізична природа невіддільна від кібернетичної складової. Зокрема, системи моніторингу типу AeroScore [14] функціонують шляхом експлуатації як фізичних (радіоефір), так і кібернетичних вразливостей пристроїв. У зв'язку з цим, одним із ключових завдань роботи є врахування в розроблених моделях потенційного впливу сучасних засобів реалізації кіберфізичних загроз, що можуть призвести до перехоплення управління або знищення літальних апаратів.

1.2 Моделі з використанням мережі Петрі

Перевагою мереж Петрі є те, що вони дозволяють візуалізувати складні системи, розбити їх на більш простіші компоненти, провести симуляцію паралельних та асинхронних процесів [3].

В даній реалізації мережі, позиції станів відображають рівень сигналу окремого апарату, що буде впливати на загальну стійкість системи, переходи визначають різні чинники, що можуть впливати на сам рівень сигналу, такі як вплив засобів РЕП або природних перешкод [15], можлива втрата сигналу через значну віддаленість від контрольного пункту, наявність допоміжного

сусіднього апарату, що може дублювати сигнал. Дуги визначають як змінюється сигнал в залежності від переходу.

Для реалізації мереж Петрі було обрано python бібліотеку Graphviz [16], що надає потужне поєднання автоматичного розміщення елементів та програмної генерації, що робить його пристосованим для побудови мереж Петрі. Використання Python дозволяє створювати розширені реалізації мереж Петрі з власними правилами переходів, додатковою логікою та адаптацією під комплексні специфічні задачі.

В статті [11] представлено комплексний підхід до моделювання систем інспекції дронів за допомогою кольорових мереж Петрі. Дослідження базується на стандарті IEEE для фреймворку застосування дронів та пропонує модульний дизайн моделі для систем інспекції. Однак, цікавим залишається моделювання в умовах з несприятливими факторами, як-от в військових умовах.

В статті [9] розглядають мережу агентів БПЛА, які співпрацюють один з одним без контролюючого центру, припускаючи самоорганізуючу структуру.

Автори оцінили різні сценарії застосування, зокрема, сканування зони інтересів множинними БПЛА для розвідувальних цілей, патрулювання цінних об'єктів для захисту від ворожих ударів, пошук території з можливістю нанесення ударів за потреби та інші. Однак, вони не враховують важливих факторів, які зумовлені кіберфізичними загрозами у вигляді пристроїв РЕП, впливу рельєфу та інших.

У статті [17] розглядають питання оптимізації продуктивності для класу мереж Петрі. Автори зазначають, що мережі Петрі широко застосовуються для моделювання гнучких виробничих систем (ГВС). Дослідження присвячене проблемі оптимізації продуктивності ГВС, змодельованих за допомогою мереж Петрі, з метою максимізації продуктивності системи в межах заданого бюджету шляхом оптимізації як кількості, так і типів ресурсів, включаючи сенсори та пристрої. Автори розробили генетичний алгоритм у поєднанні зі змішаним цілочисельним лінійним програмуванням (MILP) для розв'язання цієї проблеми. Однак, сам апарат мережі Петрі, не досить пристосований до гнучкого відображення результатів моделювання, хоча саме застосування генетичного алгоритму є перспективним.

У статті [4] представлено дослідження з моделювання оцінки безпеки

безпілотних літальних апаратів (БПЛА) за допомогою мереж Петрі. Наразі спостерігається зростаюча тенденція використання безпілотних літальних апаратів у різних сферах діяльності, як цивільних, так і військових. Таким чином, мережі Петрі є схваленим апаратом для військових потреб, в тому числі, хоча відкриті рішення з цього питання практично відсутні.

В цій роботі додатково показано процес моделювання оцінки безпеки БПЛА за допомогою мереж Петрі, який може бути прийнятий сертифікаційними органами з урахуванням рекомендацій STANAG 4671 - специфікації вимог до льотної придатності БПЛА (USAR) для аналізу несправних станів, що призводять до найбільш небезпечних подій [18]. Робота свідчить про те, що відкритим питанням залишаються питання моніторингу стану та забезпечення спостережності, з метою коригування позицій і забезпечення доступності мережі БпЛА.

Моделювання БпЛА для наближення до реалістичних умов, має здійснюватись з урахуванням реальних стандартів. В стандарті IEEE [19] наведено льотні характеристики БПЛА із параметрами висота польоту, швидкість, радіус польоту, витривалість. Тому розробка моделей має відбуватись з урахуванням цих параметрів.

1.3 Моделі з використанням клітинкового автомату

Клітинні автомати дозволяють формально описувати властивості середовища функціонування безпілотних літальних апаратів та підвищувати швидкість обчислення траєкторії їх польоту, зокрема під час моніторингу об'єктів критичної інфраструктури [20].

В даній реалізації апарат тривимірних клітинних автоматів застосовується для формалізованого опису простору, властивостей зон та об'єктів, що обмежують рух, а також для розробки методу моделювання польоту безпілотного літального апарату. Запропонований підхід дозволяє підвищити швидкість обчислення траєкторії польоту та створити ефективну систему моніторингу.

У статті [21] розглядається проблема планування покривного шляху БПЛА та пропонується алгоритм на основі клітинних автоматів для

спірального шаблону. Алгоритм оновлюється асинхронно та тестується на картах з перешкодами. Однак, підхід не розглядає сценарії з динамічними загрозами, характерними для військового застосування.

У статті [22] представлено техніку на основі клітинних автоматів для планування шляхів у розподіленій команді роботів у реальному часі. Автори тестували різні командні формації та підтвердили ефективність методу на реальних мініроботах E-risk з низькими обчислювальними витратами. Проте підхід не враховує специфічних загроз кіберфізичного характеру, притаманних умовам застосування БПЛА.

В роботі [23] досліджено обчислення найкоротшого шляху в клітинних автоматах, що заклало теоретичні основи для подальшого розвитку цього напрямку.

У роботі [24] представлено практичне застосування цих концепцій для планування шляхів роботів, демонструючи ефективність підходу в різноманітних сценаріях.

Однак, попри широке застосування клітинних автоматів у задачах планування траєкторій, їхня дискретна природа зумовлює суттєві обмеження при моделюванні реального поля бою: модель передбачає синхронність переходів між станами та не відображає кіберфізичних і топологічних перешкод, властивих бойовому середовищу.

1.4 Методи оптимізації мереж БпЛА

Оптимізація мереж БпЛА є багатофакторним завданням, яке охоплює показники покриття, енергоефективності, зв'язності, уникнення зіткнень, безпеки та відмовостійкості.

Важливою метою є забезпечення максимальної площі спостереження при мінімальній надлишковості, а також ефективне використання енергетичних ресурсів, що включає управління зарядом батарей і вибір оптимальних маршрутів [25, 26].

Одночасно з цим актуальним завданням є підтримання стійкої комунікації між дронами та наземними станціями, що безпосередньо впливає на якість виконання завдань у динамічних умовах. Додатково особлива увага

приділяється запобіганню зіткненням і взаємним перешкодам, а також протидії кіберзагрозам та забезпеченню стійкості мережі [27].

Для вирішення цих завдань застосовується широкий спектр алгоритмів. Серед класичних підходів планування маршрутів використовуються алгоритм A^* [28], алгоритм Дейкстри [29], метод швидко досліджуваних дерев (RRT [30]) та мурашиний алгоритм (ACO). Вони дозволяють знаходити оптимальні траєкторії в залежності від умов середовища та наявності невизначеностей. Для групових сценаріїв поширеними є методи ройового інтелекту, зокрема оптимізація методом рою частинок (PSO), генетичні алгоритми (GA) та метод оптимізації за допомогою штучного бджолиного рою (ABC), які добре підходять для еволюційної оптимізації маршрутів та енергоефективного розподілу завдань [31].

Не менш важливими є методи мережевої оптимізації. Алгоритм Флойда–Воршелла [32] використовується для вибору найкоротших маршрутів у мережі зв'язку, діаграми Вороного допомагають ефективно розподіляти зони покриття, а фільтр Калмана застосовується для прогнозування позицій дронів і стабілізації зв'язку в реальному часі.

Зростаючу роль відіграють методи машинного навчання [33], зокрема підкріплювальне навчання (Deep Q-Networks, PPO, DDPG), які дозволяють адаптивно налаштовувати маршрути відповідно до умов середовища, а також нейронні мережі, що використовуються для виявлення аномалій у мережевій роботі та виявлення потенційних збоїв.

Практична реалізація оптимізаційних підходів забезпечується за допомогою інструментів і фреймворків. MATLAB і Simulink застосовуються для моделювання динаміки польоту та комунікацій, Gazebo (у зв'язці з ROS) забезпечує реалістичне 3D-середовище для тестування, NS-3 та OMNeT++ [34, 35] використовуються для симуляції комунікаційних мереж, а SUMO [36] дозволяє враховувати транспортну інфраструктуру при плануванні маршрутів. Для задач маршрутизації ефективними є Google OR-Tools та бібліотека NetworkX у Python, тоді як PyTorch і TensorFlow відкривають можливості впровадження глибинного підкріплювального навчання. На рівні комунікацій і безпеки важливими є використання технологій LoRaWAN і 5G, застосування програмно-конфігурованих мереж (SDN) та моделей Zero Trust, що

підвищують захист від кіберзагроз.

Загалом, робочий процес оптимізації мереж дронів передбачає визначення цілей, побудову математичної моделі мережі (наприклад, на основі теорії графів), симуляцію різних сценаріїв, застосування відповідних алгоритмів оптимізації та перевірку результатів у реальних умовах. Подальше масштабування здійснюється на основі показників ефективності. Прикладні сценарії включають доставку вантажів, пошуково-рятувальні операції та військову розвідку. У кожному з цих випадків використовуються спеціалізовані комбінації алгоритмів: наприклад, для доставки — поєднання алгоритму A^* з генетичними алгоритмами та застосування LoRaWAN/5G, для пошуку й порятунку — підкріплювальне навчання і фільтри Калмана, а для військового застосування — ройові алгоритми з інтеграцією SDN [37] для підтримки реального часу.

Таким чином, сучасні підходи до оптимізації мереж дронів поєднують класичні алгоритми, ройовий інтелект, машинне навчання та кіберзахист, що робить їх придатними для складних і мінливих умов реального світу. Автори статті [38] формально визначають FANET як новий тип мобільних ad-hoc мереж (MANET), у яких вузлами є безпілотні літальні апарати (БПЛА). Згідно з цим визначенням, системи з одиночним БПЛА не можуть утворювати FANET, що актуально лише для мультипліт-БПЛА систем. Дослідження підкреслює, що комунікація є однією з найважливіших проблем проектування для мульти-БПЛА систем, оскільки вона критично важлива для кооперації та співпраці між БПЛА. Якщо всі БПЛА безпосередньо підключені до інфраструктури, такої як наземна база або супутник, комунікація між БПЛА може здійснюватися через інфраструктуру. Однак така архітектура комунікації на основі інфраструктури обмежує можливості мульти-БПЛА систем.

Автори детально аналізують відмінності між FANET, MANET та VANET за кількома ключовими параметрами. Це фундаментальне дослідження встановлює FANET як окрему сім'ю ad-hoc мереж з унікальними характеристиками та викликами. Робота демонструє важливість спеціалізованих рішень для мульти-БПЛА систем та окреслює напрямки для майбутніх досліджень. Особливе значення має визначення специфічних вимог

FANET щодо мобільності, масштабованості та надійності, що відкриває можливості для розробки більш ефективних комунікаційних архітектур для автономних систем БПЛА.

Таким чином, перспективним залишається моделювання комунікаційних архітектур, які відображають здатність комунікувати між самими пристроями, а не тільки пристроєм та центром керування. Ця властивість має бути врахована в моделях при оптимізації розташування пристроїв у мережі.

1.5 Проблеми безпеки безпілотних літальних апаратів

Мережі безпілотних літальних апаратів (БПЛА), особливо у форматі FANET (Flying Ad-Hoc Networks) [38], активно застосовуються у військовій справі, пошуково-рятувальних операціях, моніторингу довкілля та доставці вантажів. Їхня ефективність значною мірою залежить від обміну даними між дронами та наземними станціями. Водночас відкрите та динамічне середовище створює значні виклики для конфіденційності та цілісності даних.

Конфіденційність (Privacy): Основна мета забезпечення конфіденційності полягає у захисті переданих даних від несанкціонованого доступу. У мережах БПЛА існують кілька проблем:

1. Перехоплення трафіку (Eavesdropping): зловмисники можуть використовувати спрямовані антени чи спеціальні приймачі для перехоплення сигналів і витоку даних [39].

2. Витік метаданих: навіть якщо дані зашифровані, аналіз трафіку дозволяє відстежувати маршрути, частоту передачі, що може розкрити тактичну інформацію.

3. Атаки з боку інсайдерів: компрометація одного з дронів або наземної станції відкриває доступ до чутливої інформації.

4. Використання слабких криптографічних протоколів: через обмежені ресурси (процесор, батарея) дрони часто застосовують спрощені методи шифрування, які можуть бути вразливими [40].

Цілісність (Integrity). Цілісність означає, що дані не можуть бути змінені або підроблені без виявлення. Основні проблеми для UAV [41]:

1. Man-in-the-Middle атаки (MITM): зловмисник може втрутитися у канал зв'язку, змінюючи координати, команди або сенсорні дані.

2. Підробка пакетів (Packet Injection): навмисне введення підроблених повідомлень, які можуть спровокувати неправильні дії дронів (наприклад, змінити траєкторію).

3. Replay-атаки: повторне надсилання старих коректних повідомлень для введення системи в оману.

4. Вразливості протоколів зв'язку: MAVLink, який широко використовується для управління БПЛА, у стандартній реалізації не має вбудованої криптографічної автентифікації, що створює ризик маніпуляцій.

Приклади наслідків атак: викрадення відеопотоку з розвідувального дрону призводить до витоку конфіденційних даних, модифікацію команд навігації може спричинити падіння БПЛА або його захоплення, викривлення телеметрії може паралізувати роботу всієї ройової мережі.

Поточні рішення та підходи щодо проблем цілісності включають: використання легковагових криптографічних алгоритмів (Ascon, Hoodyak, GIFT-COFB) для шифрування і автентифікації повідомлень у дронах з обмеженими ресурсами, застосування цифрових підписів і протоколів автентифікації (наприклад, HMAC) для підтвердження цілісності команд, використання блокчейн-технологій для фіксації журналів польотів та транзакцій у децентралізованій системі. [40]

Однак, серед вказаного переліку загроз практично відсутня увага до проблеми порушення цілісності внаслідок наявних вразливостей у ПЗ БПЛА, також не пропонуються способи виявлення таких вразливостей.

1.6 Моделі та показники для аналізу продуктивності на основі апарату комплексних мереж

Автори [12] представляють дослідження з управління груповим рухом великомасштабного рою дронів, що є складною та критичною проблемою в сучасних роевих робототехнічних системах. Автори вводять концепцію точкового управління на основі самоорганізованої моделі зграйного руху з використанням набору обраних дронів-драйверів, у якій розглядаються різні

стратегії вибору дронів-драйверів з мережевої перспективи. Результати досліджень показують, що можна управляти груповим рухом рою дронів, контролюючи лише набір дронів-драйверів, і, крім того, добре обраний набір дронів-драйверів може виконати завдання з кращою ефективністю та надійністю. Це дослідження демонструє потужність мережевого підходу до управління складними системами, де невелика кількість стратегічно розміщених контрольних елементів може ефективно керувати поведінкою всієї системи. Запропонована структура точкового управління базується на теорії складних мереж та принципах самоорганізації, що дозволяє досягти координованої поведінки рою при мінімальних управляючих впливах. Різні стратегії вибору дронів-драйверів аналізуються з точки зору топології мережі, що забезпечує оптимальне розподілення управляючих функцій.

В роботі [13] досліджують каскадні відмови та еластичність комунікаційних мереж роїв БПЛА. Як важлива нова сила в інформаційній війні, рої БПЛА привертають все більше уваги військових та науковців різних країн. На сьогодні великомасштабні та низьковартісні рої БПЛА поступово застосовуються в розвідувальних операціях. Невразливість та еластичність їх комунікаційної мережі є ключовими факторами, що визначають, чи може рій успішно виконати розвідувальну місію. Об'єктом дослідження є комунікаційна мережа рою БПЛА, що виконує розвідувальні місії. Мережа рою витягується як модель тришарової взаємозалежної мережі. Автори застосовують теорію безмасштабних мереж та нове рівняння ймовірності з'єднання для встановлення трьох підмереж. Потім конструюється тришарова взаємозалежна мережа з використанням правил міжшарових з'єднань вузлів з найбільшим ступенем. Класична модель M-L розширюється до взаємозалежної мережі. Пропонується правило перерозподілення міжшарового навантаження для симуляції процесу каскадних відмов мереж роїв. Далі виконуються випадкові атаки на вузли мережі та спостерігається невразливість та еластичність цієї мережі. Результати симуляції показують, що продуктивність взаємозалежної мережі є кращою, ніж одношарової мережі завдяки ефекту взаємозалежних зв'язків. Аналізуючи експериментальні результати, висунуто деякі практичні пропозиції для покращення невразливості та еластичності комунікаційної мережі розвідувального рою

БПЛА. Дослідження демонструє важливість багатошарової архітектури для забезпечення стійкості комунікаційних систем роїв БПЛА. Тришарова модель дозволяє більш точно відобразити складну структуру взаємодій у реальних системах та оцінити їх критичні вразливості.

Автори роботи [42] представляють фундаментальне дослідження з оптимізації в складних мережах. Багато складних систем можуть бути описані в термінах мереж взаємодіючих одиниць. Останні дослідження показали, що широкий клас як природних, так і штучних мереж демонструє дивовижно поширену особливість: наявність високо гетерогенних розподілів зв'язків, що забезпечує надзвичайне джерело стійкості до збурень. Хоча більшість теорій щодо походження цих топологій використовують графи, що ростуть, автори показують, що простий процес оптимізації також може пояснити спостережувані закономірності, що демонструються більшістю складних мереж. Використовуючи еволюційний алгоритм, що включає мінімізацію щільності зв'язків та середньої відстані, виявляються чотири основні типи мереж: (а) розріджені експоненціально-подібні мережі, (б) розріджені безмасштабні мережі, (в) зіркові мережі та (г) високощільні мережі, що, очевидно, визначають три основні фази. Ці обмеження забезпечують нове пояснення масштабування показника близько -3 . Окреслюються еволюційні наслідки цих результатів. Дослідження має фундаментальне значення для розуміння принципів формування оптимальних топологій мереж, що може бути застосовано для проектування ефективних комунікаційних архітектур роїв БПЛА. Запропонований еволюційний підхід до оптимізації мережевих структур дозволяє знайти компроміс між ефективністю передачі інформації та економією ресурсів, що є критично важливим для автономних систем з обмеженими енергетичними та обчислювальними можливостями.

Інтеграція розглянутих підходів відкриває можливості для створення адаптивних роєвих систем, здатних динамічно реконфігурувати свою структуру залежно від поточних умов та завдань. Особливо перспективним є застосування цих принципів для розробки стійких до електронної війни систем управління роями БПЛА в умовах сучасних бойових дій.

1.7 Аналіз безпеки та вразливостей ПЗ

Традиційні методи ідентифікації вразливостей базуються на статичному аналізі кодів високого рівня [43]. Для прошивок БпЛА, що часто є бінарними файлами, очищеними від налагоджувальних символів (stripped binaries), такі методи малоефективні. Хоча фазинг (fuzzing) [44] залишається потужним інструментом, він має низьку швидкість при роботі з великими прошивками дронів. Використання LLM для реверс-інжинірингу дозволяє автоматизувати пошук патернів помилок (наприклад, переповнення буфера), проте точність аналізу все ще критично залежить від якості початкового декомпільованого представлення прошивок.

Класичні методи, які використовуються широко в сучасності, не завжди є доречними для вирішення задач, які стосуються прошивок БпЛА. Специфікою цих задач є їх обмеженість в часовому контексті, бо часто аналіз проводиться щодо трофейних зразків, у встановлені терміни. Також залучатись повинні висококваліфіковані спеціалісти, кількість яких в оперативних умовах теж обмежена. Залучення великих мовних моделей (LLM) у цю задачу є гарним виходом, оскільки LLM може за певних умов виконувати повноцінні функції експерта чи реверсного інженера. Проблемою тут є те, щоби налаштувати аналіз автоматизовано, а також запобігти неточному виконанню інструкцій. Ця проблема вирішується в даній роботі.

Джерело [45] дає можливість виконання досліджень за допомогою засобу сучасного статичного аналізу, який спирається на графи потоку керування, даних для аналізу коду. Цей підхід є придатним для пошуку помилок, які мають типові паттерни, зокрема це стосується вразливостей типу переповнення буфера, та витоку даних. Запуск коду при цьому не відбувається. Підхід має свою слабкість по відношенню до зразків, вміст яких є обфускованим, чи захищеним спеціальними методами. Автоматично інтерпретувати обфускований код є доволі складною задачею, а отже, це висуває додаткові виклики до методів статичного аналізу. Присутність кваліфікованого експерта, програм-деобфускаторів, може бути вирішенням. Але, в умовах обмеженості часу та кваліфікованих кадрів цікавим є залучення потужних можливостей LLM щодо деобфускування та надання логічних

висновків.

Засоби динамічного аналізу за ознаками, які видобуваються при виконанні програми, у віртуальному контрольованому середовищі - теж можуть бути застосованими. Тому, ряд існуючих робіт спрямований на розвиток саме цих методів. Зокрема, засоби динамічного аналізу, наприклад такі як у [46], можуть виявляти ряд вразливостей в реальному часі. Разом із цим, необхідно мати висококваліфікованих інженерів-реверсерів, які повинні контролювати хід дослідження. Це є додатковою складністю застосування динамічних методів. Перехід до повністю автоматизованих методів пошуку вразливостей міг би бути слушним вирішенням.

В роботі [47], присвяченій пошуку вразливостей методом фазингу, який добре зарекомендував себе серед методів динамічного аналізу, показується область застосування та результати дії цього методу. Однак, поряд із ефективними спрацьовуваннями слід зауважити і про недоліки, серед яких є відносна повільність та неповне покриття.

Дослідники у роботі [48] показують можливість застосування механізмів фазингу для аналізу на вразливості програмного забезпечення БпЛА. Існуючою проблемою є повне покриття коду, це може бути особливою проблемою при дослідженні складних прошивок та іншого масштабного програмного забезпечення (ПЗ). Метод є не достатньо швидким, при вимогах оперативної роботи. Вирішити цю проблему можна шляхом розробки гібридних підходів, які знижують час дослідження, однак, не знижують при цьому точність.

Масштабність досліджуваних програм це додатковий виклик щодо аналізу на вразливості, існують також показники типу цикломатичної складності коду, що свідчать про необхідність залучення значних ресурсів для повноцінного пошуку вразливостей. Потенційна протидія механізмам анти-налагодження, зокрема так як розглянуто в роботі [49], знижує продуктивність аналізу. В системах БпЛА особливо нагальним є продуктивність та швидкодія, тому ці проблеми обов'язково мають бути взяті до уваги.

Залучення LLM в процес аналізу наявності вразливостей надає низку можливостей, які є відповіддю на існуючі проблеми. Зокрема, в роботі [50]

показано покращення результатів виявлення аналізу із використанням LLM. Однак ця робота не дає рішення щодо архітектури, яка дасть можливість автоматизованого аналізу бінарних файлів. Модель взаємодій між LLM та допоміжними зовнішніми інструментами залишається відкритим питанням.

Робота [43] присвячена ідентифікації вразливих ділянок коду, причому показано, що LLM справляється із цією задачею навіть у обфускованому та модифікованому коді. Однак, в чистому виді ці рішення не можна застосувати до ПЗ БпЛА, тому рішення потребують доопрацювання.

Автори роботи [51] продемонстрували, що наявність контекстних даних покращує результати бінарного аналізу. Ця властивість має бути врахована також і ПЗ БпЛА. Робота цих авторів присвячена перевагам taint аналізу, однак, обмежуватись лише цим видом дослідження є недоцільним у загальному випадку. Для загального випадку треба запропонувати підхід до сполучення можливостей LLM із інструментами бінарного аналізу, які розширюють контекст, та чіткими інструкціями, які запобігають галюцинуванню моделей та скеровують процес по заданому алгоритму дій.

Стаття [52] розглядає питання розширення та збагачення контексту в області виявлення слабкостей коду (CWE). Автори показали, що збагачений контекст (за допомогою інструментів, чи настанов користувача) істотно і позитивно впливає на точність виявлення слабкостей. Можна припустити, що такий підхід буде ефективним і щодо виявлення вразливостей у бінарних зразках, а не тільки у високорівневому коді. Розповсюдження такого підходу на задачі зворотної розробки та аналізу бінарних зразків залишається відкритою задачею, яку вирішено в рамках цього дисертаційного дослідження [53].

Існуючі роботи, зокрема [54] проводили порівняння ряду популярних моделей (а саме, Claude-3.5-Naiku, GPT-4o-Mini, DeepSeek-R1 та інших) в різних режимах функціонування. В роботі показано наочно переваги можливостей з логічних висновків, притаманні цим моделям. Але, ця робота не концентрується на зразках ПЗ БпЛА та наявній специфіці, не проаналізовані питання розширення контексту. Таким чином, нагальним було би подібне дослідження, орієнтоване на зразки ПЗ БпЛА, представлені у їх бінарному виді, а також розробка комунікаційної архітектури збагачення

контексту.

Запропонований у роботі метод, алгоритм його реалізації та модель архітектури для бінарного аналізу ПЗ БпЛА спрямовані саме на усунення зазначених недоліків існуючих підходів. Модель архітектури для вирішення висвітлених проблем доцільно спроектувати на основі нового підходу за допомогою протокола MCR [55].

Зосередженість запропонованих в рамках цього дисертаційного дослідження методів та підходів на бінарних зразках зумовлюється тим, що фахівці кібербезпеки в умовах аналізу ПЗ БпЛА найчастіше мають справу саме з ними, а не з вихідними кодами на високорівневій мові програмування. Дослідження трофейних зразків у військових умовах [15] - це саме та задача, на яку орієнтовані запропоновані у роботі рішення. Іншою актуальною задачею є розробка систем швидкого реагування на поширення шкідливого програмного забезпечення (ШПЗ) [56].

Ці потреби зумовлюють вимоги щодо масштабованості архітектурних та програмних рішень, часові обмеження та дефіцит людських ресурсів, перспективу застосування до безпеки програмного забезпечення мереж БпЛА.

Висновки до розділу 1

1. Виконано аналіз моделювання та безпеки мереж БпЛА. Проаналізовані особливості їх функціонування та фактори агресивного зовнішнього середовища (вплив засобів радіоелектронної протидії, топологічні перешкоди, наявність шкідливого ПЗ), які будуть визначати та впливати на рівень їхньої доступності, цілісності та конфіденційності. Також розглянуто існуючі підходи до забезпечення кібербезпеки БпЛА, алгоритми маршрутизації в динамічних мережах, та інструменти для виявлення вразливостей у бінарних прошивках.

2. Розглянуто існуючі моделі, методи та підходи на основі апарату мереж Петрі, клітинкових автоматів та комплексних мереж, що застосовуються для аналізу продуктивності та прогнозування станів рою БпЛА. Зроблено висновок про необхідність побудови нових моделей, методів та алгоритмів, що дозволяють у комплексі враховувати просторову структуру мережі, джерела кіберфізичних загроз (РЕП, особливості рельєфу), а також механізми захисту від недокументованих програмних можливостей.

3. Для моделювання зміни станів пристроїв, прокладання безпечних маршрутів та виявлення вразливостей з урахуванням військової специфіки середовища пропонується використати апарат звичайних та кольорових мереж Петрі, генетичні алгоритми та можливості великих мовних моделей, для комплексного аналізу надійності та безпеки структурно-складних мобільних систем.

4. Сформульовані цілі та завдання дисертаційної роботи.

РОЗДІЛ 2

ПОБУДОВА МОДЕЛЕЙ ТА СЦЕНАРІЇВ РОБОТИ БЕСПЛОТНИХ ЛІТАЮЧИХ ПРИСТРОЇВ З УРАХУВАННЯМ СПЕЦИФІКИ АТАК КІБЕРФІЗИЧНОГО ТИПУ

У цьому розділі проаналізуємо кіберфізичні характеристики засобів радіоелектронної протидії (РЕП), побудуємо моделі функціонування мережі БпЛА, які базуються на апараті мереж Петрі, і відповідні безпечні сценарії роботи. Для моніторингу та прогнозування стану мережі розробимо класичну мережу Петрі для окремого пристрою та кольорову мережу Петрі для множини пристроїв. Для цього побудуємо логіку зміни станів системи, значення якої буде визначатись поточним рівнем якості сигналу під впливом засобів РЕП, топологічних перешкод та відстані до ретранслятора. Далі сформулюємо багатокритеріальну цільову функцію і розробимо метод визначення оптимальної конфігурації мережі рухомих пристроїв за допомогою генетичного алгоритму. Також, на основі контекстних даних про рельєф і загрози розробимо архітектуру прокладання безпечних маршрутів за допомогою LLM та дослідимо додаткові показники пропускної здатності каналів зв'язку.

2.1 Дані пристроїв радіоелектронної протидії як основа побудови моделей

Для урахування специфіки впливу пристроїв РЕП на поведінку БпЛА, максимально наближеної до реальності, проаналізуємо кіберфізичні характеристики пристроїв РЕП, отриманих із відкритих джерел [57] на Таблиці 2.1.

Таблиця 2.1 – Моделі та специфікації ворожого РЕП

Назва	Частота	Потужність
R-330Zh “Zhytel”	800 ... 960; 1227.6; 1575.42; 1500 ... 1700 and 1700 ... 1900 MHz, GPS, GSM, Inmarsat, Iridium mobile satellite suppression.	1000 W
”SHYPOVNYK-AERO”	25-100; 400-500; 800-925; 2400-2485 MHz.	0,1 km
RP-377UVM1 «LESOCHEK»	MHz – 20-80; 100-130; 120-197, 150-408, 386-1020.	20 W
LPD-801 anti-drone gun	2400-2483,5; 5725-5825; 1575-., 1602-.	10;5;4;4 – accordingly to the frequency subrange
EW and “POLE-21” UAV	GPS/Galileo/GLONASS/BeiDou,	80W, 25 km
R-330 BMW	25 – 960 MHz	
EW complex “Sylok-01” UAV	390-490 MHz; 870-950 MHz; 1200-1300 MHz; 1550-1600 MHz; 2200-2500 MHz; 4900-5900 MHz	50W, 4 km
R-934UM	100-400 MHz	1000 W
“Altaiets-AM”	100-965 MHz	200 W

Назва	Частота	Потужність
«Leer-2»	30-2700 MHz	200-500 W
“Lorandyt”	137-174, 410-470, 100-500 MHz	100 W
EW RB-341V “Leer-3”	880-915, 935-960, 1710-1785, 1805-1880 MHz.	3,5-6 km
EW “Krasukha”	2,9-3,2 HHZ	250 km
EW RB-531B “Infaua”	25-2500	75W, 0,15 km
EW R-330, R-378A, R-378B “Mandat”	1,5 – 100 MHz	1000 W

Наявні дані дозволяють врахувати в моделі:

1. Типи БПЛА, вразливих до цього типу РЕП.
2. Дальність РЕП.
3. Ймовірність ураження РЕП (слід враховувати експертну оцінку, залежно від потужності цього засобу РЕП).
4. Тип ураження (посадка та/або виведення з ладу; дезорієнтація).
5. Ми можемо врахувати точність визначення місцезнаходження РЕП за даними розвідки, залежно від потужності джерела. Чим потужніше джерело, тим точніше його можна локалізувати за допомогою радіорозвідки. Точність визначення місцезнаходження слід враховувати при встановленні дальності.
6. Також слід врахувати, що дія ворожих пристроїв може полягати у розповсюдженні шкідливого програмного забезпечення (ШПЗ) через технологію ОТА (over-the-air). В мережах типу “mesh” ШПЗ розповсюджується найбільш активно від зараженого пристрою [56].

