Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.056.59
DOI: https://doi.org/10.30837/2522-9818.2025.2.111

Є. Сопов, Д. Крицький, А. Артьомова, І. Артьомов

МЕТОДИКА ПОБУДОВИ ДОВІРЧОЇ МАРШРУТИЗАЦІЇ В РОЙОВИХ МЕРЕЖАХ БПЛА НА ОСНОВІ АНАЛІЗУ ТРАФІКУ ТА ВИЯВЛЕННЯ АНОМАЛІЙ

Предметом дослідження є процеси забезпечення безпечної маршрутизації та обміну даними між безпілотними літальними апаратами в складі ройових мереж в умовах дії кіберзагроз, зокрема атак типу *Black Hole*. **Мета роботи –** розроблення та моделювання захищеного механізму передачі інформації в ройових мережах БПЛА, що зважає на рівень довіри до вузлів та можливість виявлення шкідливих учасників мережі на основі аналізу їх поведінки. **Дослідження** також спрямовано на розроблення методики захищеної та енергоефективної маршрутизації в ройових мережах безпілотних літальних апаратів на основі блокчейн-технологій і моделей оцінювання довіри. Запропонована методика забезпечує стійкість до кіберзагроз, збереження цілісності інформації та мінімізацію витрат ресурсів. **Завдання,** які передбачено розв'язати в дослідженні: здійснити комплексний аналіз вразливостей традиційних протоколів маршрутизації, що застосовуються в ройових мережах БПЛА (FANET), з метою виявлення потенційних загроз інформаційній безпеці; обґрунтувати доцільність використання механізмів оцінювання довіри (*trust-based mechanisms*) як засобу підвищення надійності та стійкості маршрутизації до внутрішніх атак; реалізувати модель атаки типу *Black Hole* в симуляційному середовищі NS-3 для дослідження її впливу на функціювання ройової мережі; розробити механізм обліку кількості переданих пакетів кожним вузлом як базовий інструмент для побудови системи оцінювання довіри між агентами мережі; здійснити візуалізацію результатів моделювання для забезпечення наочності, подальшого аналізу й порівняння ефективності запропонованих рішень. **Методи,** використані в дослідженні, передбачають моделювання мережі FANET у симуляторі NS-3.36, застосування мобільної моделі *RandomWaypoint*, протоколу маршрутизації AODV, статистичного аналізу показників передачі пакетів вузлами та побудову графічної інтерпретації довірчих метрик. Розроблений код реалізує атаку *Black Hole* внаслідок утручання на рівні *NetDevice* та забезпечує логування всіх переданих пакетів у вигляді CSV-файлу для подальшого аналізу. У дослідженні використано комплекс методів, що поєднують інструменти симуляційного моделювання, аналітичного аналізу та візуалізації. Основу експериментального середовища становить моделювання ройової мережі БПЛА (FANET) у симуляторі NS-3.36 із застосуванням мобільної моделі *RandomWaypoint*, яка відтворює характерну поведінку вузлів у динамічному середовищі. Для організації маршрутизації використано протокол *Ad hoc On-Demand Distance Vector* (AODV), що дає змогу дослідити вплив внутрішніх атак на процес побудови маршрутів у мережі. Модель атаки *Black Hole* реалізовано способом втручання у процес обміну маршрутною інформацією, що допомагає симулювати шкідливу поведінку вузлів. **Результати.** Дослідження довело ефективність запропонованого підходу до встановлення зловмисників у ройовій мережі. Метрики виявили нетипову активність вузла, який атакує, відсутність передачі пакетів, що відрізняється від поведінки звичайних вузлів. Це сприяє оперативному виявленню загроз і вилученню зловмисника з маршрутизації. Графічна візуалізація чітко демонструє розподіл активності між вузлами, що спрощує інтерпретацію результатів без потреби в глибокому аналізі логів. **Висновки.** Запропонований *trust*-механізм у поєднанні з аналізом активності вузлів ефективно захищає FANET-мережі від атак типу *Black Hole*. Перспективним є розширення моделі внаслідок упровадження більш складних методів оцінювання довіри, таких як багатофакторний аналіз, блокчейн чи машинне навчання. Також доцільно розробити адаптивні алгоритми маршрутизації з автоматичним вимкненням або ізоляцією підозрілих вузлів.

Ключові слова: ройова мережа БПЛА; FANET; AODV; атака *Black Hole*; довіра (*trust*); симуляція в NS-3; безпека маршрутизації; захист від атак; *NetDevice*; виявлення зловмисників.

Вступ

Швидкий розвиток технологій мобільного зв'язку п'ятого покоління (5G New Radio, 5G NR) відкриває нові можливості для застосування в різних сферах, зокрема в промисловому виробництві, телемедицині, хмарній освіті та автономних системах управління безпілотними літальними апаратами [1]. Завдяки таким властивостя, як надвисока пропускна здатність, мінімальні затримки передачі та висока щільність з'єднань, 5G NR створює сприятливі умови для широкомасштабного розгортання ройових систем БПЛА. Це забезпечує ефективне виконання складних місій з багатьма завданнями в динамічному середовищі з високим рівнем автономності та кооперації між апаратами. Комплексний підхід до управління групами роботів [16] наголошує на значенні адаптивних стратегій для динамічних середовищ.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Основою взаємодії в таких системах є ройові мережі БПЛА (FANET – *Flying Ad-Hoc Networks*), що функціюють як самоконфігуровані бездротові мережі без централізованої інфраструктури. Водночас відкритий характер цих мереж, висока мобільність вузлів і часта зміна топології створюють сприятливі умови для реалізації низки кіберзагроз. Найбільш поширеними серед них є атаки типу *Black Hole, Replay, Sybil* та *Man-in-the-Middle* (MITM), що дають змогу зловмисникам перехоплювати, спотворювати або повністю блокувати передачу інформації, що критично впливає на стабільність і безпечність функціювання системи загалом.

Попри значну кількість наявних рішень у сфері маршрутизації, зокрема протоколів AODV і GPSR, а також впровадження стандартних криптографічних інструментів на основі DTLS, наявні підходи демонструють обмежену ефективність у контексті високої мобільності, змінної топології та обмежених обчислювальних ресурсів, притаманних ройовим мережам БПЛА. Застосування традиційного шифрування та централізованих механізмів виявляється недостатнім для забезпечення надійного захисту маршрутної інформації в умовах децентралізованої динамічної мережі.

У зв'язку з цим актуальним постає завдання розроблення нового підходу до захищеної маршрутизації, який поєднує механізм оцінювання довіри до мережевих вузлів, використання легкого блокчейну для збереження маршрутної інформації та консенсусного алгоритму на основі *Proof-of-Traffic* (PoT). Така архітектура має забезпечити розподілений характер прийняття рішень, знизити енергоспоживання внаслідок пасивної синхронізації блоків і водночас зберігати стійкість до типових атак, що спостерігаються у FANET. Важливим також є увага до вимог масштабованості, енергоефективності та автономності, які є ключовими для практичного застосування систем такого класу.

Аналіз останніх досліджень і публікацій

Проблематика захищеної маршрутизації в ройових мережах безпілотних літальних апаратів активно розробляється в сучасній науковій літературі. Ванг та інші [2] запропонували алгоритм маршрутизації, що базується на легкому блокчейні з використанням консенсусного механізму *Proof-of-Traffic* (PoT). Такий підхід дає змогу зменшити навантаження на мережу та знизити енергоспоживання, що є критичним для обмежених за ресурсами мультиагентних систем.

У дослідженні Альшаммарі та інших [3] розглянуто підхід до побудови безпечної *ad-hoc*-мережі БПЛА з використанням блокчейн-технологій, який не знижує пропускну здатність системи. Запропонована мережева архітектура забезпечує підвищений рівень захисту інформації та стійкість до атак. Ґупта Р. та інші [4] зосередили увагу на створенні адаптивної мережевої архітектури з використанням унікальних ідентифікаторів, механізмів участі в консенсусі та контролю безпеки маршрутів. Такий підхід є особливо актуальним для реалізації динамічних ройових систем, що функціюють у змінному середовищі.

У праці [10] запропоновано архітектуру безпечного обслуговування мережі БПЛА, що поєднує методи глибокого навчання з блокчейн-технологією. Досягнуті результати демонструють високу ефективність протидії кіберзагрозам, навіть в умовах обмежених обчислювальних можливостей.

К. Мершад [11] розробив протокол PROACT, який базується на паралельній генерації блоків кількома вузлами на основі моделі накопиченої довіри. Такий механізм сприяє зниженню затримок і покращенню масштабованості системи.

Останнє з розглянутих досліджень – система BETA-UAV [12], яка забезпечує автентифікацію вузлів у ройових мережах із використанням смартконтрактів. Система гарантує актуальність сесій зв'язку та захищає від атак типу *replay*, *spoofing* та *impersonation.* Її реалізація на платформі *Ethereum* підтвердила високу ефективність і низьке споживання ресурсів.

Розглянуті дослідження створюють наукове підґрунтя для формування комплексного підходу, що інтегрує блокчейн-технології, моделі довіри та енергоефективні стратегії маршрутизації в ройових мережах БПЛА.

Визначення не розв'язаних раніше частин загальної проблеми. Мета роботи й завдання

Ройові мережі безпілотних літальних апаратів розвиваються паралельно зі зростанням складності завдань, які ці системи покликані виконувати у сферах моніторингу, безпеки, логістики та надзвичайного реагування. Тоді як мобільність, автономність і самоорганізація забезпечують таким

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32) ISSN 2524-2296 (online)

системам унікальні переваги, саме ці характеристики викликають значні труднощі для підтримки надійного та безпечного обміну інформацією всередині рою.

У реальних умовах ройові мережі БПЛА функціюють у середовищі з високою динамікою топології, нестабільними каналами зв'язку та обмеженим енергозабезпеченням. Це робить їх особливо вразливими до атак з боку внутрішніх або зовнішніх суб'єктів, здатних впливати на процес маршрутизації, викривляти дані, порушувати логіку маршруту або навіть повністю блокувати інформаційний обмін. Найбільш поширеними є атаки типу *Black Hole*, MITM (*Man-in-the-Middle*), *Replay* та *Sybil*, спрямовані на порушення цілісності, автентичності або вчасності передачі маршрутної інформації.

