Проблематика організації зв'язку та управління роями безпілотних летальних апаратів (дронів)

Сергій Тараповський
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: tarapovskyi@gmail.com
ORCID: 0009-0004-4951-6056

Михайло Антонішин
науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: antonishin.mihail@gmail.com
ORCID: 0000-0002-2665-0066

Олексій Грамак
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: Hramakoleksij@gmail.com
ORCID: 0009-0008-5603-9779

Роман Войцеховський
ад'юнкт кафедри управління військами інституту державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Олег Тарасов
кандидат військових наук, доцент
доцент кафедри військової підготовки
Національний авіаційний університет
03058, проспект Любомира Гузара, 1, Київ, Україна
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

Анотація. Стаття досліджує важливі аспекти організації зв'язку та управління роями безпілотних летальних апаратів (дронів). Автори розглядають проблеми, пов'язані з вирішенням завдань по забезпеченню безперебійного зв'язку в ході бойового застосування дронів, координації їх дій при виконанні завдань в режимі реального часу. В статті аналізуються різні підходи до вирішення цих проблем, а також надаються рекомендації щодо покращення ефективності управління роями дронів. Досвід використання безпілотних літальних апаратів під час повномасштабного вторгнення росії в Україну показав, що постійно виникає потреба у впровадженні нових підходів до застосування дронів, в тому числі використання роїв, які дозволять значно збільшити ефективність нанесення вогневого ураження противнику. І саме для роїв дронів критично важлива координація та злагодженість в процесі їх застосування. В залежності від способів застосування роїв дронів в системі управління розрізняють три основні підходи до керування ними: одиночне машинне управління, централізоване управління та розподілене управління. Для забезпечення

безперервного управління роями дронів необхідно забезпечити стійкість та захищеність каналів управління роями дронів. Це досягається шляхом використання різних протоколів передачі даних, стандартів каналів зв'язку та здійснення шифрування даних.

Ключові слова: БпЛА, дрони, безпілотні системи, системи зв'язку, системи управління, безпілотні комплекси, стандарти управління, SUAV, LoRa, LoRaWAN, стандарт IEEE 802.11s, модуль SUCOM.

Вступ (Introduction)

"Ройова війна" – це спосіб використання безпілотних літальних апаратів (Далі – дронів) у бойових діях в складі організованих груп (роїв) дронів за єдиним замислом для досягнення загальної мети. Існують різні підходи щодо організації управління роями дронів. Дрони можуть застосовуватися окремо під різним керівництвом, керуватися з одного центрального пункту або об'єднуватися в мережу для автономної роботи. У матеріалах [1-3] розглядають актуальне питання, пов'язане зі створенням та застосуванням роїв дронів військового призначення.

Світ дедалі більше переходить від поодинокого використання дронів до їх організації в керовані групи масового застосування – рої дронів – мобільних автономних безпілотних апаратів (повітряних, наземних, підводних чи надводних), запрограмованих на виконання відповідних завдань. Сучасний стан створення та перспективи використання роїв дронів, зокрема військового призначення, в провідних країнах світу свідчить, що з розвитком штучного інтелекту, складних систем озброєння та новітніх матеріалів рої дронів можуть перейти на етап домінування на полі бою протягом найближчих 10-15 років. Прикладом застосування дронів з одиночним машинним управлінням є рейд хуситів на саудівський нафтопереробний завод у березні 2021 року за допомогою 12 дронів та централізованого управління є організація сирійськими опозиційними силами у січні 2018 року атаки 13 дронами на авіабазу Гемінме та базу матеріально-технічного забезпечення Тартус російської армії в Сирії.

