ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

УДК 629.7.014-519.066:004.7-027.551 **doi: 10.32620/aktt.2024.4.11**

Р. І. ДЕМУРА

Національний аерокосмічний університет імені М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

ВИКОРИСТАННЯ VPN ТА RIS ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗВ'ЯЗКУ В ДИНАМІЧНИХ МЕРЕЖАХ РОЇВ БПЛА: ШЛЯХИ ІНТЕГРАЦІЇ, РОЗПОДІЛ РЕСУРСІВ ТА РЕЗУЛЬТАТИ СИМУЛЯЦІЇ

Предметом *вивчення в статті є інтеграція технологій віртуальних приватних мереж (VPN) та налаштовуваних інтелектуальних поверхонь (Reconfigurable Intelligent Surfaces, RIS) у роєві системи безпілотних літальних апаратів (БПЛА).* ***Метою*** *є дослідження можливостей покращення продуктивності та безпеки роєвих систем БПЛА шляхом застосування VPN для шифрування та захисту даних, а також RIS для оптимізації маршрутизації сигналу в складних середовищах.* ***Завдання:*** *аналіз існуючих підходів до забезпечення безпеки та продуктивності мереж у роєвих системах БПЛА, оцінка ефективності інтеграції VPN та RIS у різних сценаріях роботи рою, таких як міське середовище з високою щільністю забудови, відкриті простори та складні багаторівневі середовища, проведенні симуляційних досліджень для порівняння продуктивності та безпеки роєвих систем БПЛА з використанням VPN і RIS, а також без них. Використовуваними методами є моделювання та симуляція мережевих і комунікаційних систем за допомогою NS-3 (Network Simulator 3). Моделювання включає різні сценарії роботи роєвих систем БПЛА, що дає змогу порівняти вплив VPN та RIS на ефективність комунікацій. Отримані такі* ***результати:*** *інтеграція VPN та RIS у роєві системи БПЛА дозволяє значно підвищити продуктивність мережі, знизити затримки сигналу, підвищити енергоефективність та забезпечити високий рівень безпеки даних. Симуляційні дослідження показали, що VPN надає надійний захист даних і знижує ризик перехоплення, тоді як RIS оптимізують передачу сигналу в умовах складних середовищ, покращуючи загальну ефективність рою.* ***Висновки****. Стаття демонструє, що інтеграція VPN та RIS у роєві системи БПЛА є перспективним підходом для забезпечення безпеки та ефективності комунікацій в умовах динамічного середовища. Отримані результати вказують на необхідність подальших досліджень у напрямку вдосконалення цих технологій, зокрема у сфері адаптації до нових видів загроз і підвищення енергоефективності.*

Ключові слова: *безпілотні літальні апарати (БПЛА); роєві системи; віртуальні приватні мережі (VPN); Reconfigurable Intelligent Surfaces (RIS); мережева безпека; оптимізація сигналу.*

1. Вступ

1.1. Актуальність теми

Безпілотні літальні апарати (БПЛА) сьогодні стали невід'ємною частиною багатьох сфер діяльності, від військових операцій до гуманітарних місій. Концепція роїв БПЛА, що передбачає координацію великої кількості дронів, відкриває нові можливості для ефективного виконання складних завдань. Однак, з цією концепцією виникають і значні виклики, серед яких ключовим є забезпечення безпечного та надійного зв'язку між дронами.

Зростаюча кількість загроз, пов'язаних із кібератаками, змушує розробників зосереджуватися на створенні мережевих рішень, що можуть забезпечити як високу продуктивність, так і стійкість до зовнішніх впливів. У науковій літературі значна увага приділяється питанням інформаційної безпеки та захисту даних, зокрема методам шифрування та захищеного передавання інформації в мережах Internet of Drones (IoD) [1].

Одним із перспективних підходів до вирішення цих проблем є використання віртуальних приватних мереж (Virtual Private Networks, VPN). VPN вже широко застосовуються для захисту комунікацій у традиційних мережах, але їхній потенціал у контексті роїв БПЛА потребує додаткового дослідження. Забезпечення надійного і безпечного зв'язку між дронами в рою є одним з ключових завдань, яке вимагає розроблення та впровадження інноваційних рішень.