2.1.1 Обчислення пропускної здатності та продуктивності передачі сигналу в мережах БпЛА

Алгоритм обчислення продуктивності:

- D - дрон
- H - дрон ретранслятор
- $c \approx 299792458(m/s)$ - приблизна швидкість світла

Дрон виходить з зони дії РЕП за час, який дорівнює часу вертикального підйому вище радіуса впливу з заданою швидкістю v_a^D .

Пропускна здатність це мінімальний час, необхідний для надходження сигналу від наземної базової станції G до D через будь який ретранслятор H .

$$tl(D) = \frac{distance(G,H) + distance(H,D)}{c} + CD_H + CD_E \cdot in_ew_zone(D) \quad (2.1)$$

- CD_H - стала затримка, в наслідок обробки сигналу хабоом
- CD_E - стала затримка, зумовлена впливом РЕП
- $in_ew_zone(D)$ визначається наступним чином:

$$in_ew_zone(D) = \begin{cases} 1, & \text{якщо } D \text{ знаходиться в активному радіусі} \\ & \text{будь-якого засобу РЕП,} \\ 0, & \text{якщо } D \text{ не знаходиться в радіусі дії} \\ & \text{жодного засобу РЕП.} \end{cases}$$

Нехай $snr(H, D)$ співвідношення повної потужності сигналу до повної потужності шумів, для сигналу який отримав дрон D з хабу H

Потужність отриманого дроном сигналу будемо обчислювати за формулою втрати сигналу, при поширенні у вільному просторі (FSPL):

$$fspl(d, f) = \left(\frac{c}{4\pi df} \right)^2, \text{ де:}$$

- d – відстань від передавача до приймача,
- f – частота сигналу.

Нехай P_T - потужність пристрою, що передає сигнал (дрона або засобу РЕП) T . Тоді потужність сигналу, отриманого дроном D , дорівнюватиме $P_T \cdot \text{fspl}(\text{distance}(T, D), f)$.

Знаючи смугу пропускання каналу та SNR у даній конфігурації системи, максимальна пропускна здатність каналу обчислюється за теоремою Шеннона - Гартлі:

$C = B \log_2(1 + \text{snr}(H, D))$, де B - ширина смуги пропускання каналу в Герцах.

Якщо $\text{snr}(H, D) < 1$, ми вважаємо неможливим потік інформації від передавача H до дрона D .

Нехай P_H - потужність передавача H , а S_D - чутливість приймача D , тоді потужність сигналу, отриманого дроном D , становить $P_D^r = P_H \cdot \text{fspl}(\text{distance}(H, D), f)$. Якщо $P_D^r < S_D$, ми вважаємо неможливим потік інформації від H до D .

Для проведення симуляції поведінки мережі дронів, можуть використовуватись дані варіанти топологічних зв'язків мережі пристроїв:

1. Сітчаста мережа (mesh).
2. Релейна мережа (star).
3. Змішана мережа.

Логічні зв'язки визначають як пристрої в мережі можуть взаємодіяти між собою. Графічне представлення реалізоване за допомогою графів, де вузли це пристрої, а ребра це канали зв'язку.

В сітчастій мережі всі пристрої можуть спілкуватись між собою та ретранслювати дані до інших пристроїв. Сітчаста мережа визначається наступним чином:

- D - множина всіх БПЛА
- g - пункт керування
- G_m - граф логічних зв'язків

$$G_m = (D \cup \{g\}, L_m), \text{ де}$$

$$(g, d) \in L_m \forall d \in D, (d_1, d_2) \in L_m \forall d_1, d_2 \in D, d_1 \neq d_2$$

В мережі реле лише спеціальний тип пристрою здатний ретранслювати

сигнал до інших пристроїв. Топологія визначається наступним чином:

- R - множина звичайних пристроїв, які виконують поставлене завдання.
- H - пристрої, які виконують функцію ретранслятора і підключені до наземного пункту керування за допомогою ретранслятора
- g - пункт керування

$$G_r = (H \cup R \cup \{g\}, L_r), \text{ де}$$

$$(g, h) \in L_r \forall h \in H, (h, r) \in L_r \forall h \in H \forall r \in R$$

Власна топологія дозволяє застосувати будь-який граф $G = (D, L)$,

- D - множина пристроїв;
- L - множина можливих зв'язків між пристроями.

2.2 Моделі в формі мереж Петрі

2.2.1 Маршрути дронів для моделювання мереж Петрі

Представлено три сценарії маршрутів безпілотних літальних апаратів (БПЛА), які відображають різні умови експлуатації. Кожен маршрут складається з координатних точок, з'єднаних лінією, що показує траєкторію польоту дрона від базової станції до цільової точки.

1. Сприятливі умови польоту.

У першому випадку дрон здійснює політ, не заходячи за межі радіогоризонту та не потрапляючи в зону дії засобів РЕП. Маршрут характеризується прямою траєкторією з постійним зв'язком між БПЛА та базовою станцією (Рис. 2.16).

2. Проходження через зону РЕП.

У другому випадку дрон потрапляє в зону дії засобів РЕП та згодом виходить з неї. Даний сценарій моделює реальні умови експлуатації, де неможливо повністю уникнути зон електронної протидії (Рис. 2.17)

3. Політ за межами радіогоризонту.

У третьому випадку маршрут дрона проходить за межами радіогоризонту базової станції. Такий політ характеризується втратою прямого радіозв'язку через топографічні особливості місцевості та вимагає застосування автономних систем навігації (див. Рис. 2.18).

2.2.2 Загальна мережа Петрі для кожного дрона

Мережа Петрі моделює стани та динаміку дронів на полі бою. Створює представлення спрямованого графа за допомогою бібліотеки Graphviz для моделювання складних переходів станів та взаємодій, що керують поведінкою дронів у бойових умовах.

Структура мережі Петрі складається з шести позицій (P1-P6), що представляють різні операційні стани бойових дронів, при цьому кожна позиція може містити маркери (візуалізовані як заповнені кола), які вказують на поточний статус або стан дрону. Позиції стратегічно розташовані для відображення операційного потоку та залежностей станів дронів систем у бойових сценаріях.

Сім переходів (T1-T7) моделюють ключові події та фактори, що впливають на операції дронів:

- **T1 (Відновлення дистанції +1)**: Зменшення відстані до центру керування, для покращення сигналу;
- **T2 (Вплив відстані -1)**: Моделює обмеження дальності, що впливають на ефективність дрона;
- **T3 (Вплив топологічних перешкод -2)**: Враховує рельєф та топологічні перешкоди;
- **T4 (Вплив РЕП -всі)**: Охоплює вплив засобів РЕП, при якому сигнал втрачається без можливості на відновлення.
- **T5 (Поява активного пристрою +1)**: Моделює події активації або розгортання дрона;
- **T6 (Вплив менш потужного РЕП -всі)**: Представляє ефекти слабших систем, де пристрій може вийти з зони дії РЕП. Сигнал втрачається повністю, але відновлюється через заданий час.
- **T7 (Залишити зону РЕП +всі)**: Симулює вихід дронів із зон РЕП.

Модель охоплює динаміку поля бою, включаючи інтерференції сигналів пристроїв та засобів радіоелектронної протидії, обмеження рельєфу, обмеження операційної дальності та події життєвого циклу дрона. Взаємопов'язана структура дозволяє проводити аналіз того, як ці фактори взаємодіють для впливу на загальну ефективність місії дрона та здатність до

виживання.

Візуалізація підтримує фіксоване позиціонування для послідовного аналізу, при цьому початковий розподіл маркерів по станах (P1-P6) настраюється через параметри функції, що дозволяє дослідникам моделювати різні сценарії поля бою та конфігурації розгортання дронів для тактичного аналізу (Рис. 2.1).

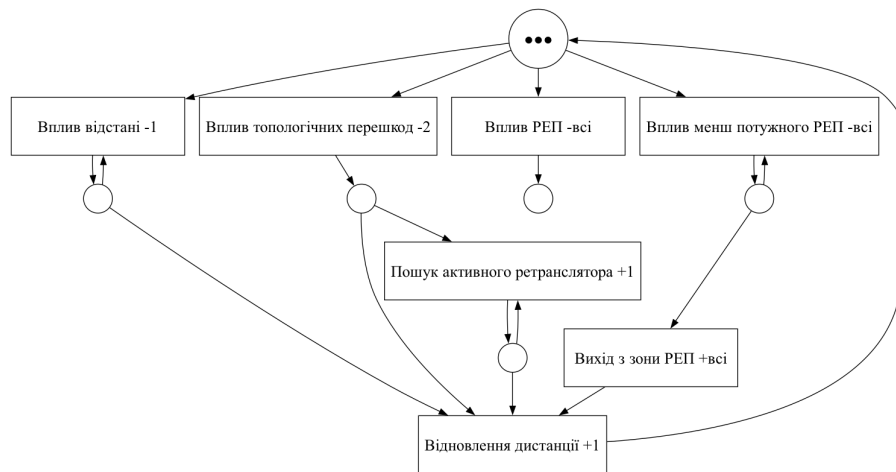


Рисунок 2.1 – Початковий стан мережі петрі для окремого дрона

Нехай D - звичайний дрон, H - дрон-ретранслятор, G - наземна станція управління. Нехай $Q(D,t)$ - рівень якості сигналу дрона D у момент часу t . Якість сигналу змінюється відповідно до переходів у моделі мережі Петрі.

Змінні стану:

- $Q(D,t) \in \{0,1,2,3\}$ - поточний рівень якості сигналу (кількість фішок в позиції);
- $d(D,H,t)$ - відстань від дрона D до найближчого ретранслятора H у момент часу t ;
- $O(D,t) \in \{0,1\}$ - індикатор наявності топологічних перешкод;
- $E(D,t) \in \{0,1,2\}$ - рівень впливу РЕП, де:
 - 0 = немає впливу РЕП;
 - 1 = вплив менш потужного РЕП;
 - 2 = вплив РЕП повної потужності.
- **Позиції**: Рівень якості сигналу $Q(D,t)$, представлений фішками;
- **Переходи**: Сім переходів T1–T7, як визначено вище;

– **Дуги:** З'єднують позиції з переходами з відповідними вагами.

Умови активації переходів:

Перехід T_i активований при маркуванні M , якщо:

1. Усі вхідні позиції мають достатню кількість фішок;
2. Зовнішні умови (відстань, наявність РЕП, перешкоди) виконуються.

Правила спрацювання:

Коли перехід T_i спрацює:

- Вхідні фішки споживаються відповідно до ваг дуг;
- Вихідні фішки створюються відповідно до ваг дуг;
- Система переходить до нового маркування M' .

Якість сигналу змінюється відповідно до наступних переходів:

1. T1: Вплив відстані (−1)

$$Q(D, t + \Delta t) = Q(D, t) - 1, \quad \text{якщо } d(D, H, t + \Delta t) > \max d(D, H, t) \quad (2.2)$$

2. T2: Вплив топологічних перешкод (−2)

$$Q(D, t + \Delta t) = Q(D, t) - 2, \quad \text{якщо } O(D, t) = 1 \quad (2.3)$$

3. T3: Вплив потужних РЕП (−all)

$$Q(D, t + \Delta t) = 0, \quad \text{якщо } E(D, t) = 2 \quad (2.4)$$

4. T4: Вплив менш потужного РЕП (−all)

$$Q(D, t + \Delta t) = 0, \quad \text{якщо } E(D, t) = 1 \quad (2.5)$$

5. T5: Поява активного пристрою (+1)

$$Q(D, t + \Delta t) = Q(D, t) + 1 \quad (2.6)$$

6. T6: Вихід із зони дії РЕП (+all)

$$Q(D, t + \Delta t) = Q_{\text{stored}}(D, t), \quad \text{якщо } E(D, t) = 0 \quad (2.7)$$

7. T7: Відновлення дистанції (+1)

$$Q(D, t + \Delta t) = Q(D, t) + 1, \quad \text{якщо } \max d(D, H, t) > d(D, H, t) \quad (2.8)$$

Цей алгоритм було застосовано для генерації станів мережі БпЛА, використавши можливі сценарії руху окремого пристрою під впливом ворожих факторів. Отримані стани було візуалізовано за допомогою бібліотеки “graphviz”.

На рис 2.2 пристрій пройшов шлях, під час якого був відсутній вплив топологічних чи кіберфізичних перешкод, відповідно зберігся максимальний сигнал.

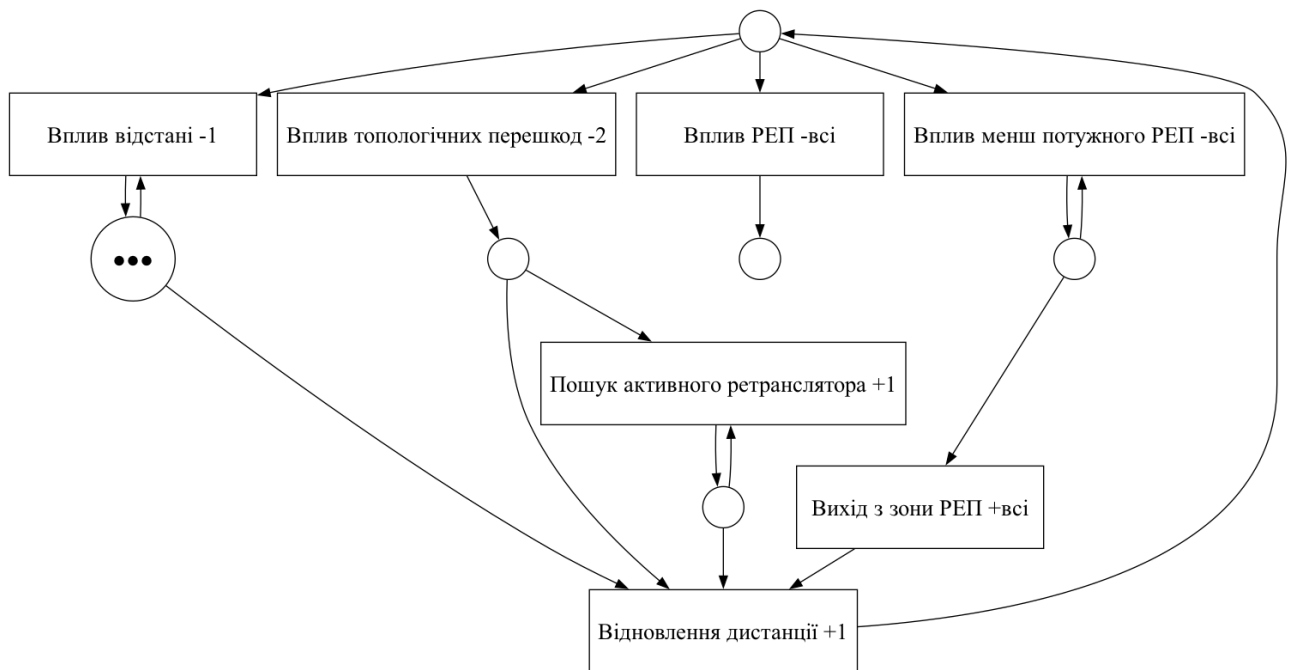


Рисунок 2.2 – Загальна мережа Петрі, вплив відстані на рівень сигналу

На рис 2.3, пристрій відалився від ретрансляторів, та потрапив в зону де сигнал зменшується під дією топологічних перешкод. Далі пристрій буде намагатись знайти додаткові активні ретранслятори або зменшити відстань до джерела сигналу.

На рис. 2.4 пристрій почав шукати активний ретранслятор, та відновлювати свій сигнал. Також, якщо пристрій не знайде додатковий ретранслятор, він може збільшити свій сигнал за допомогою зменшення

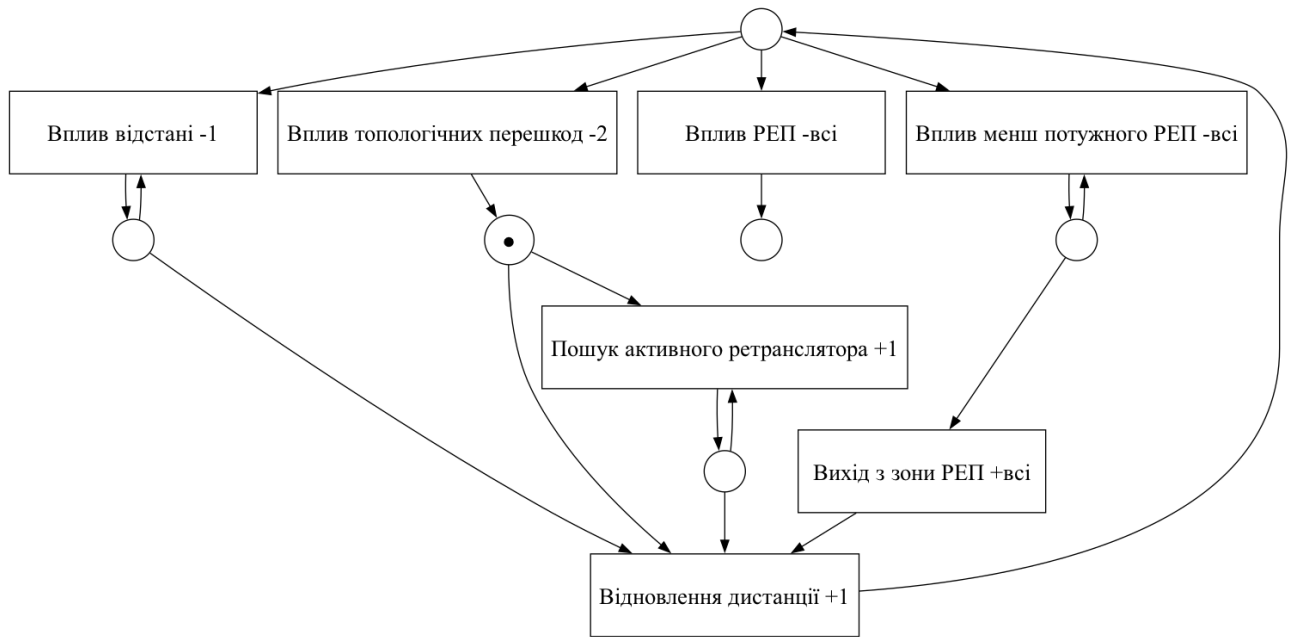


Рисунок 2.3 – Загальна мережа петрі, вплив топологічних перешкод

відстані до вже активного. У іншому випадку відбудеться перехід на початкову позицію з однією фішкою.

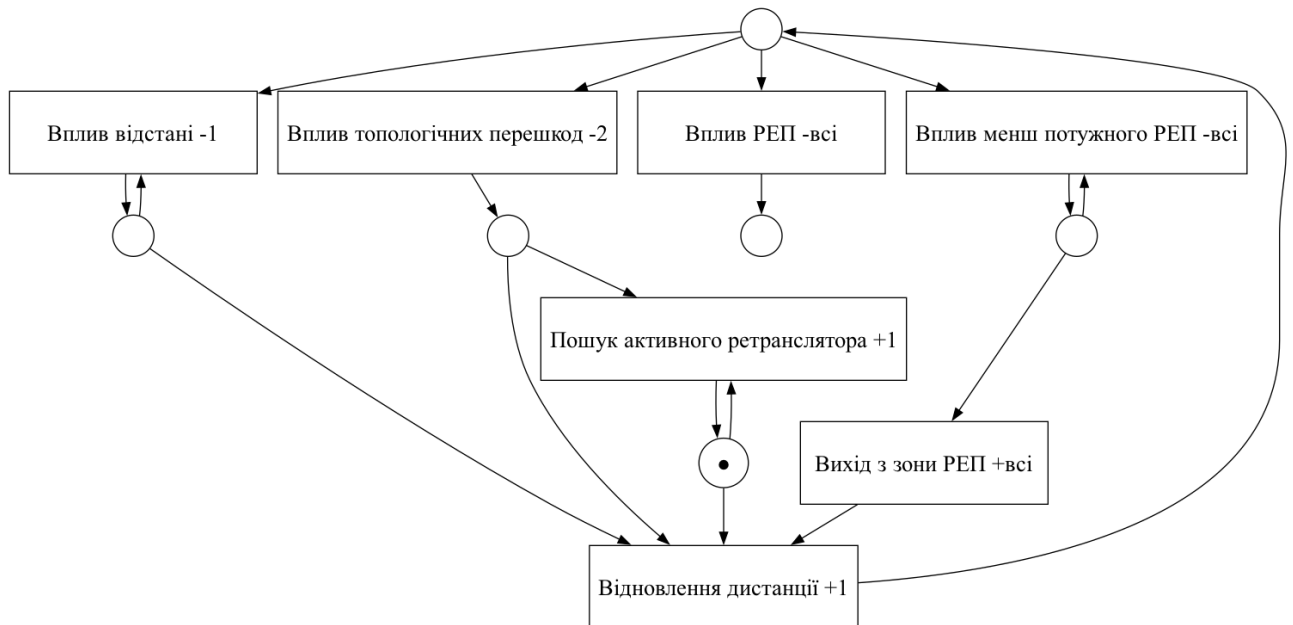


Рисунок 2.4 – Загальна мережа Петрі, пошук ретранслятора

На рис. 2.5 сигнал відповідає двом фішкам, що означає збільшення сигналу, завдяки додатковому ретранслятору. На цьому етапі пошук

ретранслятора закінчено.

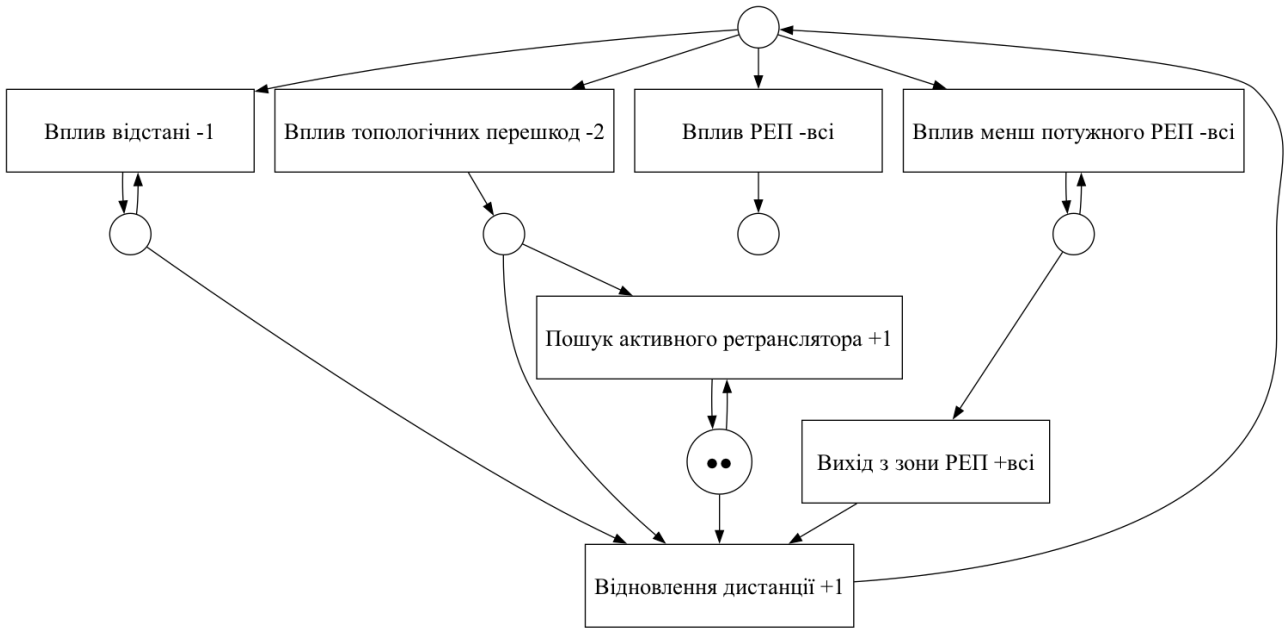


Рисунок 2.5 – Загальна мережа Петрі після знайденого ретранслятора

На рис. 2.6 фішки повернулись до початкового стану. Оскільки відстань до активних ретрансляторів не змінилась, на останньому переході рівень сигналу залишився не змінним.

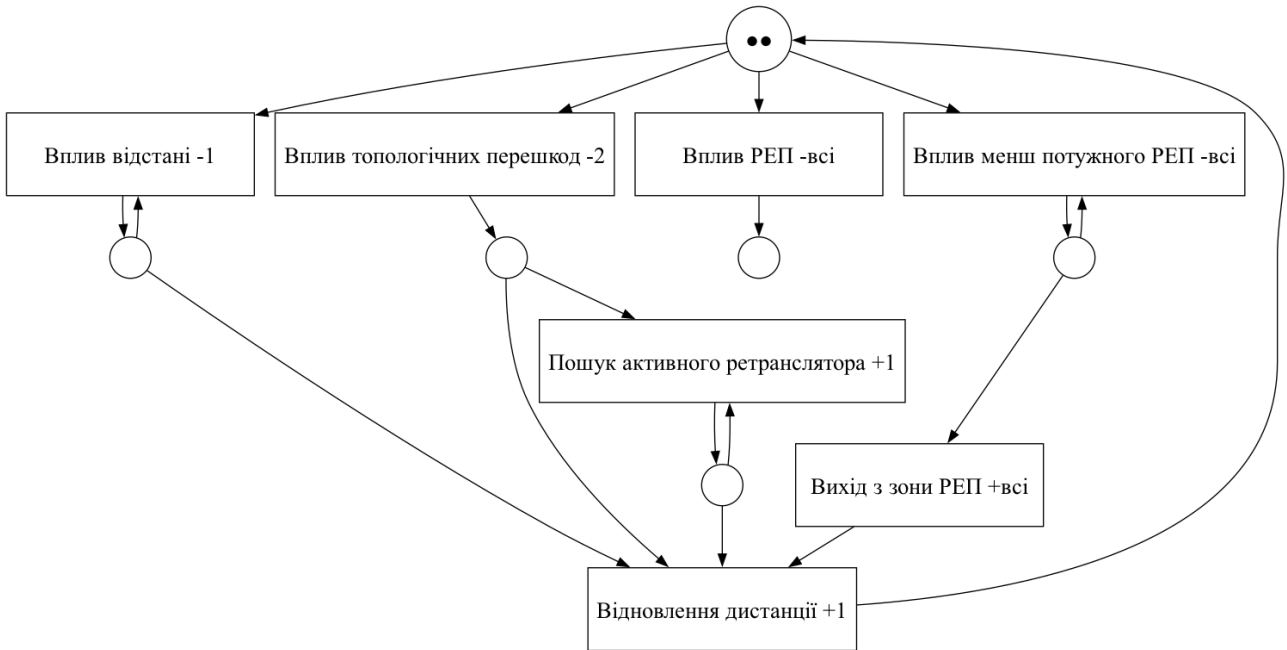


Рисунок 2.6 – Загальна мережа Петрі, завершення циклу

2.2.3 Кольорова мережа Петрі для множини дронів

Загальна мережа Петрі моделює стан та динаміку всієї мережі дронів на полі бою. Створює комплексне представлення системи за допомогою бібліотеки Graphviz для моделювання взаємодій між різними операційними станами дрової мережі в умовах радіоелектронної протидії (Рис. 2.7).

Мережа складається з п'яти основних позицій, що представляють ключові стани дрової мережі:

- **Підключені дрони** – дрони з активним зв'язком із командним центром, що отримують команди та передають телеметрію в режимі реального часу.
- **Зони РЕП** – область простору, в якій засоби радіоелектронної протидії противника пригнічують сигнал, унеможливаючи підтримання зв'язку дрона з командним центром.
- **Втрачений зв'язок** – стан дрона, при якому канал керування повністю розірваний і відновлення зв'язку через наявні ретранслятори є неможливим.
- **Автономний політ** – режим роботи дрона без зовнішнього керування, при якому він виконує заздалегідь запрограмований маршрут або алгоритм дій до відновлення зв'язку.
- **Слабкий сигнал** – стан дрона з деградованим каналом зв'язку, при якому рівень сигналу є недостатнім для надійної передачі даних, але зв'язок ще не втрачено повністю.

Система включає сім типів переходів, що моделюють критичні події мережі:

1. **Вхід у зону РЕП** – перехід дрона з режиму активного зв'язку до стану глушіння внаслідок потрапляння в зону дії засобів радіоелектронної протидії противника.
2. **Вихід із зони РЕП** – відновлення можливості встановлення зв'язку після того, як дрон залишає зону дії джерела перешкод.
3. **Успішний пошук ретранслятора** – встановлення зв'язку через найближчий доступний ретрансляційний вузол із рівнем сигналу, достатнім для повноцінної роботи.
4. **Тайм-аут** – перехід дрона в режим автономного польоту після перевищення встановленого часового порогу очікування відновлення зв'язку.

5. **Вплив відстані** – погіршення якості сигналу до критичного рівня внаслідок перевищення максимально допустимої відстані між дроном та найближчим ретранслятором.

6. **Раптова втрата сигналу** – миттєве переривання каналу зв'язку через фізичні перешкоди, імпульсні завади або раптове вимкнення ретранслятора.

7. **Відновлення зв'язку** – успішне повторне підключення дрона до командного центру після виходу з автономного режиму польоту.

Модель використовує унікальну систему маркування для відстеження індивідуальних дронів та рівня їх сигналу:

- **Колір фішки** — унікальний ідентифікатор конкретного дрона:
- **Кількість фішок** - рівень якості сигналу:
 - **1** - відсутній сигнал (критичний стан).
 - **2** - слабкий сигнал (мінімальний зв'язок).
 - **3** - середній сигнал (стабільний зв'язок).
 - **4** - сильний сигнал (оптимальний зв'язок).

