

Л. Ю. Остапенко, В. С. Харченко

Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна

СИСТЕМА ДЛЯ МОДЕЛЮВАННЯ ПОДОЛАННЯ ПЕРЕШКОД І ОРГАНІЗАЦІЇ КОМУНІКАЦІЙ В НЕБЕЗПЕЧНИХ ПРОСТОРАХ: СТРУКТУРА ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

Анотація. У статті представлено комплексну систему моделювання подолання перешкод та організації комунікацій у небезпечних просторах із застосуванням розв'язків безпілотних апаратів. Запропоновані моделі середовища, перешкод, динамічних впливів та БПА дозволяють відтворювати сценарії роботи у зруйнованих або важкодоступних приміщеннях, враховуючи статичні й динамічні об'єкти, а також кіберфізичні впливи. Архітектура симулятора побудована на базі Python та рушія Panda3D з інтеграцією засобів збору й аналізу даних (InfluxDB, Grafana, Docker), що забезпечує гнучке налаштування параметрів та відтворення широкого спектра сценаріїв. У статті наведено результати експериментів, що демонструють ефективність алгоритмів маршрутизації (A*, Greedy Best-First тощо) та координації рою для розгортання ланцюжка зв'язку з використанням Li-Fi. Доведено, що система є корисним навчально-дослідницьким інструментом для перевірки алгоритмів, аналізу надійності рою, оцінки енергоефективності та стійкості до кібервпливів. Перспективи розвитку передбачають інтеграцію з ROS, розширення бібліотеки датчиків та моделювання протоколів мережевого рівня.

Ключові слова: моделювання, безпілотні апарати, розгортання рою БПА, небезпечне середовище, маршрутизація, маршрути, оминання перешкод, комунікації, Li-Fi, Panda3D, кіберфізичні впливи.

Вступ

Надзвичайні ситуації (техногенні аварії, стихійні лиха, військові дії тощо) часто призводять до відмов, руйнування або знищення стаціонарної інфраструктури зв'язку. У таких умовах виникає потреба у швидкому розгортанні тимчасових мереж, здатних передавати дані від сенсорів і постраждалих до кризових центрів. Безпілотні літальні апарати (БПЛА, або просто безпілотні апарати – БПА) все частіше розглядаються як перспективний засіб відновлення комунікацій у важкодоступних і небезпечних зонах. Зокрема, дрони можуть слугувати “літаючими” ретрансляторами або навіть базовими станціями для створення тимчасових мереж там, де наземний зв'язок відсутній. Наприклад, у роботі розглядається мережа оптичного зв'язку Light Fidelity (LiFi) на базі рою дронів для збору даних у зруйнованих аварією приміщеннях, що дозволяє оперативно передавати інформацію до рятувального штабу навіть за відсутності радіозв'язку. Інше дослідження демонструє можливості дронів відновлювати радіозв'язок у зонах лиха, підтримуючи комунікацію рятувальників. Також розглядається використання різних безпілотних платформ (наземних, надводних) залежно від типу середовища та завдань [1]. Дрони вже застосовуються для моніторингу стану критичної інфраструктури та безпеки міст [2], пошуку постраждалих, а також гуманітарного розмінування та виявлення вибухонебезпечних предметів [3]. Зокрема, досліджуються методи використання БПЛА для виявлення мін та вибухівки на небезпечних територіях [4], а також гібридні роботизовані системи з біологічними сенсорами для пошуку вибухових пристроїв [5]. Всі ці задачі потребують ретельної попередньої перевірки алгоритмів і моделювання сценаріїв, адже безпілотні апарати мають працювати в динамічних, непередбачуваних умовах.

Небезпечний простір (НП) визначається як динамічне 3D-середовище, що містить механічні перешкоди та різноманітні фізичні й інформаційні

(кібернетичні) впливи, які можуть зашкодити мобільним роботизованим засобам, ускладнити їх пересування або порушити комунікації [6]. Прикладами НП є великі зруйновані приміщення (енергетичні, транспортні чи промислові об'єкти), природні середовища з перешкодами (ліси, гори) чи акваторії, потенційно нашіпиговані вибухонебезпечними предметами [7]. Забезпечення стійкого зв'язку у успішного подолання таких просторів силами рою БПА є нетривіальною задачею, що потребує застосування спеціальних алгоритмів маршрутизації, уникнення зіткнень та координації рою. Водночас самі НП можуть включати кібератаки та електромагнітні завади (глушіння сигналів, спуфінг GPS тощо), які слід враховувати при проектуванні систем зв'язку [8].

Для дослідження подібних сценаріїв та відпрацювання алгоритмів на практиці створюються програмні симулятори. Відомі симулятори (OMNeT++, Gazebo, AirSim тощо) дозволяють відтворювати окремі аспекти поведінки рою дронів, але наразі відсутній універсальний інструмент, який би однаково добре моделював і комунікаційні мережі, і фізичну динаміку безпілотних систем [9, 10]. Тому розробка спеціалізованих систем моделювання під конкретні задачі – актуальне завдання. Важливо підкреслити, що запропонована в цій статті симуляційна система не призначена для реального застосування під час розмінування чи інших небезпечних операцій. Вона слугує виключно навчально-дослідницьким інструментом – середовищем для відпрацювання програмних рішень, перевірки алгоритмів та експериментального аналізу поведінки розв'язків БПА до їх розгортання на практиці.