Тривалий час та впритул дослідженнями застосування роїв дронів займається WestPoint. У їхніх матеріалах [4] розглядається потенціал технології дронових роїв – здатності дронів приймати автономні рішення на основі спільної інформації. Ця технологія може революціонізувати динаміку конфліктів, зокрема в області забезпечення національної безпеки. Рої дронів можуть використовуватися для проведення пошукових (розвідувальних) дій, виявлення та знищення ворожих ракет в ході виконання завдань протиповітряної оборони держави та протиповітряного прикриття дій військ (сил) в операціях (бойових діях), а також може застосовуватись, як новий вид засобів ведення воєнних дій в складі сил оборонни. Для розкриття повного потенціалу дронових роїв необхідно розвивати можливості в чотирьох ключових напрямках: розмір рою, його різноманітність, індивідуальна настроюваність та забезпечення стійкості роботи каналів обміну даними. У публікації порталу DefenceBribge [5] зазначають, що в рої мається спроможність автономно координувати дії великих груп дронів, використовуючи їхні штучні інтелект та здатність сприймати навколишнє середовище. Вони працюють разом, виконуючи спільні завдання, і реагують швидко та точно на зміни у своєму оточенні. Ця технологія може знайти застосування як у військових, так і цивільних сферах, включаючи боротьбу з лісовими пожежами та пошук зниклих осіб.

Матеріали та методи (Materials and Methods)

В матеріалах статті [6] пропонується метод обслуговування роїв дронів, який дозволить досягти високої ефективності виконання визначених завдань. Заснований на характеристиках роїв дронів, таких як низька вартість, висока цілісність та доволі частий обмін інформацією, він поєднує метод оцінки надійності багаторівневої складної мережі з методом групового обслуговування. Враховуючи вартість групування обслуговування, механізми відмов дронів у різних режимах та вплив обслуговування на систему, автори оптимізують стратегію

групування обслуговування, використовуючи багатоцільове планування вартості та надійності системи. Порівняно з існуючими методами обслуговування “вчасно” (just in time), цей метод може значно знизити загальну вартість обслуговування роїв, забезпечуючи високу стійкість місій роїв. Результати підтверджують його доцільність та ефективність. Для ілюстрації методу використано універсальний сценарій місії роїв дронів. Схематично це ілюструється в трьох-рівневій моделі, яка проілюстрована на рисунку 1.

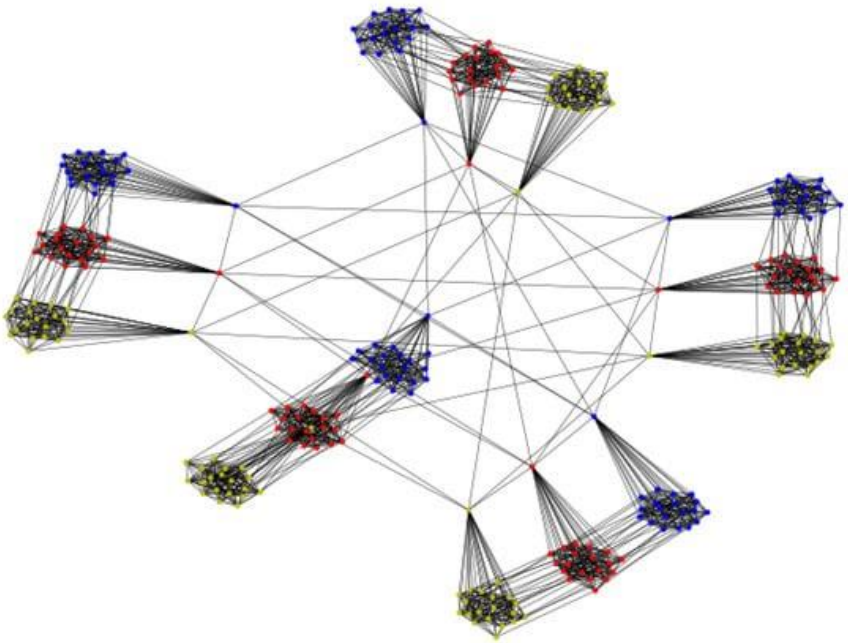


Рисунок 1. Трьох-рівнева комплексна мережева модель.