Ефективне управління роєм БПЛА вимагає стабільної, швидкої та захищеної мережі зв’язку, здатної протистояти зовнішнім загрозам і забезпечувати гнучкість у динамічних умовах. Це ставить перед розробниками задачі пошуку рішень, які б відповідали високим вимогам до безпеки та продуктивності.

Таким чином, дослідження можливостей застосування VPN для забезпечення безпеки та оптимізації комунікацій у роєвих системах БПЛА є актуальним завданням, що потребує подальшого вивчення та розробки інноваційних підходів.

1.2. Аналіз публікацій

Аналіз літератури показує, що основні виклики у цій сфері пов'язані з унікальними характеристиками роїв БПЛА. У роботі [2] аналізуються і розробляються моделі кібербезпеки флотів (системи роїв БПЛА) з урахуванням різних типів порушників і загроз. Однак не враховуються можливості VPN як ефективних контрзаходів.

Постійний рух БПЛА призводить до частих змін у структурі мережі, що ускладнює застосування традиційних методів захисту [3].

Обмежена обчислювальна потужність і енергоресурси БПЛА значно знижують можливості застосування складних криптографічних алгоритмів.[4].

У дослідженні [5] аналізується вплив кібератак на загрози функцій безпеці автономних транспортних систем, зокрема, роїв БПЛА з використанням так званої методики SISMECA.

БПЛА можуть бути фізично захоплені противником, що створює ризик компрометації ключів шифрування [6].

У роботі [7] аналізуються так звані кіберчастотні вразливості БПЛА та їх вплив на безпеку.

Зі збільшенням кількості БПЛА у рою зростає складність управління безпекою мережі [8]. Існуючі дослідження пропонують різні підходи до вирішення цих проблем, включаючи використання легких криптографічних протоколів [9], динамічне управління ключами [10], та застосування технологій блокчейну [11]. Однак, більшість цих рішень мають обмеження щодо масштабованості або вимагають значних обчислювальних ресурсів.

У цьому контексті, VPN, а також RIS (Reconfigurable Intelligent Surface, реконфігуровні інтелектуальні поверхні) є перспективними технологіями, які потенційно можуть розв’язувати багато з вищезазначених проблем. VPN-технології забезпечують шифрування даних та створення захищених тунелів між вузлами мережі [12, 13], в той час як RIS пропонують гнучку архітектуру, яка може адаптуватися до динамічних змін у мережі [14].

Проте, незважаючи на потенційні переваги, ефективність VPN та RIS у контексті роїв БПЛА залишається недостатньо вивченою. Існуючі дослідження здебільшого фокусуються на застосуванні цих технологій у статичних або повільно змінюваних мережах [15, 16]. Таким чином, існує потреба у детальному аналізі їх ефективності та придатності для забезпечення безпеки зв'язку в динамічних мережах роїв БПЛА.

VPN-технології займають особливе місце серед цих методів завдяки своїй здатності забезпечувати конфіденційність та цілісність даних. Віртуальні приватні мережі (VPN) стали незамінними інструментами для забезпечення конфіденційності та захисту даних у сучасних комунікаційних мережах. VPN створює захищене з'єднання через публічну мережу, таку як інтернет, дозволяючи користувачам передавати дані без ризику перехоплення сторонніми. Для рою БПЛА це означає, що всі команди управління, телеметрія, і дані, що передаються між дронами та центральною станцією управління, будуть надійно захищені від зовнішніх загроз.

Таким чином, на підставі огляду публікацій робимо висновок про необхідність подальшого дослідження інтеграції VPN та RIS у контексті роєвих систем БПЛА. Хоча обидві технології вже продемонстрували свою ефективність у забезпеченні захисту даних та оптимізації мережевих з'єднань у менш динамічних середовищах, їх адаптація до умов рою БПЛА потребує додаткового аналізу. Особливо важливим є вивчення можливостей VPN у забезпеченні безпечного зв’язку при високих швидкостях руху дронів та частих змінах топології мережі, а також оцінка здатності RIS динамічно переналаштовувати сигнали для підтримки стабільного зв'язку в умовах складних і мінливих середовищ. Ці аспекти є критично важливими для підвищення ефективності та надійності роєвих систем БПЛА в сучасних умовах.

1.3. Мета, задачі і структура статті

Ця стаття має на меті дослідити можливість інтеграції технологій віртуальних приватних мереж та реконфігуровних інтелектуальних поверхонь для оптимізації мережевого управління та забезпечення безпечної комунікації у роєвих системах БПЛА. Особлива увага приділяється аналізу переваг і викликів, пов'язаних із застосуванням цих технологій у реальних умовах.