Метою дослідження є розроблення комплексної системи моделювання, що дозволяє тестувати та вдосконалювати методи подолання перешкод і забезпечення безперервних комунікацій роєм інтелектуальних безпілотних апаратів у небезпечних кіберфізичних просторах. Для досягнення поставленої мети необхідно вирішити такі завдання:

проаналізувати сучасні підходи та існуючі моделі використання БПА для підтримки зв'язку в екстремальних ситуаціях, а також наявні симулятори безпілотних систем (їхні можливості та обмеження в контексті НП);

сформулювати вимоги до симулятора, який об'єднує фізичну модель середовища і мережеві аспекти, включно з врахуванням перешкод та кібер-впливів;

розробити моделі компонентів системи (середовище, перешкоди, впливи, дрони і рій) та архітектуру програмного симулятора на їх основі;

реалізувати прототип симулятора та провести експериментальні дослідження ефективності запропонованих алгоритмів розгортання мережі БПА в різних сценаріях НП.

1 Огляд проблематики та стану досліджень

Застосування безпілотних апаратів у небезпечних просторах. У останні роки з'явилося багато досліджень, присвячених використанню безпілотних систем для забезпечення зв'язку та збору інформації в екстремальних умовах. Зокрема, концепція літаючих ad hoc-мереж (FANET) передбачає, що дрони утворюють автономну бездротову мережу, обмінюючись даними між собою та з наземними вузлами. Такі мережі довели ефективність у військових і рятувальних операціях, при моніторингу довкілля, у сільському господарстві тощо. Оглядом роботи відзначають необхідність розробки масштабованих і гнучких архітектур зв'язку для роєвих систем, здатних підтримувати різні конфігурації та завдання. Одним із ключових сценаріїв є використання БПА як ретрансляторів у зонах лиха, де дрони швидко створюють тимчасову мережу для координації рятувальників і передачі даних постраждалим. Наприклад, у роботі запропоновано мережу БПА на основі LiFi для аварійного об'єкта, а у дослідженні[11] запропоновано аналіз надійності роєвих сенсорних мереж для міського моніторингу. Для забезпечення зв'язку під час масових подій (концерти, мітинги) дрони розглядаються як тимчасові базові станції стільникового зв'язку. Зокрема, автори роботи описують алгоритм оптимального розгортання декількох дронів-BS для обслуговування великого скупчення користувачів, що дозволило суттєво покращити покриття і якість зв'язку в пікові періоди.

Особливу увагу дослідників привертають рої БПА та їхня самоорганізація. Рій – це група дронів, що діють спільно, координуючи свої дії для досягнення спільної мети. Перевагами роєвих систем є підвищена надійність (відмова одного апарата не призводить до провалу місії), ширше покриття та гнучкість перенастроювання під нові задачі[12]. Водночас виникають виклики: розробка протоколів зв'язку між багатьма рухомими вузлами, уникнення зіткнень у тривимірному просторі, узгодження рішень великої кількості агентів у реальному часі[13,14]. Запропоновано різні підходи до координації: від біонатхнених алгоритмів (за аналогією з поведінкою птахів чи комах) до методів машинного навчання. Наприклад, у роботі[15] описано модель роєвої комунікації для пошуково-рятувальних місій, де використовуються

алгоритми кластеризації (K-means) та методи на основі випадкового лісу для оптимізації розміщення дронів і покращення потужності сигналу. Інші огляди узагальнюють архітектури управління роєм та окреслюють відкриті проблеми, зокрема забезпечення надійного обміну даними і справедливого використання каналу всіма дронами в мережі.

Симулятори та моделювання мереж БПА. Для перевірки алгоритмів зв'язку і маршрутизації у мережах дронів застосовуються мережеві симулятори загального призначення – передусім NS-3 та OMNeT++[16,17]. Вони підтримують моделювання бездротових ad hoc-мереж (зокрема, маневрених мереж UAV, відомих як MANET/FANET) і здатні імітувати передачу трафіку, відмови вузлів, змінну навантаженість каналу тощо. Дослідження показали, що ці інструменти дозволяють досить масштабовано відтворювати мережі з десятків і сотень вузлів[18]. NS-3 відзначається наявністю великої бібліотеки протоколів, а OMNeT++ – гнучкістю і зручним графічним інтерфейсом[19]. Проте їхнім недоліком є обмежена можливість моделювати фізичний рух дронів у 3D-просторі та враховувати реальні перешкоди середовища (будівлі, рельєф, перешкоди радіохвиль)[20]. З іншого боку, фізичні симулятори (Gazebo, AirSim, MATLAB/Simulink тощо) дозволяють детально моделювати польотну динаміку, сенсорні дані (камери, LiDAR) і навіть алгоритми автопілота для безпілотників[21]. Такі засоби використовуються для відпрацювання навігації та керування, але зазвичай не моделюють навантаження мережевого трафіку.

Актуальним трендом є створення інтегрованих середовищ співсимуляції (co-simulation), що об'єднують кілька спеціалізованих симуляторів для одночасного моделювання різних аспектів системи[22]. Існують рішення поєднання NS-3 з Gazebo (для врахування затримок і втрат у радіоканалі під час 3D-руху дронів) або зв'язки OMNeT++ з SUMO (для одночасної симуляції руху транспорту і роботи мережі)[23]. Попри наявність таких інструментів, універсального симулятора роєвих БПА на сьогодні не існує[10]. Кожна платформа має свої обмеження, тому дослідники часто створюють власні тестові полігони під конкретні потреби[24]. У зв'язку з цим у даній роботі запропоновано спеціалізований симулятор, орієнтований на сценарії забезпечення зв'язку в небезпечних просторах. Він поєднує базове фізичне моделювання середовища з елементами мережевої моделі, надаючи гнучкі засоби налаштування параметрів. Нижче описано концептуальні моделі, закладені в основу системи, та її програмну архітектуру.

2 Моделі системи

При розробці симулятора формалізовано кілька моделей, що описують різні аспекти небезпечного простору і компонентів рою. Кожна модель визначає параметри, які можуть налаштовуватися користувачем для побудови конкретного сценарію.