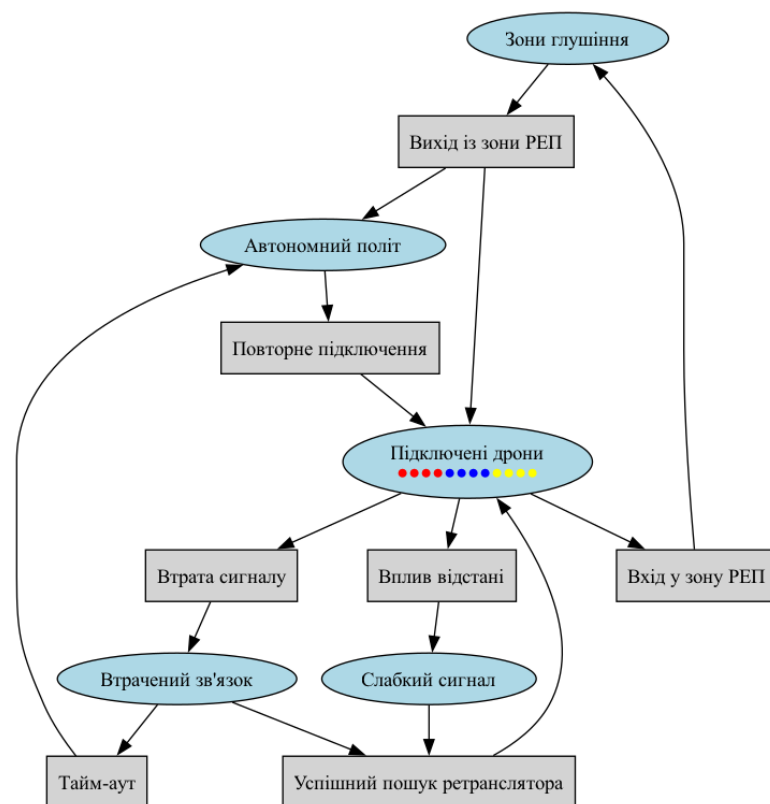


Рисунок 2.7 – Кольорова мережа Петрі для множини пристроїв

Математичне представлення змінних стану кольорової моделі:

– D_i - дрон з індексом i , де кожен дрон має унікальний колір для ідентифікації

– $n(D_i, t)$ - рівень сигналу, кількість фішок дрону D_i у момент часу t

– $I(d(D_i, EW), \text{Power}(EW)) \in \{0, 1\}$

– $\text{State}(D_i) \in \{JZ, AF, CD, LCD, LS\}$ - поточний стан дрона D_i :

– JZ - знаходиться в зоні глушіння

– AF - автономний політ

– CD - підключені дрони

– LCD - дрони з втраченим зв'язком

– LS - низький сигнал

1. Вихід із зони РЕП

$$n_{AF}(D_i, t + \Delta t) = 1 \quad (2.9)$$

якщо дрон D_i з кольором c більше не під впливом РЕП:
 $I(d(D_i, EW), \text{Power}(EW)) = 0$.

2. Повторне підключення

$$n_{CD}(D_i, t + \Delta t) = 4 \quad (2.10)$$

якщо дрон D_i з кольором c знайшов активний ретранслятор.

3. Втрата сигналу

$$n_{LCD}(D_i, t + \Delta t) = 1 \quad (2.11)$$

якщо дрон D_i далеко за перешкодою або надто далеко від найближчого ретранслятора.

4. Вплив відстані

$$n_{LS}(D_i, t + \Delta t) = 2 \quad (2.12)$$

якщо $d(D_i, H_{\text{nearest}}) > d_{\text{max}}$ для дрона D_i .

5. Вхід у зону РЕП

$$n_{JZ}(D_i, t + \Delta t) = 0 \quad (2.13)$$

якщо дрон D_i під впливом РЕП: $I(d(D_i, EW), \text{Power}(EW)) = 1$

6. Тайм-аут

$$n_{AF}(D_i, t + \Delta t) = 1 \quad (2.14)$$

якщо $(\Delta t) > T_{\text{timeout}}$ для дрона D_i .

7. Успішний пошук ретранслятора

$$n_{CD}(c, t + \Delta t) = 4 \quad (2.15)$$

якщо $d(D_i, H_{\text{nearest}}) < d_{\text{max}}$ для дрона D_i .

2.3 Методи оптимізації

2.3.1 Розробка методів оптимізації для розподіленої мережі об'єктів

Нашою головною метою є оптимізація мережі із врахуванням певних факторів, що впливають на загальний стан мережі.

У критеріях оптимізації необхідно враховувати наступні аспекти. Ми повинні переконатися, що максимальна кількість БПЛА залишається підключеною до мережі безпосередньо або через концентратори пристроїв для максимальної надійності мережі у разі виходу з ладу окремих дронів. Також ми повинні максимізувати кількість дронів в зоні зв'язку або забезпечити надійний механізм ретрансляції.

Ми повинні підтримувати мінімальний поріг сили сигналу, щоб уникнути втрату зв'язку БПЛА з мережею. Ми можемо стратегічно планувати розташування ретрансляторів, щоб посилити слабкі сигнали та розширити ефективну дальність окремих пристроїв. Також ми повинні забезпечити мінімізацію втрати керівних повідомлень від центру управління до дронів. Цього можна досягти, забезпечивши високу надійність та захист критичних пристроїв між центром управління та віддаленими дронами, враховуючи також засоби кібербезпеки.

Ще одним важливим питанням є забезпечення стійкості мережі до засобів РЕП. Ми можемо розподілити залежності управління між кількома ретрансляторами, щоб зменшити кількість критичних точок. Також слід здійснити розміщення дронів таким чином, щоб уникнути відомих позицій

засобів РЕП. Нам слід запровадити таку конфігурацію, щоб підтримувати цілісність мережі, якщо певні пристрої будуть скомпрометовані.

Для реалістичності сценарію нам слід враховувати енергоефективність мережі. Це означає, що потрібно оптимізувати позиції дронів, щоб зменшити споживання енергії, спричинене надмірною відстанню або залежністю від підсилення сигналу. Це завдання також пов'язане з мінімізацією неефективних переміщень, зберігаючи при цьому покриття мережі та зв'язок.

У випадку використання дронів для розвідки потрібно максимізувати географічну зону, що контролюється пристроями, зберігаючи при цьому зв'язок з центром управління. Також важливо забезпечити покриття критичних регіонів, щоб врахувати потенційні втрати пристроїв. Коли ми розглядаємо використання дронів для ураження цілі, критерії слід змінити, враховуючи координати цілі для бойових дронів.

Також враховуються складні характеристики мережі, такі як важливість і пріоритетність пристроїв на певних позиціях. Наприклад, ми надаємо пріоритет захисту та посиленню дронів, які виступають посередниками, оскільки їх втрата може критично вплинути на продуктивність мережі. Щоб зробити нашу мережу стабільною, слід збалансувати навантаження мережі та запобігти передчасному виснаженню енергетичних ресурсів дронів. Також, на практиці, ми можемо чергувати ролі БПЛА (наприклад, кінцевий вузол чи вузол-ретранслятор), щоб уникнути виснаження енергії.

Об'єднавши ці критерії, ми приходимо до задачі багатокритеріальної оптимізації.

Для врахування всіх критеріїв використаємо композицію цільової функції наступного вигляду:

$$\begin{aligned}
J = & w_1(N - (|A_{alive}| + |A_{completed}|))^2 \\
& + w_2 \sum_{i \in T} \left[(x_i - x_i^t)^2 + (y_i - y_i^t)^2 + (z_i - z_i^t)^2 \right] \\
& + w_3 \left(\frac{N(N-1)}{2} - \sum_{i,j=1}^N L_{ij} \right)^2 \\
& + w_4 (S_{normal} - S_i)^2 \rightarrow \min
\end{aligned} \tag{2.16}$$

де N – загальна кількість БПЛА, A – множина «живих» БПЛА, підключених до мережі та центру управління, $|A_{alive}|$ – кількість активних дронів, $|A_{completed}|$ – кількість знищених дронів, які успішно виконали місію, $T \subseteq A$ – підмножина БПЛА, які мають досягти цільових координат (x_i^t, y_i^t, z_i^t) , w_1, w_2, w_3, w_4 – вагові коефіцієнти відповідних складових критерію, другий доданок відображає квадрат евклідової відстані БПЛА з підмножини T до цільових координат, $\frac{N(N-1)}{2} = C_N^2 = \frac{N!}{2!(N-2)!}$ – загальна можлива кількість з'єднань між двома пристроями, $\sum_{i,j=1}^N L_{ij}$ – загальна кількість існуючих з'єднань між i -м та j -м БПЛА, третій доданок з вагою w_3 відповідає за максимізацію мережевої зв'язності, четвертий доданок з вагою w_4 забезпечує уникнення зон з нульовим рівнем сигналу, де $S_i > 0 \forall i \in A$, а S_i – рівень сигналу i -го БПЛА.

Рівень сигналу визначається за формулою

$$S_i = S_0 - \alpha d_{ic} + \beta \sum_{j \in A, j \neq i} f(d_{ij}), \tag{2.17}$$

де d_{ij} – відстань від БПЛА i до БПЛА j , $f(d_{ij})$ – це рівень сигналу від сусідніх БПЛА (наприклад, $f(d_{ij}) = \exp(-d_{ij})$ або $f(d_{ij}) = 0$, якщо $d_{ij} > r$, де r – максимальна дальність зв'язку БПЛА), α – коефіцієнт ослаблення сигналу на відстані d_{ic} до центру керування, β – коефіцієнт підсилення від вузлів БПЛА.

Отже, ми врахували наступні показники:

1. уникнення знищення засобами РЕП супротивника та максимізацію кількості активних дронів;

2. виконання місії БПЛА шляхом націлювання на пункт призначення;
3. максимізацію мережевої зв'язності (в ідеальних умовах);
4. рівень сигналу в нормальній зоні та уникнення зон нульового сигналу.

Зауважимо, що 1 та 3 корелюють.

За певних умов мережеву зв'язність можна розглядати як пропускну здатність мережі. У таблиці 2.2 наведено необхідні припущення:

Таблиця 2.2 – Припущення для розглядання мережевої зв'язності як пропускну здатності

Припущення	Умова, яка дозволяє розглядати зв'язність як пропускну здатність
Всі з'єднання симетричні та рівні	Кожне з'єднання надає ту саму пропускну здатність (наприклад, 1 Мб/с)
Відсутність інтерференції, колізій	БПЛА застосовують ортогональні канали або ідеальний TDMA/CDMA
Відсутність накладних витрат маршрутизації, перевантажень	Абсолютно ефективна маршрутизація, або всі БПЛА комунікують лише з сусідами
Всі БПЛА ефективно використовують канал	Відсутність бездіяльних БПЛА або нестачі пропускну здатності
Топологія статична під час комунікації	Мобільність та зміни топології не впливають на пропускну здатність

За цих умов:

1. Кожна активна ланка безпосередньо додає відомий додатковий обсяг пропускну здатності.
2. Таким чином, загальна кількість зв'язків (тобто зв'язність) стає пропорційною загальній пропускну здатності мережі.

$$\begin{aligned}
J = & w_1 \sum_{i \in T} \left[(x_i - x_i^t)^2 + (y_i - y_i^t)^2 + (z_i - z_i^t)^2 \right] \\
& + w_2 \left(\frac{N(N-1)}{2} - \sum_{i,j=1}^N L_{ij} \right)^2 \\
& + w_3 \varphi(d_i^{EW}, r_i) \\
& + w_4 (d_i^{hub})^2 \rightarrow \min
\end{aligned} \tag{2.18}$$

де $d_i^{EW} = \sqrt{(x_i - x_i^{EW})^2 + (y_i - y_i^{EW})^2 + (z_i - z_i^{EW})^2}$ – відстань між i -м БПЛА та будь-яким засобом РЕП, r_i – радіус зони активної дії засобу РЕП, $\varphi(d_i^{EW}, r_i) = e^{-\frac{(d-r)^2}{\sigma^2}}$, де σ – заданий параметр функції. Значення σ залежить від зони, в якій знаходиться БПЛА. Наприклад, σ можна задати пропорційно до середнього радіусу зони активної дії засобу РЕП: $\sigma = 3r$; $\sigma = 0,3r$; $\sigma = r$.

Для оцінки ефективності топології мережі та визначення прийнятної кількості з'єднань для кожного окремого вузла пропонується використання функції на основі нормального розподілу Гаусса.

$$\left(\frac{1}{\sqrt{2\pi}} e^{-\frac{(N-\mu)^2}{2}} \right)$$

У даному виразі параметр N позначає фактичну кількість встановлених з'єднань для конкретного дрона, тоді як μ відображає найкраще значення кількості зв'язків.

$e^{-\frac{(N-\mu)^2}{2}}$ - забезпечує максимальне значення функції при $N = \mu$. Будь-яке відхилення від заданого сталого параметра в обидві сторони (збільшення або зменшення кількості зв'язків) викликає симетричне спадання результуючого показника.

Математична логіка такої моделі полягає у введенні штрафних балів як за надмірну щільність каналів зв'язку, що призводить до перевантаження ефіру та колізій, так і за недостатню кількість ліній, що загрожує ізоляцією вузла.

Цільова функція множини пристроїв виглядає наступним чином:

$$J = w_1 \sum_{i \in T} \left[(x_i - x_i^t)^2 + (y_i - y_i^t)^2 + (z_i - z_i^t)^2 \right] + \sum_{i \in D} \left[w_2 \frac{1}{\sqrt{2\pi}} e^{-\frac{(N_i - \mu)^2}{2}} + w_3 \varphi(d_i^{EW}, r_i) + w_4 (d_i^{hub})^2 \right] \rightarrow \min \quad (2.19)$$

Для проведення експерименту було створене досліджувальне середовище наближене до реального бойового сценарію, в якому безпілотні літальні апарати повинні були пройти по ворожій території та досягнути зазначеної цілі. Середовище складалось з базової станції, постійним пунктом дислокації пристроїв та місцем контролю та збору інформації мережі дронів, цільових локації яку повинна була досягти частина пристроїв та виконати тактичне завдання та джерела радіоелектронної протидії, що проектує сферу заданого радіусу, призначену для порушення або повного припинення комунікацій дронів.

Приклад вхідного json файлу(Повний файл наведено в "Додатку А"):

Приклад вхідних даних сценарію оптимізації

```

1 [
2 { "longitude": 33.65, "latitude": 51.35, "type": "base", "
3   ↳ signal_radius": 50.0, "height": 0.0 },
4 { "longitude": 34.45, "latitude": 51.43, "type": "EW", "
5   ↳ signal_radius": 50.0, "height": 0.0 },
6 { "longitude": 34.2, "latitude": 52.00, "type": "EW", "
7   ↳ signal_radius": 50.0, "height": 0.0 },
8 { "longitude": 34.75, "latitude": 51.52, "type": "target", "
9   ↳ signal_radius": 0.0, "height": 0.0 },
10 { "longitude": 33.80, "latitude": 51.37, "type": "drone", "
11   ↳ signal_radius": 40.0, "height": 200.0, "max_height": 20000.0
12   ↳ }
13 ]

```

Наявність топологічних перешкод, та джерел кіберфізичного впливу створює складність прокладання маршруту, адже задача полягає не лише в правому досягненні цілі, а й в збереженні комунікаційного каналу з базовою

станцією та цілісності апаратів.

Кожен пристрій має обмеження на політ в діапазоні певних висот, частина пристроїв відноситься до категорії атакуючих пристроїв, інша залишається працювати як ретранслятори.

При вхідній формі пристрої розміщуються щільно в межах однієї купи біля базової станції, на низьких висотах. Далі розміщення мережі поступово оптимізується, що також дозволяє покроково спланувати маршрут їхнього руху.

Комунікаційна мережа підтримується за допомогою послідовності з'єднань між пристроями, де кожен дрон може передавати сигнали іншим пристроям в межах свого радіусу досяжності. Це створює додаткові задачі, адже позиція окремого пристрою не лише впливає на самого себе, а й на цілісність всієї мережі. Втрата одного пристрою може розділити мережу та обірвати комунікацію з базовою станцією.

Таким чином однією з цілей оптимізації було забезпечити просування мережі дронів, наблизивши частину з них близько до цілі, але не допустити розрив зв'язку з базовою станцією. Кожен дрон повинен отримувати команди по ланцюжку комунікації незалежно від його позиції.

Друга задача оптимізації уникнути засобів РЕП, розміщених на шляху до цілі. Ідеальне розміщення було б якнайдалі від усіх загроз, але при цьому потрібно зберегти зв'язок з базою та досягнути зазначеної цілі. Тому потрібно було знайти оптимальне розташування з мінімальним впливом на якість сигналу.

Третя задача полягала в пошуку такої мережі, яка б дозволила кожному пристрою підтримувати декілька зв'язків з іншими дронами. Таким чином, втрата одного дрону та комунікаційного зв'язку не призвела б до катастрофічних наслідків. Пристрої з одним з'єднанням вказують на вразливу частину мережі, в той час як велика кількість пристроїв наближена один до одного також створюють неефективне кластерування.

Четверта задача була в уникненні топологічних перешкод, дрони можуть збільшувати свою висоту, забезпечуючи прямий зв'язок, але при цьому потрібно було слідкувати, щоб вони не віддалялись один від одного на критичну для передачі сигналу відстань. Також набір висоти створює кращі умови для радіоелектронної розвідки, в наслідок існує загроза кібернетичних

атак, спуфінгу або перехоплення керування.

Для вирішення цієї багатоцільової задачі був обраний генетичний алгоритм, що імітує процеси природного відбору, для виділення оптимальних рішень. Алгоритм працював з популяцією конфігурації дронів, де кожна конфігурація представляла набір позиції для всіх безпілотних літальних апаратів. Гени популяції відповідали довготі, широті та висоті конкретного дрону.

Процес еволюції проходив через сотню поколінь за цикл оптимізації. За допомогою цільової функції оцінювалась придатність кожного покоління, в залежності від їх ефективності. Цільова функція поєднувала всі показники в єдине число, використовуючи ваги в залежності від важливості показника.

Після ретельної оцінки алгоритм виконував відбір найкращих популяцій як батьківських для наступних поколінь. Такий алгоритм гарантує збереження оптимальних характеристик поточної популяції та передачу наступним поколінням. Дві батьківські конфігурації поєднувались для виробництва нащадків, кожна позиція дрону в нащадку має 50% ймовірність успадкувати конфігурацію від 1 батька і 50% від другого. Це вибіркове поєднання дозволяє об'єднувати корисні характеристики з різних комбінацій в нові, оптимальніші комбінації.

2.3.2 Прокладання маршрутів за допомогою LLM

Засоби РЕП, глушіння GPS, атаки на мережеву інфраструктуру, втрата каналів керування або навмисне порушення зв'язку можуть призвести до часткової або повної відмови в доступі до БПЛА. Традиційні алгоритми планування шляху (такі як A* [58], Дейкстри [59]) не завжди можуть вирішити задачі в цих сценаріях, оскільки вони спираються на повне знання середовища та вимагають стабільного каналу зв'язку для перерахунку траєкторій. Крім того, їм бракує здатності враховувати семантичні або високорівневі обмеження, такі як необхідність уникати зон потенційної кібератак або динамічно змінюваних ландшафтів загроз.

Використання великих мовних моделей (LLM) як компонента планування траєкторії БПЛА пропонує нове рішення для цих обмежень

шляхом інтеграції різномірних джерел даних: карт рельєфу місцевості, цілей місії, зон радіоелектронної протидії, зон ризику кібервторгнення, енергетичних обмежень та потенційних перебоїв зв'язку. LLM здатні генерувати маршрути, які враховують не лише фізичні перешкоди, але й логіку інформаційної безпеки - уникаючи зон можливого перехоплення сигналу, мінімізуючи час перебування в зонах з погіршеним зв'язком та забезпечуючи повернення до безпечної зони у разі втрати контролю.

Важливо, що LLM можуть інтерпретувати контекст місії, виражений природною мовою, та генерувати адаптивні рішення навіть за відсутності повністю структурованої моделі середовища. Це дозволяє автономну роботу в умовах, коли не всі загрози відомі заздалегідь або коли операційне середовище змінюється під час місії. Крім того, LLM можуть пропонувати кілька альтернативних маршрутів з поясненнями їхніх компромісів, підтримуючи інтерактивне прийняття рішень в системах управління та контролю.

Під час розрахунку маршруту ми враховуємо такі фактори: силу сигналу, вплив перешкод (включаючи зони дії пристроїв супротивника) та висоту місцевості на основі даних відкритих карт [60]. Крім того, LLM керується за допомогою структурованих підказок, для яких створено спеціальні шаблони. Ці шаблони динамічно заповнюються необхідними координатами.

Сила сигналу розраховується за формулами 2.20, 2.21. Вона представлена як дійсне число та може набувати від'ємних значень через вплив пристроїв РЕП [12]. Сила сигналу передавача на заданій відстані розраховується на основі формули втрат на трасі у вільному просторі, коли відстань між пристроями значно більша за довжину хвилі сигналу.

$$\frac{S_r}{S_t} = k \left(\frac{\lambda}{d} \right)^2 \quad (2.20)$$

де S_r – сила сигналу приймача; S_t – сила сигналу передавача; k – постійне значення; λ – довжина хвилі сигналу; d – відстань між передавачем і приймачем.

Розрахунок сили сигналу, що приймається від передавача, здійснюється

за виразом

$$S_r = \min(S_t, S_{rmax}) \quad (2.21)$$

де S_r – отримана приймачем сила сигналу; S_{rmax} – максимальна сила сигналу отримувача.

Вплив засобів радіоелектронної протидії спричиняє зниження рівня потужності сигналів між вузлами мережі БПЛА.

$$\hat{S} = S - S_s \quad (2.22)$$

де S – початкова сила сигналу; \hat{S} – сила придушеного сигналу; S_s – сила сигналу засобу РЕП.

Таким чином, ми можемо ввести зони доступності для кожного конкретного БПЛА, та врахувати можливість або заборону маршрутизації через території, розташовані у відповідних зонах.

Щоб чітко встановити контекст LLM та запобігти галюцинаціям, застосуємо структуровані запити для введення деталей місії. У дужках $\{.\}$ наведено конкретні дані, які завантажуються на вхід LLM у json-файлі зазначеної структури.

На рисунку 2.8 представлено шаблон запитів, призначеного для донесення контексту місії БПЛА до LLM. Шаблон містить ключові параметри місії, такі як тип завдання (наприклад, розвідка, доставка, спостереження), координати початку та цілі, обмеження, пов'язані з часом та зонами ризику, а також правила поведінки у разі втрати сигналу або виявлення загрози. Кожне поле структуровано таким чином, щоб забезпечити LLM достатнім контекстом для створення відповідного та безпечного плану маршруту. Використання структурованих заповнювачів ($\{...\}$) дозволяє динамічно заповнювати дані, специфічні для місії, під час автоматизованої попередньої обробки, забезпечуючи узгодженість та мінімізуючи неоднозначність в інтерпретації моделлю.

На рисунку 2.9 представлено структурований шаблон запиту, який використовується для передачі контексту, пов'язаного з рельєфом, до LLM.

```

MISSION TYPE: Reaching destination point
MISSION ID: Destination Point-{DATE}-{SEQUENCE}
PRIORITY: {HIGH/MEDIUM/LOW}
OPERATIONAL TIMEFRAME: {START_TIME} to {END_TIME}
PRIMARY OBJECTIVE: Disrupt enemy {RADAR_TYPE} radar operation in
{GEOGRAPHIC_DESCRIPTION}
SECONDARY OBJECTIVES:
- Collect electronic signatures during engagement
- Assess effectiveness of jamming operations
- Maintain concealment of friendly positions
RULES OF ENGAGEMENT:
- Minimize civilian infrastructure impact
- Maintain electronic emission discipline
- Coordinate with friendly air operations in AO
A MISSION SUCCESS CRITERIA:
- Enemy radar down time >80% during critical window
- No compromise of friendly jammer positions
- Collection of target radar characteristics

```

Рисунок 2.8 – Шаблон запиту опису місії

Він містить інформацію, отриману з цифрових моделей рельєфу, наприклад, [60]. Дані можуть включати значення відносної висоти, характеристики схилів та помітні топографічні особливості (наприклад, хребти, долини, плато). Ці дані допомагають LLM оцінити видимість, обмеження на лінії прямої видимості та можливість підтримки зв'язку між БПЛА та ретрансляційними вузлами. Шаблон підтримує динамічне заповнення даних про рельєф та сегменти рельєфу, що дозволяє адаптивно генерувати маршрути, що враховують фізичні перешкоди та ослаблення сигналу.

На рисунку 2.10 показано структуру запиту, що використовується для опису відомих або підозрюваних засобів супротивника, таких як системи РЕП, станції активних перешкод. На рисунку 2.11 представлено вторинні характеристики для оцінки кіберфізичних вразливостей. Поля включають геолокацію, робочий діапазон, очікуваний вплив сигналу, класифікацію загроз. Ця інформація є критично важливою для планування з урахуванням кібербезпеки, дозволяючи LLM генерувати маршрути, що уникають зон з високим ризиком порушення зв'язку або впровадження шкідливого сигналу. Шаблон гарантує, що характеристики кожного пристрою чітко визначені та можуть бути включені до розрахунків маршрутів з урахуванням загроз.

Наведені запити містять детальний опис пристроїв, місії. За потреби, зайві поля можна виключити. Ці показники враховуються LLM залежно від

```

Terrain Description Prompt Template
TERRAIN ANALYSIS (Pre-processed):
Area of Operations: Grid reference {UTM_COORDINATES}
DEM Analysis:
- Elevation range: {MIN_ELEVATION}m to {MAX_ELEVATION}m
- Dominant terrain features: {HILLS/VALLEYS/RIDGES} at bearings
{AZIMUTH_LIST}
- Line-of-sight calculations completed for target area
Key Terrain Features:
- Hill Mass Alpha: {COORDINATES}, elevation {HEIGHT}m, provides
{MASKING/OBSERVATION}
- Valley Bravo: {COORDINATES}, width {DISTANCE}m, concealment factor
{HIGH/MEDIUM/LOW}
- Ridge Charlie: {COORDINATES}, commanding view of
{AREA_DESCRIPTION}
Visibility Analysis:
- Dead zones: {COORDINATE_POLYGONS}
- Optimal observation positions: {COORDINATE_LIST} with
{LOS_DISTANCE}km range
- Concealed approach routes: {ROUTE_DESCRIPTIONS}
Terrain Constraints:
- Impassable areas: {COORDINATES_AND_REASONS}
- Seasonal limitations: {WEATHER_DEPENDENT_FACTORS}
- Civilian activity zones: {RESTRICTED_AREAS}

```

Рисунок 2.9 – Шаблон запиту опису рельєфу

мети місії.

Архітектура запропонованого рішення включає такі компоненти для автоматизації підготовки даних, завантаження даних у LLM та обробки результатів:

1. Препроцесор (скрипт Python), який аналізує карти висот, перетворює координати в нормалізовану сітку та створює JSON з контекстом для LLM, який дані з карти висот, цілі, обмеження, початкові точки.

2. Генератор запитів (скрипт Python) - готує шаблон місії для поточного вигляду, підставляє координати, висоти з карт, обмеження та іншу інформацію. Шаблон запиту для LLM коригується оператором-людиною з урахуванням цілей конкретної місії, генератор може надати типові приклади.

3. LLM – компонент (через API) - отримує згенеровану підказку та контекстні дані, обробляє їх та виводить шлях та/або послідовність дій у форматі JSON.

4. Постпроцесор (скрипт Python) - візуалізує маршрут, виконує перевірку правильності маршруту, візуалізує на карті, за необхідності запускає повторний запит до LLM.


```

HOSTILE ELECTRONIC WARFARE THREAT ASSESSMENT:
PRIMARY TARGET:
- System Type: {RADAR_DESIGNATION} ({FREQUENCY_BAND}-band radar)
- Location: {PRECISE_COORDINATES} (confidence: {HIGH/MEDIUM/LOW})
- Technical Characteristics:
  * Operating frequency: {FREQUENCY_RANGE} MHz
  * Detection range: {RADAR_RANGE}km
  * Azimuth coverage: {DEGREES} degrees
  * Elevation scan: {MIN_ANGLE} to {MAX_ANGLE} degrees
  * Pulse repetition frequency: {PRF_RANGE}
  * Peak power output: {POWER_ESTIMATE}W
SUPPORTING EW INFRASTRUCTURE:
- Communication links: {FREQUENCY_BANDS} at {POWER_LEVELS}
- Backup power systems: {GENERATOR_SPECIFICATIONS}
- Operator patterns: {ACTIVITY_SCHEDULE}
DEFENSIVE MEASURES:
- Physical security: {DEFENSIVE_POSITIONS}
- Relocation capability: {MOBILE/STATIC} with {MOVEMENT_TIME} setup
time

```

Рисунок 2.10 – Шаблон запиту опису кіберфізичних характеристик пристроїв РЕП супротивника

```

SECONDARY THREATS:
- Adjacent radar systems: {LOCATIONS_AND_TYPES}
- Communication intercept assets: {SIGINT_POSITIONS}
- Air defense coverage: {SAM_LOCATIONS_AND_RANGES}
VULNERABILITY ASSESSMENT:
- Susceptible frequencies: {VULNERABLE_BANDS}
- Power threshold for disruption: {JAMMING_POWER_REQUIRED}
- Critical timing windows: {OPTIMAL_ENGAGEMENT_TIMES}

```

Рисунок 2.11 – Шаблон запиту опису вторинних характеристик для оцінки кіберфізичних вразливостей

2.4 Контрольний приклад моніторингу стану пристроїв з використанням моделей Петрі

Було проведено експеримент зі спостереження за станами мережі, за допомогою моделі у формі кольорової мережі Петрі. У наступній таблиці 2.3 наведено розподіл станів дронів на кожному з п'яти кроків симуляції кольорової мережі Петрі. Дані відображають переміщення 76 дронів між різними станами.

На рисунку 2.12 видно чіткий перехід від стабільного стану (Крок 0) до стану значної деградації (Крок 4) з наступною фазою відновлення (Крок 5),

Таблиця 2.3 – Розподіл станів БпЛА за кроками симуляції мережі Петрі для множини пристроїв

Стан	Крок 0	Крок 1	Крок 2	Крок 3	Крок 4	Крок 5
Підключені дрони	76	54	37	28	9	72
Дрони з втраченим зв'язком	0	22	17	9	14	0
Зони РЕП	0	0	22	31	46	0
Автономний політ	0	0	0	8	7	4

що підтверджує логічну коректність механізмів відновлення та резервних переходів мережі Петрі.

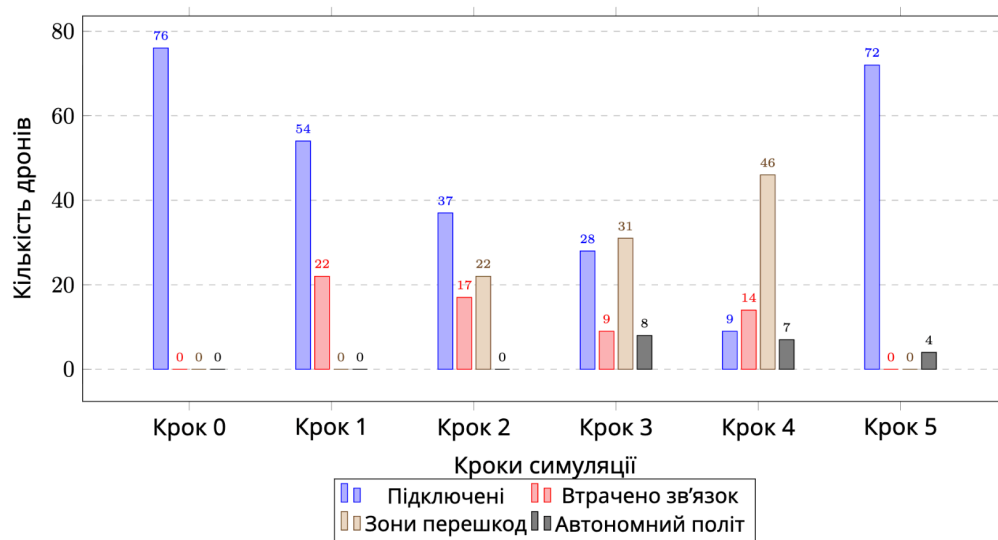


Рисунок 2.12 – Кроки симуляції кольорової мережі

На рисунку 2.13 зображений стан, коли один з дронів втратив зв'язок, залетівши за радіогоризонт, інший потрапив в зону дії РЕП, третій має стабільний зв'язок.