Аналіз наявних рішень показує, що поширені протоколи маршрутизації, зокрема AODV та GPSR, не зважають на зміну довіри до вузлів та не мають вбудованих засобів виявлення аномалій у поведінці учасників мережі. Застосування класичних криптографічних схем (наприклад, DTLS) є обмеженим через високу енерговитратність і невідповідність вимогам децентралізованих, масштабованих систем з обмеженими ресурсами. Крім того, відсутність об'єднаної структури, яка б поєднувала довірчі механізми із засобами захисту маршрутизації на структурному рівні, залишає такі системи вразливими до складних багаторівневих атак. Як описано в роботі [10], поєднання блокчейну з глибоким навчанням може значно підвищити ефективність виявлення атак.

З метою узагальнення основних недоліків традиційних підходів та визначення напрямів їх усунення доцільно подати відповідні спостереження в табличній формі (табл. 1).

Таблиця 1. *Недоліки чинних підходів і шляхи вдосконалення*

Ключова проблема	Недоліки наявних рішень	Можливі способи розв'язання
Виявлення зловмисних вузлів у режимі реального часу	Відсутність оцінки довіри у AODV, GPSR	Побудова динамічного довірчого рівня з аналізом поведінки вузлів
Захист від внутрішніх атак (*Black Hole, Sybil*)	DTLS не працює без централізованої інфраструктури	Інтеграція блокчейну з локальною автентифікацією вузлів
Енергоспоживання та масштабованість	PoW/PoS надто ресурсомісткі для малопотужних БПЛА	*Proof-of-Traffic* (PoT) як легкий консенсус для FANET
Неспроможність адаптації до динамічної топології	Статичні таблиці маршрутів швидко застарівають	Пасивна синхронізація маршрутної інформації через блокчейн
Роз'єднаність засобів безпеки та довіри	Системи довіри не інтегровані в логіку маршрутизації	Об'єднана архітектура маршрутизації, довіри та захисту даних

Аналіз показує, що забезпечення надійної маршрутизації в ройових мережах БПЛА потребує комплексного підходу, який передбачає оцінювання довіри, захист маршрутної інформації та адаптивність до змін у структурі мережі. Водночас такий підхід має зважати на обмеження, пов'язані з ресурсами та відсутністю централізованого керування.

Відповідно, **метою дослідження** є розроблення методики захищеної та енергоефективної маршрутизації в ройових мережах безпілотних літальних апаратів на основі блокчейн-технологій і моделей оцінювання довіри, яка забезпечує стійкість до кіберзагроз, збереження цілісності інформації та мінімізацію витрат ресурсів.

Для досягнення поставленої мети передбачається виконати низку **завдань**:

1) здійснити комплексний аналіз вразливостей традиційних протоколів маршрутизації, що застосовуються в ройових мережах БПЛА (FANET), з метою виявлення потенційних загроз інформаційній безпеці;

2) обґрунтувати доцільність використання механізмів оцінювання довіри (*trust-based mechanisms*) як засобу підвищення надійності та стійкості маршрутизації до внутрішніх атак;

3) реалізувати модель атаки типу *Black Hole* в симуляційному середовищі NS-3 для дослідження її впливу на функціювання ройової мережі;

4) розробити механізм обліку кількості переданих пакетів кожним вузлом як базовий інструмент для побудови системи оцінювання довіри між агентами мережі;

5) візуалізувати результати моделювання для забезпечення наочності, подальшого аналізу та порівняння ефективності запропонованих рішень.

Розроблення адаптивної, енергоощадної та стійкої до атак архітектури маршрутизації на основі довіри та блокчейну має потенціал суттєво підвищити надійність ройових систем БПЛА та забезпечити

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

безперервність їх функціювання в агресивному кіберсередовищі.

Матеріали й методи

Для забезпечення захищеної маршрутизації в ройових мережах безпілотних літальних апаратів (UAS) було застосовано комплексний досліджувальний підхід, що охоплює побудову трирівневої архітектури з елементами довірчого аналізу, блокчейн-реєстру та феромонної маршрутизації. Загальний фреймворк реалізовано з огляду на особливості мереж 5G NR, які забезпечують низьку затримку, високу щільність сполучень і покращену пропускну спроможність для високодинамічних сценаріїв повітряної мобільності.

Необхідність упровадження захищеної маршрутизації в ройових мережах UAS зумовлена численними загрозами, зокрема атакою типу *Black Hole*, приклад якої подано на рис. 1.

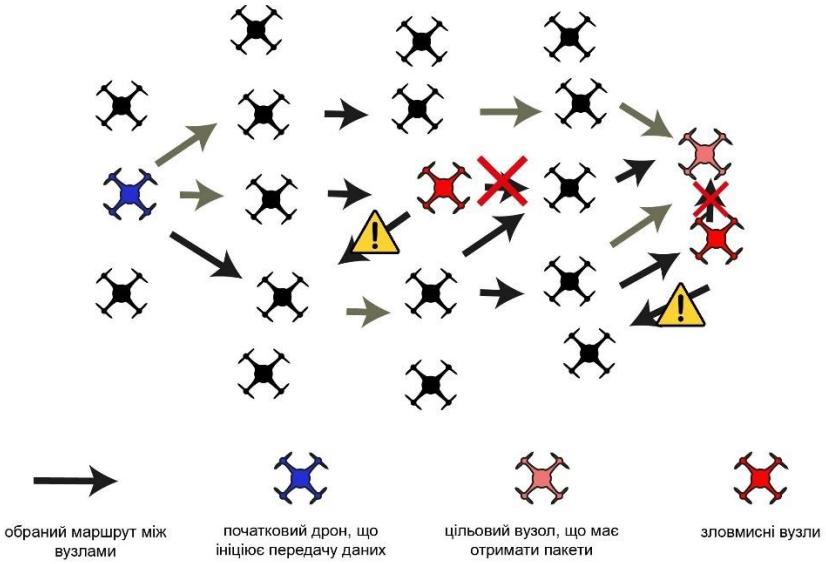

Рис. 1. Сценарій атаки типу *Black Hole* в ройовій мережі БПЛА

На рис. 1 зображено типову ситуацію, що може виникнути в ройовій мережі безпілотних літальних апаратів, коли відбувається внутрішнє проникнення зловмисних вузлів. Вони вбудовуються в маршрут між легітимними дронами – початковим дроном та цільовим вузлом – і перехоплюють або блокують передані пакети даних.

Стрілки ілюструють шляхи маршрутизації, якими рухаються пакети. Зловмисні вузли можуть виконувати атаки типу *Black Hole* (перехоплення з подальшим знищенням пакета), *Man-in-the-Middle* (втручання в процес передачі) або *Replay* (повторне надсилання раніше перехоплених повідомлень).

Через такі атаки окремі ділянки маршруту стають недоступними або небезпечними для передачі, що призводить до порушення комунікації, затримок у доставці та зниження ефективності всієї місії.

Безпечна маршрутизація в ройових мережах БПЛА на основі довіри та PoT-блокчейну. Ройові мережі БПЛА, відомі також як FANET (*Flying Ad-hoc Network*), дають змогу координувати дії рою дронів для виконання складних місій. Водночас така мережа є вразливою до зловмисних вузлів: компрометований дрон може перехоплювати чи модифікувати пакети, відмовлятися їх ретранслювати або впроваджувати атаки "людина посередині". Традиційні підходи захисту (шифрування каналів) не гарантують виявлення зрадницьких вузлів і можуть потребувати значних ресурсів. Необхідна надійна архітектура маршрутизації, що забезпечує відсіювання зловмисників, довірче обрання маршрутів і стійкість до атак з огляду на обмежені обчислювальні та енергетичні ресурси дронів (рис. 2).

Принцип функціювання маршрутизації в рої БПЛА, основаної на поєднанні географічного аналізу, довірчих показників і блокчейн-автентифікації. Початковий дрон ініціює передачу інформації до цільового вузла, прокладаючи маршрут крізь низку проміжних вузлів, кожен з яких оцінюється з погляду надійності та участі в трафіку.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Запропонована архітектура узгоджується з підходами, запропонованими Х. Чжоу [9], де блокчейн використовується для підвищення стійкості мережі рою БПЛА.

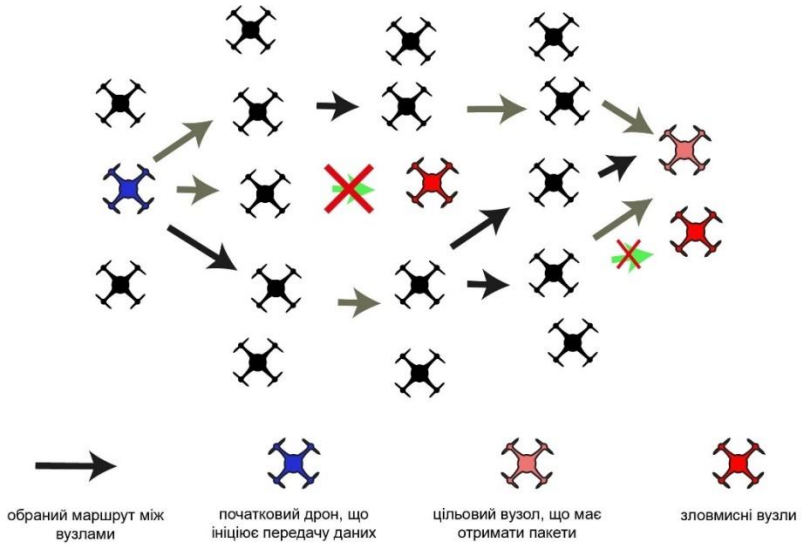

Рис. 2. Архітектура побудови довірчих маршрутів у рої БПЛА

Ключовим елементом механізму є вилучення з маршруту дронів, ідентифікованих як потенційно зловмисних, що можуть ігнорувати, блокувати або модифікувати передані пакети. Таких учасників виявляють за допомогою локальних перевірок автентичності з використанням дайджестів блоків (HN) у розподіленому реєстрі, що зберігається в кожному дроні до старту місії.

Побудова маршруту здійснюється з огляду на напрямок до цільового вузла (вектор $v_{s,d}$), що дає змогу скоротити кількість перевірок та обмежити коло потенційних хопів. Після попереднього фільтрування береться до уваги інтенсивність феромонної активності, яка відтворює ступінь залученості вузла до успішної маршрутизації в минулому. Вузол із найвищим рівнем феромону обирається як пріоритетний для подальшої передачі пакетів, оскільки ймовірність його компрометації зменшується зі зростанням навантаження.