Модель середовища. Небезпечний простір представлено у вигляді тривимірної області заданої форми і розмірів. В загальному випадку форма середовища може бути прямокутною (наприклад, кімната,

ангар) або довільною (фрагмент ландшафту, акваторії). Параметрами моделі є габарити простору (довжина, ширина, висота або радіус), а також візуальне відображення оточення. Середовище може містити межі (стіни, підлога, стеля), за які дрони не можуть вилітати. У симуляторі передбачено завантаження 3D-моделі рельєфу чи об'єкта як середовища або генерацію примітивного простору із заданими розмірами сцени.

Модель перешкод. Перешкоди – це об'єкти середини НП, які заважають руху дронів або блокують лінії зв'язку. Модель перешкод включає як статичні, так і динамічні об'єкти. Статичні перешкоди характеризуються фіксованим положенням та розмірами (наприклад, зруйновані колони, завали, стіни). Динамічні перешкоди можуть змінювати своє розташування або параметри з часом (наприклад, рухомі технічні засоби, транспорт або плаваючі об'єкти на воді). Кожна перешкода описується формою (геометричною моделлю), розмірами, початковими координатами та (для рухомих) траєкторією або законом руху. У системі підтримується завдання довільної кількості перешкод різних типів: їх можна розміщувати через конфігураційний файл або генерувати автоматично із заданими статистичними характеристиками (щільність, розподіл розмірів). При завантаженні сцени симулятор перевіряє колізії – чи не перетинаються об'єкти між собою, – і коригує розміщення при необхідності.

Модель динамічних впливів. Окрім твердих перешкод, у НП можуть бути присутні явища, що негативно впливають на видимість, фізичний стан та зв'язок. Модель динамічних впливів охоплює різного роду ефекти: задимленість, туман, запыленість, вогонь, пару, а також електромагнітні завади та кібератаки. Кожен вплив визначається типом, джерелом або площею поширення, інтенсивністю та законом динаміки (наприклад, туман може розсіюватися з часом, радіоперешкоди можуть з'являтися й зникати стрибкоподібно). У рамках симуляції фізичні ефекти (дим, туман) моделюються переважно графічно – через систему часток у рушії (що впливає на видимість сенсорів дронів). Інформаційні впливи реалізовані на рівні моделі зв'язку: вводиться коефіцієнт шуму на канал або імітуються раптові розриви з'єднання. Кібернетичний вплив може бути змодельовано як сценарій, коли один чи кілька дронів починають діяти некоректно (компрометовані вузли) або надходять помилкові дані про стан системи. Такі ситуації дозволять протестувати живучість алгоритмів рою за умов цілеспрямованих атак. В поточній реалізації симулятора динамічні впливи обмежені простим відключенням зв'язку при заданому рівні перешкод; у перспективі планується додати більш детальне моделювання (наприклад, поширення диму по області, модель затухання радіосигналу тощо).

Моделі БПА та рою. У симуляторі кожен безпілотний апарат представлено як окремий агент з певними параметрами. До основних технічних характеристик моделі БПА належать: максимальна швидкість та висота польоту, запас енергії (ємність батареї), потужність в стаціонарному стані, потужність в

польоті, дальність зв'язку, набори сенсорів (камера, тепловізор, газоаналізатор тощо, залежно від сценарію). Також фіксуються габарити дрона для врахування при зіткненнях і мінімально допустима дистанція до інших дронів або інших перешкод. Підтримується декілька типів апаратів – наприклад, багатопропелерні БПЛА заданого розміру, безпілотні наземні роботи, надводні дрони – з різними характеристиками. Стартове розміщення дронів задається окремо (координати або депо старту). Інтелектуальні можливості агентів задаються через програмні “поведінкові компоненти” – функції, що визначають реакцію БПА на певні події (втрата зв'язку, виявлення нової перешкоди, низький заряд батареї тощо). Таким чином, моделюється простий рівень автономності: дрони можуть самостійно приймати локальні рішення (наприклад, облетіти перешкоду або повернутися на зарядку при розряді акумулятора). Рій БПА розглядається як множина агентів, що обмінюються повідомленнями і діють узгоджено. В моделі передбачено два підходи до координації: централізований (через виділений головний вузол або зовнішній центр керування) та децентралізований (кооперативний рій без лідера). У централізованому випадку один із дронів (або базова станція) збирає інформацію від усіх учасників і обчислює нові позиції та маршрути для них; у децентралізованому – кожен дрон виконує алгоритм координації самостійно, обмінюючись даними лише з сусідами. В обох випадках ключовим компонентом є алгоритм керування роєм – правило, за яким дрони коригують своє положення для підтримання зв'язності мережі. У прототипі реалізовано спрощений алгоритм: періодично кожен БПА порівнює рівень сигналу від сусідів і зміщується у бік того вузла, сигнал від якого найслабший (тобто “лаєє дірку” у покритті мережі). Така поведінка аналогічна до рою бджіл, які реорганізуються при втраті окремих особин. Надалі планується випробувати й інші методи координації (на основі правил рою частинок, оптимізації роєм бджіл, Q-навчання тощо).

3 Архітектура симулятора

Розроблений симулятор має модульну архітектуру і реалізований мовою програмування Python. За візуалізацію тривимірного середовища та обрахунок фізичної взаємодії агентів відповідає ігровий рушій Panda3D. Вибір Python + Panda3D обумовлений гнучкістю налаштування поведінки агентів і можливістю швидкого прототипування алгоритмів керування роєм. Подібний підхід використовувався й іншими розробниками симуляторів – наприклад, у роботі Annaz наведено платформу навчального полігону для БПЛА з використанням Panda3D [25].

Архітектура складається з низки модулів, що відповідають моделям системи (рис. 1). Модуль середовища завантажує або генерує сцену заданих розмірів, встановлює моделі статичних об'єктів (рельєф, будівлі, межі тощо) та освітлення. Модуль перешкод опрацьовує конфігураційні дані про перешкоди: завантажує 3D-моделі або параметри примітивів (куб, сферу) для кожної перешкоди, задає їх початкове розташування.