На рисунку 2.14 дрон, що втратив зв'язок через топологічні перешкоди, знайшов ретранслятор та повернув собі стабільний сигнал. Дрон що потрапив під дію РЕП перейшов в автономний режим.

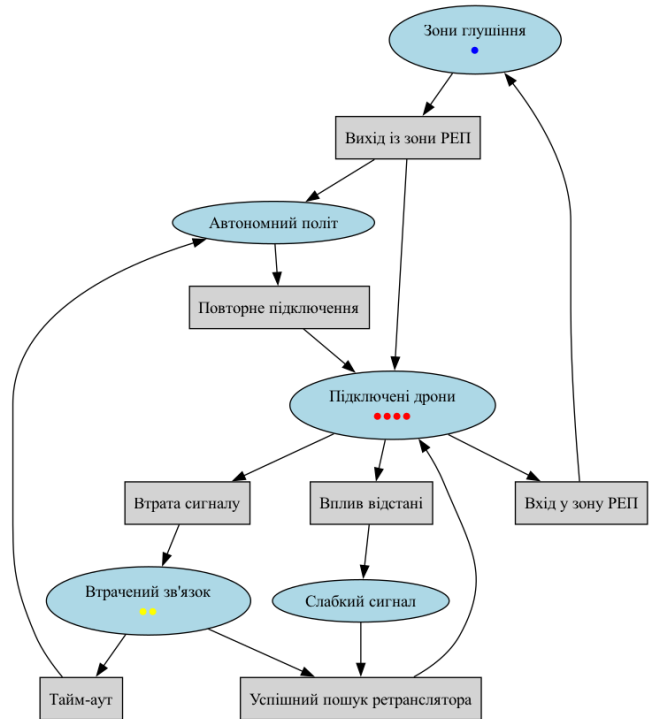


Рисунок 2.13 – Стани пристроїв під час втрати зв'язку

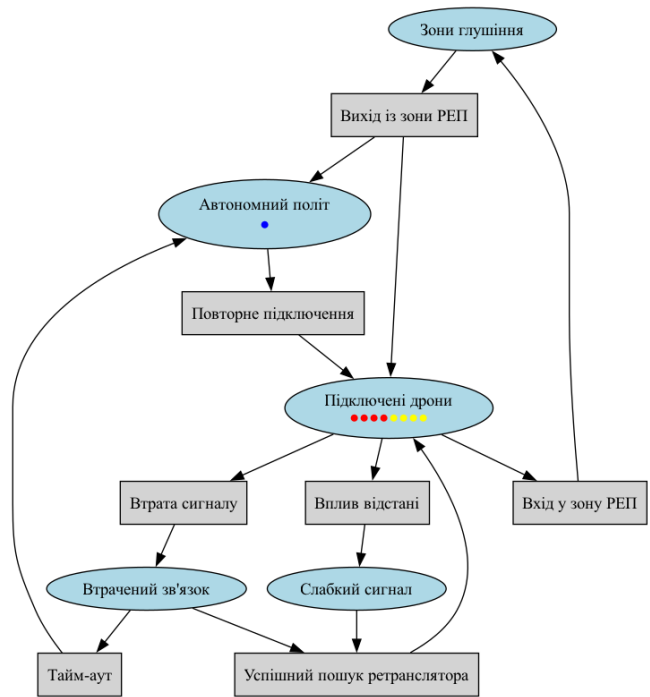


Рисунок 2.14 – Етап відновлення зв'язку

На рисунку 2.15 один з дронів має стабільний сигнал, інші 2 відлетіли далеко від ретранслятора тому мають слабкий сигнал.

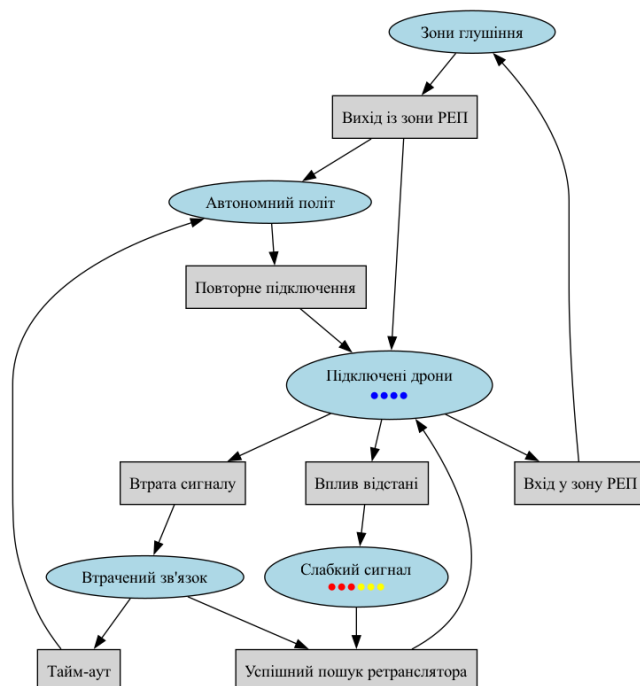


Рисунок 2.15 – Стани пристроїв зі слабким сигналом

2.5 Контрольний приклад моделей і методів оптимізації маршрутів БпЛА

Було виконано кілька експериментів щодо дослідження працездатності методу прокладання та оптимізації маршрутів БпЛА. Перший експеримент стосувався планування місії дронів у різних умовах згідно сценаріїв, описаних в п.2.2.1

Для врахування рельєфу дані вихідного датасету [60] були піддані розбору за допомогою розробленого парсера, який представляє вхідні дані у вигляді JSON файлу(Лістинг 2)

Було проведено експеримент, щодо дослідження працездатності розробленого методу оптимізації. Впроваджено обмеження щодо висоти руху дронів, дистанцію яку вони можуть змінити між циклами оптимізації, з метою послідовного моделювання зміни руху пристроїв, забезпечивши в подальшому побудову ефективного маршруту дронів до цілі.

Для проведення експерименту ми створили сценарій з 8 дронів 3 засобів РЕП та цілі. (Табл. 2.4) Початкова висота дронів становила 5000м. та технічне обмеження 20000м. вище якого дрон не може підніматись. Радіус сигналу

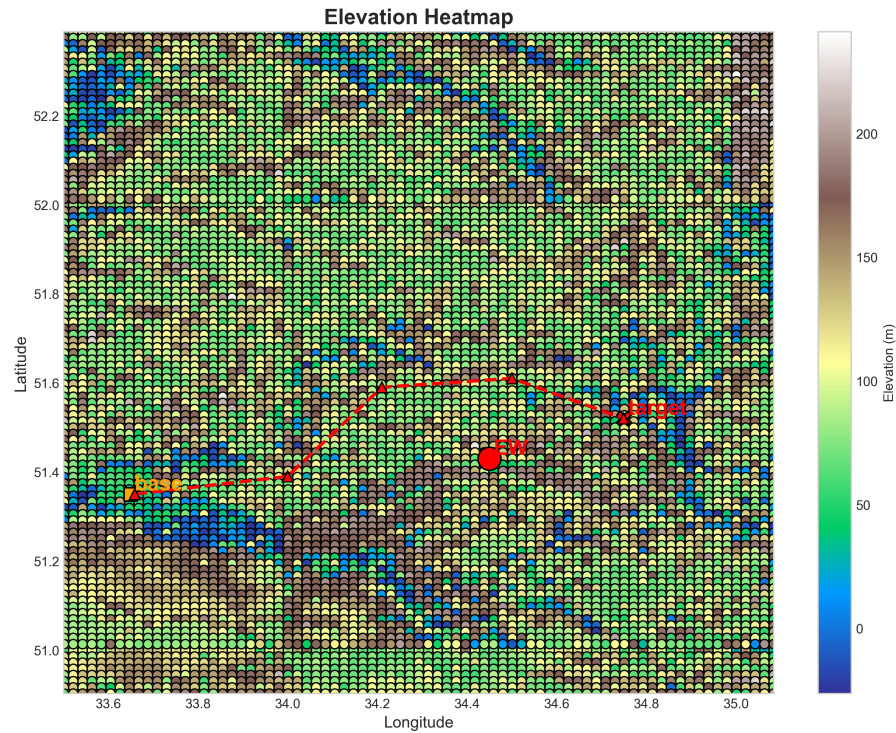


Рисунок 2.16 – Сценарій 1: Сприятливий маршрут без перешкод

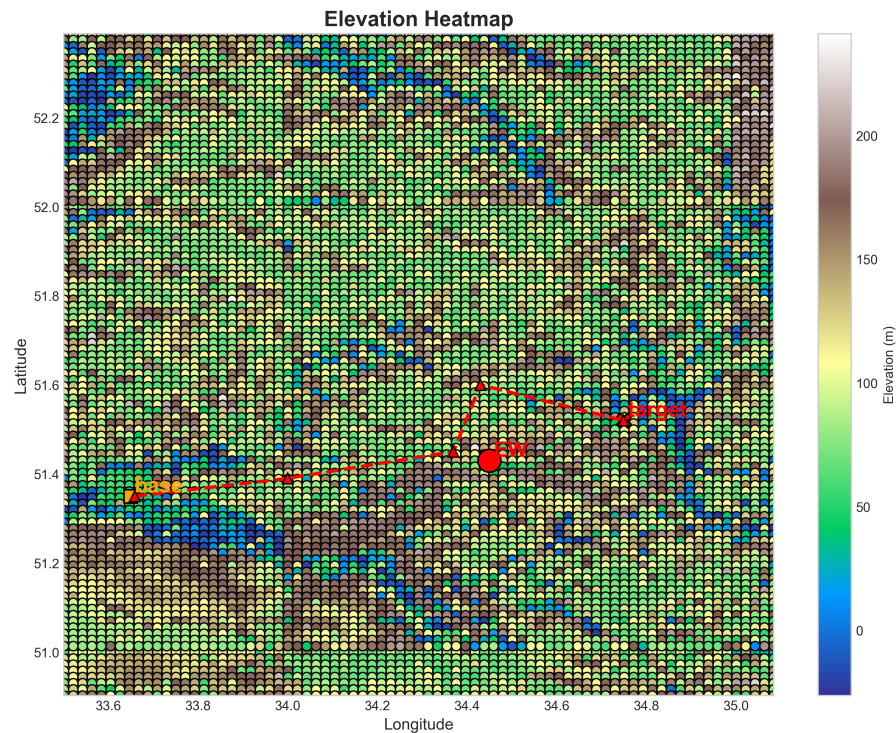


Рисунок 2.17 – Сценарій 2: Маршрут через зону РЕП

кожного дрону дорівнював 15000м., в якості цільової функції оптимізації використали формулу 2.19.

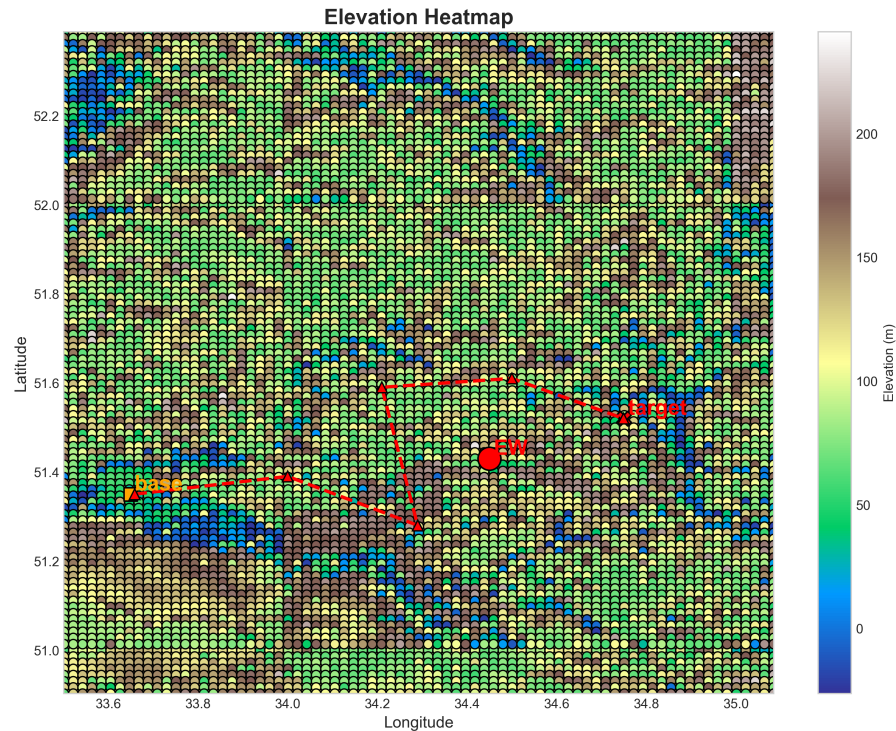


Рисунок 2.18 – Сценарій 3: Маршрут за межами радіогоризонту

Таблиця 2.4 – Порівняння методів оптимізації

Метод	Score	Відстань	Час
Генетичний	213.31	0.08 км	0.82 с
Жадібний послідовний	3483	4.50 км	0.01 с
Градiєнтний	70048	41.19 км	0.30 с

Градiєнтний спуск показав найгірший результат, за допомогою нього вдалось отримати лише 70,048 в цільовій функції. Метод обчислює значення для кожного дрону окремо і обмежується локальним пошуком (Рис.2.19). Жадібний послідовний алгоритм показав значно кращий результат - 3,483. Алгоритм вже розміщує дрони послідовно від бази до цілі, для кожного наступного пристрою обирається найкраща позиція в залежності від попереднього враховуючи зв'язність з уже розміщеними. Проте ключовим обмеженням до кращого результату в даній задачі є те, що вже розміщені дрони не можуть бути переміщені на пізніших кроках (Рис. 2.20). Генетичний алгоритм досяг найкращого результату - 213. На відміну від попередніх, даний алгоритм оптимізує одночасно всю конфігурацію з восьми дронів протягом 100

поколінь. Це дозволє знаходити такі позиції для пристроїв, де буде баланс між просуванням до цілі, зв'язністю мережі та уникненням кіберфізичних загроз (Рис. 2.21).

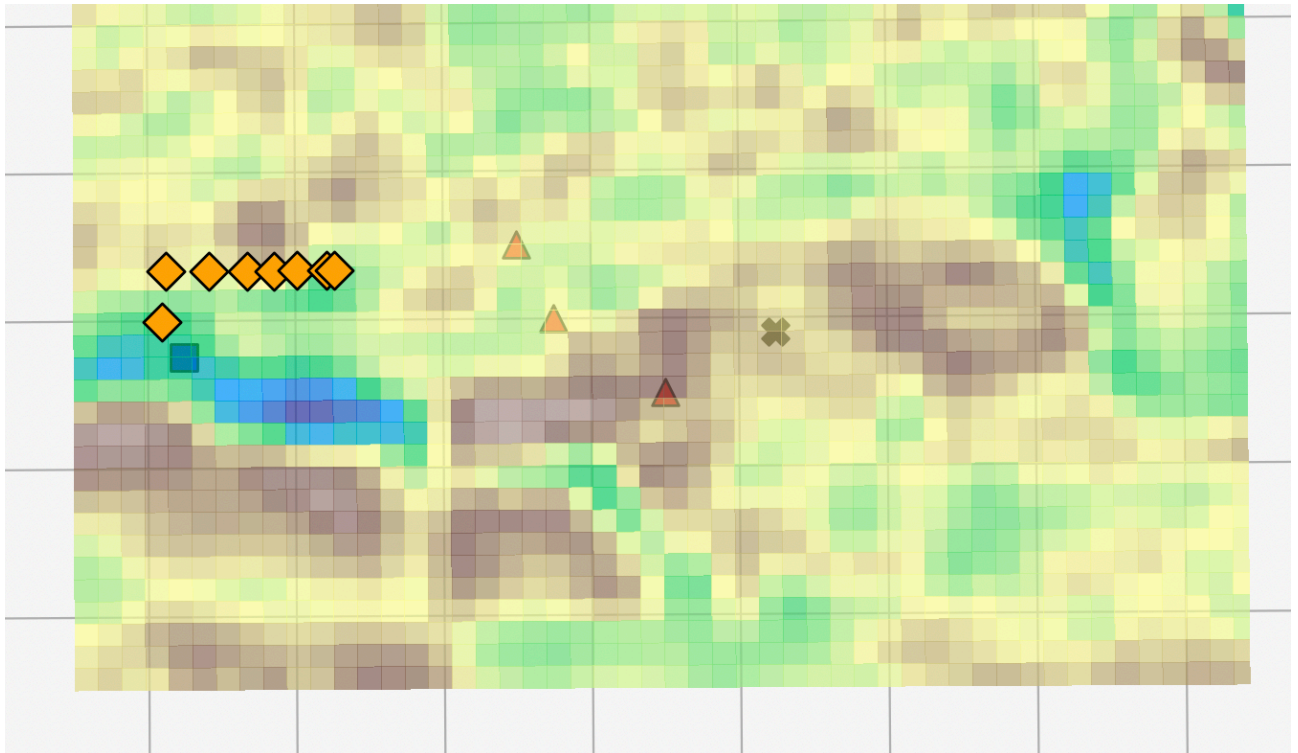


Рисунок 2.19 – Оптимізація позиціонування пристроїв за допомогою градієнтного спуску

На рисунку, який описує оптимізацію за допомогою градієнтного спуску видно, що точки сконцентровані в одній групі в зоні певного схилу. Це говорить про те, що алгоритм потрапив у локальний мінімум (внаслідок особливостей рельєфу) і не зміг з нього вибратися.

Ефективність: Найгірші показники в таблиці - величезний Score (70048) та аномальна дистанція (41.19 км).

Висновок: Для таких складних карт градієнтний спуск є непридатним, оскільки він занадто залежний від початкової точки та легко застрягає в неоптимальних зонах.

На рисунку, який описує розміщення дронів в результаті дії жадібного алгоритму, точки вишиковуються в певну лінію, намагаючись робити найкращий вибір. Алгоритм не заглядає вперед, а просто обирає наступний

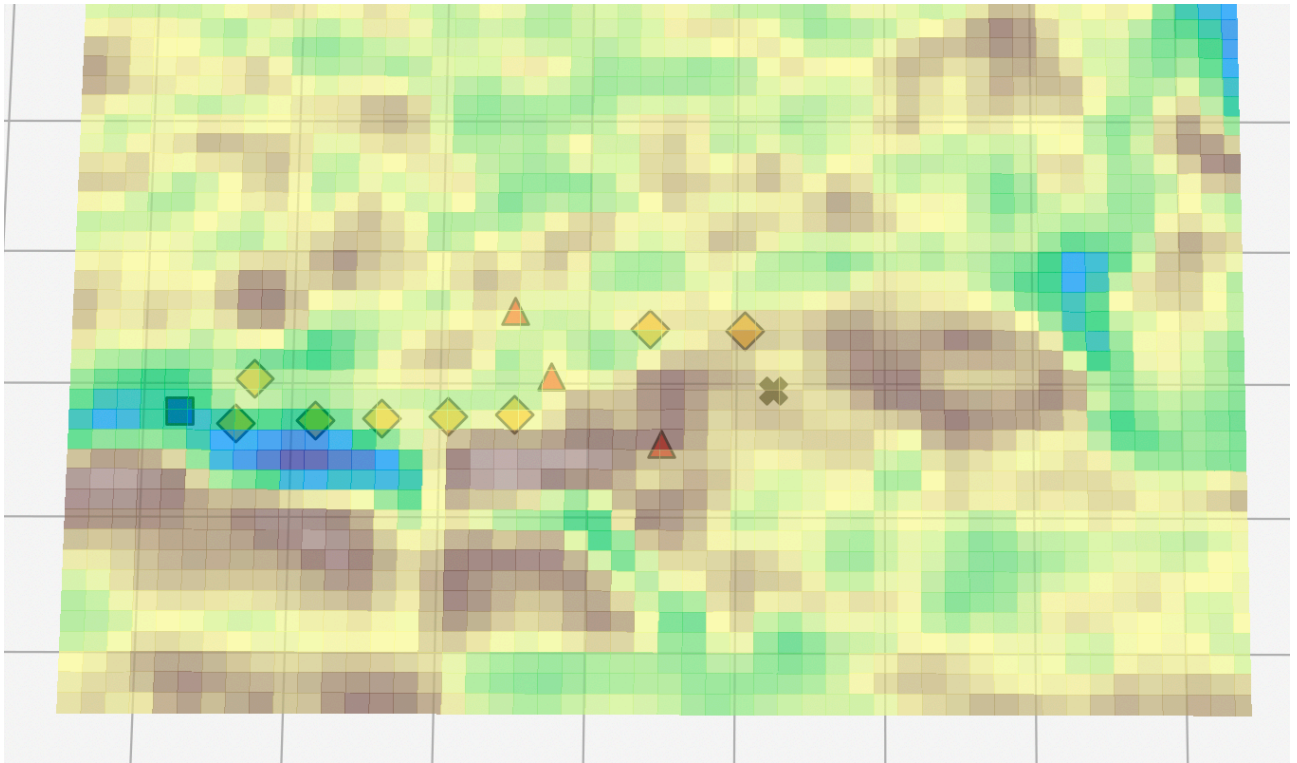


Рисунок 2.20 – Оптимізація позиціонування пристроїв за допомогою жадібного послідовного

найвигідніший крок в поточному контексті. Показник Score (3483) цього алгоритму значно гірший за генетичний, а дистанція зросла до 4.50 км. Однак, алгоритм показав хороший результат по швидкодії - 0.01 с.

Алгоритм доцільно використовувати для систем реального часу, де критично важливо прийняти рішення миттєво, навіть якщо воно не буде найкращим.

Розглядаючи поведінку пристроїв на карті, видно, що у випадку генетичного алгоритму точки (дрони) розосереджені по всій площині пошуку, що дозволяє алгоритму уникати локальних мінімумів і знаходити глобально оптимальне рішення. За даними таблиці, саме цей алгоритм досяг найнижчого (найкращого) показника цільової функції (213.31) та мінімальної дистанції (0.08 км.). Таким чином, цей алгоритм найкраще підходить для складних ландшафтів, де точність важливіша за швидкість обчислень, хоча 0.82 с. - це достатній рівень швидкодії.

Для оцінки розробленого алгоритму при застосуванні з різною кількістю БПЛА було проведено експеримент, що вимірює залежність часу виконання та

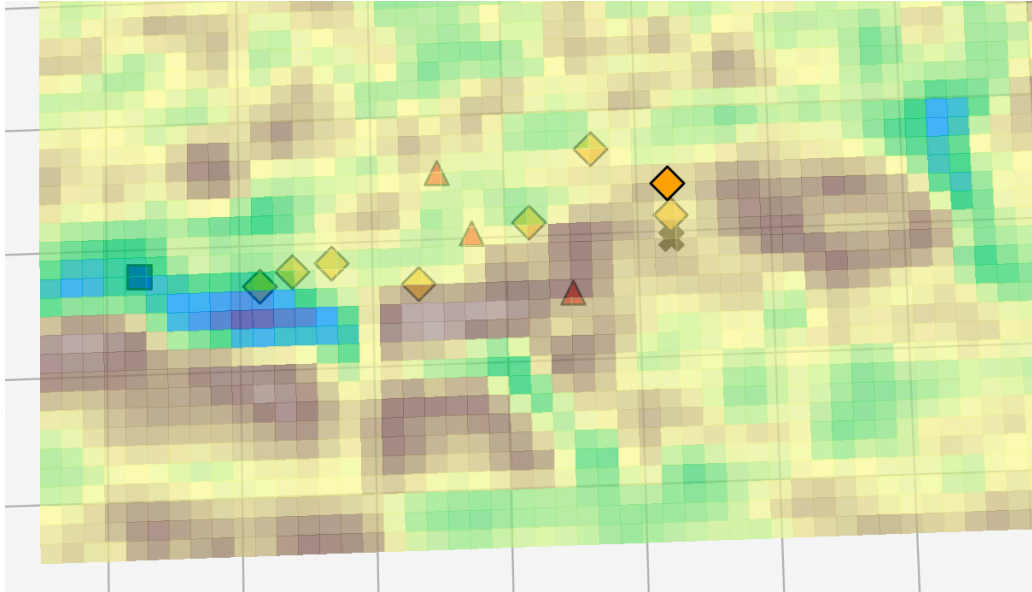


Рисунок 2.21 – Оптимізація позиціонування пристроїв за допомогою генетичного алгоритму

Таблиця 2.5 – Порівняльна характеристика ефективності роботи алгоритму

Кількість пристроїв	Час (с)	Значення цільової функції
10	1.23	185.42
20	3.67	142.18
50	18.45	98.33
100	65.21	76.92

результату від розміру мережі. Експеримент проводився на чотирьох конфігураціях рою з однаковими параметрами генетичного алгоритму та ідентичними вхідними даними (відстань 55.6 км, 3 зони електронної протидії), змінювалася лише кількість дронів від 10 до 100 одиниць. Час виконання генетичного алгоритму для різної кількості дронів склав 1.2 с для 10 дронів, 3.7 с для 20 дронів, 18.5 с для 50 дронів та 65 с для 100 дронів. (Таблиця 2.5)

Перевірено ефективність прокладання маршруту за допомогою LLM, з використанням шаблону запитів та без. У першому експерименті (Рис. 2.22) модель Claude Sonnet 4.6 прокладала маршрут дрона від бази до цілі без структурованого шаблону - маршрут пройшов через зону прямої видимості

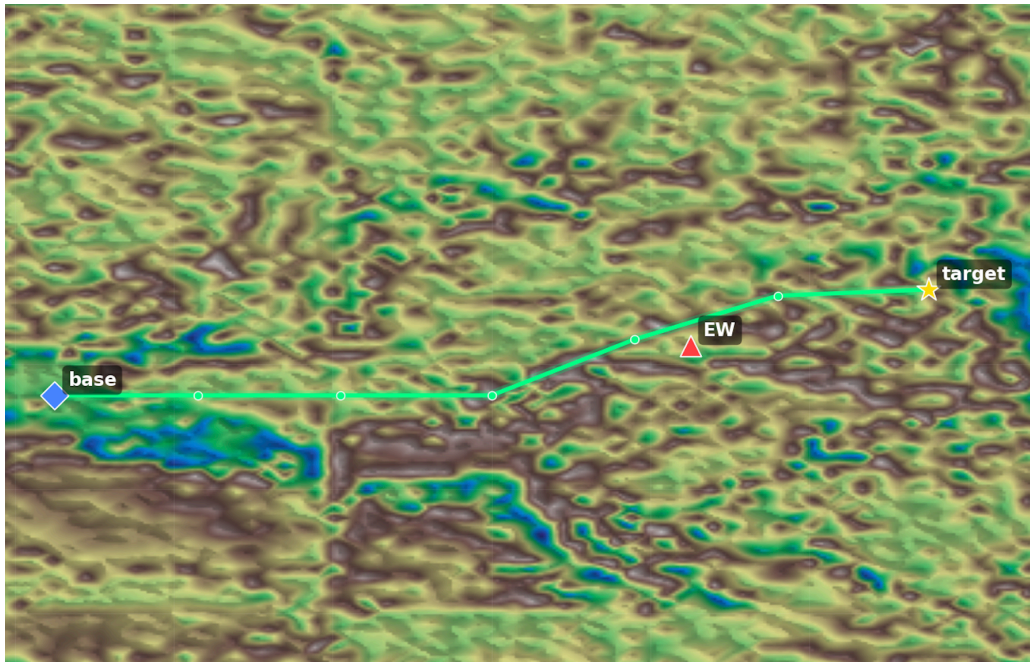


Рисунок 2.22 – Прокладання маршруту руху БпЛА без використання шаблону інструкції

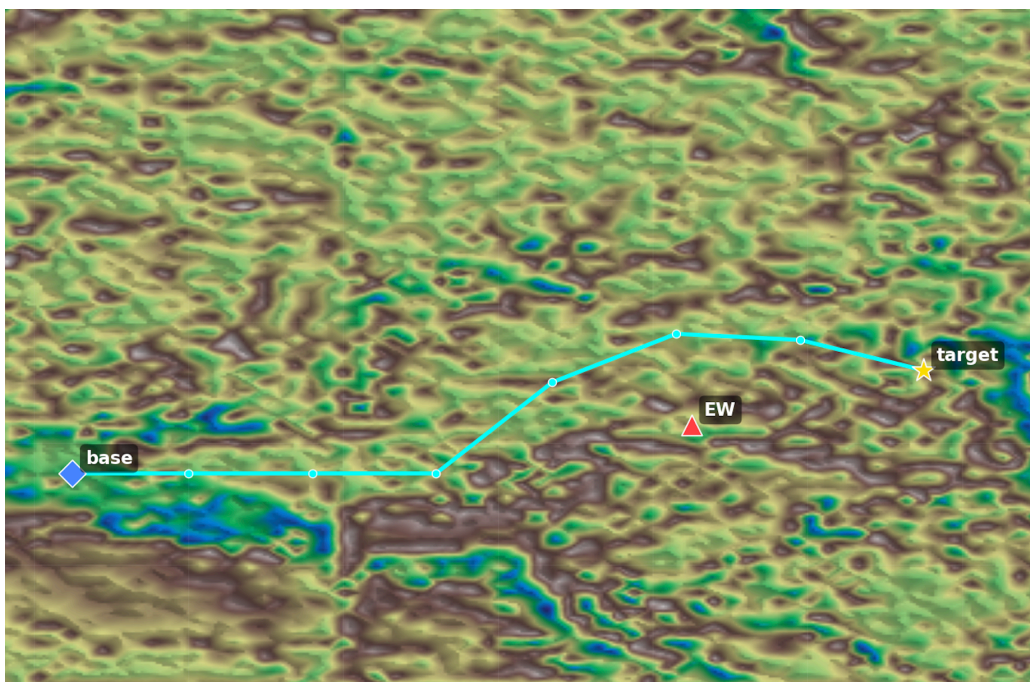


Рисунок 2.23 – Прокладання маршруту руху БпЛА з використання шаблону

РЕП станції, комунікація з пристроєм ускладнилась, в наслідок впливу топологічних перешкод та кіберфізичних загроз. У другому експерименті використовувався формалізований шаблон опису місії, зони покриття, правил

ведення операції та аналізу рельєфу - модель побудувала маршрут, повністю оминаючи зону виявлення РЕП та високі форми рельєфу. Результат підтвердив, що наявність структурованого контекстного шаблону дозволяє LLM враховувати зовнішні фактори та генерувати обґрунтовані рішення (Рис. 2.23).

Висновки до розділу 2

1. Сформульована задача побудови безпечних сценаріїв поведінки та оптимальної конфігурації мережі безпілотних літальних апаратів (БпЛА) в умовах кіберфізичного впливу, як пошук оптимальних маршрутів та просторового розміщення пристроїв для забезпечення надійної комунікації, обходу зон радіоелектронної протидії та адаптації до складного рельєфу.

2. Визначені критичні параметри для моделювання зон впливу ворожих технічних засобів радіоелектронної протидії: частотні діапазони, потужність та радіус придушення сигналів зв'язку та навігації. На основі цих властивостей та параметрів розроблено дві моделі з використанням апарату мереж Петрі (для окремого пристрою та для множини БпЛА) з метою спостереження за станами мережі та оцінки сценаріїв її роботи. Додатково визначено показники доступності мережі шляхом розрахунку пропускну здатності комунікаційного каналу в умовах завад.