Завдяки такому підходу система забезпечує стабільне функціювання, навіть у присутності зловмисних вузлів, значно зменшує загальне енергоспоживання (внаслідок уникнення широкомовного розсилання запитів) і підвищує загальну стійкість до атак типу *Black Hole*, MITM або *Replay*.

Архітектурна модель ґрунтується на трирівневій структурі, що поєднує:

1) шар довіри (*Trust Layer*) – для оцінювання надійності вузлів на основі поведінкових метрик;

2) PoT-блокчейн-рівень – для розподіленого збереження довірчих даних і автентифікації;

3) маршрутизаційне ядро (*Routing Core*) – для побудови маршрутів з огляду на довіру та підтвердження легітимності вузлів.

Такий підхід дає змогу інтегрувати блокчейн і систему оцінювання довіри для забезпечення стійкої та захищеної маршрутизації в децентралізованих ройових мережах БПЛА. Особливу увагу приділено консенсусному механізму PoT, що є альтернативою енерговитратним алгоритмам на кшталт *Proof-of-Work* і спеціально адаптований до умов обмежених обчислювальних ресурсів у бездротових мережах. Структурну взаємодію між рівнями зображено на рис. 3.

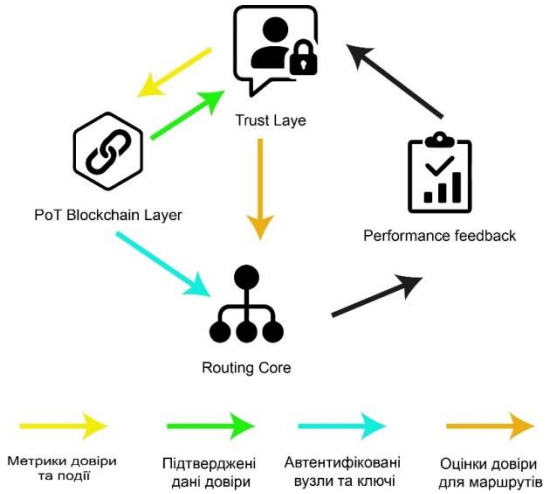

Рис. 3. Трирівнева архітектурна модель системи безпечної маршрутизації для ройової мережі БПЛА

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Кожен дрон в мережі містить модуль управління довірою (верхній рівень), під'єднаний до локального блокчейн-модуля (рівень PoT) і до модуля маршрутизації (нижній рівень). Шар довіри збирає інформацію про поведінку сусідніх БПЛА (успішність передачі пакетів, затримки, відмови тощо) і розраховує метрики довіри. Ці дані можуть передаватися в блокчейн-рівень, що діє як розподілений реєстр авторитетності вузлів. Блокчейн за допомогою консенсусу PoT узгоджує між дронами спільне бачення надійних і зловмисних учасників та зберігає криптографічні "сліди" (гіші) їх поведінки. Маршрутизаційне ядро виконує пошук маршрутів у децентралізованій мережі (на основі протоколу типу AODV), але, зважаючи на додаткову інформацію, воно отримує від шару довіри оцінки надійності потенційних наступних вузлів маршруту й перевіряє за блокчейном автентичність і відсутність компрометації цих вузлів. Теоретичні основи відмовостійкої маршрутизації, розроблені Євдокименком [13], підтверджують важливість динамічної адаптації до змін топології. Як наслідок, обираються тільки безпечні проміжні вузли: дрони з достатнім рівнем довіри та присутні в реєстрі блокчейну як легітимні учасники (не вилучені за зловмисність).

1. Шар довіри (*Trust Layer*)

Шар довіри відповідає за оцінювання надійності кожного вузла та каналу зв'язку на основі досвіду їх поведінки. Кожен БПЛА локально веде таблицю довіри, оновлюючи її після обміну повідомленнями із сусідами. Основний принцип: якщо сусідній вузол успішно доставляє пакети й підтримує стабільний зв'язок, рівень довіри до нього зростає; якщо ж пакети губляться без причин або вузол відмовляється ретранслювати дані, рівень довіри падає. Такий підхід дає змогу виявляти зловмисних чи ненадійних учасників мережі на основі їх поведінкових властивостей.

Для кількісного оцінювання використовується метрика, аналогічна феромону в алгоритмах мурашиної колонії. Після успішної доставки пакета через сусіда n вузол-джерело підсилює мітку довіри (феромон) для цього сусіда на величину, обернено пропорційну затримці доставки або кількості стрибків. Формально приріст довіри $\Delta P_{n,t}$ обчислюється за формулою

$$\Delta P_{n,t} = 1/\ln \ell_{n,t} \qquad (1)$$

де $\ell_{n,t}$ – затримка доставки пакета через вузол n у момент часу t.

Загальне оновлення феромонної мітки довіри до вузла n на момент часу $t+1$ відбувається відповідно до рівняння

$$P_{n,t+1} = (1-\rho) P_{n,t} + \Delta P_{n,t}, \qquad (2)$$

де $\rho \in (0,1)$ – коефіцієнт згасання, що імітує "випаровування" довіри з часом; $P_{n,t}$ – поточне значення довіри до вузла n у момент часу t; $\Delta P_{n,t}$ – приріст довіри на основі нової доставки.

Якщо ж передача через n (сусіда) не вдалася або виявлено факт підміни / пошкодження пакета, рівень довіри до нього зменшується. Ця метрика виконує роль локального рейтингу надійності та з часом згасає без підтвердження, зважаючи на динаміку мережі.

На основі метрик довіри кожен дрон самостійно вирішує, кого вважати підозрілим. Якщо сусід накопичує негативну історію (високу частку невдалих передач), модуль довіри може позначити його як потенційно зловмисний та повідомити про це іншим рівням. Зокрема, коли рівень довіри падає нижче певного порогу, генерується подія про зловмисний вузол, що передається в блокчейн-рівень для колективного внесення цього вузла до "чорного списку" (списку U_m – множини розпізнаних зловмисних БПЛА).

$$T_n < T_{threshold} \Rightarrow u_n \in U_m \qquad (3)$$

де T_n – поточний рівень довіри до вузла u_n; $T_{threshold}$ – встановлений пороговий рівень довіри; U_m – множина вузлів, класифікованих як зловмисні.

Отже, шар довіри є першим рубежем безпеки: він локально фільтрує сумнівних сусідів та ініціює глобальне поширення інформації про них через блокчейн.

Шар довіри тісно інтегрується з блокчейном і маршрутизатором. З одного боку, він постачає блокчейн-рівню інформацію про надійність, наприклад повідомлення про виявленого зловмисника або періодичні узагальнені показники довіри (на рис. 3 цей напрям позначено жовтою стрілкою "Метрики довіри та подій"). З іншого боку, сам отримує від блокчейну підтверджену глобальну інформацію про довіру: наприклад, рішення більшості про вимкнення певного вузла з мережі або про присвоєння йому статусу надійного після успішної автентифікації (на рис. 3 стрілка "Підтверджені дані довіри"). Крім того, маршрутизатор запитує у шару довіри рейтинги сусідів у процесі вибору наступного хопу (стрілка "Оцінки довіри для маршрутів"), а після

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

побудови маршруту маршрутизатор повертає до шару довіри інформацію про успішність чи неуспішність доставки *Performance feedback*. У такий спосіб формується зворотний зв'язок: маршрутизаційне ядро повідомляє, які вузли виправдали довіру або підвели, і *Trust Layer* коригує метрики відповідно.

Шар довіри виконує роль системи локальної репутації для сусідів, що слугує основою для прийняття рішень і на рівні блокчейну (глобальна репутація), і на рівні маршрутизації (вибір безпечних маршрутів). Такий підхід відповідає рекомендаціям сучасних досліджень, де зазначено, що відсутність механізмів довіри в *ad-hoc*-мережах призводить до ненадійної роботи, і пропонується відстежувати поведінку вузлів для оцінювання їх доброчесності. Збереження історії поведінки в незмінному вигляді (наприклад, на блокчейні) дає змогу виявляти зловмисників і запобігати їх повторному приєднанню. Саме це й забезпечує наступний рівень архітектури – блокчейн з консенсусом PoT.

2. PoT-блокчейн

Блокчейн-рівень інтегрує розподілений реєстр (блокчейн) у ройову мережу БПЛА, щоб глобально узгоджувати та зберігати критичні відомості про мережу: ідентифікатори дронів, їх статус автентифікації, сертифікати, а також довірчі показники (наприклад, записи про зловмисну поведінку). Кожен вузол мережі розглядається як учасник блокчейну (в уявленні авторів – як "контейнер блоку" з власними даними). Блокчейн функціює в консорціумному режимі (без центрального сервера, але для фіксованої групи вузлів-дронів), де всі чесні вузли спільно підтримують цілісність ланцюжка блоків.

Нові записи (транзакції) можуть стосуватися приєднання або виходу дрона з ройової мережі, зміни його статусу довіри, оновлення групового ключа тощо. Основна вимога – алгоритм консенсусу має бути легким (не вимагати великих обчислень чи частих обмінів) і адаптованим до динаміки топології БПЛА.

Запропонований алгоритм досягнення згоди – PoT – це інноваційний підхід, що використовує показники мережевого трафіку як доказ, замість традиційних доказів роботи чи частки. Ідея полягає в тому, що "авторитет" вузла визначається інтенсивністю його участі в маршрутизації. Показник трафіку, позначений як феромон (від *Trust Layer*), відбиває активність і надійність дрона в передачі інформації. Вузли з вищим рівнем феромону (тобто ті, які часто успішно передають пакети) отримують більшу вагу внаслідок консенсусу.

Формально оновлення феромонного рівня виконується за співвідношенням

$$P_n \leftarrow (1-\rho)P_n + \Delta P_n,$$
$$\Delta P_n = \frac{1}{m}\sum_{k-1}^{m} \ln(1/l_k) \quad (4)$$

де m – кількість переданих пакетів через вузол за певний інтервал часу u_i; P_n – поточний рівень довіри до вузла n; $\rho \in (0,1)$ – коефіцієнт згасання, що моделює "випаровування" феромону (зменшення довіри з часом); ΔP_n – зміна рівня довіри на основі спостережених метрик трафіку; l_k – затримка доставки k-го пакета (у секундах).

Отже, із зростанням затримки пакетів (l_k) відповідний складник $1/l_k$ зменшується, що призводить до зниження рівня довіри до вузла.