Ще одним розглянутим методом у [7] є запропонована схема крос-доменної аутентифікації на основі блокчейн (BCDAIoD). Цей метод використовує ланцюг з багато ланцюжковою архітектурою, що дозволяє ефективно здійснювати запити та оновлювати різні типи даних. В процесі крос-доменної аутентифікації дрони можуть формувати групи для зменшення навантаження на вузли управління доменами. Крім того, BCDAIoD використовує механізм обміну даними між доменами для планування бойової роботи дронів наперед, що в подальшому підвищує ефективність їх застосування. Результати експериментів показали, що час крос-доменної аутентифікації та обчислювальні витрати BCDAIoD значно менші, ніж при існуючих методах обслуговування великої кількості дронів, зображено на рисунку 2.

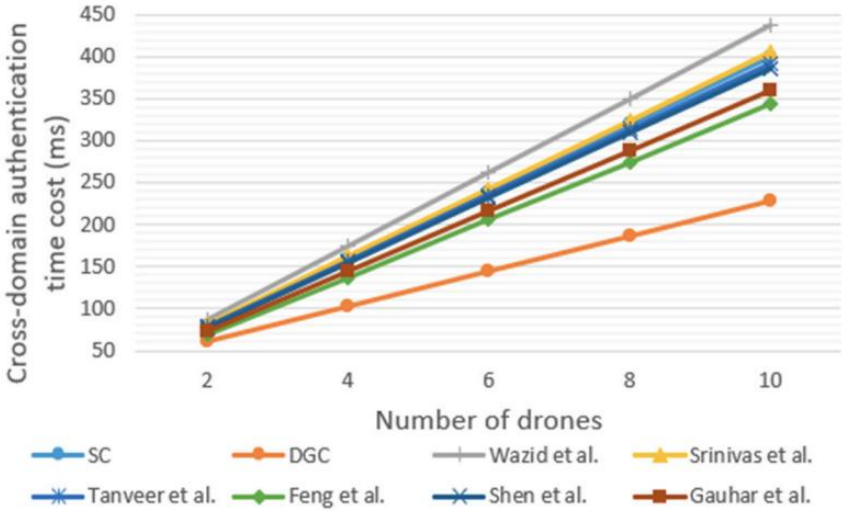


Рисунок 2. Час крос-доменної аутентифікації та обчислювальні витрати.

Автори статті [8] пропонують ефективний метод планування маршруту для кількох дронів, які мають виконувати завдання в різних регіонах. Метод розбиває процес розв'язання на два етапи. По-перше, враховуючи швидкість польоту та ширину області сканування, автори запропонували нову схему розподілу регіонів на основі мінімального споживання ресурсів. За допомогою цієї схеми визначається розподіл завдань та попереднє планування маршрутів дронів. По-друге, враховуючи траєкторії руху дронів, оптимізуються на основі динамічного алгоритму для зменшення часу переходу між регіонами. Числові експерименти підтвердили ефективність запропонованого методу: час виконання завдань для однорідних та різнорідних (різнотипних) дронів зменшився відповідно на 5,1% та 3% порівняно з використанням вдосконаленого алгоритму.

У [9] пропонують ефективну модель оцінки загроз та ієрархічну схему призначення завдань для роїв дронів у великомасштабних сценаріях групового перехоплення цілей (об'єктів). Ця робота вирішує проблему призначення завдань для мульти-дронів в умовах великомасштабних групових перехоплень. Модель враховує динамічні обмеження, специфічні для дронів, та точно описує загальну ефективність спільного перехоплення кількома дронами. Ієрархічна схема використовує алгоритм мережевого потоку для оптимізації конфігурації роїв дронів та/або визначення пріоритетності цілей. Результати симуляцій застосування роїв дронів підтверджують доцільність та ефективність запропонованої ієрархічної схеми призначення завдань для роїв дронів.

В [11] пропонують гібридну архітектуру комунікації для роїв безпілотних літальних апаратів (дронів), яка використовує гетерогенні радіомережеві протоколи на основі комунікаційних протоколів стандарту передачі даних IEEE 802.11s. таких як: LoRa та LoRaWAN. Стаття обговорює переваги, обмеження, можливу реалізацію у відповідних сценаріях використання.