3. Беручи до уваги необхідність мінімізації впливу засобів радіоелектронного придушення за умови збереження цілісності мережі, задача просторової оптимізації сформульована наступним чином: розподілити пристрої у просторі так, щоб мінімізувати комплексну цільову функцію, яка враховує відстань до цілі місії, топологічні перешкоди, необхідну висоту польоту та щільність мережевих з'єднань. Водночас, для забезпечення гнучкості керування в динамічному середовищі, задачу безпечної маршрутизації додатково зведено до застосування підходу на основі LLM, які прокладають оптимальні траєкторії з урахуванням висотних даних рельєфу (датасет Copernicus DEM).

4. Розроблені моделі та процедури були перевірені на контрольних прикладах симуляційного моделювання, за результатами яких було показано адекватну поведінку моделі Петрі згідно з досліджуваним сценарієм під час експериментальної перевірки для 76 пристроїв протягом шести кроків. Крім того, доведено, що отримана за допомогою генетичного алгоритму конфігурація забезпечує точність пошуку рішення (за показником Score) в середньому у 16 разів вищу за жадібний послідовний алгоритм та майже у 330 разів вищу за метод градієнтного спуску. Хоча генетичний алгоритм потребує

дещо більше часу на обчислення (0.82 с), він забезпечує збіжність до глобального оптимуму, уникаючи застрягання у локальних мінімумах складних ландшафтів. Також на контрольному прикладі для мережі до 100 пристроїв підтверджено ефективність методу прокладання маршрутів за допомогою LLM для обходу кіберфізичних загроз із застосуванням реальних топографічних даних, взятих з датасету [60].

РОЗДІЛ 3

МЕТОДИ ВИЯВЛЕННЯ НЕДОКУМЕНТОВАНИХ МОЖЛИВОСТЕЙ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ БЕСПЛОТНИХ ЛІТАЮЧИХ ПРИСТРОЇВ

У цьому розділі запропонуємо підхід до виявлення недокументованих можливостей у програмному забезпеченні БпЛА. Використаємо можливості Великих мовних моделей (LLM) у поєднанні з декомпіляторами через стандартизований протокол MCP у якості основи для аналізу машинного коду. Будемо вважати, що розроблена архітектура пошуку вразливостей є ефективною у порівнянні з існуючими методами динамічного аналізу, якщо вона дозволяє автоматизувати процес, знаходити помилки (наприклад, переповнення буфера) за значно менший час та приймає рішення з високим відсотком істинно позитивних спрацювань. Під час розробки методу автоматизованого аналізу будемо враховувати необхідність жорсткого задання контексту для штучного інтелекту, щоб уникнути помилкових висновків моделі, для чого побудуємо спеціалізовані структуровані шаблони запитів. Також розробимо загальну програмну модель та покроковий алгоритм виявлення вразливостей, які перевіримо в ході експерименту на реальних тестових бінарних зразках програмного забезпечення БпЛА.

3.1 Зворотна розробка прошивок за допомогою LLM

Застосування LLM для зворотної розробки вимагає задання контексту за допомогою шаблону запитів, інтеграції з зовнішніми інструментами аналізу, зокрема за допомогою Model Context Protocol (MCP).

Зв'язок між компонентами встановлюється за допомогою стандартизованого протоколу MCP [61], що дозволяє безперешкодно замінювати різні декомпілятори без зміни основної логіки взаємодії з LLM. Сервер MCP працює зовні клієнта та реалізований як окремий серверний додаток, що складається з двох модулів: мосту MCP та плагіна IDA Pro. Міст MCP надає стандартизований інтерфейс для зв'язку з клієнтами MCP, тоді як

плагін IDA Pro реалізує логіку серверної частини, надаючи доступ до RESTful JSON-RPC API для доступу до функціональності декомпілятора.

Міст MCP відіграє вирішальну роль посередника між клієнтськими додатками та плагіном IDA. Він забезпечує відповідність протоколу через Model Context Protocol, що дозволяє незалежно працювати плагіну в декомпіляторі IDA. Оскільки клієнт MCP може бути ініційований до завантаження плагіна, міст залишається активним весь час, підтримуючи динамічне та гнучке керування робочим процесом аналізу.

Технічно міст реалізовано як окремий сервер Python. Він автоматично аналізує код плагіна IDA, генерує визначення API та надає їх зовнішнім клієнтам, забезпечуючи безперешкодну сумісність між гетерогенними системами. Основна функція `make_jsonrpc_request` забезпечує надійний проксі-механізм для ретрансляції запитів до плагіна IDA через HTTP. Вона створює стандартизовані повідомлення JSON-RPC 2.0 з унікальними ідентифікаторами, інкапсулюючи назву методу, список параметрів та ідентифікатор запиту. Помилки, що повертаються плагіном IDA, автоматично перетворюються на винятки Python з розширеними діагностичними повідомленнями, включаючи коди помилок та детальні описи. Це дозволяє клієнтам LLM отримувати змістовну інформацію про збої під час виконання.

Сервер MCP для IDA Pro реалізовано у вигляді плагіна мовою Python, який функціонує як HTTP-сервер та надає програмний інтерфейс на основі архітектури REST із передачею даних у форматі JSON для доступу до можливостей декомпілятора. Плагін побудований на основі вбудованого модуля веб-сервера мови Python та взаємодіє з IDA Pro через програмний інтерфейс IDAPython, забезпечуючи контрольований і надійний доступ до середовища дизасемблювання та декомпіляції.

Архітектура запропонованої системи наведена на рисунку 3.1.

3.2 Пошук вразливостей в прошивках за допомогою LLM

3.2.1 Виявлення вразливостей в бінарних зразках БпЛА

Сучасні мережі безпілотних літальних апаратів є складними системами, успішна робота яких, в тому числі залежить від встановленого програмного

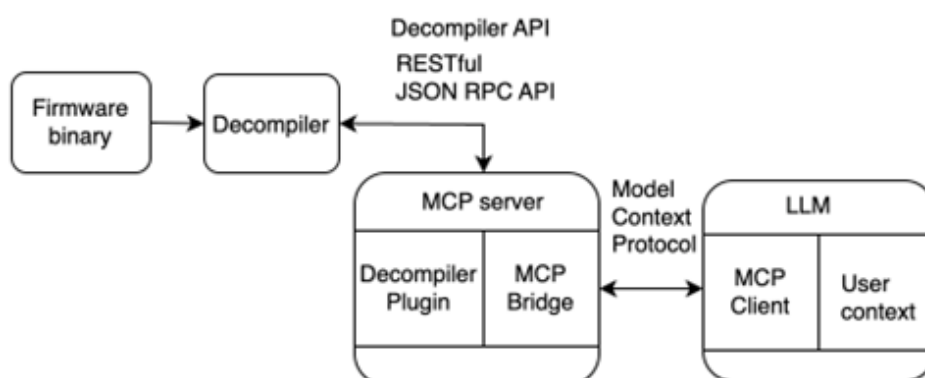


Рисунок 3.1 – Архітектура системи зворотної розробки з допомогою LLM

забезпечення. Порушення цілісності пристроїв через впровадження шкідливого програмного забезпечення дозволяє зловмисниками перехоплювати керування та маніпулювати даними телеметрії. Використання комерційних прошивок або аналіз прошивок трофейних пристроїв з закритим кодом значно ускладнює пошук вразливостей, досліднику необхідно витратити час на проведення статичного та динамічного аналізу, маючи в наявності тільки асемблерний код. Також необхідні великі технічні ресурси для проведення фазингу. З розвитком нових технічних функцій, збільшується кількість можливих вразливих модулів, наявних в комплексному апаратному забезпеченні пристроїв. Використання LLM, значно пришвидшує пошук автоматично аналізуючи код, спрощуючи його, додаючи коментарі та виконуючи інші засоби форматування. Сучасні дослідження підтверджують, що великі мовні моделі досить ефективно можуть знаходити вразливості навіть в захищеному, обфускованому коді. Порівнюючи з наявною базою LLM може робити висновки про потенційно вразливі частини коду, розробити послідовність дій для експлуатації. Досліднику необхідно лише зробити перевірку отриманого результату, висновки щодо наявних вразливостей, та затвердити виправлення в майбутніх версіях коду. Це стає можливим за рахунок здатності моделей робити логічні висновки та інтеграцією з інструментами зворотної розробки та динамічного аналізу за допомогою протоколу MCP (Model Context Protocol). Впровадження автоматизованих методів на основі LLM дозволяє масштабувати та пришвидшити процес виявлення загроз.

3.2.2 Побудова шаблону запитів для бінарного аналізу та пошуку вразливостей

Запит до LLM для проведення бінарного аналізу повинен враховувати наступні положення:

1. Необхідно контекстуалізувати специфіку аналізованого бінарного файлу та описати архітектуру, операційну систему, компілятор, інші відповідні дані (розмір, положення точки входу, тип – ELF/PE/raw).

2. Запит має бути добре структурованим та містити такі частини:

- Завдання, коротка мета аналізу;
- Інструкції, які має виконати LLM;
- Обмеження (наприклад, заборона використання методу грубої сили);
- Результати дослідження (наприклад, звіт);

3. Повинні бути чіткі інструкції щодо використання інструментів (зокрема, інструментів MCP).

4. Звітність має бути обов'язковою, а формат звіту має бути вказаний (наприклад, .md або інший стандартний файл). Слід наголосити, що звіт повинен містити логічне пояснення, підкріплене практичними прикладами коду.

5. LLM має бути наказано уникати хибних спрацьовувань та має бути зазначений тип вразливості, який потрібно знайти.

6. Аналіз слід зупиняти лише після повного охоплення коду (не генерувати звіт, доки не буде перевірено кожну функцію).

На рисунку 3.2 наведено шаблон такого запиту.

3.2.3 Метод виявлення вразливостей за допомогою LLM та нова архітектурна модель пошуку вразливостей

Розглянемо методику у вигляді покрокового алгоритму для виявлення та обробки вразливостей у програмному забезпеченні БПЛА з урахуванням відомих вразливостей. Алгоритм включає такі основні етапи: попередня обробка, статичний аналіз, динамічний фаззинг, зворотне проектування за допомогою LLM, кореляція CVE та звітність. Структура алгоритму

```

Task:
You are tasked with analyzing a binary file using IDA Pro through the
MCP server. The goal is to perform a static reverse engineering process
and identify vulnerabilities or recover logic, depending on the mode.
Target Info:
- CPU Architecture: [ARCH]
- OS: [OS_TYPE]
- Compiler: [COMPILER_TYPE]
- Binary Type: [ELF/PE/Raw/Other]
Instructions:
1. Start with decompiled view using IDA Pro.
2. If information is lacking -- disassemble the function and inspect
assembly.
3. Use MCP tools for:
  - Number conversion (`convert_number`)
  - Extracting xrefs, call graphs, and control flow
  - Type correction assistance
4. Rename all unknown functions and variables to **descriptive
names**.
5. Add comments to explain control logic and unusual behaviors.
6. If task = vulnerability analysis:
  - Check all functions for memory corruption, type confusion, use-
after-free, etc.
  - Only report high-confidence issues.
  - Describe exploitability, crash reproduction steps, and potential
patching.
7. If task = password/key extraction:
  - Trace constants and logic flow.
  - DO NOT guess or brute-force passwords.
  - If value cannot be derived statically -- explain why.
Restrictions:
- No brute-force.
- No external guesswork or statistical assumptions.
- No manual base conversion – always use tools.
- Do not terminate until all relevant functions are analyzed.

Output:
- Save all findings and methodology to `report.md`.
- Use clear Markdown formatting:
  - Section: Overview
  - Section: Analysis per Function
  - Section: Vulnerabilities (if any)
  - Section: Recommendations or Patch (if any)
- Prompt the user with final results only after report is complete.

```

Рисунок 3.2 – Шаблон запиту для бінарної зворотної розробки з LLM

представлена на рисунку 3.3.

Нехай V – це бінарний файл (прошивка, бібліотека або виконуваний файл БПЛА), M – метадані про бінарний файл (наприклад, архітектура, платформа, підсистема БПЛА), а CVE_DB — публічна база даних CVE, що містить відомі бінарні вразливості (наприклад, канали MITRE/NVD). Виходом алгоритму є R — структурований звіт про вразливості, який включає як нещодавно виявлені, так і відповідні CVE вразливості.

Введемо наступні позначення, для опису математичного алгоритму:

```

1. Preprocessing:
  1.1 Extract metadata from B: architecture, format (ELF/PE), stripped/unstripped
  1.2 IF B is stripped THEN
    Attempt symbol recovery (e.g., via heuristics or pattern matching)
  ENDIF
2. Static Analysis:
  2.1 Select decompiler (IDA, Ghidra, Binary Ninja) based on platform
  2.2 Decompile and analyze B to construct CFG/DFG
  2.3 Identify suspicious patterns:
    - Buffer overflows
    - Use-after-free
    - Integer overflows
    - Format string issues
  2.4 IF dangerous patterns found THEN
    Tag B as "memory-risk"
3. Dynamic Fuzzing:
  3.1 Create sandbox environment (e.g., QEMU, ASAN builds)
  3.2 Execute fuzzing using AFL++ or LibFuzzer
  3.3 FOR each crash DO
    IF ASAN or valgrind confirms memory violation THEN
      Store crash signature
    ENDIF
  ENDFOR
4. LLM-Assisted Reverse Engineering:
  4.1 IF M.requires_deep_inspection THEN
    Extract vulnerable-looking functions
    Generate LLM prompt with function code, metadata, task
    Query LLM for vulnerability analysis
    IF LLM reports exploitable issue THEN
      Store vulnerability type, location, PoC
    ENDIF
  ENDIF
5. CVE Correlation:
  5.1 FOR each confirmed vulnerability V in B DO
    Compute or extract:
    - Function name
    - Code fingerprint (e.g., hash, opcode signature)
    - File/module name
    - Behavior trace (if crash)
  5.2 Search CVE_DB for match by:
    - Affected software component
    - Code fingerprint similarity
    - Vulnerability class (e.g., heap overflow in MAVLink parser)
  5.3 IF match found in CVE_DB THEN
    Tag V with CVE ID (e.g., CVE-2024-38952)
    Retrieve CVSS score and remediation data
  ELSE
    Tag V as "potential 0-day"
  ENDFOR
6. Reporting and Remediation:
  6.1 Generate report R:
    - List of vulnerabilities
    - Mapped CVEs (if any)
    - Severity ratings (CVSS or inferred)
    - Exploitation conditions and PoC
    - Recommended fixes (code or architecture)
  6.2 Export R as:
    - Human-readable PDF/Markdown
    - JSON for integration with SIEM, issue trackers
RETURN R

```

Рисунок 3.3 – Алгоритм DetectMemoryCorruptionWithCVE(B, M, CVE_DB)

для виявлення вразливостей, пов'язаних із пошкодженням пам'яті

- M — Шкідливе програмне забезпечення (Malware).
- $D = \{D_1, D_2, \dots, D_n\}$ — Множина автономних дронів у рою.

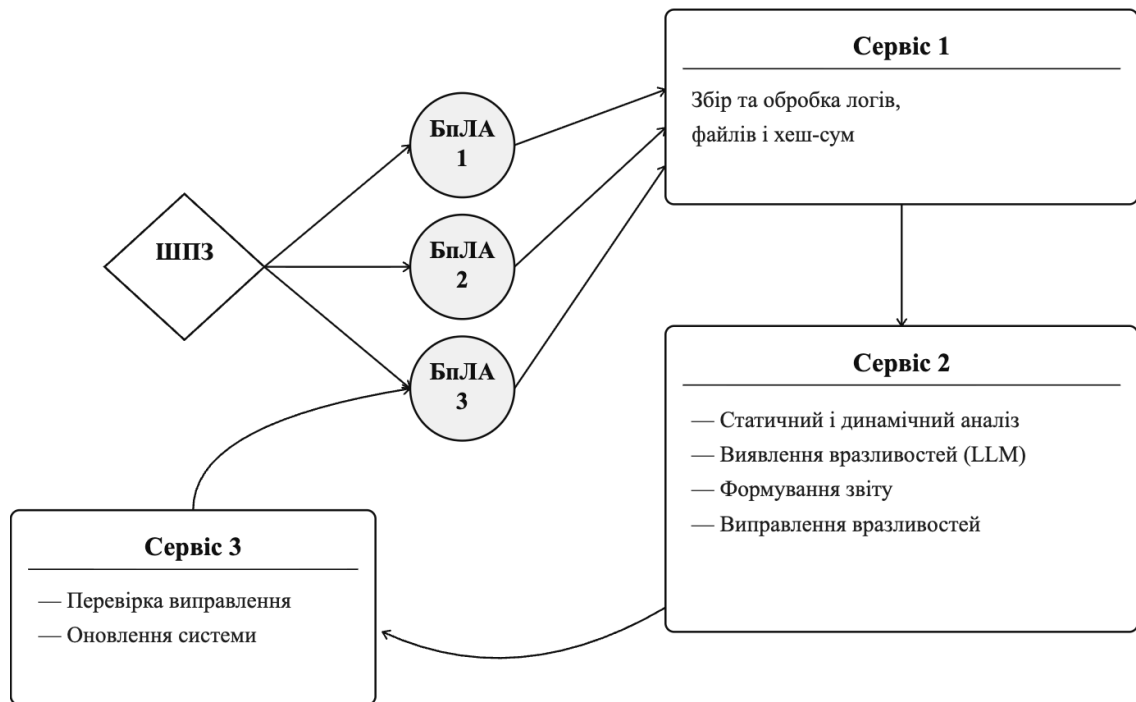


Рисунок 3.4 – Нова архітектурна модель виявлення вразливостей у ПЗ БпЛА в складі архітектури роботи центра безпеки

- S_1 — Security Service 1: Збір та обробка даних (логи, файли, хеші).
- S_2 — Security Service 2: Аналіз (статичний/динамічний, LLM) та генерація патчів.
- S_3 — Security Service 3: Верифікація патчів та оновлення системи.

На основі аналізу запропонованих рішень, інтеграція моделі в загальну систему захисту зображена на рис. 3.4 та описується наступним чином:

Схематичне представлення на 3.4 ілюструє практичне впровадження розробленої моделі в структуру центру управління кібербезпекою безпілотних авіаційних систем. Ця архітектурна побудова спрямована на ефективну протидію розповсюдженню шкідливого коду та запобігання використанню системних уразливостей у комунікаційному середовищі БпЛА. Встановлено, що процеси ідентифікації деструктивного впливу ШПЗ та виявлення компрометованих ділянок базуються на тих самих фундаментальних принципах, що й стандартний пошук вразливостей. З огляду на це, представлена модель архітектури є релевантною для реалізації механізмів цифрового самозахисту (імунітету) в межах централізованої системи безпеки

автономного рою. 3.4 фактично відображає концептуальну схему імунного захисту групи БпЛА, яка розгортається у п'ять послідовних стадій.

1. Етап моніторингу та ідентифікації загроз (пункти 1–2) передбачає систематичну передачу дронами телеметричних показників, системних журналів та контрольних сум (хешів) критично важливих конфігурацій до центру обробки.

2. У ситуаціях, коли фіксуються аномальні відхилення або невідповідність хеш-значень, центр ініціює запит на отримання повних дамів бінарних файлів для проведення ретельного дослідження.

3. Процедура інтелектуального аналізу за допомогою LLM та формування захисних рішень (пункти 3–4) включає автоматизовану обробку отриманих зразків згідно з авторською методикою.

4. Саме на цій стадії, де визначається траєкторія атаки та генерується програмне виправлення (патч), задіюється базова архітектурна модель, що була деталізована на рис. 1.

5. Важливою складовою представленої схеми є процес верифікації патчів (пункт 5) — перевірка працездатності та безпеки автоматично згенерованого коду перед його фінальним розгортанням.

6. Після успішного затвердження, виправлення безпеки транслуються через криптографічно захищені канали зв'язку на вибрані вузли або на всі пристрої рою за допомогою технології Over-the-Air (OTA).

7. Такий інтегрований підхід дозволяє максимально оперативно нейтралізувати джерела інфекції або інші цифрові загрози в масштабах усієї мережі безпілотних апаратів.

Нижче наведено формалізований алгоритм дій при виявленні вразливості:

```

1 Phase I: Detection (Monitoring)
2 foreach drone  $D_i \in D$  do
3   if threat_detected( $M, D_i$ ) then
4     | Extract logs  $L_i$ , capture files  $F_i$ , calculate hashes  $H(F_i)$ 
5     | Transmit  $\{L_i, F_i, H(F_i)\} \rightarrow S_1$ 
6   end
7   else
8     | Continue routine telemetry
9   end
10 end
11 Phase II: Analysis & Generation (Intelligence)
12 if data_received( $S_1$ ) then
13   | Invoke  $S_2$  for Static/Dynamic analysis
14   | Run LLM_vulnerability_discovery( $L_i, F_i$ )
15   | Generate Security Report  $R$  and Patch  $P$ 
16   | Send  $P \rightarrow S_3$ 
17 end
18 Phase III: Remediation (Action)
19 foreach drone  $D_i \in D$  do
20   | Apply patch  $P$  via  $S_3$ 
21   if verify_patch( $P, D_i$ ) == Valid then
22     | Update system to version  $V_{new}$ 
23   end
24   else
25     | Rollback to  $V_{stable}$  and trigger administrator alert
26   end
27 end

```

3.3 Контрольний приклад експериментальної перевірки запропонованого методу та архітектури для виявлення вразливостей

Для проведення експериментів було використано наступні вихідні дані та програмні рішення:

1. Як вихідні зразки було використано бінарні зразки ПЗ БпЛА у кількості 21 екземпляра, в частині з них були задокументовані вразливості, відомі досліднику, інша частина вразливостей була впроваджена дослідником самостійно.

2. Для реалізації методу та втілення моделі комунікаційної архітектури було використано наступні програмні рішення:

- LLM Claude Sonnet 4.0 та протокол MCP;
- декомпілятор IDA Pro Hex-Rays;
- декомпілятор Binary Ninja;
- фаззер AFL++.

З огляду на те, що вразливості були відомі, стало можливим визначити показник істинно-позитивних спрацювань, важливих для цього експерименту. Ці дані наведено в Табл. 3.1.

Таблиця 3.1 – Результати порівняльного аналізу методів виявлення вразливостей

Метод	Істинно-позитивні, %	Хибно-позитивні, %	Середній час, хв
Фазинг з використанням AFL++	93.3	0.0	40.4
Binary Ninja та Claude Sonnet 4.0	66.7	0.3	4.2
IDA Pro Hex-Rays та Claude Sonnet 4.0 (стандартний режим)	80.0	0.26	3.5
IDA Pro Hex-Rays та Claude Sonnet 4.0 (режим розширеного мислення)	94.7	0.28	9.7

Аналіз був виконаний по різних типах ПЗ систем БпЛА, серед яких були

не лише прошивки самих БпЛА, а й застосунки, притаманні скоріше центрам управління БпЛА.

Зокрема, особливу увагу було приділено категорії драйверів Living Off The Land (LOLDrivers). Цей клас програмного забезпечення становить критичну небезпеку для інфраструктури БпЛА, передусім для наземних пунктів управління, що функціонують у середовищі Windows.

Хоча LOLDrivers за своєю природою не є шкідливими та мають легітимне цифрове підписання, наявність у них вразливостей дозволяє зловмисникам маніпулювати режимом ядра. Експлуатація таких драйверів відкриває можливості для обходу систем захисту, несанкціонованого читання чи модифікації пам'яті ядра, а також виконання довільного коду з найвищими привілеями.

У контексті експлуатації безпілотних систем компрометація наземної станції через вразливий драйвер може призвести до:

- перехоплення та підміни телеметричних даних;
- дистанційного втручання в роботу автопілота;
- повної втрати контролю над виконанням польотного завдання.

Практична апробація методу здійснювалася на прикладі драйвера BdApiUtil.sys. Результати аналізу (рис. 3.5) підтвердили здатність системи точно ідентифікувати функції, придатні для деструктивного використання, та надавати змістовні рекомендації щодо запобігання їх експлуатації. Підсумковий звіт, сформований LLM, містить два ключові блоки:

1. Технічна ідентифікація: стислі метадані драйвера та набір індикаторів компрометації (IoC), включаючи унікальні хеш-суми.

2. Аналітичний розбір: розгорнута характеристика виявленої вразливості та її класифікація згідно з чинними стандартами безпеки.

Для аналізу було використано драйвер BdApiUtil.sys (Рис. 3.5), присутній на ОС Windows, яку оператори можуть використовувати для обробки та візуалізації розвідданих, отриманих безпосередньо з БпЛА.

Консольний інструментарій та динамічні бібліотеки складають основу програмного забезпечення БпЛА. З метою верифікації запропонованого підходу було проведено серію тестів, спрямованих на виявлення критичних дефектів у бінарних файлах такого типу.

CVE Classification**CRITICAL** - Arbitrary Process Termination without Authentication**Root Cause**

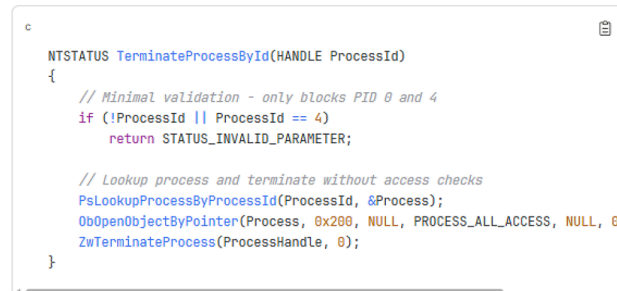
The driver exposes IOCTL handlers that allow terminating any process by Process ID (PID) without performing proper access control checks or privilege validation.

Technical Analysis**Vulnerable Components:****1. Device Creation (DriverEntry - 0x28860)**

- Device created without security descriptor
- Any user can open handle to \DosDevices\BdApiUtil
- No access control restrictions implemented

2. IOCTL Dispatcher (DeviceIoControlDispatcher - 0x28630)

- Handles multiple IOCTL codes without authentication
- IOCTL 0x800024B4 triggers process termination via standard API
- IOCTL 0x800024B8 triggers process termination via SSDT manipulation
- No privilege checks before processing dangerous operations

3. Process Termination Handlers: TerminateProcessById (0x152b0):


```

c
NTSTATUS TerminateProcessById(HANDLE ProcessId)
{
    // Minimal validation - only blocks PID 0 and 4
    if (!ProcessId || ProcessId == 4)
        return STATUS_INVALID_PARAMETER;

    // Lookup process and terminate without access checks
    PsLookupProcessByProcessId(ProcessId, &Process);
    ObOpenObjectByPointer(Process, 0x200, NULL, PROCESS_ALL_ACCESS, NULL, 0,
        ZwTerminateProcess(ProcessHandle, 0));
}

```

Рисунок 3.5 – Результат пошуку вразливостей в драйвері BdApiUtil.sys

Варто зауважити, що консольні компоненти часто вразливі до класичних помилок керування пам'яттю, таких як:

- stack-based buffer overflow (переповнення стекового буфера);
- use-after-free (використання пам'яті після її вивільнення);
- double-free (подвійне очищення однієї ділянки пам'яті);
- format string vulnerabilities (вразливості рядка форматування).

Для проведення експерименту було відібрано репрезентативні бінарні зразки, що містять навмисно інтегровані вразливості. Ці дефекти моделюють реальні загрози, які зустрічаються у вбудованих прошивках (firmware) та модулях планування польотних завдань. Незважаючи на відносно лінійну логіку виконання обраних файлів, вони є ефективними еталонами для оцінки спроможності LLM інтерпретувати низькорівневі конструкції коду.

Практичним прикладом роботи методу є аналіз утиліти MAVLink Router (mavlink-routerd). На рис. 3.6 представлено фрагмент аналітичного звіту, в якому успішно ідентифіковано та описано механізм переповнення буфера у

зазначеному застосунку.

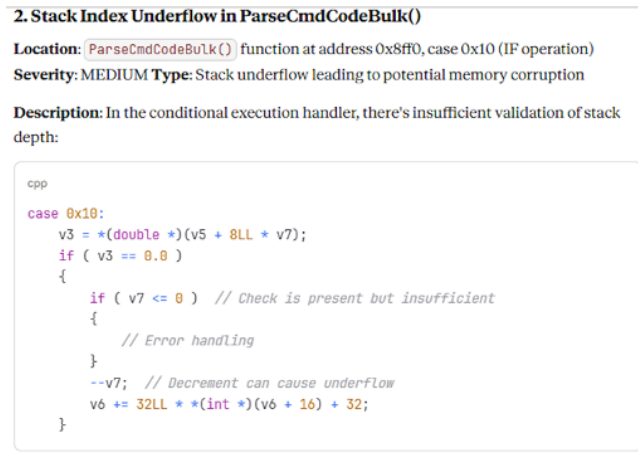


Рисунок 3.6 – Фрагмент звіту застосунку mavlink-routerd

Окремий етап досліджень був присвячений аналізу спеціально підготовлених програмних засобів із штучно внесеними дефектами безпеки. Для проведення цього експерименту вразливість була імплементована у вихідний код відкритого проєкту на мові C++, яка є загальноприйнятим стандартом для розробки високонавантажених компонентів систем БпЛА.

Результати, представлені на рис. 3.7, демонструють успішну верифікацію та локалізацію вразливості. Це підтверджує високу ефективність запропонованого методу в ідентифікації безпекових ризиків у програмному забезпеченні, що побудоване за принципами об'єктно-орієнтованого програмування (ООП). Отримані дані свідчать про здатність системи аналізувати складні ієрархії класів та взаємодії між об'єктами, що є характерним для сучасного ПЗ керування безпілотними комплексами.

Для об'єктивної оцінки ефективності розробленого методу було проведено порівняльне дослідження з використанням динамічного аналізу, а саме — фазингу на базі інструмента AFL++ із застосуванням розширених стратегій мутацій. Вибір AFL++ обумовлений тим, що він, подібно до нашого статичного підходу, здатний обробляти довільні бінарні файли, зокрема ті, з яких видалено налагоджувальну інформацію (stripped binaries). Це ставить обидва методи в схожі умови нестачі вхідних даних, що забезпечує репрезентативність та коректність отриманих результатів.

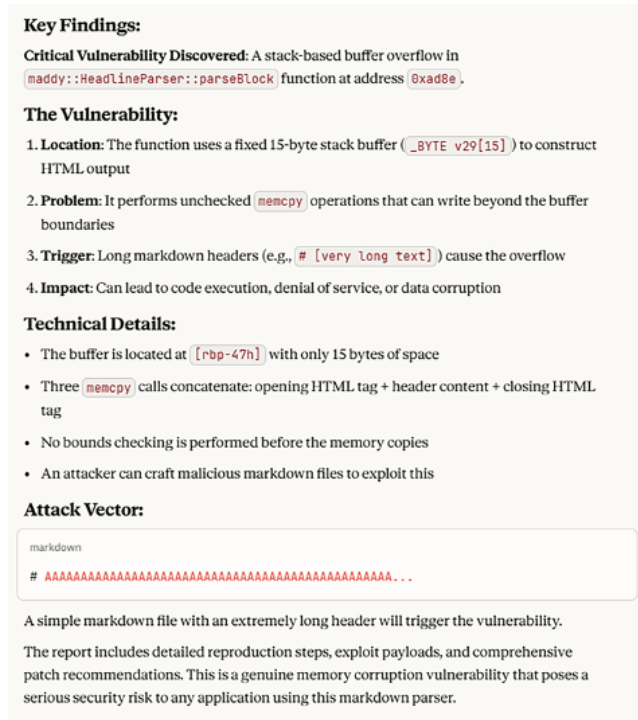


Рисунок 3.7 – Фрагмент звіту про вразливість переповнення буферу

Крім того, у межах експерименту було проведено крос-платформенне порівняння різних конфігурацій інтеграції LLM із середовищами зворотного проектування:

1. Поєднання Binary Ninja та Claude Sonnet 4.0 через протокол MCP;
2. Зв'язка IDA Pro Hex-Rays із Claude Sonnet 4.0, протестована у різних режимах функціонування мовної моделі.