Вирішуються наступні задачі:

– дослідження сучасного стану технологій VPN та RIS та їх потенціалу для застосування в роєвих системах БПЛА (розділ 2);

– аналіз архітектури мережі та методів інтеграції VPN і RIS у роєві системи БПЛА, включаючи оцінку впливу цих технологій на продуктивність та безпеку мережі (розділ 3);

– оцінка результатів симуляцій з

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

використанням NS-3 (Network Simulator 3) для визначення ефективності VPN та RIS в різних сценаріях роботи рою БПЛА (розділ 4);

– формулювання висновків і рекомендацій щодо подальшого впровадження та дослідження VPN та RIS у роєвих системах БПЛА (розділ 5).

Структура статті включає п'ять розділів. У першому розділі викладено актуальність теми та сформульовано мету, завдання та структуру дослідження. Другий розділ зосереджується на аналізі актуальних досягнень у сфері технологій VPN (віртуальних приватних мереж) та RIS. У цьому контексті особлива увага приділяється вивченню можливостей їх ефективного впровадження в систему управління роями безпілотних літальних апаратів (БПЛА). Третій розділ присвячено детальному розгляду структури мережею. Особливо увага приділяється аналізу того, як застосування технологій VPN та RIS впливає на ефективність функціонування та рівень захищеності роєвих систем. У цій частині роботи досліджуються ключові аспекти взаємодії між компонентами мережі та оцінюється їх вплив на загальну продуктивність системи. У четвертому розділі представлено детальний аналіз результатів проведеного симуляційного експерименту. Ця частина зосереджена на демонстрації та оцінці практичної ефективності впровадження технологій VPN та RIS в роєвих системах БПЛА. Нарешті, розділ 5 підсумовує основні висновки та надає рекомендації для подальших досліджень.

2. Інтеграція VPN та RIS у роєвих системах БПЛА

2.1. Архітектура мережі

Reconfigurable Intelligent Surfaces (RIS) — це новітня технологія, яка передбачає використання спеціальних поверхонь, що можуть змінювати характеристики відбиття радіохвиль. RIS складаються з великої кількості елементів, кожен з яких може налаштовувати фазу і амплітуду відбитих хвиль, спрямовуючи сигнал у потрібному напрямку або створюючи зони зі зменшеними перешкодами.

У контексті БПЛА RIS можуть бути застосовані для оптимізації сигналу, покращення якості зв’язку та зменшення впливу перешкод. Використання реконфігурованих інтелектуальних поверхонь (RIS) в системах з безпілотними літальними апаратами суттєво підвищує ефективність роботи роїв. RIS дозволяють адаптувати бездротове середовище до потреб системи, покращуючи якість сигналу та збільшуючи дальність зв'язку. Крім того, завдяки здатності керувати поширенням радіосигналу, RIS можуть зменшити енергоспоживання дронів, що є особливо важливим для тривалих місій.

Інтеграція VPN та RIS у роєві системи БПЛА відкриває нові можливості для підвищення безпеки та ефективності комунікацій. Загалом архітектура мережі представлена на рисунку 1.

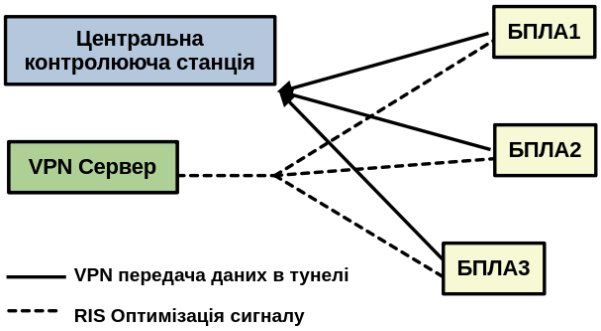

Рис. 1. Інтеграція VPN та RIS у роєві системи БПЛА

VPN забезпечує захист даних і конфіденційність зв'язку, тоді як RIS оптимізує фізичний рівень передачі сигналу, що дозволяє ефективно використовувати доступні ресурси і знижувати ризик збоїв у зв'язку. Інтеграція VPN та RIS забезпечує комплексний підхід до захисту роїв БПЛА.