Таблиця 1. Протоколи обміну даними та частоти, на яких вони працюють

Протоколи	Частоти
LoRa та LoRaWAN	433 МГц, 868 МГц та 915 МГц
SUCOM	LTE (900 МГц, 1800 МГц та 2600 МГц)

В матеріалах [12] розглядають інтелектуальну кластерну систему комунікації для роїв дронів у місіях пошуку та рятування. Протокол ICBM-UAV використовує кластеризацію для збереження заряду батарей дронів та оптимізації обчислень. Ця робота виявила переваги ICBM-UAV над існуючими протоколами, такими як AODV, OSLR щодо пропускної здатності каналів обміну даними, а також протоколу PDR щодо зони стійкого прийому сигналу, враховуючи наявність перешкод.

Таблиця 2. Протоколи управління

№	Назва протоколу	Короткий опис	Недоліки
1	ICBM-UAV	ICBM-UAV дозволяє військовим ефективно використовувати дрони для розвідки, моніторингу та оборони.	ICBM-UAV використовується лише на висотних дронах, які можуть працювати на висотах понад 9000 метрів.
2	SBUS	SBUS є серійним протоколом, який передає сигнали від радіопередавача до приймача. Він дозволяє передавати багато каналів інформації через один канал.	1. Моноканальний: SBUS передає всі канали через один серійний канал, що може призвести до збоїв у випадку перешкод або інтерференції. 2. Складність налаштування: Для використання SBUS потрібно налаштовувати перетворювачі сигналу, що може бути складним для початківців.

Продовження таблиці 2.

2	SBUS	SBUS є серійним протоколом, який передає сигнали від радіопередавача до приймача. Він дозволяє передавати багато каналів інформації через один канал.	3. Обмежена кількість каналів: Хоча SBUS передає багато каналів, максимальна кількість обмежена до 16.
3	DSMX	Ці протоколи використовуються в радіосистемах Spektrum. DSMX може автоматично перемикатися на новий частотний канал у разі втрати сигналу.	1. DSMX має 23 канали, що дозволяє йому перемикатися між ними. Це забезпечує менше шансів на інтерференцію. 2. Динамічний режим частоти: DSMX може автоматично перемикатися між частотами, що допомагає уникнути перешкод.
4	DSM2		1. Кількість каналів: DSM2 має лише 2 канали, що обмежує можливості управління. 2. Сприйнятливість до перешкод: Через обмежену кількість каналів DSM2 може страждати від інтерференції з іншими пристроями.
5	FPort	FPort – це комбінований протокол, який об'єднує SBUS і SmartPort. Він дозволяє передавати сигнали і телеметрію одночасно.	FPort є протоколом який на даний момент все ще виходить з піна SmartPort (S.Port) на приймачі, і цей пін зазвичай інвертується.
6	PPM	PPM (Pulse Position Modulation) і PWM (Pulse Width Modulation) - це аналогові протоколи, які використовуються для передачі сигналів від радіопередавача до приймача.	1. Чутливість до шуму: якщо імпульси зміщуються, може виникнути спотворення сигналу. 2. Обмежена точність: положення імпульсу вимірюється відносно опорної точки, що може обмежити точність передачі.
7	PWM		1. Втрати потужності: вимикання та вмикання може призвести до втрати потужності. 2. Електромагнітний шум: швидке переключення може створити електромагнітний шум.
8	MAVLINK	MAVLINK - це відкритий протокол для комунікації між дронами та земною станцією. Він використовується для передачі телеметрії, команд і стану дрона.	1. Втрати потужності: вимикання та вмикання джерела живлення може призвести до втрати потужності. 2. Електромагнітний шум: Швидке переключення може створити електромагнітний шум.
9	SmartPort	Протокол SmartPort дозволяє передавати телеметричні дані між дроном і пультом дистанційного керування, забезпечуючи важливою інформацією про стан дрона.	1. Безпека: Якщо протокол не забезпечує належний рівень захисту даних, це може призвести до витоку конфіденційної інформації. 2. Сумісність: Якщо SmartPortal не підтримує стандартні протоколи або не сумісний з іншими системами, це може обмежити його використання. 3. Продуктивність: Якщо протокол має низьку швидкість передачі даних або велику затримку, це може вплинути на ефективність системи.