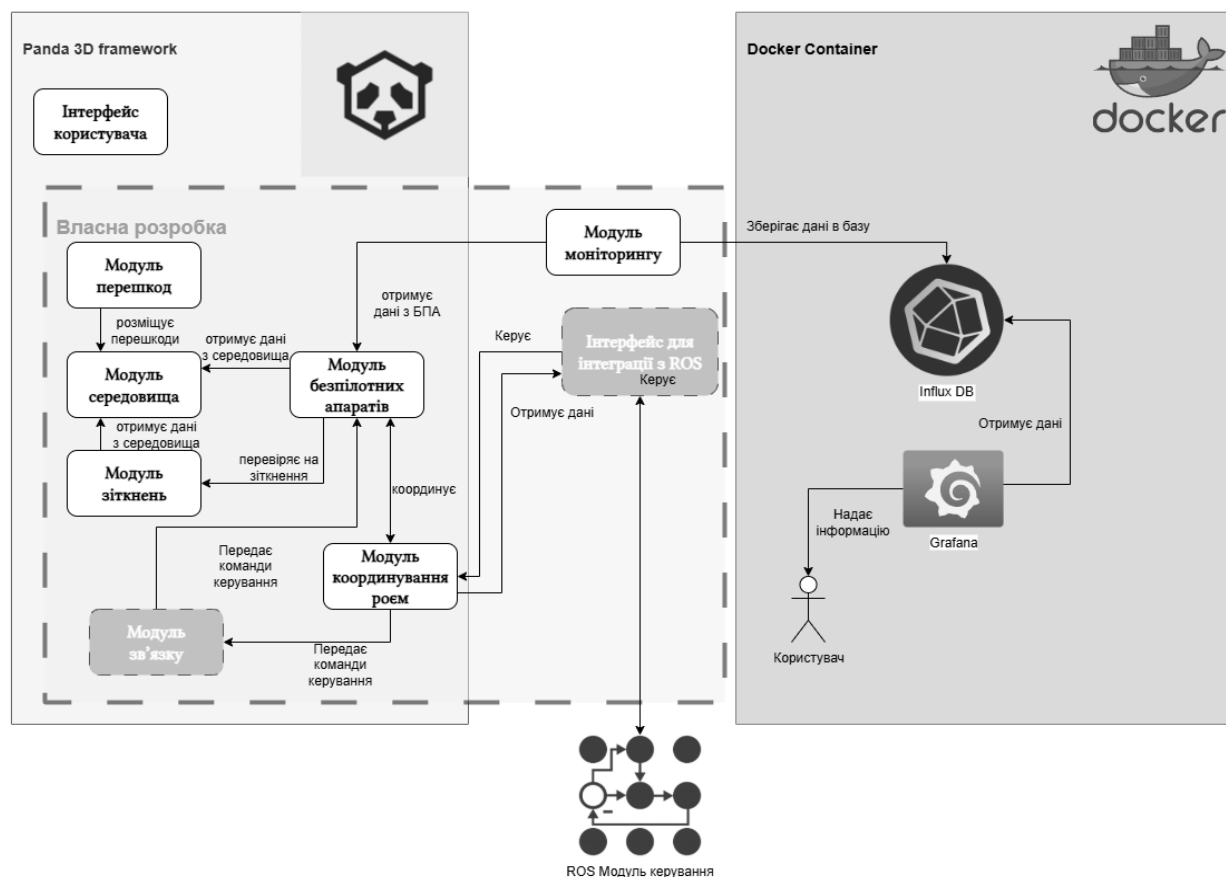


Рис. 1. Архітектура системи

Динамічні перешкоди створюються з прив'язаними функціями руху (наприклад, періодичне переміщення по заданій траєкторії). Модуль виявлення колізій (CollisionHandler) відстежує зіткнення дронів з перешкодами чи між собою, використовуючи механізми фізичного рушія. При зіткненні польоти відповідних дронів зупиняються або змінюється їхній маршрут (залежно від налаштувань сценарію – можна або моделювати “аварію” дрона, або примусити його облетіти перешкоду).

Модуль безпілотних апаратів відповідає за створення і параметризацію об'єктів-дронів у симуляції. Кожен агент ініціалізується з атрибутами, визначеними в моделі БПА: встановлюється 3D-модель дрона (умовна або детальна), маса, радіус дії сенсорів, запас заряду тощо. Рух дрона здійснюється або за попередньо розрахованою траєкторією, або згідно з алгоритмом керування роєм у реальному часі.

Модуль зв'язку (запланований до розробки) буде реалізувати обмін повідомленнями між агентами і моделювати фізичний канал. Якщо між двома агентами знаходиться перешкода, модуль на першому етапі розробки буде забороняти зв'язок. Також на другому етапі для радіоканалу враховуватимуться фонові завади і можливі перешкоди від кіберфізичних впливів.

Модуль координації роєм реалізує обраний алгоритм керування роєм. Він може працювати у двох режимах: централізовано – як окремий процес або потік на “наземному” вузлі, що збирає телеметрію від усіх дронів і обчислює для них нові цільові

точки; або децентралізовано – як метод, викликаний для кожного дрона локально з використанням лише часткової інформації. Цей модуль тісно пов'язаний з модулем зв'язку: у децентралізованому режимі кожен дрон має список сусідів (тих, з ким є радіозв'язок), і рішення про рух ухвалюється на підставі локальних показників (рівня сигналу, кількості сусідів, відстані до цільової точки тощо). У централізованому – глобальний контролер має повні дані про мережу та може виконувати, наприклад, оптимізацію розміщення всього рою (ця задача комбінаторна і вимагає значних обчислювальних ресурсів при великій кількості дронів).

Додатково заплановано інтеграцію з Robot Operation System (ROS)[26], модуль координації роєм заплановано як інтерфейс між системою моделювання і пристроєм або програмою керування роєм на основі ROS.