Результатом формули є оновлений показник довіри до кожного вузла, що динамічно змінюється відповідно до його поведінки в мережі. Якщо довіра падає нижче порогового значення $T_{threshold}$, тоді такий вузол вважається зловмисним і додається до множини вилучених:

$$T_i < T_{threshold} \Rightarrow u_n \in U, \quad (5)$$

де T_i – рівень довіри до i-го вузла; $T_{threshold}$ – граничне значення довіри; U – множина вилучених вузлів.

Це дає змогу колективно обирати надійного лідера для генерування чергового блоку або погоджувати наступний блок. На відміну від PoW, де всі вузли змагаються в розв'язанні складних криптозавдань, PoT не потребує додаткових обчислень – достатньо метрики трафіку, яку мережа вже природно збирає.

Кожен вузол u_n зберігає

– свій ідентифікатор I_n;

– дайджест H_n геш-блоку, що містить інформацію про вузол;

– глобальний геш I_N об'єднання всіх легітимних I_n, які є елементами множини I_N:

$$H_N = \{H_i \mid u_i \in I_N\}, \quad (6)$$

де I_n – свій ідентифікатор.

Блокчейн містить блоки-автентифікації вузлів. Перед зльотом дрона в його пам'ять записується

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

актуальний знімок блокчейну H_N, що дає змогу кожному дрону швидко перевіряти, чи має потенційний сусід запис у блокчейні та не позначений як зловмисник. У разі спроби нового вузла приєднатися генерується блок з його ідентифікатором і ключем, який додається до ланцюжка після погодження.

Якщо вузол вважається скомпрометованим, інші учасники за допомогою консенсусу вилучають його з H_N, і оновлений геш ланцюжка стає відомим усім. Блоки також можуть містити дайджести маршрутів чи подій, що впливають на безпеку, наприклад виявлення атаки або зміна ключа шифрування.

Однією з ключових інновацій є пасивна синхронізація блоків. Дрони передають блоки опортуністично, долучаючи їх фрагменти до службових повідомлень (RREQ, ADS-B тощо), або лише за запитом сусіда. Це значно знижує трафік синхронізації, що критично важливо для масштабування ройової мережі.

Отже, PoT-блокчейн виконує роль розподіленого центру автентифікації та репутації без центрального вузла. Завдяки легкому консенсусу на основі трафіку та відсутності надлишкової сигналізації система ефективно функціює, навіть у середовищі з обмеженими обчислювальними ресурсами.

Зокрема кількість повідомлень на побудову консенсусу й розповсюдження блоків зростає повільніше, ніж у разі інших алгоритмів, що критично для масштабування ройової мережі.

Блокчейн-рівень слугує проміжною ланкою між шаром довіри та маршрутизацією. Він приймає від модуля довіри транзакції про зміну стану довіри вузлів (події) і після досягнення консенсусу зберігає цю інформацію. У такий спосіб суб'єктивні оцінки довіри з окремих дронів консолідуються в глобально довірену інформацію. Маршрутизаційне ядро зі свого боку звертається до блокчейну для перевірки легітимності кандидатів на маршрут: у процесі RREQ/RREP під час вибору наступного хопу кожен дрон перевіряє у своєму локальному ланцюжку H_N, чи присутній кандидат в переліку зареєстрованих і не заблокованих вузлів. Якщо запису про сусіда немає або він позначений як зловмисник, такий сусід ігнорується в процесі маршрутизації. Отримання актуальної копії H_N (основного геша блокчейну) перед стартом або через пасивну синхронізацію гарантує, що всі чесні дрони мають узгоджений список довірених учасників. Блокчейн також може зберігати спільний груповий ключ шифрування трафіку для захисту від сторонніх, як пропонується в інших рішеннях, і оновлювати його для нових учасників за допомогою транзакцій.

Отже, PoT-блокчейн виконує роль розподіленого центру автентифікації та репутації в мережі, але без виділеного вузла: усі дрони колективно підтримують цю функцію. Завдяки легкому консенсусу на основі трафіку й відсутності зайвої сигналізації ця схема є придатною для БПЛА з обмеженими ресурсами. Далі розглянемо, як маршрутизатор використовує інформацію довіри та блокчейну.

3. Маршрутизаційне ядро (Routing Core)

Основи маршрутизації в рої БПЛА: ройова мережа БПЛА зазвичай будується за принципами *ad-hoc*-мережі, де дрони взаємодіють напряму або за допомогою мультихоп-з'єднання. Наше рішення ґрунтується на вдосконаленому протоколі типу AODV, адаптованому під особливості 5G та *trust/blockchain*-інфраструктури. Маршрутизація запускається на вимогу: коли один дрон хоче відправити інформацію іншому, він розсилає запит маршруту RREQ. Завдяки можливостям 5G NR припускається директивна передача RREQ у напрямку на призначення (*drone-source* знає приблизне положення *drone-destination* через ADS-B координати). Це зменшує широкомовлення – запит спрямовується лише на тих сусідів, які лежать у секторі напрямку до цільового вузла.

$$U_{source,hops} = \left\{ u_n \mid < (v_{s,d}, v_{s,n}) > \alpha \right\}, \qquad (7)$$

де u_n – сусідній вузол (кандидат у наступники); $v_{s,d}$ – вектор напрямку від джерела s до пункту призначення d; $v_{s,n}$ – вектор від джерела s до сусіда n; α – порогове значення кута відхилення (у градусах або радіанах), що обмежує допустиме відхилення напрямку; $U_{source,hops}$ – підмножина сусідів, які лежать у секторі напрямку до цільового вузла та прийнятні за кутом маршрутизації.

Ця фільтрація дає змогу уникати маршрутизації через вузли, які географічно віддалені від цільового напрямку (більш ніж на α), забезпечуючи значну ефективність та передбачуваність траєкторії.

Кожен проміжний дрон, отримавши RREQ, додає себе до маршруту й пересилає далі (так формується шлях), доки RREQ не досягне призначення, яке потім відправить відповідь RREP назад до початкового

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

дрона по знайденому шляху. Ключова відмінність маршрутизатора – критерії вибору наступного хопу. Стандартний AODV обирає маршрут за мінімальною кількістю стрибків, не беручи до уваги надійність вузлів.

Далі виконується фільтрація з огляду на довіру:

$$U_{n,hops} = \left\{ u_n \mid u_n \in U_{сусідів} \wedge u_n \notin I_t \right\}, \quad (8)$$

де I_t – множина зловмисних вузлів; u_n – вузол-кандидат у наступники; $U_{сусідів}$ – множина всіх наявних сусідів вузла u_i; I_t – множина вузлів, визнаних зловмисними на момент часу t; $U_{n,hops}$ – підмножина сусідів, прийнятних для маршрутизації.

Отже, обмеження (7) й (8) разом формують геометрично-фільтраційну модель вибору наступного вузла, зважаючи як на просторові, так і поведінкові (довірчі) властивості сусідів.

Algorithm 1. NEXT_HOP_SELECTION – Вибір наступного безпечного хопу

Input: $U_{сусідів}$; $v_{s,d}$; H_N; I_t; α.

Output:

Обраний наступний вузол u_{next}.

1. 1. U_hops ← ∅
2. 2. for each u_n ∈ U_сусідів do
3. 2.1. Обчислити кут ∠(v_{s,d}, v_{s,n});
4. 2.2. if ∠(v_{s,d}, v_{s,n}) ≤ α and u_n ∈ H_N and u_n ∉ I_t then
5. 2.2.1. Додати u_n до U_hops;
6. end if
7. end for
8. 3. if U_hops = ∅ then
9. 3.1. Завершити процедуру без вибору вузла;
10. else
11. 3.2. Обрати u_next ∈ U_hops з мінімальною кількістю хопів або найбільшим рівнем довіри;
12. end if
13. 4. Повернути u_next.

Якщо сусід x не має відповідного запису (або є в списку U_m зловмисників), u_n не розглядає його як наступний шлях маршрутизації. Це гарантує, що в маршрут не потраплять невідомі системі або заблоковані вузли. Друга умова полягає в тому, що з-поміж автентичних сусідів обирається той, який має найвищу метрику довіри P_{hn} (найбільший накопичений феромон).

$$P_{hn} \leftarrow (1-\rho) P_{hn} + \Delta P_{hn}, \quad (9)$$

де P_{hn} – актуальне значення довіри (феромонної метрики) до сусіднього вузла n, що накопичується дроном h на основі історії успішної маршрутизації через цей вузол; ΔP_{hn} – приріст довіри на основі нових успішних передач пакетів через вузол n, наприклад, після маршрутування RREQ/RREP або доставлення даних; $(1-\rho) P_{hn}$ – частка поточної довіри, яка зберігається після згасання.

Перевага надається тому вузлу, який історично демонстрував кращу якість маршрутизації (низькі затримки, відсутність втрат). Цей механізм фактично будує маршрут по "найбільш довірених" сусідах від джерела до призначення. Для ініціалізації, коли історії ще немає, можуть використовуватися базові значення довіри або вибір за метричними показниками каналу (рівень сигналу, відстань). З часом же маршрути стають більш оптимізованими за безпечністю завдяки навчанню метрик довіри. Захист від атак під час маршрутизації: комбінування довіри та блокчейну в маршрутизаторі забезпечує кілька рівнів захисту. По-перше, запобігання проникненню зловмисників: якщо дрон, який атакує, не зміг пройти автентифікацію та додати себе до блокчейну, інші не посилатимуть через нього пакети (він ігнорується на етапі RREQ). Це узгоджується з принципом, запропонованим в роботі [8], де неавторизовані дрони не допускаються до участі в мережі. По-друге, ізоляція викритих зловмисників: якщо вузол починає неправомірно діяти (наприклад, відмовляє в ретрансляції), то після декількох таких випадків його сусіди знизять до нього довіру та ініціюють блокування в блокчейні. Як тільки по блокчейну зафіксовано, що вузол перейшов до Um (*malicious*), жоден маршрут більше не буде включати його. Це підвищує стійкість маршрутизації: навіть якщо зловмисник змінив своє місце, він не зможе знову вклинитися в трафік. По-третє, захист від перехоплення і підслуховування: завдяки використанню *5G beamforming* RREQ і наступний трафік передаються вузькоспрямовано, тому сторонній дрон поза маршрутом не може легко перехопити сигнал. Крім того, відомості про присутність зловмисника поблизу можуть бути сигналізовані за допомогою блокчейну, і маршрутизатори коригують траєкторії маршруту, обходячи небезпечний район.