Канали передачі даних роїв дронів поділяються на два типи:

- Канали стану (State Channels), що передають інформацію про стан дронів таку як координати, швидкість, висота, заряд батареї та інші параметри. Це допомагає уникнути зіткнень та координувати дії дронів.

• Канали завдань (Task Channels), що передають дані про завдання, які дрони виконують. Наприклад, якщо один дрон знайшов об’єкт для доставки, він може сповістити інші дрони про це, щоб вони не витрачали час на пошук.

Передача інформації в обох типах каналів зв’язку здійснюється за допомогою бездротового зв’язку. Умови протидії високої інтенсивності можуть призвести до погіршення або навіть втрати зв’язку між пунктом управління та “роєм дронів”.

Механізми шифрування обміну даними у каналах зв’язку є важливою складовою для забезпечення його конфіденційності та захисту. Використання криптографічних методів, таких як шифрування та розшифрування, допомагає забезпечити безпеку обміну інформацією у рої дронів.

Найчастіше використовуються наступні методи шифрування:

- Ієрархічне шифрування на основі ідентичності. Цей метод використовує ієрархічні ідентифікатори для шифрування повідомлень. Кожен дрон має свій ідентифікатор, і за допомогою цього механізму вони можуть обмінюватися зашифрованими повідомленнями.

- Псевдоніми. Для анонімного обміну даними можна використовувати псевдоніми. Кожен дрон може використовувати псевдонім для шифрування та розшифрування повідомлень, не розкриваючи свою справжню ідентичність.

- Криптографічні протоколи. Використання криптографічних протоколів, таких як публічний ключ, хеш-функції та симетричне шифрування, допомагає забезпечити конфіденційність та автентифікацію даних. [13-17]

Результати (Results)

Базуючись на матеріалах вищенаведених досліджень, пропонується застосовувати три основні способи управління роями дронів – одиночне машинне управління, централізоване управління та розподілене управління, схематично проілюстроване на рисунку 5.