Конфігурація і інтерфейс. Для зручності створення сценаріїв, всі вхідні параметри системи задаються у вигляді текстових конфігураційних файлів. Зокрема, використано формати YAML та CSV: YAML-файл описує загальні параметри середовища і сценарію (розміри області, кількість дронів, режими координації, умови середовища та ін), тоді як CSV-файли можуть використовуватися для переліку координат перешкод чи шляхових точок. Такий підхід полегшує повторне використання сценаріїв і внесення змін без зміни коду. Графічний інтерфейс симулятора надає огляд сцени у 3D-режимі від третьої особи; користувач може обертати камеру, змінювати

масштаб та кут огляду. Доступна можливість взяти під контроль один з дронів ціль (обрати зі списку на клавіатурі), щоб перевірити роботу алгоритму керування роєм у реальному часі.

Моніторинг і збір даних. У ході симуляції система збирає телеметричні дані: координати всіх дронів, стан їх батарей, статистику зв'язності мережі (які вузли зв'язані, через які ретранслятори проходить маршрут від джерела до бази), затримки доставки повідомлень тощо. Для зберігання цих даних використано часово-рядну базу даних InfluxDB, у яку модуль моніторингу надсилає записи в реальному часі. Це дозволяє будувати графіки та метрики під час експерименту за допомогою Grafana – зручного інструменту візуалізації. Налаштовано кілька панелей Grafana, що відображають, наприклад, заряди батарей мережі з часом, рівень сигналу на різних ділянках, відстань, пройдену кожним дроном, тощо. Архітектура передбачає також можливість контейнеризації: всі компоненти (симулятор, СУБД, Grafana) можуть бути розгорнуті в середовищі Docker для спрощення встановлення та перенесення на різні платформи. За допомогою Docker-образу симулятор легко запускати на навчальних комп'ютерних класах або в хмарній інфраструктурі.

4 Експериментальні дослідження

Експериментальні дослідження були проведені з метою оцінки ефективності та працездатності запропонованої системи моделювання у різних сценаріях. Для експериментів були використані спеціально розроблені конфігурації простору з перешкодами та запропоновані алгоритми пошуку маршрутів для БПА.

4.1 Умови експериментів. Для експериментів використовувався сценарій побудови ланцюжка зв'язку між двома заданими точками за допомогою

БПА які передають інформацію по технології Li-Fi. Між точками початку та фінішу розміщені перешкоди статичного типу, Побудова ланцюжка відбувається за алгоритмом A* зі спрощенням шляху за допомогою функції видимості (прибрані всі проміжні точки розміщення які можуть бути прибрані без втрати видимості між точками). За сценарієм нові БПА з'являються на точці їх старту щойно точка звільняється від попереднього БПА, польоти відбуваються з урахуванням інших БПА в якості рухомих перешкод. Перед початком руху відбувається розрахунок траєкторії польоту, яка може бути змінена під час руху. Умовна максимальна дальність передачі сигналу була встановлена на рівні 8 метрів. Пряма дистанція між стартовою та фінішною точками: 57 м, Загальна довжина побудованого маршруту: 97.53 м, Кількість БПА: 15. Час пошуку маршруту для ланцюжка БПА не входить в час розгортання системи.

Виміри під час експериментів:

- довжина пройденого шляху усіма БПА;
- кількість сегментів траєкторій маршрутів БПА;
- час розгортання систем.

4.2. Експеримент 1 (рис. 2). Особливості: Експеримент був проведений з використанням A* зі спрощенням шляху за допомогою функції видимості для побудови шляху для БПА до найближчої точки ланцюжка. Для переміщення з точки базування до місця розташування в ланцюжку було використано метод розміщення по траєкторії ланцюжка (БПА дістаються найближчої точки ланцюжка до точки зльоту і розподіляються по ньому спочатку в сторону кінцевої точки потім початкової точки). Ця стратегія значно зменшує навантаження на модуль керування бо траєкторія відома заздалегідь, але в разі виявлення рухомих перешкод потрібні додаткові способи уникнення зіткнень і перебудови ланцюжка.

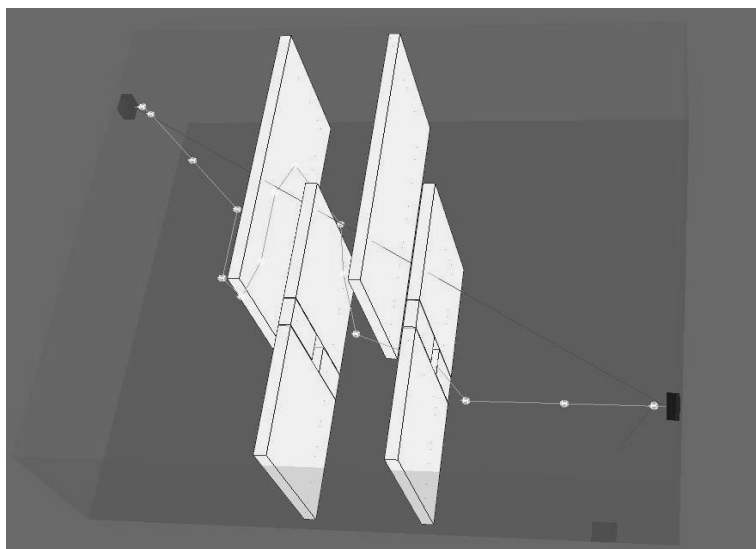


Рис. 2. Результат експерименту 1

Виміри:

- довжина пройденого шляху БПА: 791.14 м;
- кількість сегментів траєкторій дронів: 120;
- час розгортання системи: 22 сек.