Загальна вибірка для дослідження склала 21 бінарний зразок, що охоплює широкий спектр потенційних вразливостей. Детальні кількісні та якісні показники цього порівняння систематизовано та наведено у табл. 3.1

Висновки до розділу 3

1. Запропонована архітектура взаємодій між LLM контекстом користувача та інструментами бінарного аналізу, яка відрізняється від існуючих рішень високою гнучкістю, масштабованістю та використанням стандартизованого протоколу MCR для виявлення недокументованих можливостей у прошивках БпЛА.

2. Визначені ключові параметри та структурований підхід до формування файлів інструкцій, що забезпечує їх багаторазове використання на різних зразках коду. Від існуючих рішень ця структура відрізняється наявністю сталих блоків інструкцій та змінних полів, які заповнюються залежно від конкретного зразка, що зводить роботу дослідника до простих дій і значно знижує вимоги до кваліфікації інженера.

3. Беручи до уваги обмеження класичних методів динамічного аналізу щодо швидкості роботи та високого порогу входу для спеціалістів, задачу пошуку вразливостей зведено до виконання формалізованого покрокового алгоритму. Цей алгоритм поєднує можливості семантичного розбору LLM та декомпіляції машинного коду.

4. Розроблений загальний метод пошуку вразливостей та автоматизації реверс-інжинірингу, практична частина якого представлена у формі алгоритму взаємодії з LLM, що забезпечує підвищену швидкодію порівняно з існуючими підходами.

5. Розроблений метод та архітектурна модель були перевірені на контрольних прикладах під час аналізу реальних бінарних файлів, довівши свою високу ефективність. Встановлено, що інтеграція IDA Pro та Claude Sonnet 4.0 у режимі розширеного мислення забезпечує найвищу точність виявлення вразливостей (94,7%), що перевищує показники класичного фазингу (AFL++). Водночас запропонований підхід дозволяє прискорити процес аналізу від 4 до 11,5 разів порівняно з динамічними методами, зберігаючи при цьому вкрай низький та прийнятний рівень хибно-позитивних спрацювань (не більше 0,3%).

РОЗДІЛ 4

ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ ТА МЕТОДІВ

У цьому розділі об'єднаємо розроблені у роботі моделі, методи та алгоритми в рамках єдиного програмного комплексу для забезпечення кіберфізичної стійкості мереж БПЛА, ґрунтуючись на визначеному сценарії виконання місії в умовах зовнішнього ворожого впливу. Також, наведемо приклад покрокового застосування розроблених рішень для моніторингу станів рою, прокладання безпечних маршрутів та просторової оптимізації мережі.

Наведемо опис практичного застосування розробленого програмного забезпечення, яке реалізує алгоритми та архітектурні рішення, викладені у роботі. Наведемо приклади його використання в рамках обчислювальних експериментів: для симуляції роботи мережі зі 100 БПЛА з метою прогнозування критичних станів під дією засобів РЕП та топологічних перешкод, розрахунку пропускної здатності каналів зв'язку, а також для автоматизованого пошуку бінарних вразливостей у модулях польотного контролера PX4.

Плануються наступні дії:

1. Провести спостереження стану мережі БПЛА, як стан кожного пристрою, так і зріз станів усієї мережі, на основі розроблених моделей у формі мереж Петрі.
2. Використати частину спостережуваних пристроїв для визначення можливості та планування виконання місії (100 екземплярів). В сценарії сплановано місію БПЛА, виходячи із даних рельєфу та розташування пункту призначення. Пристрої повинні уникати населених пунктів, однак, обійти задані точки.
3. Додатковою задачею є оптимальне виконання місії - при залученні заданого в розділі критерію оптимізації.
4. При виконанні п. 2) 3) необхідно врахувати додаткові дані, зокрема - затримки, які виникають, та пропускну здатність мережі
5. Під час виконання місії вважається, що у складі пристроїв може

міститись вразливість, яка потребує негайного виявлення та виправлення. Провести аналіз щодо часу опрацювання зразків прошивок пристроїв, та можливі комунікаційні затримки. Зробити висновок про придатність методу для використання в реальних умовах.

4.1 Моніторинг станів вузлів мережі БпЛА засобами апарату мереж Петрі

Для проведення експерименту було взято 100 дронів, та прокладено різні маршрути для кожного з них. (Рисунок 4.1)

Під час симуляції можна було спостерігати за силою сигналу ста дронів. Таблиця 4.1 містить детальний розподіл кількості дронів відповідно до кожного рівня сигналу (від 0 до 3).

Таблиця 4.1 – Розподіл сигналів дронів за кроками симуляції

Крок (x)	Сигнал 0	Сигнал 1	Сигнал 2	Сигнал 3
Крок 0	0	0	0	100
Крок 1	2	76	12	10
Крок 2	24	21	53	2
Крок 3	26	0	74	0
Крок 4	36	0	64	0
Крок 5	0	0	100	0

1. Крок 0: Симуляція починається з того, що всі дрони підтримують максимальний рівень сигналу. Усі 100 пристроїв знаходяться на рівні 3, що свідчить про правильну конфігурацію мережі перед початком активної фази місії.

2. Крок 1-2: На першому кроці значна частина мережі стикається з певними перешкодами, що призводить до зниження сигналу до мінімального значення. Лише 10 пристроїв зберігають максимальний рівень сигналу, тоді в 76 пристроїв сигнал знизився на 1. На другому кроці спостерігається подальше погіршення: 24 дрони фіксують нульовий сигнал, що вказує на

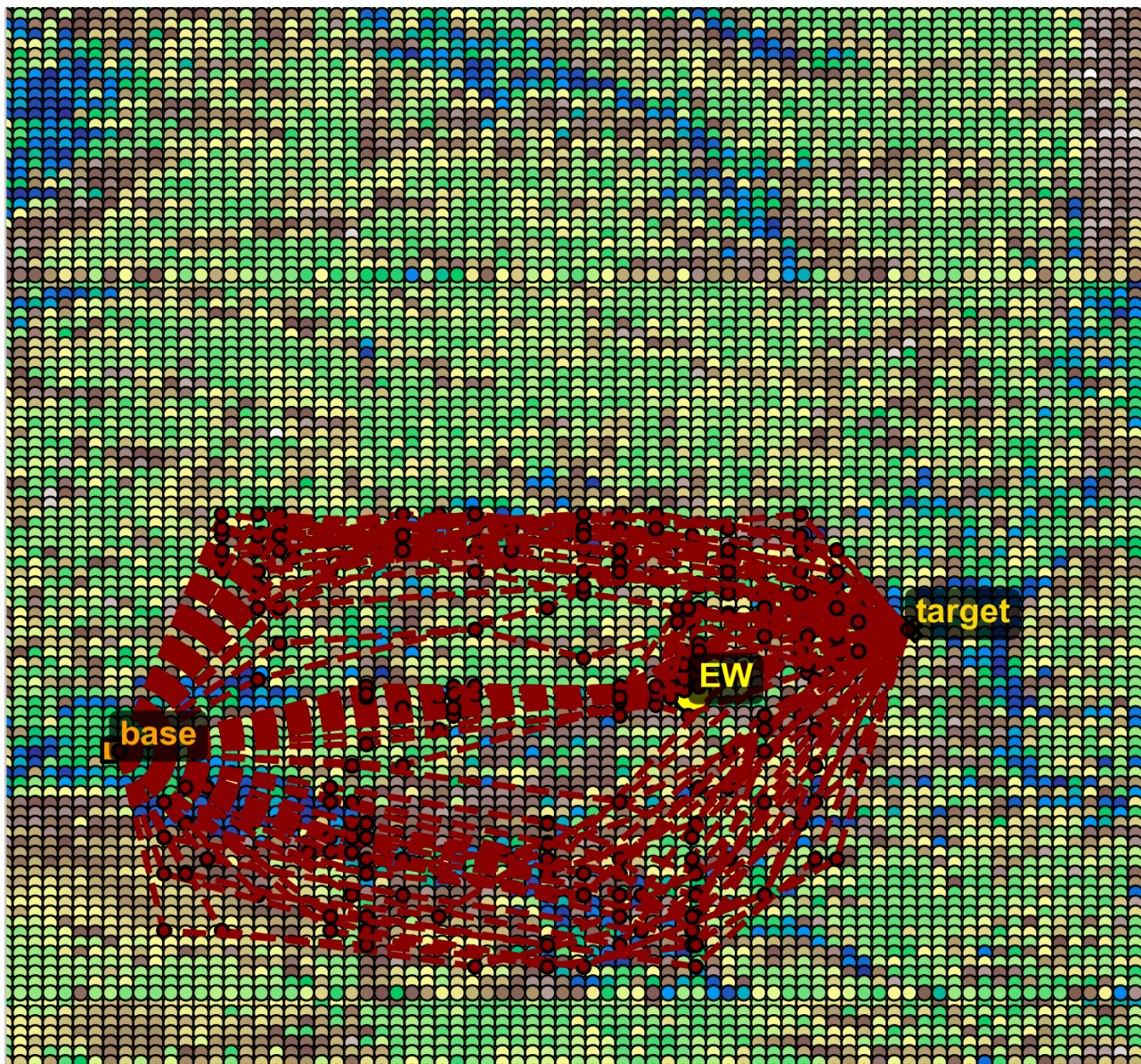


Рисунок 4.1 – Тестові маршрути БпЛА

потрапляння частини рою в зони інтенсивного завадового впливу.

3. Крок 3-4: Система намагається адаптуватися, переводячи 74 дрони на помірний рівень. Проте четвертий крок стає критичною точкою місії: кількість пристроїв із повною втратою сигналу сягає максимуму — 36 одиниць. Це спричинено проходженням рою поблизу засобів РЕП.

4. Крок 5: Згодом сигнал нормалізується до рівня 2 залишаючись під впливом лише фактора відстані. Усі 100 пристроїв успішно вирівнюють показники зв'язку, що підтверджує стійкість архітектури мережі.

Також на рис. 4.2 можна бачити графічне представлення розподілу сигналу.

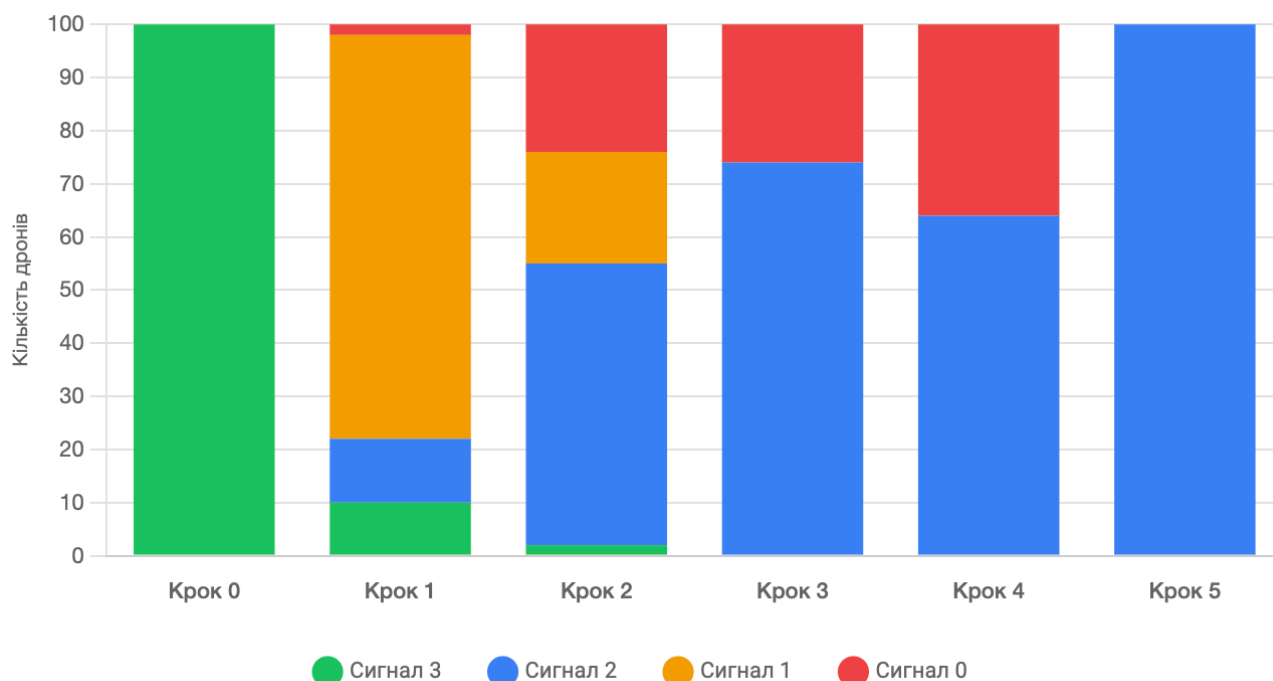


Рисунок 4.2 – Графік розподілу сигналів загальної мережі Петрі

Наведений аналіз стосувався моделі окремого пристрою. Далі розглянемо динаміку станів усього рою із 100 БпЛА як єдиної мережі.

Аналіз динаміки станів множини пристроїв за кроками симуляції:

1. Крок 0: Початкове підключення 100 пристроїв забезпечує повну керованість системи на старті.

2. Крок 1–2: Кількість підключених пристроїв стрімко падає до 50 через настання умов втрати зв'язку. На другому кроці 10 пристроїв потрапляють у зони впливу РЕП.

3. Крок 3–4: На третьому кроці 19 пристроїв перебувають під впливом РЕП, а 28 переходять в автономний режим. На четвертому кроці 41 пристрій знаходиться в автономному стані, вузли переходять у режим самостійної навігації.

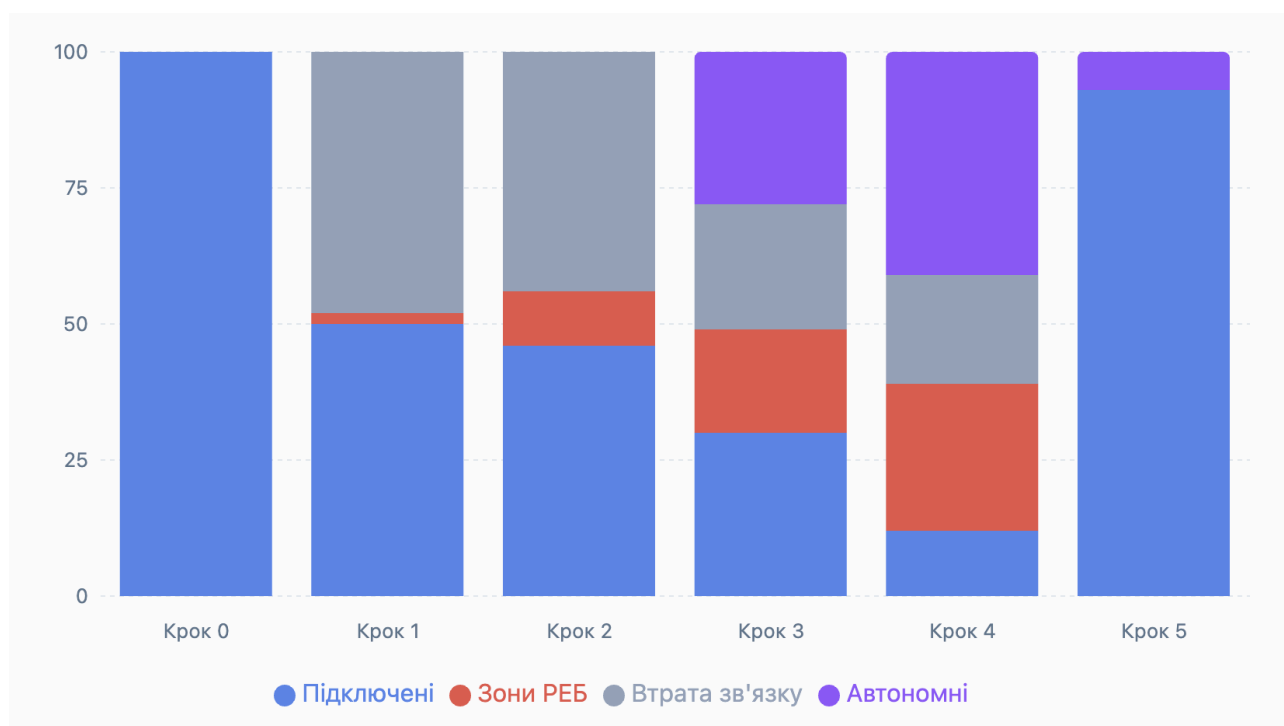
4. Крок 5: Після виходу з зони впливу РЕП, переважна більшість пристроїв (93) успішно відновлює підключення до мережі.

У таблиці 4.2 наведено результати експерименту, в якому можна проаналізувати кількість дронів та в якому стані вони перебували на кожному етапі.

Таблиця 4.2 – Розподіл станів дронів за кроками симуляції

Крок	Підключені	Зони РЕП	Втрата зв'язку	Автономні
Крок 0	100	0	0	0
Крок 1	50	2	48	0
Крок 2	46	10	44	0
Крок 3	30	19	23	28
Крок 4	12	27	20	41
Крок 5	93	0	0	7

Також на рис. 4.3 можна бачити графічне представлення розподілу дронів відповідно наявних станів.

**Рисунок 4.3** – Графік станів кольорової мережі петрі

4.2 Прокладання маршрутів за допомогою LLM

Використовуючи розроблені шаблони запитів, було поставлено завдання. Запит, який вказує LLM виконати необхідні дії, наведений на рисунку 4.4.

```
Generate a complete tactical drone mission dataset in JSON
format for the following scenario:
MISSION PARAMETERS:
Single drone reconnaissance mission
Start point: [latitude, longitude]
Target: [specific facility type] at [latitude, longitude]
Mission duration: [X hours]
Flight profile: NOE (Nap-of-Earth) stealth operations

THREAT ENVIRONMENT:
[N] Electronic Warfare stations with [X]km radius danger zones
[N] No-fly zones (cities, military bases)
Terrain elevation data available for optimization

ROUTE REQUIREMENTS:
Follow lowest possible terrain elevations for maximum stealth
Maintain minimum [X]km separation from all EW threat zones
Avoid populated areas and restricted airspace
Include detailed reconnaissance pattern at target
Use different ingress/egress routes for operational security

TACTICAL CONSIDERATIONS:
Prioritize terrain masking over speed
Ensure EW avoidance calculations are verified
Include reconnaissance pattern (perimeter survey)
Plan contingency routes
Maintain realistic flight speeds and timing

Generate tactically sound, operationally realistic mission data
that could be used for actual flight planning visualization and
analysis.
```

Рисунок 4.4 – Запит з завданням для LLM

Запит поєднує контекст, специфічний для місії, дані про місцевість та інформацію про загрози в цілісну інструкцію природною мовою, відформатовану для керівництва LLM у створенні безпечного та здійсненого маршруту. Він є основними вхідними даними, що запускають процес міркування моделі, включаючи динамічні значення, такі як початкова точка, пункт призначення, зони обмеженого доступу та операційні обмеження. Цей запит діє як центральне координаційне повідомлення, яке об'єднує інформацію, підготовлену модулями попередньої обробки, та вказує LLM

вирішити завдання маршрутизації в рамках заданого сценарію. Крім того, оператор може вибрати п'ять бажаних варіантів формату виводу, як показано на рисунку 4.5.

```

OUTPUT FORMAT REQUIRED:
Mission metadata (name, duration, drone count, classification)
Threat objects with precise coordinates:
EW stations (type: "ew_zone", radius_km, threat_level)
Urban areas (type: "urban_area", population, restrictions)
Infrastructure (type: "factory"/"military"/"infrastructure")

Optimized waypoint sequence with:
Precise coordinates (6 decimal places)
MSL altitude (terrain + 50m AGL for stealth)
Timestamp for each waypoint
Tactical action description
Terrain elevation notes
Mission timeline with key events
Safe corridors data with elevation statistics

```

Рисунок 4.5 – Запит з вибором формату виведення

Приклад карти, який використовується для тестового випадку, базується на відкритих даних карт рельєфу. Дані були попередньо оброблені за допомогою скрипта Python, відповідні висоти наведені у форматі JSON. Було використано LLM Claude Sonnet 4.0.

На рисунку 4.6 візуалізовано фрагмент відкритої карти з умовами місцевості, зеленим кольором показані низовини, жовтим та коричневим — висоти, які можуть перешкоджати зв'язку дрона з ретранслятором. Жовті трикутники показують розташування об'єктів, які можуть спричинити порушення кіберфізичної системи та бути потенційним джерелом поширення радіоелектронної протидії, тому маршрут було прокладено з урахуванням їх обходу. Мітки показують розташування цілі та початкової точки. Іншими словами, жовті трикутні мітки вказують на розташування пристроїв противника, включаючи системи РЕП, які розглядаються як джерела перешкод, так і потенційні вектори поширення шкідливих сигналів або впровадження шкідливого програмного забезпечення. Маршрут, згенерований LLM (показаний як шлях, що з'єднує початкову та цільову точки), стратегічно уникає цих зон високого ризику, підтримуючи зв'язок з урахуванням

місцевості та мінімізуючи вплив кіберфізичних загроз.

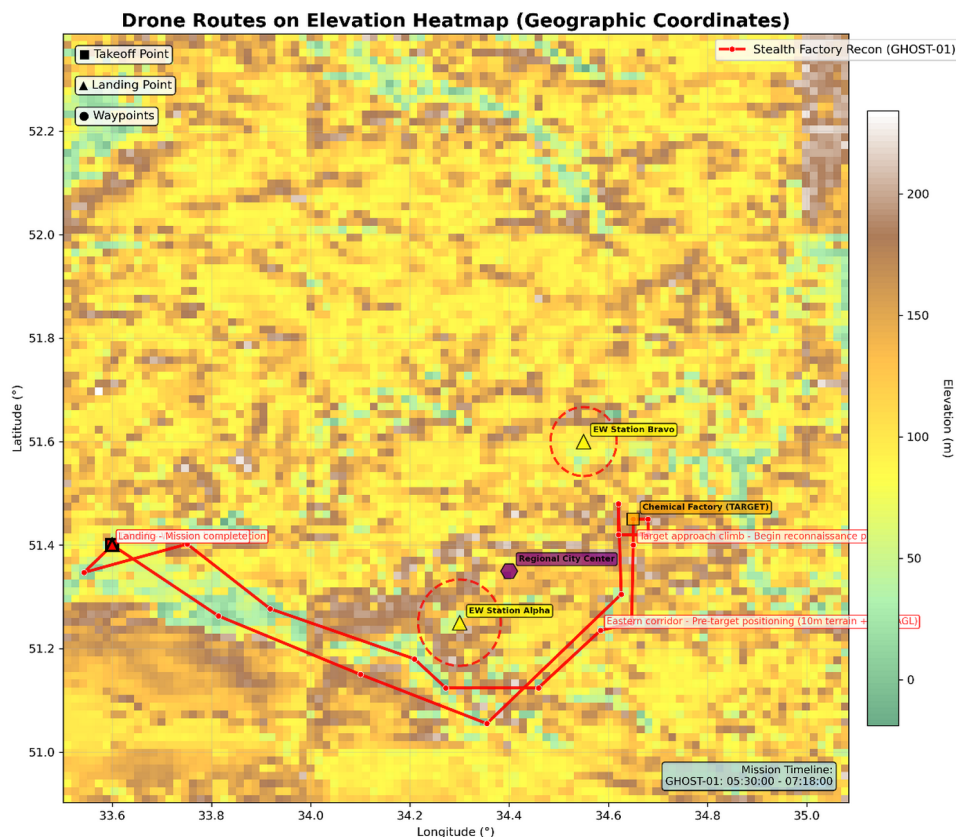


Рисунок 4.6 – Результати експеримента

Цей приклад ілюструє здатність моделі обґрунтовувати геопросторові та конфронтаційні дані, забезпечуючи безпечну та стійку навігацію БПЛА.

Розроблене програмне забезпечення також використовує розрахунки зон радіоелектронної активності та радіоелектронних перешкод. В цьому експерименті наведено зони дії пристроїв, які порушують доступність шляхом введення радіосигналів, що несуть шкідливі дані, або просто шумом на відповідних радіочастотах. Під час прокладання маршруту, залежно від мети місії, можна встановити умови для «обходу відповідних зон», що було зроблено у випадку маршруту на рисунку 4.6.

На рисунках 4.7, 4.8 представлені зони перешкод. Зони моделюються на основі ефективної дальності та сили сигналу відомих джерел загроз, використовуючи вирази 2.20 – 2.22, та враховуючи особливості рельєфу місцевості та характеристики поширення. БПЛА, що працюють у цих зонах,

можуть зіткнутися з втратою зв'язку, несправністю датчиків або ризиками кібербезпеки, такими як атаки з використанням протоколів або введенням даних. На рисунку показано, як такі шкідливі зони сигналів інтегруються в модель планування маршруту як зони виключення, що спонукає LLM генерувати шляхи, які мінімізують вплив та зберігають цілісність місії.

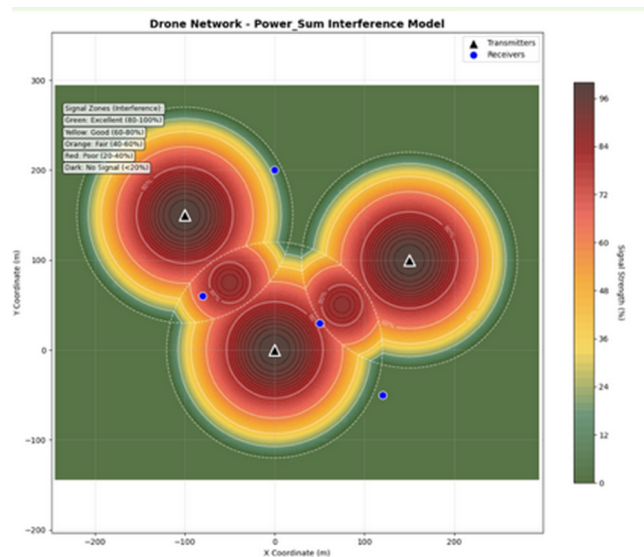


Рисунок 4.7 – Зони дії пристроїв перешкод та/або поширення шкідливих сигналів для трьох пристроїв

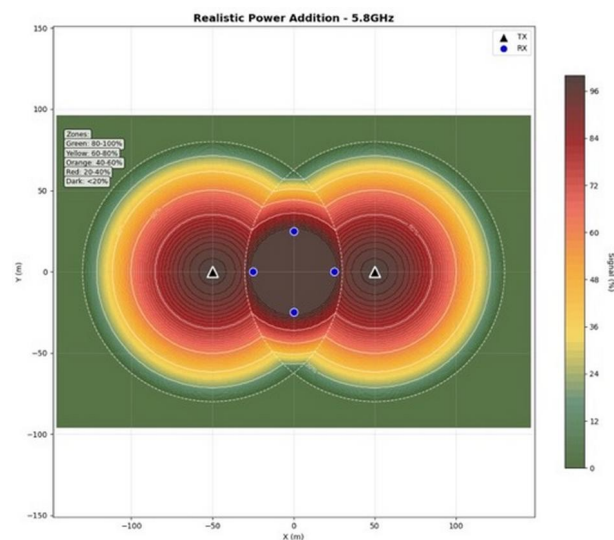


Рисунок 4.8 – Зони дії пристроїв перешкод та/або поширення шкідливих сигналів для двох пристроїв

Під час прокладання маршруту також слід враховувати зони нульового сигналу. На значення сигналу безпосередньо впливають перешкоди та розташування ретранслятора на «прямій видимості», приклад оцінювання якої наведено на рисунку 4.9.

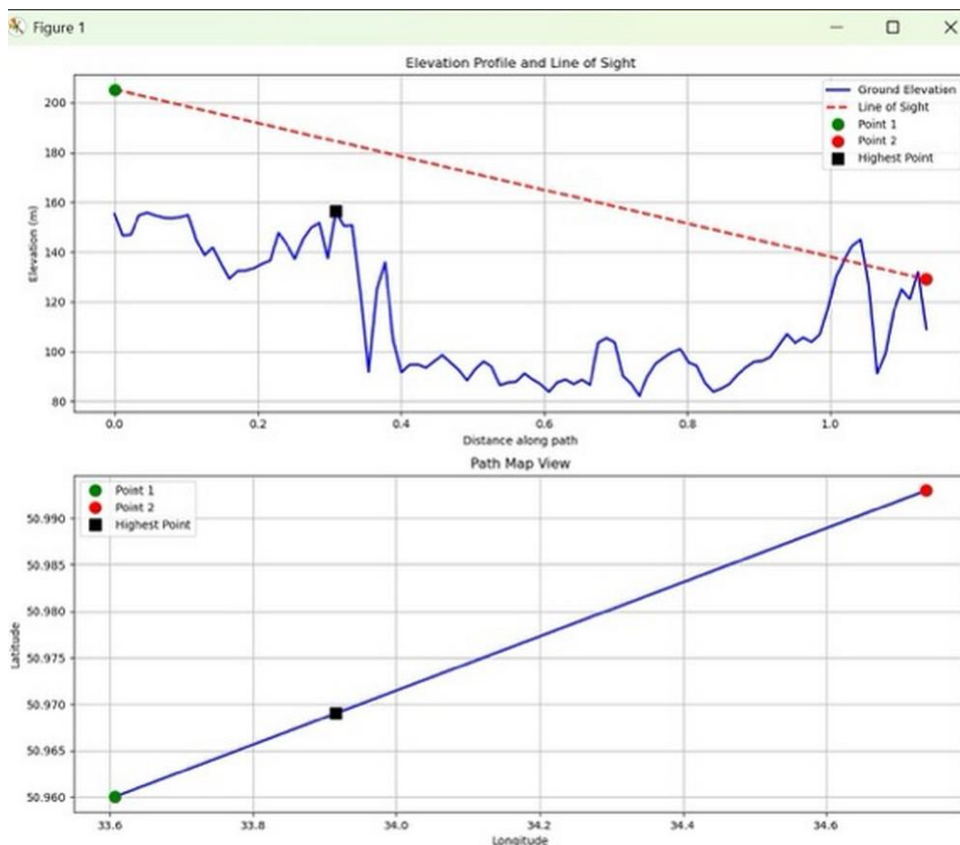


Рисунок 4.9 – Лінія видимості між робочим дроном та ретранслятором (хабом), її проекція на горизонтальну площину

Висоти рельєфу зчитуються з попередньо оброблених даних карт висот і можуть бути враховані під час прокладання маршруту. На рисунку 4.9 ми бачимо, що робочий дрон і ретранслятор не знаходяться на прямій видимості один одного, оскільки рельєф місцевості цьому перешкоджає. Відповідні зони вважаються зонами нульового сигналу, в яких дрон перестає бути керованим і діє за сценарієм, визначеним у ньому для таких випадків (наприклад, летіти вертикально вгору, доки не з'явиться сигнал).