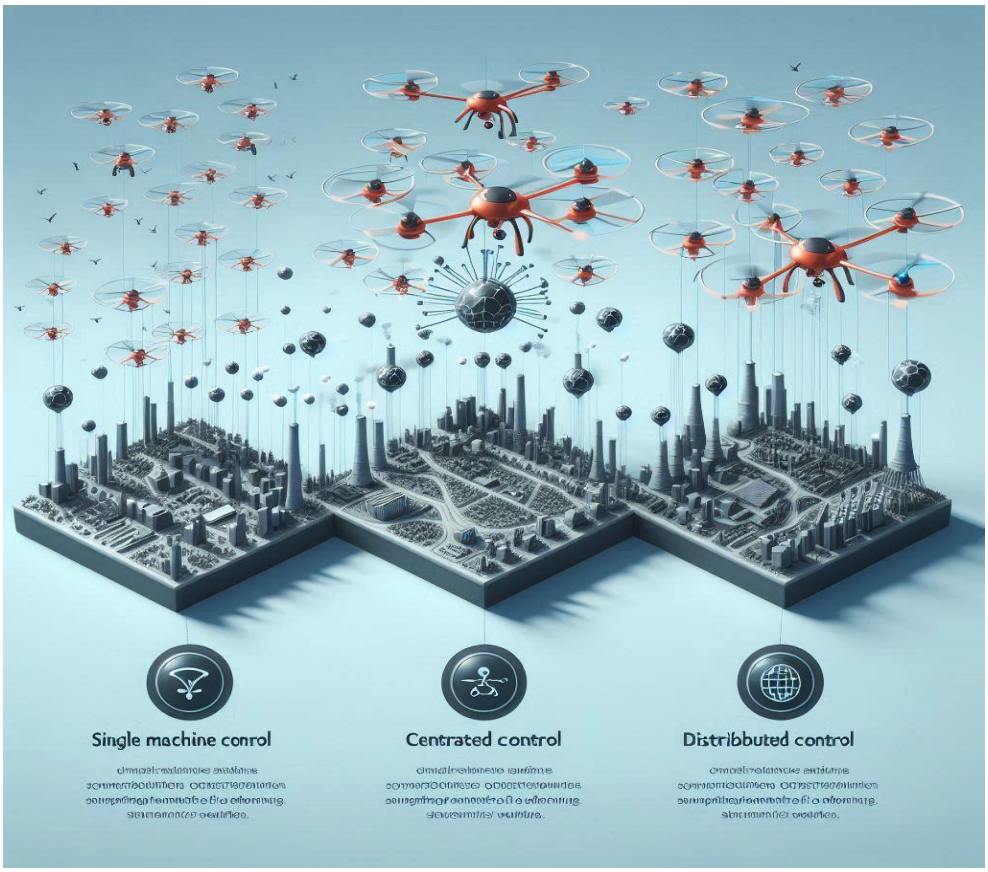


Рисунок 5. Способи управління роями дронів.

Одиночне машинне управління – це дистанційне керування сукупністю дронів з відокремлених пунктів управління, при цьому вони не можуть обмінюватися даними один з одним.

Централізоване управління – це управління роями дронів, яке передбачає передачу команди групам дронів в єдиному порядку. Розподіл обов'язків та взаємодія між дронами, а також реагування на обстановку на полі бою здійснюються через надсилання інструкцій з пункту управління. Дрони поєднанні з пунктом управління однією мережею, проте вони не взаємопов'язані між собою. Цей метод є простим у реалізації, але ступінь інтелектуальності в ході автономної взаємодії UAV. Як тільки канал передачі даних між роєм та пунктом управління порушується або пункт управління руйнується, рій дронів у повітрі виходить з-під контролю.

Розподілене управління – це управління роями дронів, яке передбачає об'єднання в загальну мережу через канали передачі даних і використання кластерного підходу для обміну інформацією та взаємодії між дронами у складі "рою". Управління відбувається без прямого втручання, це надає можливість рою дронів досягти автономних бойових спроможностей. Цей вид децентралізованої мережі, яка не потребує точок доступу, відзначається високою надійністю і може продовжувати працювати незалежно від наземного зв'язку. Навіть в разі втрати частини БПЛА мережа може реконструюватися, не впливаючи на ефективність операцій рою.

В системі зв'язку для управління роями дронів використовуються протоколи стандарту передачі даних IEEE 802.11s:

- LoRa – це бездротова технологія дальнього радіусу дії, яка дозволяє передавати дані на великі відстані (до 10 км) з використанням широкосмугового модульованого радіозв'язку.
- LoRaWAN – це мережевий протокол, побудований на основі технології LoRa, який дозволяє малопотужним пристроям обмінюватись даними на великій відстані. Топологія "зірка-зірка" використовується для взаємодії кінцевих пристроїв із шлюзами.
- Для збільшення радіусу дії рою дронів може використовуватись додатковий модуль на протоколі SUCOM, який встановлюється на будь який дрон та забезпечує дальність управління дронами до 40 км.

Обговорення (Discussions)

З розвитком технологій локалізації, навігації та комунікації рої дронів будуть працювати автономно, розподіляючи обов'язки та координуючи власні дії. Важливо вирішити відкриті проблеми, такі як контроль за автономним управлінням роями дронів.

Для стійкого функціонування системи управління роями дронів виникає потреба у протидії радіоелектронній боротьбі (РЕБ) з боку противника. Можуть використовуватися декілька методів для протидії радіоелектронній боротьбі (РЕБ), щоб зберегти функціональність та безпеку управління роями дронів.

Розглянемо деякі з ключових методів та технологій протидії РЕБ.

1. Використання захищених каналів зв'язку, в процесі якого відбувається шифрування з використанням надійних алгоритмів шифрування, таких як AES-256 або ChaCha20, для захисту даних та команд управління.

2. Частотне маніпулювання для захисту від перехоплення та придушення сигналів із застосування методів, таких як Frequency Hopping Spread Spectrum (FHSS) та Direct Sequence Spread Spectrum (DSSS). Ці методи забезпечують постійну зміну частот передачі, що ускладнює атаки на канал зв'язку.