4.3. Експерименти 2, 3 (рис. 3). Особливості: Експерименти були проведені з використанням алгоритму A* і жадібного перший-кращий (Greedy Best-First) зі спрощенням шляху за допомогою функції

видимості для побудови маршрутів БПА до їх місць розташування в ланцюжку, кожен БПА знаходить свій шлях індивідуально. Виміри:

- довжина пройденого шляху усіма БПА: 865 м;

- кількість сегментів маршрутів: 147;
- час розгортання системи: 1 год 40 хв 21 сек (A*);
- час розгортання системи: 1 год 36 хв 34 сек (Greedy Best-First).

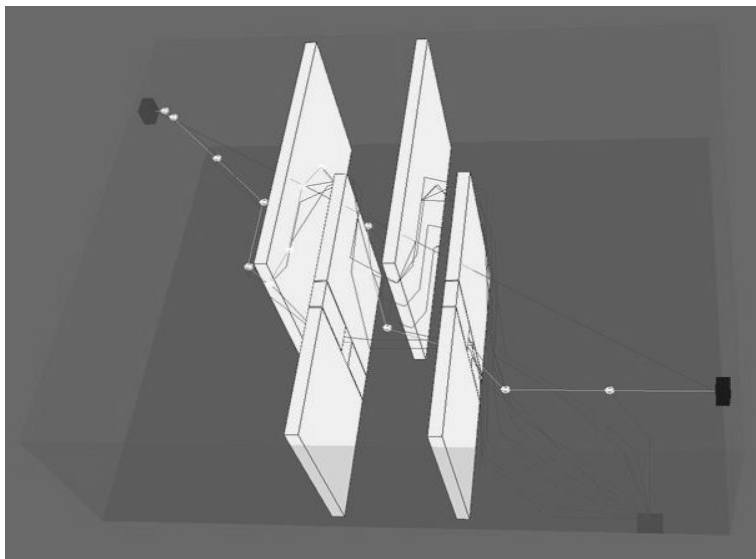


Рис. 3. Результати експерименту 2, 3

4.4. Експеримент 4 (рис. 4). Особливості: Експеримент був проведений з використанням жадібного перший-кращий (Greedy Best-First) пошуку для

побудови маршрутів БПЛА до їх місць розташування в ланцюжку, кожен БПА знаходить свій шлях індивідуально.

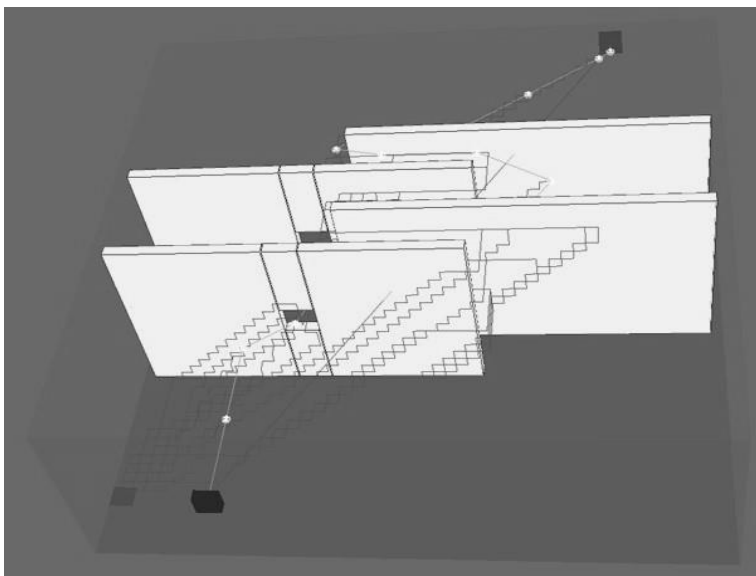


Рис. 4. Результат експерименту 4

Виміри:

- довжина пройденого шляху усіма БПЛА: 1316 м;
- кількість сегментів маршрутів: 1316;
- час розгортання системи: 1 год 43 хв 59 сек.

4.5. Аналіз результатів експериментів. Додатково був проведений Експеримент з використанням алгоритмів RRT та RRT* але нажаль вони не впорались з поставленою задачею, ними було побудовано ланцюжок лише до середини а далі пошук не дав результатів. Найбільш вдалим є варіант розміщення БПЛА за допомогою вже побудованого маршруту

ланцюжка як зроблено в експерименті 1, але тут також є свої мінуси: БПЛА під час підміни БПА наприклад для повернення на перезарядку потрібно використовувати додаткові засоби для обходу БПА які займають свої місця в ланцюжку або все ж використовувати інший алгоритм для повернення на точку базування.

Результати експериментів 2 і 3 показують велику схожість алгоритмів побудови шляху через що результати дуже подібні один до одного, лише за рахунок меншої кількості обчислень Жадібний пошук перемагає по часу.

Експеримент 4 показує, що алгоритм спрощення шляху за допомогою функції видимості дозволяє значно зменшити кількість дій (сегментів шляху), що зменшує складність подальших розрахунків і прискорює розгортання системи.

Висновки та перспективи

У статті представлено комплексну освітньо-дослідницьку систему моделювання для відтворення сценаріїв подолання перешкод та організації комунікацій у небезпечних просторах із застосуванням роевих безпілотних апаратів. Система дозволяє детально моделювати ситуації, в яких традиційні мережі зв'язку недоступні або зруйновані, і досліджувати можливості рою БПА щодо швидкого відновлення інформаційного зв'язку.

Основні результати роботи можна підсумувати таким чином:

Проаналізовано сучасні технології та рішення у сфері використання безпілотних апаратів для забезпечення зв'язку в критичних ситуаціях. Показано, що роеві системи з розподіленим управлінням здатні забезпечити живучі комунікації у складних умовах, завдяки надлишковості вузлів і гнучкій перебудові мережі [11].