Перевірка достовірності запропонованих маршрутів проводилася за допомогою запропонованих метрик, у тому числі візуально, на основі

експертної думки. Перевірка достовірності маршруту, запропонованого LLM, проводиться з урахуванням наступних критеріїв:

1. Безперервність маршруту (відстань між будь-якими двома сусідніми точками не перевищує заданої, всі точки маршруту $(x_i, y_i, z_i) \in M$, де M – область карти, що розглядається).

2. Маршрут оминає заборонені позиції (зони розташування небезпечних пристроїв противника).

3. Лінія видимості між ретранслятором та дроном не переривається висотами місцевості.

4. Маршрут включає точку призначення – ціль.

Залежно від цілей місії, можливо перевірити наявність циклів, петель на маршруті (точок повторного відвідування). Для складних маршрутів ці перевірки повинні виконуватися автоматично, проте бажаним є візуальний контроль маршруту людиною.

4.3 Розрахунок продуктивності та пропускної здатності БпЛА

Для проведення експерименту створили 6 дронів один з яких виконує роль ретранслятора. (рис. 4.10). Ретранслятор отримує та передає інформацію на базову станцію, за допомогою оптоволокна, інші дрони спілкуються безпроводним способом. Для всіх пристроїв задані фіксовані значення потужності передавача, чутливості приймача.

На рис. 4.11 додали засіб РЕП, який буде впливати на комунікацію пристроїв. В цьому прикладі використана сітчаста мережа, тобто лише ретранслятор може спілкуватись з іншими пристроями. Граф топології зображено на рис. 4.12.

Ми можемо обчислити пропускну здатність за формулою Шеннона в біт/с, від ретранслятора до дрона в кожному напрямку, враховуючи перешкоди які створює засіб РЕП (Таблиця 4.3).

Перемістивши РЕП ближче до мережі дронів можемо побачити, що пристрої D0 та D1 повністю перестали отримувати інформацію від ретранслятора (Таблиця 4.4). Інші пристрої все ще можуть приймати та передавати дані.

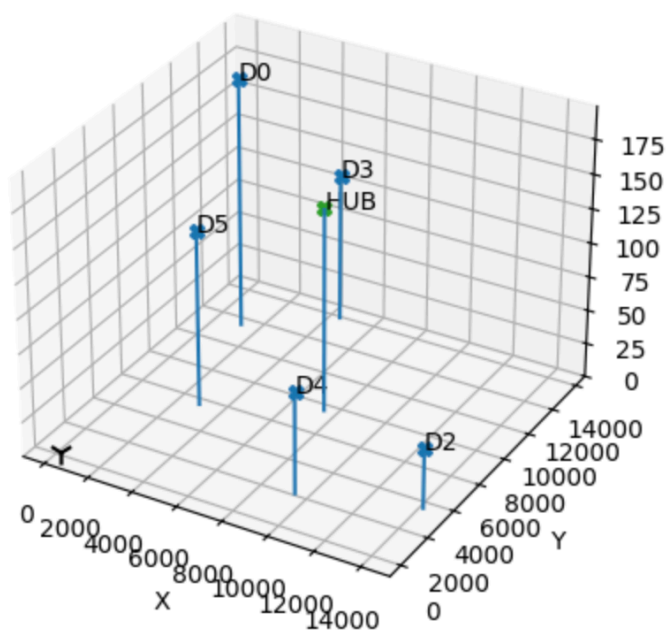


Рисунок 4.10 – Візуалізація розміщення дронів

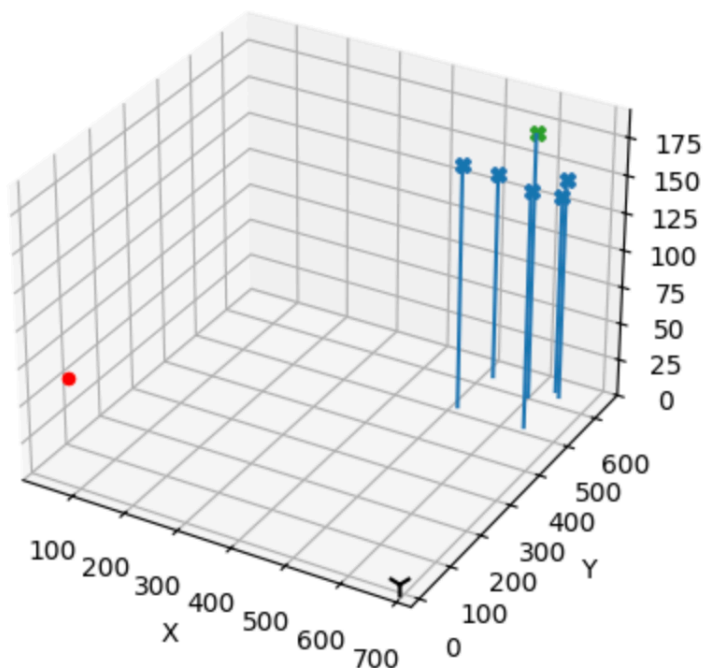


Рисунок 4.11 – РЕП поруч з мережею дронів

На рис. 4.13 зображено відповідний граф, де ребра представлені у вигляді значень пропускної здатності між дроном та ретранслятором.

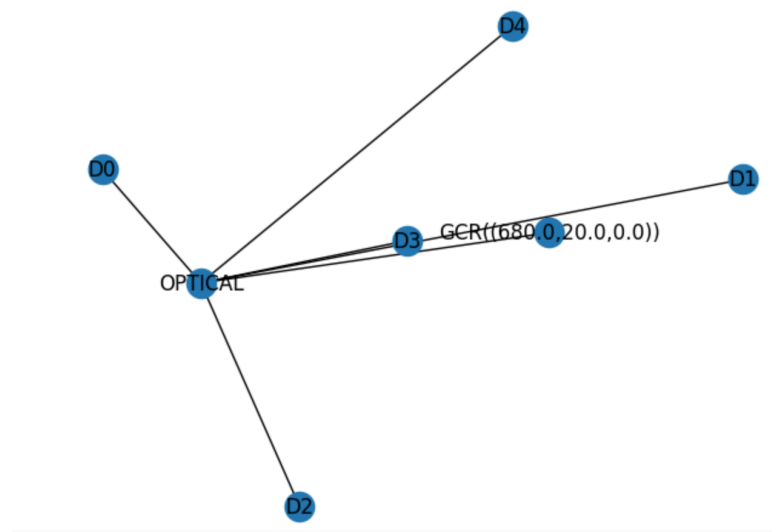


Рисунок 4.12 – Граф сітчастої мережі

Таблиця 4.3 – Пропускна здатність від ретранслятора до БПЛА в кожному напрямку

	D0	D1	D2	D3	D4	HUB
D0	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	2.435333e+08
D1	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	2.489414e+08
D2	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	3.532522e+08
D3	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	3.264365e+08
D4	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	0.000000e+00	1.957968e+08
HUB	1.469914e+08	1.499190e+08	2.631184e+08	2.377865e+08	9.216709e+07	0.000000e+00

Таблиця 4.4

	D0	D1	D2	D3	HUB
D0	0.0	0.0	0.000000e+00	0.000000e+00	9.077154e+07
D1	0.0	0.0	0.000000e+00	0.000000e+00	9.409247e+07
D2	0.0	0.0	0.000000e+00	0.000000e+00	1.683409e+08
D3	0.0	0.0	0.000000e+00	0.000000e+00	1.475633e+08
HUB	0.0	0.0	1.019531e+08	8.906505e+07	0.000000e+00

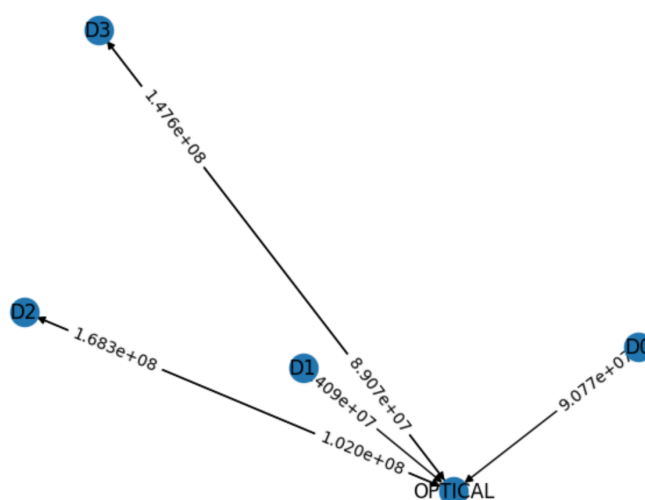


Рисунок 4.13 – Граф значень пропускної здатності між дроном та ретранслятором

4.4 Оптимізація позиціонування мережі БпЛА

Для проведення експерименту було підготовлено групу з 16 пристроїв, що повинні досягти цільової точки для виконання місії. З метою моделювання умов місцевості з топологічними перешкодами було використано набір даних цифрової моделі висот (DEM) [60], який дозволяє оперувати точними значеннями висот у кожній точці заданих координат.

Задано початкову конфігурацію системи, де всі дрони зібрані біля базової станції, далі відбувається оптимізація їх позиції в межах певного обмеженого сектору. Наступний цикл використовує вже конфігурацію з першого циклу, як початкову, та повторно проводить алгоритм оптимізації. Це дозволяє оцінити прогрес самого алгоритму та скорегувати наш підхід. Також це відображає реальну картину розгортання БпЛА, що координуваними переміщеннями поступово наближуються до цілі, підлаштовуючись під актуальну зміну середовища.

На рис. 4.15 зображений початковий стан мережі.

1. Синій квадрат - пункт дислокації, початкове місце вильоту всіх пристроїв
2. Жовті ромби - БпЛА

3. Червоні трикутники - РЕП
4. Синій хрестик - ціль, яку повинні досягти пристрої

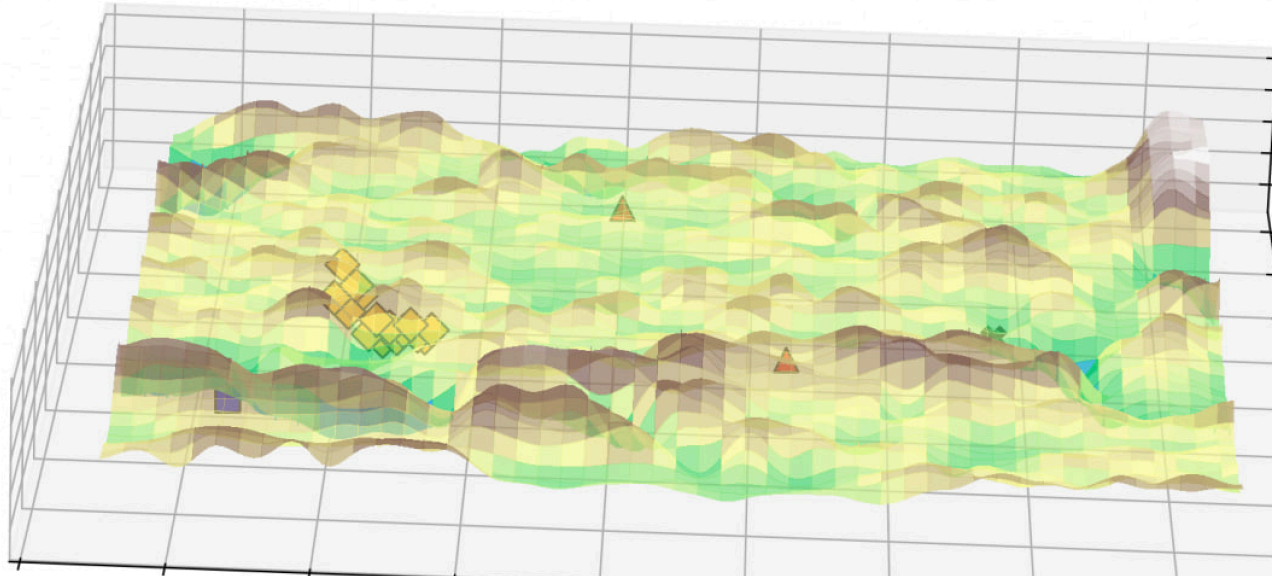


Рисунок 4.14 – Початковий стан мережі

Після першого циклу оптимізації дрони значно змінили свою відстань (Рис. 4.15). Частина, що почала виступати ретрансляторами, набрала висоту для безперешкодної передачі сигналу, в той час як ударні просунулись далі у напрямку цілі. Третина пристроїв вже досягла оптимальної кількості з'єднань, уникаючи ізоляції або надмірного скупчення, що вказує на добре збалансовану мережу.

В другому циклі дрони поступово продовжили своє просування у напрямку цілі. Топологія мережі значно змінилась, дрони розподілились рівномірно вздовж більшої траєкторії маршруту, отримавши оптимальну кількість з'єднань. Частина ударних дронів наблизилась до засобів РЕП, виникла необхідність знайти компромісне рішення продовжуючи наближатись до цілі, уникаючи дії РЕП. (Рис. 4.16)

Під кінець третього циклу дрони вже пройшли більшу частину свого маршруту (Рис. 4.17). Розподіл став майже оптимальним, забезпечуючи баланс між ефективністю і надійністю. Кожен пристрій при втраті одного з'єднання, міг зберегти комунікації в мережі, використавши резервні

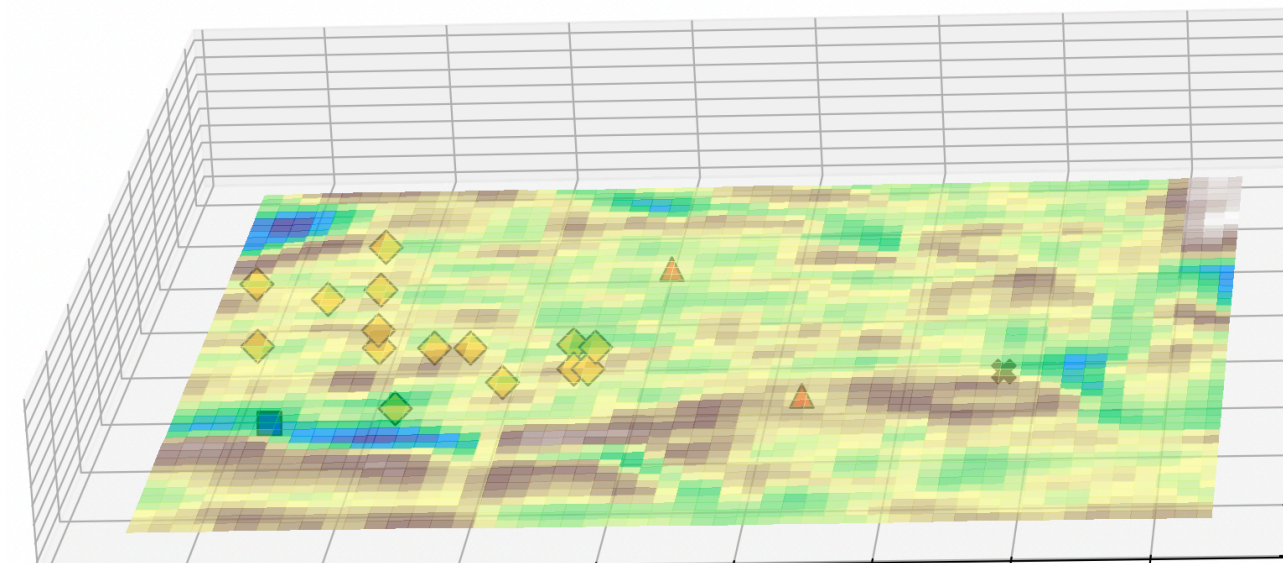


Рисунок 4.15 – Перший цикл оптимізації

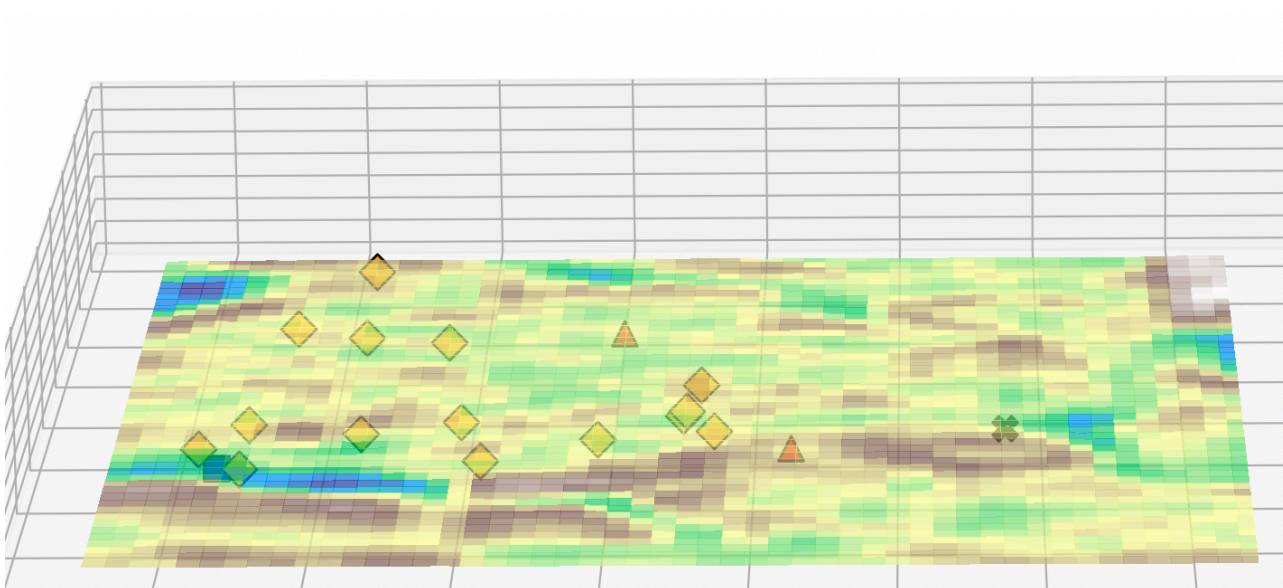


Рисунок 4.16 – Другий цикл оптимізації

ретранслятори.

На рис 4.18 результат роботи алгоритму оптимізації, можемо спостерігати, що пристрої рівномірно розподілились на всьому шляху до цілі, формуючи мережу ретрансляторів, корегують свої позиції в залежності від топологічних та кіберфізичних впливів. Частина пристроїв досягнула цілі та успішно виконала поставлене завдання, інші пристрої виступили

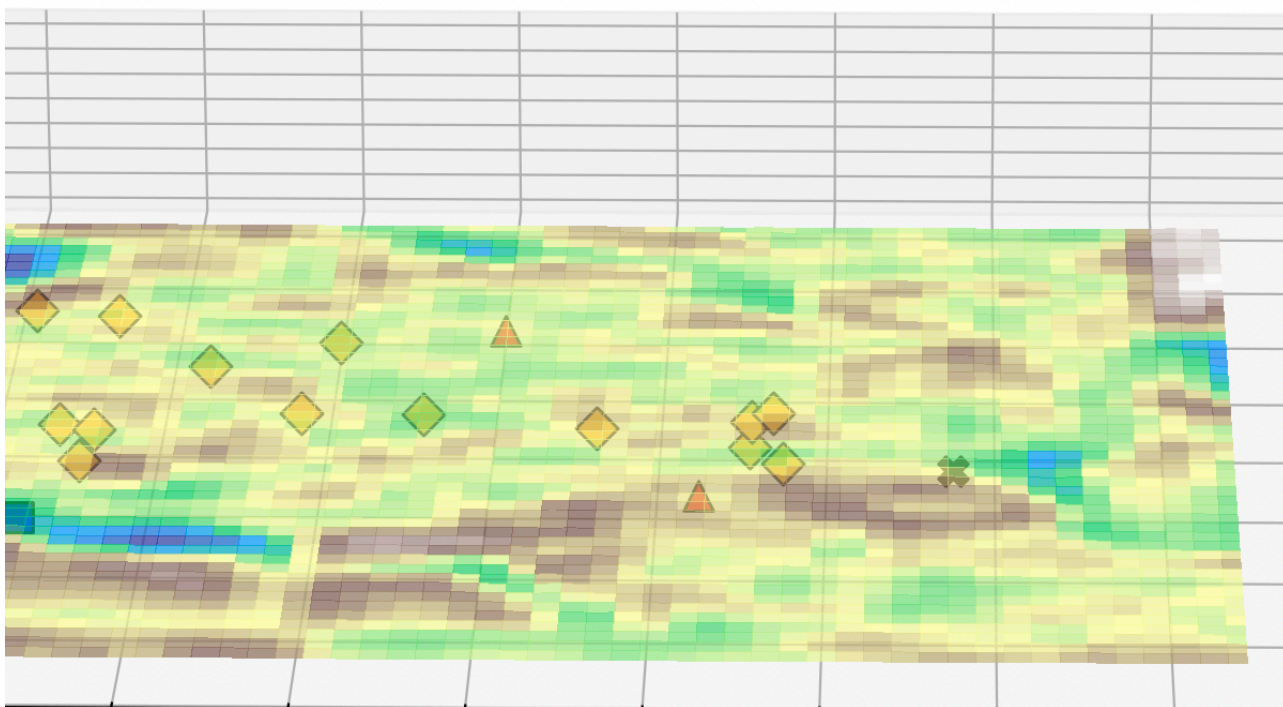


Рисунок 4.17 – Третій цикл оптимізації

ретрансляторами та допомогли забезпечити надійний сигнал обміну інформації від ударних дронів до пункту де відбувається контроль та спостереження за мережею.

В таблиці 4.5 представлено послідовний прогрес генетичного алгоритму (ГА) за п'ятьма запусками оптимізації. Детальні дані щодо збіжності **мінімальної дистанції атаки** (D_{\min}) та оцінки оптимізації у міру розвитку популяції.

Для того щоб побудувати чітку траєкторію польоту, весь процес був розділений на послідовні кроки (цикли). Це дозволило крок за кроком формувати маршрут та спостерігати за його розвитком. На кожному такому етапі рух дронів обмежувався певним радіусом польоту, який поступово збільшувався. Завдяки цьому дрони могли плавно рухатися в напрямку цілі, уникаючи на своєму шляху топологічні та кіберфізичні перешкоди.

На кожному кроці циклу генетичний алгоритм генерував 160 поколінь для пошуку найкращого варіанту шляху. Цільова функція допомагала дронам оминати особливості рельєфу та зони ризику, що дозволило створити безпечний і послідовний маршрут для польоту.

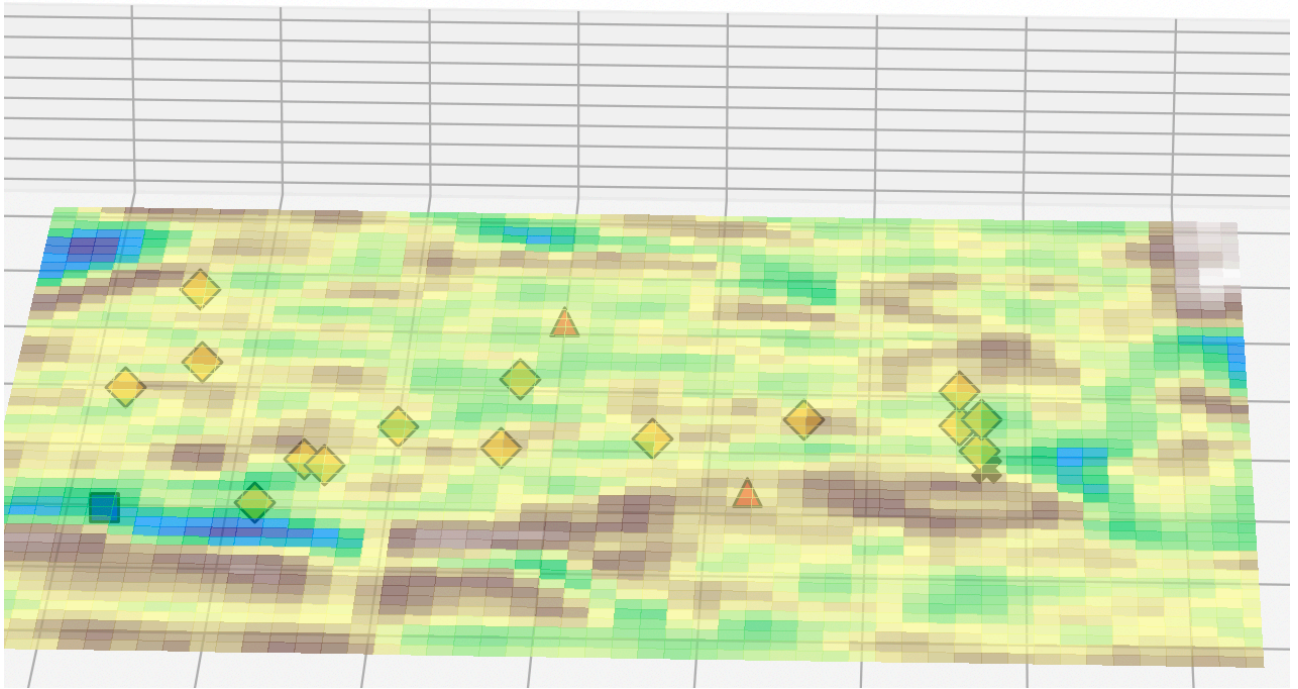


Рисунок 4.18 – Четвертий цикл оптимізації

Таблиця 4.5 – Прогрес поколінь за запусками

Крок запуску	Покоління	Мін. дист. (км)	Оцінка оптимізації
Крок 1	Пок. 0	45.6	231,805.55
	Пок. 40	44.4	165,185.28
	Пок. 80	44.4	164,704.48
	Пок. 120	44.4	164,679.00
	Пок. 160	44.4	164,678.83
Крок 2	Пок. 0	31.7	122,331.56
	Пок. 40	30.2	78,045.29
	Пок. 80	30.2	78,038.85
	Пок. 120	30.2	78,033.78

ІД запуску	Покоління	Мін. дист. (км)	Оцінка оптимізації
	Пок. 160	30.2	78,032.06
Крок 3	Пок. 0	17.5	39,060.20
	Пок. 40	15.7	22,024.93
	Пок. 80	15.4	21,793.66
	Пок. 120	15.4	21,750.01
	Пок. 160	15.4	21,747.95
Крок 4	Пок. 0	4.5	8,185.67
	Пок. 40	1.3	1,254.75
	Пок. 80	1.0	828.13
	Пок. 120	0.8	778.52
	Пок. 160	0.6	772.53
Крок 5	Пок. 0	1.0	1,848.48
	Пок. 40	0.4	510.40
	Пок. 80	0.5	491.64
	Пок. 120	0.4	472.91
	Пок. 160	0.1	456.56

На рисунку 4.19 можемо бачити графік стабільного зниження значення цільової функції

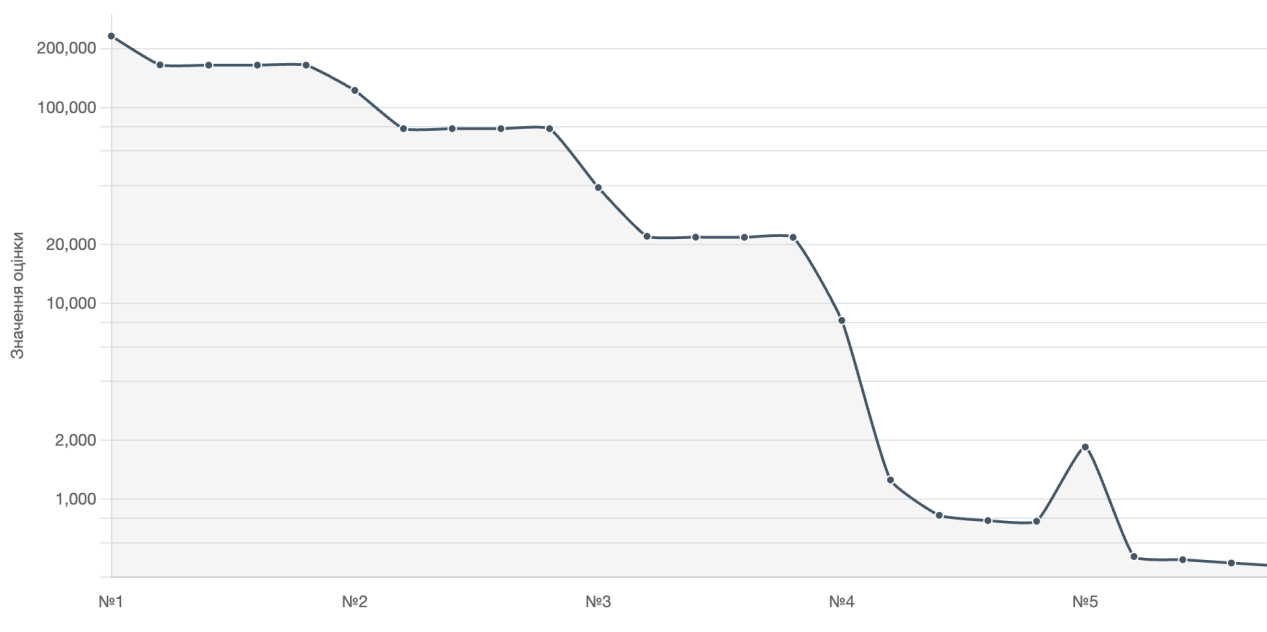


Рисунок 4.19 – Графік зміни значень оптимізації

4.5 Пошук вразливостей в зразках прошивок пристроїв

Для виявлення критичних вразливостей в програмному та апаратному забезпеченні БпЛА було використано сучасні дизасемблери та декомпілятори (IDA Pro, Binary Ninja). В них були встановлені розширення, до яких зверталось LLM за допомогою MCP(Model Context Protocol).

Нижче наведено повний запит, який містить чіткі інструкції, щодо поставленого завдання, обмежень при роботі, та структури звітування.

Лістинг 4.1: Системний запит для LLM-агента

You are security researcher trying to find binary
 → vulnerabilities in drone firmware

- GENERAL INSTRUCTIONS
- Your task is to analyze file opened in <D>
 → disassembler.
- Report for vulnerability only if you 100% sure. Avoid
 → FP results.
- Stop on the first vuln u found and do the report

- using instructions in this prompt below.
- Avoid reading big data into your memory
- BEFORE ANALYSIS
 - – print file name
 - – file type
 - – file arch
 - – file size
- TYPES OF VULNERABILITIES TO FIND:
 - – buffer overflow
 - – use-after-free (UAF)
 - – format string bugs
 - – integer overflow/underflow
 - – double free
- TYPES OF VULNERABILITIES TO SKIP:
 - – ddos
- ALLOWED MCP FUNCTIONS
 - – decompile code
 - – disassemble code
 - – xref to
 - – read function addresses
 - – rename functions
 - – rename vars
 - – add comments
- FORBIDEN MCP FUNCTIONS
 - – read raw bytes
 - – read strings
- REPORT INFO

- Produce comprehensive RE/*.md report
- detailed vuln details
- steps to reproduce
- detailed POC

Таблиця 4.6 – Огляд вразливостей в попередніх версіях прошивки PX4

CVE ID	Стан вразливості	Нотатки та логіка виправлення
CVE-2024-40427	v1.14.3	Виправляє переповнення стеку MAVLink шляхом додавання перевірки довжини корисного навантаження SERIAL_CONTROL.
CVE-2024-38952	v1.14.3 Tag	Переповнення через параметр topic_name.
CVE-2023-47625	v1.14.3	Додає перевірку working_segment_size до парсера CRSF RC для запобігання переповненню буфера.
CVE-2023-46256	v1.14.0-rc1	Heap Buffer Overflow у послідовному датчику відстані.
CVE-2024-24254	v1.14.0	Race condition під час завантаження даних геозони.
CVE-2021-34125	v1.12.3	Вимкнення команд mb, mh та mw в оболонці NuttX для запобігання витоку або дампу прошивки.