3. Надмірність та відновлення зв'язку за рахунок багаторівневого дублювання каналів, яке здійснюється шляхом використання декількох незалежних каналів зв'язку (наприклад, Wi-Fi, мобільні мережі, спеціалізовані радіоканали) для резервного обміну інформацією на випадок придушення основного каналу.

4. Автономні дії завдяки наділення дронів алгоритмами автономної поведінки, які дозволяють їм виконувати завдання або безпечно повертатися на базу у випадку втрати зв'язку.

5. Адаптивні алгоритми та штучний інтелект.

Адаптивні алгоритми маршрутизації - застосування алгоритмів, які можуть динамічно змінювати маршрути та способи зв'язку в залежності від поточних умов та виявлення перешкод.

Штучний інтелект та машинне навчання - використання штучного інтелекту для аналізу та прогнозування атак РЕБ, а також для адаптації до нових видів загроз.

6. Захист від GPS-перешкод:

Багатоканальні приймачі - використання приймачів, які можуть працювати з декількома системами супутникової навігації (GPS, GLONASS, Galileo, BeiDou), щоб зменшити залежність від одного джерела.

Інтеграція з інерційними навігаційними системами (INS) - використання INS для підтримки точності навігації в умовах придушення GPS-сигналів.

7. Детектування та локалізація перешкод.

Датчики та системи моніторингу - впровадження датчиків, які можуть виявляти та аналізувати радіоелектронні перешкоди.

Локалізація джерел перешкод - використання методів тріангуляції та аналізу спектра для визначення місцезнаходження джерел перешкод та прийняття заходів щодо їх обходу або придушення.

8. Координація та взаємодія в рої.

Взаємне узгодження та релейна зв'язка - розробка протоколів для обміну інформацією між дронами в рої, що дозволяє підтримувати зв'язок навіть при порушенні прямого зв'язку з оператором.

Динамічне розподілення задач - можливість перерозподілу задач та ролей в рої в режимі реального часу для адаптації до мінливих умов та загроз.

Важливо зазначити, що жоден з цих методів не є універсальним і найефективніший підхід буде залежати від конкретних умов застосування роїв дронів та загроз, які потенційно можуть виникати в бойовому просторі.

Для досягнення максимальної стійкості до РЕБ рекомендується використовувати комбінацію різних методів.

Висновок (Conclusion)

Хід ведення війни росії проти України, а також досвід інших військових конфліктів сучасності, чітко показує постійно зростаючу роль застосування безпілотних літальних апаратів для досягнення результатів в ході ведення операцій (бойових дій). При цьому очевидним є той факт, що форми та методи їх застосування потребують постійного удосконалення та розвитку. І застосування роїв дронів в реаліях сучасної війни є одним і пріоритетних напрямків розвитку використання безпілотних бойових систем на полі бою. При цьому особливої уваги потребує досконаліть системи організації зв’язку та управління роями безпілотних літальних апаратів (дронів), яка забезпечить найвищий рівень ефективності їх застосування. Розглянуті методи та технології забезпечення зв’язку та обміну даними дозволять організувати стійке та безперебійне управління роями безпілотних літальних апаратів (дронами).

Рекомендації (Recommendations)

Для сталого застосування роїв безпілотних літальних апаратів (дронів) у операціях (бойових діях) Сил оборони потребує вирішення завдань по оптимізації системи управління роями відповідно до умов застосування, забезпеченню стійкої протидії роботі систем радіоелектронної боротьби противника та функціонування у будь-яких погодних умовах. Для досягнення цієї мети необхідно розробити та запровадити алгоритми побудови конфігурацій роїв дронів відповідно до виникаючих завдань, створити систему зв’язку управління роями дронів з впрвадженням сучасних технологій із застосуванням штучного інтелекту, які дозволять в тому числі мінімізувати вплив РЕБ противника на безпілотні літальні апарати.