Запропоновано і реалізовано методологію моделювання НП, яка включає формалізацію простору, моделі статичних та динамічних перешкод, планування маршрутів обходу, оптимальне розташування ретрансляторів-БПА та алгоритми координації рою. Це дає змогу попередньо оцінити різні стратегії і вибрати найбільш ефективні рішення для відновлення мережі зв'язку.

Розроблено архітектуру системи моделювання, що поєднує 3D-рушій для фізичного моделювання та інструменти збору й аналізу даних. Використання Python/Panda3D спрощує імплементацію поведінки дронів, а інтеграція з InfluxDB/Grafana забезпечує зручний моніторинг результатів. Хоча поточна версія не підтримує детальну імітацію мережевих протоколів, вона дозволяє відтворювати широкий спектр сценаріїв без затрат на реальні польоти.

Експериментальні дослідження підтвердили працездатність системи та ефективність модифікованих алгоритмів пошуку шляхів. За рахунок спрощення траєкторій та продуманого порядку розгортання рою вдалось зменшити сумарну довжину маршрутів і кількість маневрів, що позитивно впливає на швидкість виконання завдання і економію заряду батарей дронів.

Показано, що симулятор може слугувати корисним інструментом як в освітньому процесі, так і в наукових дослідженнях. Він дає можливість студентам та розробникам роїв БПА безпечно випробувати різні підходи до розгортання мережі БПА, налаштувати параметри середовища, випробувати власні сценарії аварійних ситуацій та переконатися в надійності запропонованих рішень. Зокрема, можна проаналізувати питання енергоефективності (планування заряджання/заміни дронів), захисту від кібератак, оптимізувати кількість апаратів для покриття заданої території тощо.

Перспективи подальшого розвитку симулятора включають:

інтеграцію з операційною системою ROS для використання реальних контролерів дронів у контурі моделювання;

розширення бібліотеки датчиків (імітація бортових камер, тепловізорів, дистанційних датчиків);

додавання сценаріїв з кіберфізичним протистоянням (моделювання атак типу “глушіння” і засобів протидії на рівні програмного забезпечення БПА) [8];

покращення моделі середовища (рельєф місцевості, погодні умови) та реалізацію підтримки мережевих протоколів (наприклад, інтеграція модулів NS-3 для детального моделювання маршрутизації пакетів).

Усе це розширить сфери застосування симулятора і наблизить його до потреб як навчальних лабораторій з робототехніки та кібербезпеки, так і до прикладних завдань служб надзвичайних ситуацій. Врешті, виконане дослідження є внеском у розвиток інтелектуальних роевих систем, здатних ефективно виконувати завдання у складних та небезпечних умовах, мінімізуючи ризики для людей.

СПИСОК ЛІТЕРАТУРИ

1. Methods and Software Tools for Reliable Operation of Flying LiFi Networks in Destruction Conditions / H. Fesenko et al. *Sensors*. 2024. Vol. 24, no. 17. P. 1–27. URL: <https://doi.org/10.3390/s24175707>
2. Flying Sensor and Edge Network-Based Advanced Air Mobility Systems: Reliability Analysis and Applications for Urban Monitoring / H. Fesenko et al. *Drones*. 2023. Vol. 7, no. 7. P. 1–28. URL: <https://doi.org/10.3390/drones7070409>
3. A UAV-Swarm-Communication Model Using a Machine-Learning Approach for Search-and-Rescue Applications / H. Khalil et al. *Drones*. 2022. Vol. 6, no. 12. P. 372(1–21). URL: <https://doi.org/10.3390/drones6120372>
4. Emergency Communication Service Solution Based on UAV Swarm / J. Jiang et al. *Theoretical and Natural Science*. 2023. Vol. 19, no. 1. P. 222–233. URL: <https://doi.org/10.54254/2753-8818/19/20230561>
5. Chandran I., Vipin K. Multi-UAV Networks for Disaster Monitoring: Challenges and Opportunities from a Network Perspective. *Drone Systems and Applications*. 2024. Vol. 1, no. 1. P. 1–28. URL: <https://doi.org/10.1139/dsa-2023-0079>
6. Optimizing Drone Deployment for Cellular Communication Coverage During Crowded Events / C. Boucetta et al. *Proc. of IEEE ICC*. 2019. P. 1–6. URL: <https://doi.org/10.1109/MILCOM47813.2019.9020748>
7. Champion M., Ranganathan P., Faruque S. UAV Swarm Communication and Control Architectures: A Review. *Journal of Unmanned Vehicle Systems*. 2019. Vol. 7, no. 3. P. 93–106. URL: <https://doi.org/10.1139/juvs-2018-0009>
8. A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies / F. Pasandideh et al. *Remote Sensing*. 2022. Vol. 14, no. 18. P. 4459(1–28). URL: <https://doi.org/10.3390/rs14184459>
9. Oh D., Han J. Smart Search System of Autonomous Flight UAVs for Disaster Rescue. *Sensors*. 2021. Vol. 21, no. 20. P. 6810. URL: <https://doi.org/10.3390/s21206810>
10. Energy Efficient UAV-Assisted Emergency Communication with Reliable Connectivity and Collision Avoidance / N. Sharvari et al. *arXiv preprint*. 2023. P. 13. URL: <https://doi.org/10.48550/arXiv.2308.16719>