Проаналізовано прошивку польотного контролера Px4.

Ефективність запропонованої архітектури була протестована на 21 зразку програмного забезпечення, включаючи прошивку PX4 Autopilot (див. Розділ 3). Результати спрацювання LLM-орієнтованого аналізу для PX4 наведено в Табл. 4.7.

Також, було додатково зроблено ще один експеримент, щодо бібліотеки muparser. У ході аналізу мовна модель ідентифікувала три потенційні вектори

Таблиця 4.7 – Результати дії методу виявлення вразливостей

Метод	Наявні вразливості, шт.	Не знайдені вразливості, шт.	Час виявлення, хв
IDA Pro Hex-Rays та Claude Sonnet 4.0 (стандартний режим)	3	0	3.6
IDA Pro Hex-Rays та Claude Sonnet 4.0 (режим розширеного мислення)	1	0	~ 9

Buffer Overflow Vulnerability in PX4 Logger Module

Vulnerability

Location: `px4::logger::LoggedTopics::add_topics_from_file()` at address `0x80e1cb0`
File: `/src/modules/logger/logged_topics.cpp`

Root Cause

The function uses `sscanf()` with an unsafe format string `"%s %lu %lu"` (located at `0x819dcc0`) to parse `/fs/microsd/etc/logging/logger_topics.txt`. The `%s` has NO width limit, allowing unlimited input into the 80-byte `topic_name` buffer.

Vulnerable Code

```
c
char topic_name[80]; // at [sp+60h] [bp-70h]
char line[80];
uint32_t interval_ms, instance;

fgets(line, 80, fp); // Safe read
sscanf(line, "%s %lu %lu", topic_name, &interval_ms, &instance); // UNSAFE!
...
```

The `%s` can write beyond 80 bytes, overflowing into:

- Adjacent stack buffer `v17[32]`
- Saved registers
- Return address

Рисунок 4.20 – Результат пошуку вразливостей в PX4 logger module

атак. Після ретельної перевірки два з них були класифіковані як хибнопозитивні спрацьовування. Ймовірною причиною таких відхилень є висока структурна складність кодової бази, а також специфічні артефакти, що виникають у процесі декомпіляції в середовищі IDA Pro.

Попри наявність шумів, метод дозволив успішно локалізувати критичну вразливість у функції `mu::ParserBase::ParseCmdCodeBulk()` (рис. 4.21). Цей результат підтверджує здатність системи виокремлювати реальні загрози навіть у складних програмних модулях, де автоматизований аналіз часто ускладнений специфікою перетворення бінарного коду у високорівневе представлення.

2. Stack Index Underflow in ParseCmdCodeBulk()

Location: `ParseCmdCodeBulk()` function at address 0x8ff0, case 0x10 (IF operation)

Severity: MEDIUM **Type:** Stack underflow leading to potential memory corruption

Description: In the conditional execution handler, there's insufficient validation of stack depth:

```
cpp
case 0x10:
    v3 = *(double*)(v5 + 8LL * v7);
    if ( v3 == 0.0 )
    {
        if ( v7 <= 0 ) // Check is present but insufficient
        {
            // Error handling
        }
        --v7; // Decrement can cause underflow
        v6 += 32LL * *(int*)(v6 + 16) + 32;
    }
```

Рисунок 4.21 – Результат виявлення вразливостей в `muarser`

Одержані результати тестування архітектури на базі LLM та протоколу MCR доводять можливість створення автоматизованої системи для виявлення недокументованих можливостей в системах контролю пристроїв та апаратному ПЗ. Запропонована модель не лише виявляє вразливості, але й ідентифікує їх причину та генерує розширені звіти [62] з рекомендаціями щодо виправлення коду. Таким чином можна швидко в автоматизованому режимі впроваджувати патчі програмного забезпечення, підтверджувати їх та розповсюджувати на всі пристрої в мережі. Це дозволяє швидко усунути вразливість, та припинити дію загрози до того як вона може завдати непоправної шкоди. Знайдені вразливості можуть спричинити збій польотного контролера, що призведе до втрати пристрою, перехопити керування або отримати доступ до передачі даних, що створює загрозу безпеці оператора.

Висновки до розділу 4

1. Проведено комплексну експериментальну перевірку розроблених моделей та методів для забезпечення кіберфізичної стійкості мережі БпЛА. Експеримент базувався на єдиному симуляційному сценарії виконання місії в умовах зовнішнього ворожого впливу та послідовно підтвердив ефективність усіх запропонованих рішень.

2. Модель мережі пристроїв на основі використання мережі Петрі підтвердили здатність системи адекватно відображати динаміку зміни станів пристроїв, прогнозувати критичні ситуації (потрапляння в зони РЕП, втрата зв'язку через рельєф, перехід в автономний режим).

3. Підтверджено можливість безпечного планування місії за допомогою підходу на LLM. Застосований алгоритм прокладання маршруту із використанням структурованих запитів, що інтегрують дані рельєфу (Copernicus DEM) та координати розташування засобів РЕП противника, дозволив згенерувати адаптивні траєкторії. Згенеровані маршрути успішно оминули населені пункти, висотні перешкоди та зони ураження РЕП.

4. Практичне використання методу оптимізації позиціонування мережі на основі генетичного алгоритму, забезпечило необхідний баланс між переміщенням мережі БпЛА до цілі та збереженням комунікаційного ланцюга. В умовах агресивного середовища алгоритм дозволив також зменшити значення цільової функції майже в 10 разів за 100 ітерацій.

5. Крім того, показано високу ефективність роботи запропонованої моделі архітектури та методу для пошуку вразливостей в ПЗ БпЛА. Аналіз модулів польотного контролера PX4 та бібліотеки muparser показав високу швидкодію (в 4 рази вищу за класичні методи) та точність виявлення 94,7%, що дозволяє оперативно виявляти недокументовані можливості та генерувати патчі безпеки ще до того, як загроза призведе до втрати апаратів.

6. Отримані результати доводять, що розроблений інструментарій може забезпечити практичне вирішення задач доступності, цілісності та конфіденційності мереж БпЛА в умовах кіберфізичних та кібернетичних загроз.

ВИСНОВКИ

У дисертаційній роботі на основі аналізу архітектури мереж БпЛА та сучасних загроз в кіберфізичному просторі, вирішено важливу науково-технічну задачу створення моделей і методів забезпечення кіберфізичної стійкості мережі дронів та було одержано наступні результати:

1. У роботі запропоновано моделі та методи, що забезпечують збереження доступності каналів зв'язку мережі БпЛА, цілісність і конфіденційність польотних завдань, підвищують рівень спостережності за динамікою станів мережі БпЛА в умовах дії несприятливих та ворожих факторів. Запропоновані рішення ґрунтуються на підходах до забезпечення безпеки мереж БпЛА і відрізняються від відомих здатністю протистояти комплексним кіберфізичним впливам за рахунок інтеграції засобів адаптивного керування та автоматизованого аналізу захищеності програмного забезпечення.

2. Запропоновано модель мережі пристроїв, що ґрунтується на використанні узагальненої мережі Петрі для окремого пристрою та мережі Петрі для групи пристроїв з метою аналізу й моніторингу системи. Вона відрізняється від відомих моделей урахуванням згасання сигналу, особливостей рельєфу місцевості, впливу засобів радіоелектронної боротьби (РЕП), а також поширення шкідливого програмного впливу під час планування місій у військових умовах. Це забезпечує підвищення точності прогнозування безпеки безпілотних літальних апаратів удвічі. Запропоновані моделі дають змогу оцінювати рівень сигналу, визначати поточний стан системи (доступний режим, вихід із зони дії РЕП, автономний режим), а також аналізувати вплив перешкод на її функціонування, зокрема дію засобів РЕП, вплив ландшафту та згасання сигналу зі збільшенням відстані.

3. Запропоновано метод прокладання маршруту БпЛА з урахуванням впливу засобів радіоелектронної боротьби (РЕП), особливостей ландшафту (на основі даних відкритого набору висот Copernicus Digital Elevation Model), а також згасання сигналу зі збільшенням відстані. Запропонований алгоритм відрізняється від існуючих використанням можливостей логічного висновку

великих мовних моделей (LLM) і комплексним урахуванням ворожих та несприятливих чинників зовнішнього середовища. Алгоритм забезпечує прокладання маршрутів для виконання місії із залученням до 100 пристроїв, а також дає змогу оцінювати здійсненність місії. Розроблені шаблони інструкцій для LLM прискорюють процедуру побудови маршруту БпЛА в 1,5 раза з урахуванням зовнішніх загроз.

4. Запропоновано метод оптимізації позиціонування рою безпілотних літальних апаратів, що ґрунтується на багатокомпонентній цільовій функції та генетичному алгоритмі. На відміну від підходів, які формують індивідуальні траєкторії окремих апаратів, запропонований метод розглядає рій як єдину мережеву систему з колективною метою та оптимізує конфігурацію мережі БпЛА в цілому. Розв'язано задачу просування групи БпЛА до заданої цільової точки із забезпеченням безперервності комунікаційної мережі в умовах впливу засобів РЕП та наявності топологічних перешкод. Розроблений метод забезпечує в середньому в 16 вищу точність, порівняно з іншими методами.

5. Запропоновано модель комунікаційної архітектури на базі протоколу MSCP, яка дозволяє автоматизувати задачу аналізу бінарних зразків програмного забезпечення БпЛА на вразливості. Модель відрізняється масштабованістю, інструментальною незалежністю та використанням можливостей протоколу MSCP для розширення контексту аналізу. Також запропоновано метод статичного аналізу бінарних зразків програмного забезпечення БпЛА, що ґрунтується на концепції віртуального експерта з реверс-інжинірингу на базі LLM із розширенням контексту за допомогою протоколу MSCP. Запропонований метод у чотири рази швидший порівняно з існуючими підходами, зокрема фазингом, і забезпечує високу точність результатів — у середньому 93,3 % істинно позитивних виявлень вразливостей. Визначено місце запропонованої моделі в структурі центру безпеки мережі БпЛА. Розв'язувана задача спрямована на забезпечення конфіденційності, цілісності та доступності рою БпЛА. Запропоновані рішення можуть бути використані фахівцями під час дослідження експериментальних зразків, а також розробниками програмного забезпечення БпЛА для контролю якості прошивок та іншого програмного забезпечення.

6. Проведене експериментальне дослідження підтвердило

працездатність розробленого програмного комплексу, призначеного для забезпечення кіберфізичної стійкості мереж БпЛА. Інтеграція великих мовних моделей забезпечує генерацію обґрунтованих маршрутів з урахуванням зон дії засобів РЕП і топологічних перешкод, тоді як генетичний алгоритм ефективно оптимізує конфігурацію мережі, зменшуючи значення цільової функції майже в десять разів. Крім того, тестування архітектури статичного аналізу прошивок підтверджують здатність запропонованих рішень комплексно забезпечувати доступність, цілісність і конфіденційність БпЛА у ворожому середовищі. Результати роботи впроваджено у міжнародний проєкт *Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework* (Бортові обчислення у невизначеному повітряному просторі на основі розподілених структур) та в навчальному процесі в курсах “Методи штучного інтелекту в кібербезпеці”, “Кіберзахист об’єктів критичної інфраструктури”, “Аналіз бінарних вразливостей”

ПЕРЕЛІК ПОСИЛАНЬ

1. Light M. UAVs in Ukraine and Their Future in Warfare. 2024.
URL: <https://www.internationalaffairs.org.au/australianoutlook/uavs-in-ukraine-and-their-future-in-warfare/> (date of access: 03.02.2026).
2. Malinowski Z. The role of unmanned aerial vehicle in the formation of a secure military supply chain. *Security and Defence Quarterly*. 2016. Vol. 12, no. 3. P. 19—45. DOI: 10.35467/sdq/103235.
3. Wang X., Guo Y., Lu N., He P. UAV Cluster Behavior Modeling Based on Spatial-Temporal Hybrid Petri Net. *Applied Sciences*. 2023. Vol. 13, no. 2. P. 762. DOI: 10.3390/app13020762.
URL: <https://www.mdpi.com/2076-3417/13/2/762> (date of access: 05.12.2025).
4. Gonçalves P., Sobral J., Ferreira L. A. Unmanned Aerial Vehicle Safety Assessment Modelling Through Petri Nets. *Reliability Engineering & System Safety*. 2017. Vol. 161. P. 1—9. DOI: 10.1016/j.ress.2016.12.021. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0951832016300953> (date of access: 12.12.2025).
5. ArmyInform. How the Defense Forces can counter enemy electronic warfare (EW) capabilities (in Ukrainian). 2023.
URL: <https://armyinform.com.ua/2023/11/15/yak-sylam-oborony-protystoyaty-zasobam-reb-protyvnyka-dumka-eksperta/> (date of access: 28.12.2025).

6. Abro G., Zulkifli S., Masood R., Asirvadam V., Laouiti A. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats. *Drones*. 2022. Vol. 6, no. 10. P. 284.
DOI: 10.3390/drones6100284.
7. Mourtzis D., Angelopoulos J., Panopoulos N. UAVs for Industrial Applications: Identifying Challenges and Opportunities from the Implementation Point of View. *Procedia Manufacturing*. 2021. Vol. 55. P. 183—190.
DOI: 10.1016/j.promfg.2021.10.026.
8. Wang Z., Li Y., Wu S., Zhou Y., Yang L., Xu Y., Zhang T., Pan Q. A survey on cybersecurity attacks and defenses for unmanned aerial systems. *Journal of Systems Architecture*. 2023. Vol. 138. DOI: 10.1016/j.sysarc.2023.102870.
9. Xu D., Borse P., Altenburg K., Nygard K. E. A Petri Net Simulator for Self-organizing Systems. 2006.
URL: <https://api.semanticscholar.org/CorpusID:13339149> (date of access: 14.01.2026)..
10. Xie J., Chen J. Multiregional Coverage Path Planning for Multiple Energy Constrained UAVs. *IEEE Transactions on Intelligent Transportation Systems*. 2022. Vol. 23, no. 10. P. 17366—17381. DOI: 10.1109/tits.2022.3160402.
11. Fedorova A., Beliautsou V., Zimmermann A. Colored Petri Net Modelling and Evaluation of Drone Inspection Methods for Distribution Networks. *Sensors*. 2022. Vol. 22, no. 9. P. 3418. DOI: 10.3390/s22093418.
URL: <https://doi.org/10.3390/s22093418> (date of access: 14.01.2026)..

12. Zhou J., Liu K., Lu Y., Chen L. Complex network–based pinning control of drone swarm. *IFAC-PapersOnLine*. 2022. Vol. 55, no. 3. P. 216—221.
DOI: 10.1016/j.ifacol.2022.05.037.
URL: <https://www.sciencedirect.com/science/article/pii/S2405896322003007> (date of access: 18.12.2025).
13. Feng B., Zhou L., Zhang Z. Study on Cascading Failure and Elasticity of UAV Swarm Communication Network. *Mathematical Problems in Engineering*. 2022. Vol. 2022. P. 6166849. DOI: 10.1155/2022/6166849.
URL: <https://www.hindawi.com/journals/mpe/2022/6166849/> (date of access: 17.02.2026).
14. DJI. AeroScope. URL: <https://www.dji.com/global/aeroscope> (date of access: 24.02.2024).
15. Novikov O., Stopochkina I., Voitsekhovskiy A., Ilin M., Ovcharuk M. Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability. *Theoretical and Applied Cyber Security*. 2024. Vol. 6, no. 2. P. 66—76.
DOI: <https://doi.org/10.20535/tacs.2664-29132024.2.318182>. (date of access: 12.12.2025).
16. Graphviz - Graph Visualization Software. 2024. URL: <https://graphviz.org/> (date of access: 10.02.2026).
17. Shi W., He Z., Gu C., Ran N., Ma Z. Performance Optimization for a Class of Petri Nets. *Sensors*. 2023. Vol. 23, no. 3. P. 1447. DOI: 10.3390/s23031447.
URL: <https://www.mdpi.com/1424-8220/23/3/1447> (date of access: 10.02.2026).

18. Willekens J. Unmanned Aircraft System (UAS) Airworthiness Certification.
URL: <https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SCI-328/MP-SCI-328-21.pdf> (date of access: 17.02.2026).
19. IEEE Standard for Drone Applications Framework. 2021.
URL: https://cityu-dg.primo.exlibrisgroup.com.cn/permalink/86CITYU_DG/117tf3k/alma99122604608611 (date of access: 14.01.2026).
20. Zakharchenko I., Tristan A., Chornogor N., Berdnik P., Kalashnyk G., Timochko A., Zalevskii A., Dmitriiev O. Modeling of Object Monitoring Using 3D Cellular Automata. *Problemele Energeticii Regionale*. 2022. Vol. 4, no. 56. P. 06. DOI: 10.52254/1857-0070.2022.4-56.06.
URL: https://ibn.idsi.md/sites/default/files/imag_file/06_04_56_2022.pdf (date of access: 17.02.2026).
21. Song Z., Zhang H., Zhang X., Zhang F. Unmanned Aerial Vehicle Coverage Path Planning Algorithm Based on Cellular Automata. *2019 15th International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2019. P. 145—149. DOI: 10.1109/CIS.2019.00034. (date of access: 28.12.2025).
22. Ioannidis K., Sirakoulis G. C., Andreadis I. A Path Planning Method Based on Cellular Automata for Cooperative Robots. *Applied Intelligence*. 2011. Vol. 36, no. 3. P. 721—745. DOI: 10.1080/08839514.2011.606767.
URL: <https://www.tandfonline.com/doi/full/10.1080/08839514.2011.606767> (date of access: 22.12.2025).
23. Adamatzky A. Computation of shortest path in cellular automata. *Mathematical and Computer Modelling*. 1996. Vol. 23, no. 4. P. 105—113.

- DOI: 10.1016/0895-7177(96)00006-4. URL: https://www.researchgate.net/publication/239356833_Computation_of_shortest_path_in_cellular_automata (date of access: 22.12.2025).
24. Behring C., Bracho M., Castro M., Moreno J. An Algorithm for Robot Path Planning with Cellular Automata / *Theory and Practical Issues on Cellular Automata*. Springer, 2001. P. 11—19. DOI: 10.1007/978-1-4471-0709-5_2.
 25. Mozaffari M., Saad W., Bennis M., Debbah M. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *IEEE Communications Surveys & Tutorials*. 2019. Vol. 21, no. 3. P. 2334—2360. DOI: 10.1109/COMST.2019.2902890.
URL: <https://ieeexplore.ieee.org/document/8660516> (date of access: 25.01.2026).
 26. Gupta L., Jain R., Vaszkun G. Survey of Important Issues in UAV Communication Networks. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, no. 2. P. 1123—1152. DOI: 10.1109/COMST.2015.2495932.
URL: <https://ieeexplore.ieee.org/document/7317490/> (date of access: 14.01.2026).
 27. Greer C., Burns M., Wollman D., Griffor E. Cyber-Physical Systems and Internet of Things. *NIST Special Publication SP 1900-202*. 2019. . URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf> (date of access: 19.01.2026).
 28. Iyer A. A* Search Algorithm Explained. 2020. Scribd.
URL: <https://www.scribd.com/document/470779194/A-star-material> (date of access: 07.03.2026).

29. Javaid A. Understanding Dijkstra Algorithm. *SSRN Electronic Journal*. 2013. . DOI: 10.2139/ssrn.2340905. URL: <https://dx.doi.org/10.2139/ssrn.2340905> (date of access: 05.12.2025).
30. Classy T. Robotic Path Planning: RRT and RRT*. 2019. URL: <https://theclassytim.medium.com/robotic-path-planning-rrt-and-rrt-212319121378> (date of access: 24.02.2026).
31. Sabino S. A multi-objective evolutionary algorithm approach for UAV placement in mesh network formation. *Sensors*. 2018. Vol. 18, no. 12. P. 4387. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC6308967/pdf/sensors-18-04387.pdf> (date of access: 22.12.2025).
32. Kılıç A. How Floyd-Warshall Algorithm Works. URL: <https://medium.com/@umitanilkilic/floyd-warshall-algorithm-c65f274352a7> (date of access: 24.02.2026).
33. Essien G. D., Asuquo P. M., Aneke C. S. Network system optimization using machine learning analysis: A systematic review. *Global Journal of Engineering and Technology Advances*. 2026. . DOI: 10.30574/gjeta.2026.26.2.0022. URL: <https://doi.org/10.30574/gjeta.2026.26.2.0022> (date of access: 18.12.2025).
34. Baidya S., Shaikh Z., Levorato M. FlyNetSim: An Open Source Synchronized UAV Network Simulator based on ns-3 and Ardupilot. 2018. URL: <https://arxiv.org/abs/1808.04967> (date of access: 14.01.2026).
35. Haque M., Chowdhury M. Ad-Hoc Framework for Efficient Network Security for Unmanned Aerial Vehicles (UAV). 2019. P. 23—36. DOI: 10.1007/978-3-030-34353-8_2.

36. Tsioutis C., Makridis C., Timotheou S. SUAVPy: A SUMO Plugin for UAV-Based Ground Traffic Sensing. *SUMO Conference Proceedings*. 2025. Vol. 6. P. 65—77. DOI: 10.52825/scp.v6i.2610.
37. Modi T. M., Venkateswararao K., Swain P. Integration of SDN into UAV, edge computing, & Blockchain: A review, challenges, & future directions. *Computer Science Review*. 2025. Vol. 58. P. 100790.
DOI: <https://doi.org/10.1016/j.cosrev.2025.100790>. (date of access: 07.01.2026).
38. Bekmezci I., Sahingoz O. K., Temel S. Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Networks*. 2013. Vol. 11. P. 1254—1270.
DOI: 10.1016/j.adhoc.2012.12.004.
URL: <https://www.researchgate.net/publication/253954782> (date of access: 10.02.2026).
39. Wang X., Li D., Guo C. Eavesdropping and Jamming Selection Policy for Suspicious UAVs Based on Low Power Consumption over Fading Channels. *Sensors*. 2019. Vol. 19, no. 5. P. 1126. DOI: 10.3390/s19051126.
40. Patel A., Cherukuri A. K. Analysis of Light-Weight Cryptography Algorithms for UAV-Networks. *arXiv preprint arXiv:2504.04063*. 2025. .
DOI: 10.48550/arXiv.2504.04063. URL: <https://arxiv.org/abs/2504.04063> (date of access: 17.02.2026).
41. Isik O. K., Hong J.-H., Petrunin I., Tsourdos A. Integrity Analysis for GPS-Based Navigation of UAVs in Urban Environment. *Robotics*. 2020. Vol. 9, no. 3. P. 66. DOI: 10.3390/robotics9030066.

42. Ferrer-i-Cancho R., Sole R. V. Optimization in Complex Networks. *Springer*. 2003. . P. 114—126. DOI: 10.1007/978-3-540-44943-0_7. URL: https://www.researchgate.net/publication/23740085_Optimization_in_Complex_Networks (date of access: 12.12.2025).
43. Li H., Hao Y., Zhai Y., Qian Z. Enhancing Static Analysis for Practical Bug Detection: An LLM-Integrated Approach. *Proceedings of the ACM on Programming Languages*. . Vol. 8, no. 111. P. 474—499. DOI: <https://dl.acm.org/doi/10.1145/3649828>. (date of access: 25.01.2026).
44. AFLplusplus. AFL++: The AFL++ Fuzzer. 2020.
45. Hex-Rays. IDA Pro. URL: <https://hex-rays.com/ida-pro/> (date of access: 05.12.2025).
46. Valgrind: A Suite of Tools for Debugging and Profiling Programs. URL: <https://valgrind.org/> (date of access: 05.12.2025).
47. Chen C., Cui B., Ma J., Wu R., Guo J., Liu W. A Systematic Review of Fuzzing Techniques. *Computers & Security*. 2018. Vol. 75. P. 118—137. DOI: 10.1016/j.cose.2018.02.002.
48. Kim Y., Cho K., Kim S. Challenges in Drone Firmware Analyses of Drone Firmware and Its Solutions. *arXiv2312.16818*. 2024. . DOI: <https://doi.org/10.48550/arXiv.2312.16818>. (date of access: 12.12.2025).
49. Zhang B. Research Summary of Anti-debugging Technology. *Journal of Physics: Conference Series*. 2021. Vol. 1744, no. 4. P. 042186. DOI: <https://doi.org/10.1088/1742-6596/1744/4/042186>. (date of access: 22.12.2025).

50. Zhou X., Zhang T., Lo D. Large Language Model for Vulnerability Detection: Emerging Results and Future Directions. 2024.
URL: <https://arxiv.org/abs/2401.15468/> (date of access: 22.12.2025).
51. Liu P., Sun C., Zheng Y., Feng X., Qin C., Wang Y., Xu Z., Li Z., Di P., Jiang Y., Sun L. Harnessing the Power of LLM to Support Binary Taint Analysis. 2023.
URL: <https://arxiv.org/abs/2310.08275> (date of access: 03.02.2026).
52. Li Y., Li X., Wu H., Xu M., Zhang Y., Cheng X., Xu F., Zhong S. Everything You Wanted to Know About LLM-based Vulnerability Detection But Were Afraid to Ask. 2025. URL: <https://arxiv.org/abs/2504.13474> (date of access: 05.12.2025).
53. Voitsekhovskiy A., Sun P., Xie J., Stopochkina I., M.Ilin, O.Novikov. Detection of vulnerabilities in software for unmanned aerial vehicles by using large language models. *East-Eauropean Journal of Enterprise Technologies*. 2026. Vol. 1, no. 139. DOI: <https://doi.org/10.15587/1729-4061.2026.352029>. (date of access: 01.03.2026).
54. Qin W., Suo L., Li L., Yang F. Advancing Software Vulnerability Detection with Reasoning LLMs: DeepSeek-R1's Performance and Insights. *Applied Sciences*. 2025. Vol. 15, no. 12. P. 6651.
DOI: <https://doi.org/10.3390/app15126651>. (date of access: 25.01.2026).
55. Contributors M. C. P. (Introduction | Model Context Protocol.
URL: <https://modelcontextprotocol.io/docs/getting-started/intro> (date of access: 14.01.2026).

56. Tyshchenko A., Stopochkina I. Design of a simulation tool for planning UAV mission success under combat constraints. *Eastern-European Journal of Enterprise Technologies*. 2025. Vol. 5/9(137). P. 14—26.
DOI: <https://doi.org/10.15587/1729-4061.2025.340918>. (date of access: 03.02.2026).
57. Сили територіальної оборони Збройних Сил України. Засоби радіоелектронної боротьби ворога.
URL: <https://sprotyvg7.com.ua/lesson/zasobi-radioelektronnoi-borotbi-voroga> (date of access: 8.01.2026).
58. Foead D., Ghifari A., Kusuma M. B., Hanafiah N., Gunawan E. A Systematic Literature Review of A* Pathfinding. *Procedia Computer Science*. 2021. Vol. 179. P. 507—514. DOI: 10.1016/j.procs.2021.01.034.
59. Syed Abdullah F., Iyal S., Makhtar M., Jamal A. A. Robotic Indoor Path Planning Using Dijkstra's Algorithm with Multi-Layer Dictionaries. 2015.
60. European Space Agency. Copernicus Digital Elevation Model datasets (30m).
URL: <https://copernicus-dem-30m.s3.amazonaws.com/readme.html> (date of access: 12.02.2026).
61. Anthropic. Model Context Protocol Servers.
URL: <https://github.com/modelcontextprotocol/servers> (date of access: 25.01.2026).
62. Impress-U-IS-KPI. VulnerabilityDetection. 2025.
URL: <https://github.com/Impress-U-IS-KPI/VulnerabilityDetection> (date of access: 17.02.2026).

ДОДАТОК А

ВЕЛИКІ РИСУНКИ І ТАБЛИЦІ

Приклад вхідних даних симуляційного моделювання

```
[
{ "longitude": 33.65, "latitude": 51.35, "type": "base", "
  ↳ signal_radius": 50.0, "height": 0.0 },
{ "longitude": 34.45, "latitude": 51.43, "type": "EW", "
  ↳ signal_radius": 50.0, "height": 0.0 },
{ "longitude": 34.2, "latitude": 52.00, "type": "EW", "
  ↳ signal_radius": 50.0, "height": 0.0 },
{ "longitude": 34.75, "latitude": 51.52, "type": "target", "
  ↳ signal_radius": 0.0, "height": 0.0 },
{ "longitude": 33.80, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 40.0, "height": 200.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.81, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 40.0, "height": 250.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.82, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 40.0, "height": 180.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.83, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 40.0, "height": 220.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.84, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 40.0, "height": 210.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.85, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 25.0, "height": 150.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.86, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 25.0, "height": 170.0, "max_height": 20000.0
  ↳ },
{ "longitude": 33.87, "latitude": 51.37, "type": "drone", "
  ↳ signal_radius": 25.0, "height": 140.0, "max_height": 20000.0
  ↳ },
```

```
15 { "longitude": 33.88, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 160.0, "max_height": 20000.0  
    ↪ },  
16 { "longitude": 33.89, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 145.0, "max_height": 20000.0  
    ↪ },  
17 { "longitude": 33.90, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 155.0, "max_height": 20000.0  
    ↪ },  
18 { "longitude": 33.91, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 165.0, "max_height": 20000.0  
    ↪ },  
19 { "longitude": 33.92, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 150.0, "max_height": 20000.0  
    ↪ },  
20 { "longitude": 33.93, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 148.0, "max_height": 20000.0  
    ↪ },  
21 { "longitude": 33.94, "latitude": 51.37, "type": "drone", "  
    ↪ signal_radius": 25.0, "height": 158.0, "max_height": 20000.0  
    ↪ }  
22 ]
```

ДОДАТОК Б

АКТИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ РЕЗУЛЬТАТІВ
ДИСЕРТАЦІЇ

«ЗАТВЕРДЖУЮ»

Заступник директора
Навчально-наукового
фізико-технічного інституту
Національного технічного
університету України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Тетяна ПИТВІНОВА



_____ 2026 року

АКТ

впровадження результатів досліджень дисертаційної роботи
Войцеховського Андрія Валерійовича на тему «Моделі та методи
забезпечення кіберфізичної стійкості мереж дронів» на здобуття наукового
ступеня доктора філософії за спеціальністю 125 - «Кібербезпека»

Методична комісія Навчально-наукового Фізико-технічного інституту, затверджена розпорядженням №03/2025 від 10.01.2025 року, цим Актом засвідчує що результати досліджень дисертаційної роботи Войцеховського Андрія Валерійовича на тему «Моделі та методи забезпечення кіберфізичної стійкості мереж дронів» впроваджені в навчальний процес кафедри інформаційної безпеки.

Запропоновані Войцеховським А.В моделі та методи побудови маршрутів БпЛА та метод автоматизації аналізу бінарних зразків ПЗ БпЛА, використовують при викладанні дисциплін «Методи штучного інтелекту в кібербезпеці», «Кіберзахист об'єктів критичної інфраструктури» та «Аналіз бінарних вразливостей».

Голова методичної комісії
к.ф.-м.н., доцент

Сергій СМІРНОВ

Зав. кафедри інформаційної
безпеки, д.т.н., професор

Дмитро ЛАНДЕ

« 23 » _____ 2026 року