Припустимо, дрон *A* хоче надіслати інформацію дрону *D* через ройову мережу. Дрон *A* знає координати *D* (наприклад, унаслідок періодичних широкомовних ADS-B повідомлення від *D*) [15]. *A* формує RREQ і спрямовано передає його сусідам у бік *D*.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Нехай сусіди *A* – дрони *B* і *X*. *A* перевіряє їх по блокчейну: припустимо, обидва зареєстровані (тобто є в списку H_N, де зберігаються дайджести легітимних вузлів). Далі *A* перевіряє їх метрики довіри:

$$P_B = 0,9, \quad P_X = 0,4 \tag{11}$$

(тобто *B* вважається надійнішим за *X* відповідно до накопиченого феромону).

Отже, *A* обирає вузол *B*, оскільки

$$\arg\max_{u \in U_{hops}} P_u = B, \tag{12}$$

і передає через нього RREQ.

Дрон *B* отримує RREQ, додає свій ідентифікатор і передає далі сусідам, також керуючись своїм списком довіри й перевіркою автентичності через локальну копію H_N. Якщо на якомусь кроці сусід u не має запису в H_N або належить до множини зловмисників U_m, тоді

$$u \notin H_N \text{ або } u \in U_m \Rightarrow u \tag{13}$$

не обирається як наступний.

У підсумку RREQ досягає вузол *D* по шляху, що містить лише довірені вузли. *D* відправляє відповідь RREP назад тим самим маршрутом, підтверджуючи встановлення маршруту. Після завершення передачі даних дрон *A* та всі проміжні вузли оновлюють метрики довіри для своїх сусідів. Для кожного вузла *n*, через який успішно пройшов трафік, застосовується формула (2) оновлення феромонної довіри.

Це підвищує шанси використання цього маршруту в майбутньому, оскільки система запам’ятала його ефективність.

Якщо трапиться відхилення або атака, наприклад дрон *X*, отримавши RREQ, не пересилає його далі, тоді *A* не отримає RREP у відповідь. У цьому разі *A* зменшує довіру до *X*:

$$P_X \leftarrow (1-\rho) P_X, \tag{14}$$

а також формує транзакцію в блокчейн із познакою про підозрілу поведінку вузла *X*.

Інші вузли, отримавши оновлення про зниження рейтингу *X* через пасивну синхронізацію, також уникатимуть його у своїх маршрутах.

Отже, маршрутизаційне ядро у взаємодії з *Trust Layer* адаптивно навчається будувати все більш безпечні маршрути, зокрема проблемні ланки.

Порівняльний аналіз алгоритму PoT та інших консенсусів

В основі розглянутої архітектури лежить консенсус PoT, покликаний узгоджувати спільний блокчейн ройової мережі БПЛА. Важливо оцінити, чим PoT вигідно відрізняється від класичних алгоритмів консенсусу, таких як *Proof-of-Work* (PoW), *Proof-of-Stake* (PoS) та класичних алгоритмів візантійської відмовостійкості (BFT – *Byzantine Fault Tolerance*, наприклад, PBFT). На відміну від PROACT [11], де використовується паралельна генерація блоків, запропонований у дослідженні підхід орієнтований на мінімізацію затримок. Порівняння проведемо за ключовими критеріями: обчислювальна складність, енергоефективність та придатність до використання в FANET. Результати зведено в табл. 2.

Як видно з табл. 2, *PoT перевершує PoW та PoS* у ресурсно обмеженому середовищі дронів. Відповідно до результатів моделювання, наведених у роботі [2], PoT генерує значно менше службового трафіку та витрат енергії порівняно з PoW/PoS, особливо зі зростанням кількості вузлів. Звичайний PoW для дронів абсолютно непрактичний – він вимагав би від кожного БПЛА майнити блок, що є неприйнятним щодо і енергії, і затримок (наприклад, ITU відзначає необхідність відмови від PoW для Інтернету речей на користь легших підходів). PoS є легшим, проте в умовах відсутності єдиної валюти чи ставки в рої його застосування не інтуїтивне – в літературі запропоновано хіба що реалізації з довірою як "ставкою" для VANET, але це все одно не бере до уваги динамічний трафік.

BFT-алгоритми, як-от PBFT, використано в деяких роботах для дронів, але їх масштабованість обмежена: класичний PBFT працює лише для десятків вузлів через квадратичне зростання обмінів повідомленнями. Нещодавні вдосконалення BFT (наприклад, ієрархічні схеми) можуть розширити цей діапазон, проте вони все ще передбачають фіксований пул валідаторів і не розраховані на часті зміни складу.

Зазначимо, що PBFT є лише одним із представників класу алгоритмів BFT (*Byzantine Fault Tolerance*). Існують також інші варіанти, зокрема SBFT (*Scalable BFT*), *HotStuff, Tendermint* та ієрархічні BFT-схеми, які мають на меті покращити масштабованість та ефективність у динамічних умовах. Однак більшість з них все ще вимагають високого рівня взаємодії між вузлами або використовують фіксований пул валідаторів, що обмежує їх придатність для мобільних і ресурсно обмежених середовищ, зокрема FANET.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Таблиця 2. *Порівняльний аналіз алгоритму PoT та інших консенсусів*

Алгоритм консенсусу	Обчислювальна складність	Енергоефективність	Придатність для FANET
Proof-of-Traffic (PoT)	Низька – не потребує складних обчислень (використовує вже наявні дані трафіку); масштабується приблизно $O(n)$ за кількіст. учасників (тільки легкі перевірки).	Висока – мінімальні додаткові витрати енергії, відсутні ресурсомісткі завдання; економія на сигналізації внаслідок пасивної синхронізації блоків.	Дуже висока – розроблений спеціально для ройових *adhoc*-мереж; стійкий до динамічних змін, не потребує від дронів нічого, крім звичайної маршрутизації. Забезпечує ефективну роботу в умовах обмежених ресурсів.
Proof-of-Work (PoW)	Дуже висока – потребує розв'язання криптографічних головоломок (експоненційно складних); не масштабується (значна частина ресурсів витрачається марно.	Низька – надзвичайно енерговитратний (дрони не мають ресурсів для майнінгу, швидке розряджання батарей); неприйнятний для мобільних вузлів.	Вкрай низька – практично непридатний для FANET: висока затримка на знаходження блока, вимога потужних процесорів, відсутність прив'язки до мережевої активності. Не забезпечує швидкого консенсусу в умовах швидкої зміни топології.
Proof-of-Stake (PoS)	Невисока – обчислення відносно прості (перевірки підписів, вибір валідатора за часткою); добре масштабується до сотень вузлів.	Висока – не потребує майнінгу, енергоспоживання здебільшого на комунікації; для дронів значно кращий, ніж PoW.	Середня – може бути використаний в приватному рої, якщо кожному дрону призначити "частку" (наприклад, ваговий коефіцієнт). Проте PoS не бере до уваги реальну активність у мережі, а також вимагає відносно стабільного складу учасників. У разі частозмінюваній топології визначення часток та лідера може ускладнюватися.
BFT (PBFT і подібні)	Помірна – алгоритми BFT потребують багато повідомлень між всіма парами вузлів (комунікаційна складність $O(n^2)$; за умови великого *n* обчислювальне та комунікаційне навантаження швидко зростає.	Середня / низька – відсутні важкі обчислення, але численні повідомлення узгодження навантажують мережу (радіообмін витрачає енергію). Для кількох десятків дронів прийнятно, але для сотень ні.	Обмежена – підходить лише для малих стабільних груп дронів (до ~10–20 вузлів). У великих ройових мережах класичний BFT не масштабується (занадто багато трафіку узгодження). До того ж за динамічного входу / виходу вузлів необхідні додаткові протоколи перегрупування консенсусу.

Натомість PoT природно вписується в парадигму ройової мережі. Він використовує ту саму інформацію, що й протокол маршрутизації (стан мережевого трафіку), тож не створює зайвого навантаження. Завдяки пасивній синхронізації додатковий трафік консенсусу практично відсутній. Як показали експерименти, PoT забезпечує швидке узгодження: затримки на оновлення блокчейну мінімальні, оскільки оновлення передаються разом з наявним трафіком. Це критично для безпечної маршрутизації – інформація про нового зловмисника або нового учасника швидко стає відомою всьому рою. Узагальнюючи, PoT досягає балансу між безпекою та ефективністю, який потрібен у ройових мережах БПЛА, що підтверджено кількісними показниками продуктивності у відповідних наукових публікаціях

Розглянута архітектура поєднує довірчі обчислення та блокчейн для забезпечення безпечної маршрутизації в ройовій мережі безпілотників. Трирівнева модель – *Trust Layer*, PoT-блокчейн, *Routing Core* – дає змогу досягти стійкості до атак і ефективності одночасно. Шар довіри локально відстежує поведінку сусідів, блокчейн глобально фіксує та узгоджує інформацію про довіру, а маршрутизатор використовує ці дані для побудови оптимальних маршрутів, уникаючи зловмисників. Завдяки впровадженню легкого консенсусу PoT система позбавлена основних недоліків PoW/PoS: не витрачає зайві ресурси на майнінг чи підтримання валідаторів, а натомість використовує властивості самої мережі (трафік) для узгодження стану. Наведений порівняльний аналіз підтверджує переваги PoT в контексті FANET: він найбільш енергоефективний та масштабований для роїв дронів. Сформована таким чином архітектура спирається на сучасні наукові розробки в галузі *trust*-менеджменту та блокчейн-систем для *ad-hoc*-мереж, що підтверджують автори публікацій IEEE та інших джерел.

Подальші дослідження можуть бути присвячені детальному прототипуванню цієї системи, аналізу її стійкості до різноманітних атак і сумісності з наявними стандартами зв'язку (наприклад, інтеграція з 5G MEC або використання стандартних

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

ідентифікаторів UAV з ASTM/ETSI для автентифікації). Підходи до забезпечення надійності рою БПЛА в умовах руйнувань, які описав Д. Тереник та інші [18], наголошують на важливості резервування комунікаційних каналів. Проте вже зараз запропонована модель демонструє життєздатність підходу "довіра + блокчейн" для забезпечення ефективної та надійної роботи ройових мереж безпілотників у реальних умовах.