11. Kimura T., Ogura M. Distributed Collaborative 3D-Deployment of UAV Base Stations for On-Demand Coverage. IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, Toronto, ON, Canada, 6–9 July 2020. 2020. URL: <https://doi.org/10.1109/infocom41043.2020.9155283>
12. Gadre D., Immanuel J. Utilizing Drones to Restore and Maintain Radio Communication in Disaster Scenarios. Wilderness & Environmental Medicine. 2022. Vol. 33, no. 2. P. 238–244. URL: <https://doi.org/10.1016/j.wem.2021.11.007>
13. Kumar P., Singh Y., Sharma R. Swarm-Based UAV Communication Network: A Review of Challenges and Solutions. Procedia Computer Science. 2022. Vol. 198. P. 574–579. URL: <https://doi.org/10.1016/j.procs.2021.12.299>
14. Kovalyov A., Komarov M., Zabolotskiy A. Deployment of UAV Base Stations for Providing Wireless Coverage in Emergency Situations. Proc. of 2021 IEEE Int. Conf. on Emergency Science and Information Technology (ICESIT). 2021. P. 237–240. URL: <https://doi.org/10.1109/ICESIT53202.2021.9629112>
15. Han D., Xie J., Zhang Y. Fair Communications in UAV Networks for Rescue Applications. IEEE Internet of Things Journal. 2020. Vol. 7, no. 8. P. 7634–7646. URL: <https://doi.org/10.1109/JIOT.2020.2995618>
16. Fang Z., Savkin A. Strategies for Optimized UAV Surveillance in Various Tasks and Scenarios: A Review. Drones. 2024. Vol. 8, no. 5. P. 193(1–25). URL: <https://doi.org/10.3390/drones8050193>
17. Autonomous UAV Safety Oriented Situation Monitoring and Evaluation System / Z. Shi et al. Drones. 2024. Vol. 8, no. 7. P. 308(1–22). URL: <https://doi.org/10.3390/drones8070308>
18. UAV Applications for Monitoring and Management of Civil Infrastructures / A. Villarino et al. Infrastructures. 2025. Vol. 10, no. 5. P. 106(1–19). URL: <https://doi.org/10.3390/infrastructures10050106>
19. Robotic-Biological Systems for Detection and Identification of Explosive Ordnance: Concept, General Structure, and Models / G. Fedorenko et al. Radioelectronic and Computer Systems. 2023. 2. P. 143–159. URL: <https://doi.org/10.32620/reks.2023.2.12>
20. Nikolaiev M., Novotarskyi M. Comparative Review of Drone Simulators. Information, Computing and Intelligent Systems. 2024. No. 4. P. 79–98. URL: <https://doi.org/10.20535/2786-8729.4.2024.300614>
21. Koenig N., Howard A. Design and Use Paradigms for Gazebo, an Open-Source Multi-Robot Simulator. Proc. of 2004 IEEE/RSJ Int. Conf. on Intelligent Robots and Systems (IROS). 2004. P. 2149–2154. URL: <https://doi.org/10.1109/IROS.2004.1389727>
22. Varga A., Hornig R. An Overview of the OMNeT++ Simulation Environment. Proc. of 1st Int. Conf. on Simulation Tools and Techniques (SIMUTools). 2008. P. 1–10. URL: <https://dx.doi.org/10.4108/ICST.SIMUTOOLS2008.3027>
23. Baidya S., Shaikh Z., Levorato M. FlyNetSim: An Open Source Synchronized UAV Network Simulator Based on ns-3 and Ardupilot. Proc. of 21st ACM Int. Conf. on Modeling, Analysis and Simulation of Wireless and Mobile Systems. 2018. P. 37–44. URL: <https://doi.org/10.1145/3242102.3242118>
24. Kudelski M., Gambardella L., Di Caro G. RoboNetSim: An Integrated Framework for Multi-Robot and Network Simulation. Robotics and Autonomous Systems. 2013. Vol. 61, no. 5. P. 483–496. URL: <https://doi.org/10.1016/j.robot.2013.01.003>
25. Annaz F. UAV Testbed Training Platform Development Using Panda3D. Industrial Robot – Int. J. 2015. Vol. 42, no. 5. P. 450–456. URL: <https://doi.org/10.1108/IR-01-2015-0017>
26. Robot Operating System 2: Design, Architecture, and Uses in the Wild / S. Macenski et al. Science Robotics. 2022. Vol. 7, no. 66. P. eabm6074(1–8). URL: <https://doi.org/10.1126/scirobotics.abm6074>

Received (Надійшла) 12.06.2025

Accepted for publication (Прийнята до друку) 27.08.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Остапенко Леонід – аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна;

Ostapenko Leonid – PhD Student at the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine;

e-mail: l.ostapenko@student.csn.khai.edu; ORCID Author ID: <https://orcid.org/0009-0006-1590-2500>.

Харченко Вячеслав Сергійович – доктор технічних наук, професор, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна;

Kharchenko Vyacheslav – Doctor of Sciences (Engineering), Professor, Head at the Department of Computer Systems, Networks, and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine;

e-mail: v.kharchenko@csn.khai.edu; ORCID Author ID: <https://orcid.org/0000-0001-5352-077X>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=22034616000>.

System for simulation of overcoming obstacles and organizing communications in hazardous environments: structure and experimental evaluation

Leonid Ostapenko, Vyacheslav Kharchenko

Abstract. The paper presents a comprehensive simulation system for overcoming obstacles and organizing communications in hazardous environments using UAV swarms. The proposed models of environment, obstacles, dynamic influences, and UAVs enable the reproduction of scenarios in destroyed or hard-to-reach indoor areas, considering static and dynamic objects as well as cyber-physical impacts. The simulator architecture is implemented in Python with the Panda3D engine and integrated with data collection and analysis tools (InfluxDB, Grafana, Docker), providing flexible configuration of parameters and reproduction of diverse scenarios. The paper presents experimental results demonstrating the efficiency of routing algorithms (A*, Greedy Best-First, etc.) and swarm coordination for deploying a Li-Fi-based communication chain. It is shown that the system serves as a valuable research and training tool for testing algorithms, analyzing swarm reliability, evaluating energy efficiency, and resilience to cyber impacts. Future development perspectives include integration with ROS, extension of the sensor library, and modeling of network-level communication protocols.

Keywords: simulation, unmanned aerial vehicles, UAV swarm deployment, hazardous environment, routing, paths, obstacle avoidance, communications, Li-Fi, Panda3D, cyber-physical impacts.