Використані джерела (References)

1. Gorbulin, V. P., & Mosov, S. P. (2024). Roji droniv – kul'minatsiya dronizatsiyi voien. *Visnik Natsional Noi Academii Nauk Ukrai Ni, (3),* 3–11. https://doi.org/10.15407/visn2024.03.003
2. Cabinet of Ministers of Ukraine. (2024, January 10). *"Army of Drones" year: Mass production of drones in Ukraine, strike UAV companies, and operator training—Key achievements of the project*. https://www.kmu.gov.ua/news/armii-droniv-rik-masove-vyrobnytstvo-droniv-v-ukraini-udarni-roty-bpla-navchannia-operatoriv-droniv-holovni-dosiahnennia-proektu
3. U.S. Government Accountability Office. (2023). *Uncrewed aircraft systems: FAA should improve its approach to integrating UAS into the national airspace system* (GAO-23-105189). https://www.gao.gov/assets/870/861345.pdf
4. *The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It.* Modern War Institute (westpoint.edu). https://defensebridge.com/article/what-is-a-drone-swarm-an-overview-of-the-technology.html
5. Guo, J., Wang, L., & Wang, X. (2022). A Group Maintenance Method of Drone Swarm Considering System Mission Reliability. *Drones, 6,* 269. https://doi.org/10.3390/drones6100269
6. Qiao, G., Zhuang, Y., Ye, T., & Qiao, Y. (2023). BCDAIoD: An Efficient Blockchain-Based Cross-Domain Authentication Scheme for Internet of Drones. *Drones*, *7*, 302. https://doi.org/10.3390/drones7050302
7. Mehmood, A., Iqbal, Z., Shah, A., Maple, C., & Lloret, J. (2023). An Intelligent Cluster-Based Communication System for Multi-Unmanned Aerial Vehicles for Searching and Rescuing. *Electronics*, *12*, 607. https://doi.org/10.3390/electronics12030607
8. Chen, J., Zhang, R., Zhao, H., Li, J., & He, J. (2023). Path Planning of Multiple Unmanned Aerial Vehicles Covering Multiple Regions Based on Minimum Consumption Ratio. *Aerospace*, *10*, 93. https://doi.org/10.3390/aerospace10020093
9. Wu, X., Zhang, M., Wang, X., Zheng, Y., & Yu, H. (2023). Hierarchical Task Assignment for Multi-UAV System in Large-Scale Group-to-Group Interception Scenarios. *Drones*, *7*, 560. https://doi.org/10.3390/drones7090560
10. Davoli, L., Pagliari, E., & Ferrari, G. (2021). Hybrid LoRa-IEEE 802.11s Opportunistic Mesh Networking for Flexible UAV Swarming. *Drones*, *5*, 26. https://doi.org/10.3390/drones5020026
11. Ganesan, T., Jayarajan, N., Shri, & Varun, B. G. (2024). *Dynamic Control, Architecture, and Communication Protocol for Swarm Unmanned Aerial Vehicles. Computing in Intelligent Transportation Systems.* EAI/Springer Innovations in Communication and Computing. https://doi.org/10.1007/978-3-031-38669-5_3
12. Krasavtsev, B. (2022). *Нові технології військових дронів для оборони України*. Ucluster. https://ucluster.org/blog/2022/06/vijsjkovi-drony-dlja-oborony-ukrainy/
13. Liang, O. (2021). *FPV Protocols Explained (CRSF, SBUS, DSHOT, ACCST, PPM, PWM*. Oscar Liang FPV Drone Tutorials and Reviews. https://oscarliang.com/rc-protocols/
14. Liang, O. (2021). *FPV Protocols Explained. Oscar Liang FPV Drone Tutorials and Reviews.* https://hinaray.com/understanding-the-communication-protocols-and-frequency-bands-used-by-drones/
15. Hopson, M. (2023). *How Does A Drone Communicate With Controller*. https://robots.net/tech/how-does-a-drone-communicate-with-controller/
16. Liang, O. (2021). *FPV Protocols Explained 1. Oscar Liang FPV Drone Tutorials and Reviews*. https://www.dronetrest.com/t/rc-radio-control-protocols-explained-pwm-ppm-pcm-sbus-ibus-dsmx-dsm2/1357