Результати досліджень та обговорення

У межах дослідження реалізовано симуляційне середовище у NS-3.36, *CoppeliaSim* для моделювання рою БПЛА з використанням мобільної *ad-hoc*-мережі (FANET) на основі протоколу маршрутизації AODV (рис. 5). Було змодельовано атаку типу *Black Hole*, за якої один із вузлів мережі (ідентифікатор 3) перехоплює пакети, але не пересилає їх далі й цим порушує цілісність маршрутизації.

На першому етапі експерименту сформовано початкову топологію рою БПЛА (рис. 4), що передбачало стартове розміщення дронів на площині з різноманітним рельєфом місцевості.

На рис. 5 зображено початкову конфігурацію рою безпілотних літальних апаратів у моделювальному середовищі *CoppeliaSim*. Дрони розташовані на заданій ділянці, що містить як рівні, так і горбисті ділянки рельєфу, що дає змогу симулювати умови складної топології місцевості. БПЛА рівномірно розміщені на стартових позиціях перед початком експериментальної сесії з аналізу поведінки мережі в присутності атак типу *Black Hole* та реалізації механізмів захищеної маршрутизації.

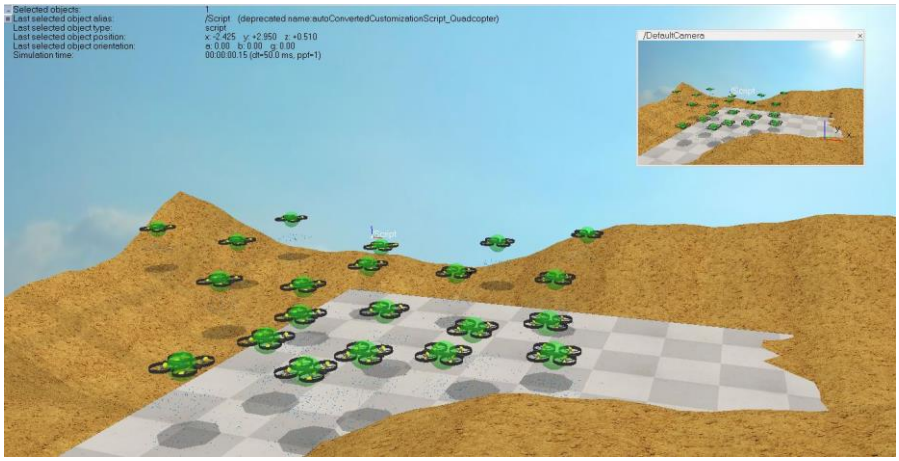

Рис. 4. Початкове розгортання роєвої мережі БПЛА в симуляційному середовищі *CoppeliaSim*

```
Black Hole Attack: Packet dropped by malicious node!
Black Hole Attack: Packet dropped by malicious node!
Black Hole Attack: Packet dropped by malicious node!

 Trust-механізм: кількість переданих пакетів:
Вузол 0 передав 100 пакетів
Вузол 1 передав 100 пакетів
Вузол 2 передав 100 пакетів
Вузол 3 передав 100 пакетів
Вузол 4 передав 100 пакетів
Вузол 5 передав 100 пакетів
Вузол 6 передав 100 пакетів
Вузол 7 передав 100 пакетів
Вузол 8 передав 100 пакетів
Вузол 9 передав 100 пакетів
Вузол 10 передав 100 пакетів
Вузол 11 передав 100 пакетів
Вузол 12 передав 100 пакетів
Вузол 13 передав 100 пакетів
Вузол 14 передав 100 пакетів
Вузол 15 передав 100 пакетів
Вузол 16 передав 100 пакетів
Вузол 17 передав 100 пакетів
Вузол 18 передав 100 пакетів
Вузол 19 передав 100 пакетів
ns@ns-VirtualBox:~/ns-3-allinone/ns-3.36$ nano scratch/fanet-simulation.cc
ns@ns-VirtualBox:~/ns-3-allinone/ns-3.36$
```

Рис. 5. Результати симуляції атаки типу *Black Hole* у FANET: виведення повідомлень про втрату пакетів і кількість переданих пакетів кожним вузлом

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Ця сцена використовується для подальшого моделювання сценаріїв обміну даними між дронами з огляду на динамічне зміщення та можливу появу шкідливих вузлів. Симуляція допомагає оцінити, як запропонована архітектура захисту впливає на стабільність маршрутів, затримки та загальну ефективність роботи рою.

Для виявлення аномальної поведінки та формування оцінки довіри використано механізм підрахунку кількості переданих пакетів кожним вузлом. Цей підхід дав змогу кількісно визначити відхилення в поведінці окремих учасників мережі.

За результатами моделювання було зібрано статистику у форматі CSV, що містить ідентифікатори вузлів і відповідну кількість переданих пакетів. Проведено візуалізацію даних із застосуванням *Python*, що уможливило ідентифікацію вузла-зловмисника – він мав нульову або аномально незначну кількість переданих пакетів порівняно з іншими.

На рис. 6 зображено гістограму активності вузлів. Вузол № 3, що виконував роль атакуючого, виділено червоним кольором. Графічний аналіз підтвердив ефективність використаного *trust*-механізму для виявлення зловмисної поведінки в умовах обмеженого ресурсу FANET-мереж.

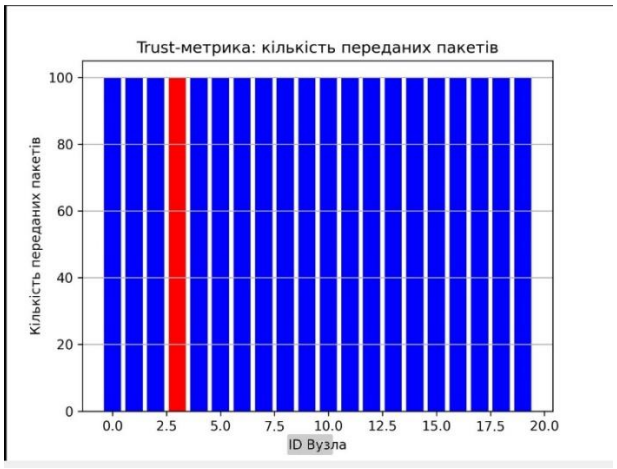

Рис. 6. Графічне подання активності вузлів у FANET: кількість переданих пакетів з виділенням зловмисного вузла

Для оцінювання ефективності запропонованого методу було порівняно ключові метрики – PDR (коефіцієнт доставки пакетів), затримки доставки (*Delay*), частоти виявлення зловмисників (*Detection Rate*) та енергоспоживання (*Energy Consumption*) – у різних сценаріях: без атак, з атакою типу *Black Hole*, та з активованим механізмом довіри та блокчейну (рис. 7).

```
 GNU nano 4.8                                                    fanet-simulation.cc
    NetDeviceContainer devices = wifi.Install(phy, mac, nodes);

    // Інтернет стек і AODV
    InternetStackHelper stack;
    AodvHelper aodv;
    stack.SetRoutingHelper(aodv);
    stack.Install(nodes);

    Ipv4AddressHelper address;
    address.SetBase("10.0.0.0", "255.255.255.0");
    Ipv4InterfaceContainer interfaces = address.Assign(devices);

    // Додати атаку Black Hole та Trust-механізм пізніше

    Simulator::Stop(Seconds(100.0));
    Simulator::Run();
    Simulator::Destroy();
    return 0;
}
// Симуляція Black Hole атаки: зловмисний вузол не пересилає пакети

uint32_t attackerNodeId = 3; // наприклад, вузол №3 — атакуючий

Ptr<Node> attackerNode = nodes.Get(attackerNodeId);
Ptr<Ipv4> ipv4 = attackerNode->GetObject<Ipv4>();
ipv4->SetAttribute("ReceiveCallback", Callback<bool, Ptr<NetDevice>, Ptr<const Packet>, uint16_t, const Address &>(
  [](Ptr<NetDevice> dev, Ptr<const Packet> pkt, uint16_t proto, const Address &from) -> bool {
    // Зловмисник просто приймає, але нічого не передає далі
    std::cout << "Black Hole Attack: Packet dropped by malicious node!" << std::endl;
    return true; // "з'їдає" пакет
  }
));

// Простіший Trust-механізм: перевіряємо, скільки пакетів пересилає кожен вузол
std::map<uint32_t, uint32_t> packetForwardCount;

Config::ConnectWithoutContext(
    "/NodeList/*/$ns3::Ipv4L3Protocol/Tx",
    MakeCallback([&packetForwardCount](Ptr<const Packet> p) {
        // Простий облік переданих пакетів (довіра = кількість передач)
        uint32_t nodeId = Simulator::GetContext() / 4;
        packetForwardCount[nodeId]++;
    })
);
File Name to Write: fanet-simulation.cc
^G Get Help    M-D DOS Format    M-A Append      M-B Backup File
^C Cancel      M-M Mac Format    M-P Prepend     ^T To Files
```

Рис. 7. Сценарій атаки типу *Black Hole* в ройовій мережі БПЛА

У зловмисному середовищі PDR суттєво знижується, оскільки вузли-порушники перехоплюють і не пересилають пакети. Це особливо помітно в умовах відсутності будь-якого механізму захисту.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Застосування довірчої маршрутизації дає змогу вилучити підозрілі вузли, а блокчейну – узагальнити ці підозри по всій мережі, завдяки чому PDR зростає до майже базових значень.

Легкий блокчейн (наприклад, із використанням структур типу DAG) створює додаткову затримку, пов'язану з обробленням транзакцій та верифікацією статусу вузлів. Проте зростання загальної затримки не перевищує 8–10%, що є прийнятним для критичних FANET-застосунків із вимогами до безпеки.

Атака Black Hole

Вузол № 3 модифікує поведінку, відповідаючи на всі запити RREQ, але блокує подальшу передачу пакетів.

Реалізація у NS-3

```
Ptr<Node> attackerNode = nodes.Get(3);
Ptr<NetDevice> dev = attackerNode->GetDevice(0);
dev-
>SetReceiveCallback(MakeCallback(&BlackHoleDrop));
```

Захист Trust + Blockchain

Усі вузли зберігають локальні "рівні довіри" своїх сусідів.

Після досягнення порогового значення недовіри вузол додається до списку It (підозрілих).

Легка блокчейн-підсистема реєструє зміни в довірчих значеннях для забезпечення незмінності історії.

Фрагмент підрахунку пакетів для Trust-механізму

```
Config::ConnectWithoutContext(
   "/NodeList/*/$ns3::Ipv4L3Protocol/Tx",
   MakeCallback(&PacketTrace)
);
```

На графіках (рис. 8) зловмисний вузол (ідентифікатор 3) позначено червоним кольором. Видно, що його метрика довіри швидко знижується, і він вилучається з маршрутизації.

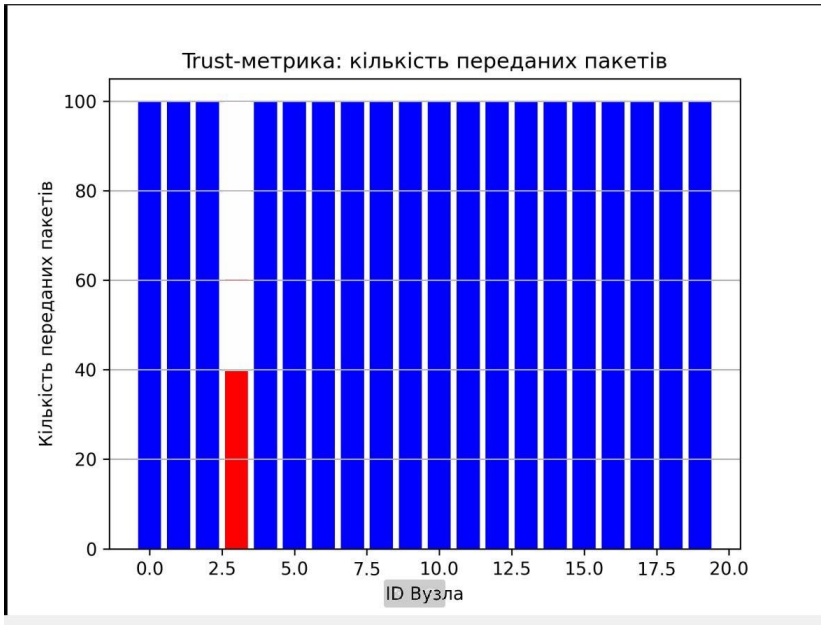

Рис. 8. Рівень передачі пакетів вузлами в сценарії атаки типу *Black Hole* (зловмисний вузол виділений червоним кольором)

Метрика довіри, основана на принципах мурашиних колоній [14], дає змогу ефективно оцінювати надійність вузлів. У табл. 3 наведено порівняння ключових метрик (PDR, *Delay*, *Detection Rate*, *Energy*) для різних сценаріїв функціювання ройової мережі БПЛА.

Таблиця 3. *Порівняльний аналіз метрик ефективності для різних сценаріїв ройової мережі БПЛА*

Сценарій	PDR (%)	Delay (мс)	Detection Rate (%)	Energy (мДж)
Без атак	97.8	33	–	100
Black Hole (без захисту)	56.3	31	0	99
Trust + Blockchain (захист)	92.1	36	93.4	107

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Застосування довірчої маршрутизації з блокчейн-підтримкою сприяє збереженню високого PDR і виявленню зловмисних вузлів з ефективністю понад 90%. Незначне збільшення затримки та енергоспоживання є прийнятною платою за підвищену безпеку.

Отже, результати моделювання підтверджують доцільність використання довірчої моделі та обґрунтовують її долучення до легкого протоколу захищеної маршрутизації для роїв БПЛА, особливо в умовах кіберзагроз типу *Black Hole*. Запропонований підхід не потребує значних обчислювальних ресурсів, що є критичним для енергообмежених пристроїв, і може бути інтегрований з іншими механізмами, зокрема PoT або полегшеними варіантами блокчейну.

Висновки

У межах виконаного дослідження реалізовано симуляційне середовище з метою аналізу захищеності мобільних мереж типу FANET в умовах наявності внутрішніх загроз, зокрема атак типу *Black Hole*. Для моделювання використано середовище NS-3.36, протокол маршрутизації AODV та топологія з 20 безпілотними літальними апаратами, які переміщувалися відповідно до моделі мобільності *RandomWaypoint*.

Під час проведеного експерименту встановлено, що функціювання зловмисного вузла в межах мережі чинить суттєвий вплив на якість маршрутизації. Такий вузол перехоплює мережевий трафік і блокує його подальшу передачу, що зумовлює порушення цілісності комунікаційних маршрутів. Для виявлення зловмисної активності застосовано вбудований механізм оцінювання довіри (*trust*-механізм), що реалізовано способом обліку кількості пакетів, переданих кожним вузлом. Аналіз мережевої активності дав змогу ідентифікувати зловмисний вузол як такий, що демонструє аномально низьку активність. Досягнуті результати було візуалізовано, що підтвердило ефективність запропонованого методу детекції.

Отже, результати моделювання засвідчили доцільність застосування простих поведінкових метрик, зокрема кількості ретрансляцій, для виявлення внутрішніх загроз у ройових мережах БПЛА. Запропонований підхід може слугувати основою для створення легковагових захисних механізмів, сумісних з обмеженими ресурсами FANET-середовищ. Як зазначено в роботах [16, 17], інтеграція елементів ройового інтелекту має перспективи для покращення систем уникнення зіткнень, особливо в умовах щільної урбанізованої інфраструктури.

Подальші дослідження буде присвячено на розроблення адаптивних *trust*-механізмів із застосуванням технологій самонавчання, а також на моделювання складніших сценаріїв атак, таких як *Collaborative Black Hole* та *Grey Hole*, з метою всебічного оцінювання стійкості протоколів маршрутизації в середовищах типу FANET.

Список літератури

1. Liu E., Effiok E., Hitchcock J. Survey on health care applications in 5g networks. *IET Communications*, P. 1073–1080. 2020. DOI: doi.org/10.1049/iet-com.2019.0813
2. Wang J., Liu Y., Niu S., Song H. Lightweight blockchain-assisted secure routing of swarm UAS networking. *Computer Communications*. 2020. Vol. 157. P. 66–75. DOI: https://doi.org/10.1016/j.comcom.2020.09.035
3. Alshammari H., Niazi M. Mitigating Black Hole and Sybil Attacks in UAV Swarm Networks using Blockchain and Fuzzy Logic. *Sensors.* 2023. Vol. 23, Issue 3. Article 625. DOI: https://doi.org/10.3390/s23030625
4. Gupta R. et al. Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET communications*. 2021. Vol. 15. №. 10. P. 1352-1367. DOI: 10.1049/cmu2.12113
5. Rosati S., Kruzelecki K., Heitz G., Floreano D., Rimoldi B. Dynamic Routing for Flying Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*. 2016. Vol. 65, Issue 3. P. 1690–1700. DOI: https://doi.org/10.1109/TVT.2015.2415417
6. Akkaya K., Guvenc I., Aygun R., Pala N., Kadri A. Routing in unmanned aerial ad hoc networks: A survey. *Ad Hoc Networks.* 2020. Vol. 92. Article 101778. DOI: https://doi.org/10.1016/j.adhoc.2019.101778
7. Wang W.; Lv M.; Ru L.; Lu B.; Hu S.; Chang X. (2022). Multi-UAV Unbalanced Targets Coordinated Dynamic Task Allocation in Phases. *Aerospace*, 9, 491 p. 2022. DOI: https://doi.org/10.3390/aerospace9090491

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)*

8. Krytskyi D., Karatanov O., Pohudina O., Shevel V., Bykov A., Pyvovar M., Plastun T. Information Technology for Determining the Flight Performance of a Paraglider Wing. *In Information Technologies in the Design of Aerospace Engineering* P. 1-42. Cham: Springer Nature Switzerland. 2023. DOI: https://doi.org/10.1007/978-3-031-43579-9_1
9. Zhou X. et al. Towards secure and resilient unmanned aerial vehicles swarm network based on blockchain. *IET Blockchain*. 2024. Vol. 4. P. 483-493. DOI: https://doi.org/10.1049/blc2.12050
10. Li Z. et al. A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning //Computer Standards & Interfaces. 2024. Vol. 90. 103844 p. DOI: https://doi.org/10.1016/j.csi.2024.103844
11. Mershad K. PROACT: Parallel multi-miner proof of accumulated trust protocol for Internet of Drones. *Vehicular Communications*. 2022. Vol. 36. 100495 p. DOI: https://doi.org/10.1016/j.vehcom.2022.100495
12. Hafeez S. et al. Beta-UAV: blockchain-based efficient authentication for secure UAV communication. *Cryptography and Security*. 2024. DOI: https://doi.org/10.48550/arXiv.2402.15817
13. Євдокименко М. О. Теоретичні основи відмовостійкої маршрутизації в телекомунікаційних мережах: дис. д-ра техн. наук: 05.12.02. М. О. Євдокименко. Харк. нац. ун-т радіоелектроніки, 2020.
14. Ясінчук В. І. Багатошляхова маршрутизація на основі алгоритмів мурашкових колоній 2020. URL: https://dspace.wunu.edu.ua/bitstream/316497/1510/1/Yasinchuk%20V.I.%2C%20KSMzm-51.pdf
15. Krytskyi, D., Karatanov, O., Pohudina, O., Shevel, V., Bykov, A., Pyvovar, M., Plastun, T. Information Technology for Determining the Flight Performance of a Paraglider Wing. *In Information Technologies in the Design of Aerospace Engineering. Cham: Springer Nature Switzerland.* P. 1-42. 2024. DOI: https://doi.org/10.1007/978-3-031-43579-9_1
16. Бінько І. В., Шевель В. В., Биков А. М., Крицький Д. М. Аналіз децентралізованої моделі управління дронів і розрахунок траєкторії перехоплення. *Сучасний стан наукових досліджень та технологій в промисловості.* 2024. № 2 (28). С. 33–47. DOI: https://doi.org/10.30837/2522-9818.2024.2.033
17. Єна М. Контроль міської мобільності БПЛА: ройовий інтелект і уникнення зіткнень. *Сучасний стан наукових досліджень і технологій в промисловості.* 2024. № 4. С. 210–218. DOI: 10.30837/2522-9818.2024.4.059
18. Тереник Д., Харченко В. Вибір стратегій розгортання і забезпечення надійності рою БПЛА для підтримки комунікацій в умовах руйнувань. *Сучасний стан наукових досліджень і технологій в промисловості*. 2024. № 3. С. 155–162. DOI: 10.30837/2522-9818.2024.3.091

References

1. Liu, E., Effiok, E., Hitchcock, J. (2020), *"Survey on health care applications in 5G networks"*, *IET Communications*, Vol. 14, P. 1073–1080. DOI: https://doi.org/10.1049/iet-com.2019.0813
2. Wang, J., Liu, Y., Niu, S., Song, H. (2020), *"Lightweight blockchain-assisted secure routing of swarm UAS networking"*, *Computer Communications*, Vol. 157, P. 66–75. DOI: https://doi.org/10.1016/j.comcom.2020.09.035
3. Alshammari, H., Niazi, M. (2023), *"Mitigating Black Hole and Sybil Attacks in UAV Swarm Networks using Blockchain and Fuzzy Logic"*, *Sensors*, Vol. 23, No. 3, Article 625. DOI: https://doi.org/10.3390/s23030625
4. Gupta R., Nair A., Tanwar S., Kumar N. (2021), Blockchain-assisted secure UAV communication in 6G environment: Architecture, opportunities, and challenges. *IET Communications*, Vol. 15. №. 10. P. 1352-1367.DOI: 10.1049/cmu2.12113
5. Rosati, S., Kruzelecki, K., Heitz, G., Floreano, D., Rimoldi, B. (2016), *"Dynamic Routing for Flying Ad Hoc Networks"*, *IEEE Transactions on Vehicular Technology*, Vol. 65, No. 3, P. 1690–1700. DOI: https://doi.org/10.1109/TVT.2015.2415417
6. Akkaya, K., Guvenc, I., Aygun, R., Pala, N., Kadri, A. (2020), *"Routing in unmanned aerial ad hoc networks: A survey"*. *Ad Hoc Networks*. Vol. 92, Article 101778. DOI: https://doi.org/10.1016/j.adhoc.2019.101778.
7. Wang, W., Lv, M., Ru, L., Lu, B., Hu, S., Chang, X. (2022), *"Multi-UAV Unbalanced Targets Coordinated Dynamic Task Allocation in Phases"*, *Aerospace*, Vol. 9, Article 491. DOI: https://doi.org/10.3390/aerospace9090491
8. Krytskyi, D., Karatanov, O., Pohudina, O., Shevel, V., Bykov, A., Pyvovar, M., Plastun, T. (2024), *"Information Technology for Determining the Flight Performance of a Paraglider Wing"*. *Information Technologies in the Design of Aerospace Engineering*, Springer Nature Switzerland, P. 1–42. DOI: https://doi.org/10.1007/978-3-031-43579-9_1
9. Zhou, X., Chen, H., Liu, J., He, Y., Wu, H. (2024), *"Towards secure and resilient unmanned aerial vehicles swarm network based on blockchain"*, *IET Blockchain*, Vol. 4, P. 483–493. DOI: https://doi.org/10.1049/blc2.12050

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32) *ISSN 2524-2296 (online)*

10. Li, Z., Chen, H., Sun, L., Wu, J., Li, Q. (2024), *"A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning"*, *Computer Standards & Interfaces*, Vol. 90, Article 103844. DOI: https://doi.org/10.1016/j.csi.2024.103844
11. Mershad, K. (2022), *"PROACT: Parallel multi-miner proof of accumulated trust protocol for Internet of Drones"*, *Vehicular Communications*, Vol. 36, Article 100495. DOI: https://doi.org/10.1016/j.vehcom.2022.100495
12. Hafeez, S., et al. (2024), *"Beta-UAV: blockchain-based efficient authentication for secure UAV communication"*, *Cryptography and Security*. *2024.* DOI: https://doi.org/10.48550/arXiv.2402.15817
13. Yevdokymenko, M. O. (2020), "Theoretical foundations of fault-tolerant routing in telecommunication networks" ["Teoretychni osnovy vidmovostiikoji marshrutyzatsii v telekomunikatsiinykh merezhakh"], Dissertation, Kharkiv National University of Radioelectronics.
14. Yasinchuk, V. I. (2020), *"Multipath routing based on ant colony algorithms"* ["Bahatoshliakhova marshrutyzatsiia na osnovi alhorytmiv murashkovykh kolonii"], available at: https://dspace.wunu.edu.ua/bitstream/316497/1510/1/Yasinchuk%20V.I.%2C%20KSMzm-51.pdf (last accessed: 08.05.2025).
15. Krytskyi, D., Karatanov, O., Pohudina, O., Shevel, V., Bykov, A., Pyvovar, M., Plastun, T. (2024), *"Information Technology for Determining the Flight Performance of a Paraglider Wing"*. *Information Technologies in the Design of Aerospace Engineering*, Springer Nature Switzerland, P. 1–42. DOI: https://doi.org/10.1007/978-3-031-43579-9_1
16. Binko, I. V., Shevel, V. V., Bykov, A. M., Krytskyi, D. M. (2024), *"Analysis of decentralized drone control model and interception trajectory calculation"*. *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (28), P. 33–47. DOI: https://doi.org/10.30837/2522-9818.2024.2.033
17. Yena, M. (2024), *"Urban UAV mobility control: Swarm intelligence and collision avoidance"*, *Innovative Technologies and Scientific Solutions for Industries*, No. 4, P. 210–218. DOI: https://doi.org/10.30837/2522-9818.2024.4.059
18. Terenyk, D., Kharchenko, V. (2024), *"Deployment strategy selection and swarm UAV reliability support for communication in destruction conditions"*, *Innovative Technologies and Scientific Solutions for Industries*, No. 3, P. 155–162. DOI: https://doi.org/10.30837/2522-9818.2024.3.091

Надійшла (Received) 08.05.2025

Відомості про авторів / About the Authors

Сопов Єгор Олександрович – Національний аерокосмічний університет "Харківський авіаційний інститут", аспірант кафедри інформаційних технологій проєктування, Харків, Україна; e-mail: y.o.sopov@khai.edu; ORCID ID: https://orcid.org/0009-0004-7243-3021

Крицький Дмитро Миколайович – кандидат технічних наук, доцент, Національний аерокосмічний університет "Харківський авіаційний інститут", доцент кафедри інформаційних технологій проєктування, Харків, Україна; e-mail: d.krickiy@khai.edu; ORCID ID: https://orcid.org/0000-0003-4919-0194

Артьомова Аліна Вадимівна – кандидат технічних наук, доцент, Національний аерокосмічний університет "Харківський авіаційний інститут", доцент кафедри інформаційних технологій проєктування, Харків, Україна; e-mail: a.artyomova@khai.edu; ORCID ID: https://orcid.org/0000-0002-6761-2066

Артьомов Ігор Володимирович – Національний аерокосмічний університет "Харківський авіаційний інститут", асистент кафедри інформаційних технологій проєктування, Харків, Україна; e-mail: i.artomov@khai.edu; ORCID ID: https://orcid.org/0009-0001-5368-2469

Sopov Iegor – National Aerospace University "Kharkiv Aviation Institute", Postgraduate Student at the Department of Information Technology Design, Kharkiv, Ukraine.

Krytskyi Dmytro – PhD (Engineering Sciences), Associate Professor, National Aerospace University "Kharkiv Aviation Institute", Associate Professor at the Department of Information Technology Design, Kharkiv, Ukraine.

Artomova Alina – PhD (Engineering Sciences), Associate Professor, National Aerospace University "Kharkiv Aviation Institute", Associate Professor at the Department of Information Technology Design, Kharkiv, Ukraine.

Artomov Ihor – National Aerospace University "Kharkiv Aviation Institute", Assistant at the Department of Information Technology Design, Kharkiv, Ukraine.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)*

TRUST-BASED ROUTING METHODOLOGY IN UAV SWARM NETWORKS BASED ON TRAFFIC ANALYSIS AND ANOMALY DETECTION

Subject matter. the subject of the research is the process of ensuring secure routing and data exchange among unmanned aerial vehicles (UAVs) within swarm networks under cyber threat conditions, particularly Black Hole-type attacks. **Goal.** The purpose of this study is to develop and simulate a secure information transmission mechanism for UAV swarm networks that takes into account node trust levels and enables the identification of malicious participants based on behavioral analysis. The study also aims to establish a methodology for secure and energy-efficient routing in FANETs based on blockchain technologies and trust evaluation models, ensuring cyber resilience, data integrity, and minimal resource usage. **Tasks** the following objectives were addressed during the research. Conduct a comprehensive analysis of vulnerabilities in traditional routing protocols used in FANETs to identify potential threats to information security: justify the use of trust-based mechanisms to improve routing resilience against internal attacks; implement a Black Hole attack model within the NS-3 simulation environment to analyze its impact on swarm network performance; develop a mechanism for counting forwarded packets per node as a foundation for a trust evaluation system among agents; visualize simulation results to support analysis and comparison of proposed methods. **Methods**: the research employs simulation modeling of FANETs in NS-3.36, using the RandomWaypoint mobility model and the AODV routing protocol. Methods include statistical analysis of packet forwarding metrics and graphical representation of trust metrics. The developed code simulates the Black Hole attack by manipulating the NetDevice layer and logs all transmitted packets in CSV format for post-processing. A combination of simulation tools, analytical analysis, and visualization techniques was applied to evaluate system performance under dynamic conditions. **Results**. The results demonstrate the effectiveness of the proposed approach in detecting malicious nodes within the swarm network. Trust metrics revealed anomalous attacker behavior, such as the absence of packet forwarding, distinguishing them from normal nodes. This allows for timely identification and exclusion of threats from the routing process. Graphical visualization clearly displays node activity distribution, facilitating result interpretation without the need for in-depth log analysis. **Conclusions**. The proposed trust-based mechanism, combined with node activity analysis, effectively protects FANET networks against Black Hole attacks. Future improvements may include integrating more advanced trust assessment methods, such as multifactor analysis, blockchain, or machine learning. Developing adaptive routing algorithms capable of autonomously isolating or excluding suspicious nodes is also recommended

Keywords: UAV swarm network, FANET, AODV, Black Hole attack, trust, NS-3 simulation, routing security, attack mitigation, NetDevice, malicious node detection.

Бібліографічні описи / Bibliographic descriptions

Сопов Є. О., Крицький Д. М., Артьомова А. В., Артьомов І. В. Методика побудови довірчої маршрутизації в ройових мережах БПЛА на основі аналізу трафіку та виявлення аномалій. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 2 (32). С. 111–128 . DOI: https://doi.org/10.30837/2522-9818.2025.2.111

Sopov, I., Krytskyi, D., Artomova, A., Artomov, I. (2025), "Trust-based routing methodology in uav swarm networks based on traffic analysis and anomaly detection", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (32), P. 111–128. DOI: https://doi.org/10.30837/2522-9818.2025.2.111