VPN гарантує конфіденційність переданих даних, створюючи безпечний тунель для комунікацій. Зі свого боку, RIS оптимізують маршрутизацію сигналу, забезпечуючи стабільні та надійні з'єднання між дронами. Така синергія технологій створює багатошарову систему захисту, що значно ускладнює для зловмисників проникнення в мережу рою.

Для ефективного управління роєм БПЛА необхідно створити складну та багатошарову архітектуру мережі, яка поєднує VPN та RIS. Основні компоненти цієї архітектури включають такі компоненти:

– центральна станція управління (ЦСУ);
– VPN-канали між ЦСУ та БПЛА;
– роєва комунікаційна мережа;
– Reconfigurable Intelligent Surfaces (RIS).

ЦСУ - це головний центр координації, який здійснює керування роєм БПЛА. ЦСУ підключена до глобальної мережі через VPN, що забезпечує надійний та захищений канал зв'язку з кожним дроном.

Кожен дрон у рою з'єднаний із ЦСУ через VPN, що дозволяє забезпечити шифрування даних і анонімність з'єднань. Це особливо важливо у випадках, коли БПЛА працюють у ворожому середовищі або здійснюють операції високої секретності.

Окрім VPN-каналів, між самими БПЛА також існують прямі канали зв’язку, які можуть бути

оптимізовані за допомогою RIS. Це дозволяє кожному дрону адаптуватися до умов середовища та забезпечувати максимально ефективне управління роєм.

RIS встановлюються на стратегічних позиціях, що можуть бути як на самих дронах, так і на наземних або повітряних платформах. RIS оптимізують маршрути сигналу, підвищуючи ефективність комунікацій та зменшуючи ризик перешкод.

2.2. Розподіл ресурсів

Розподіл ресурсів у роєвій системі БПЛА має ключове значення для забезпечення стабільної роботи всієї мережі. Використання VPN та RIS дозволяє реалізувати динамічний та ефективний підхід до управління ресурсами.

RIS дозволяють дронам оптимально використовувати доступні частоти та канали зв'язку, зменшуючи інтерференцію між сигналами і підвищуючи пропускну здатність мережі. Це дозволяє значно покращити якість зв'язку в складних умовах, таких як міська забудова або райони з великою кількістю перешкод.

VPN дозволяють динамічно перенаправляти трафік, розподіляючи його між різними маршрутизаторами і серверами. Це забезпечує гнучкість та надійність мережі, особливо в умовах підвищеного навантаження або при атаках на мережу.

На рисунку 2 зображено комбінацію VPN та RIS, яка дозволяє забезпечити рою БПЛА стабільний зв'язок і доступ до необхідних ресурсів навіть в умовах зовнішніх загроз або обмежених ресурсів. Це забезпечує більшу автономність і гнучкість дій рою.

2.3. Забезпечення безпеки та конфіденційності

Захист даних і забезпечення конфіденційності є критично важливими аспектами роботи рою БПЛА, особливо у випадках, коли дрони виконують завдання в умовах підвищеного ризику. Інтеграція VPN та RIS забезпечує багаторівневий підхід до безпеки.

Всі дані, що передаються між ЦСУ та дронами, шифруються за допомогою VPN. Це гарантує, що навіть у випадку перехоплення сигналу, зловмисник не зможе отримати доступ до важливої інформації. RIS не тільки покращують якість сигналу, але й можуть бути налаштовані таким чином, щоб зменшити ймовірність перехоплення сигналу або направити сигнал так, щоб він був недоступний для сторонніх пристроїв. Використання VPN забезпечує захист від кібератак, таких як спуфінг або перехоплення, а RIS дозволяють створювати динамічні середовища, у яких зловмиснику важко прогнозувати поведінку сигналу.

Сегментація віртуальної локальної мережі в статичних і динамічних мережах VPN дозволяє створити «тунель» між двома взаємодіючими пристроями, який забезпечує захищений зв’язок і безпечний перегляд Інтернету. У такій конфігурації вихідний пакет (включно з даними та їхніми заголовками, що можуть містити інформацію, як наприклад, адреси джерела й призначення, тип даних, довжина та порядковий номер пакета) шифрується. Потім цей пакет інкапсулюється в іншому пакеті, що містить лише IP-адреси двох пристроїв, які взаємодіють (наприклад, маршрутизаторів). Це захищає трафік і його вміст від несанкціонованого доступу, і лише пристрої з

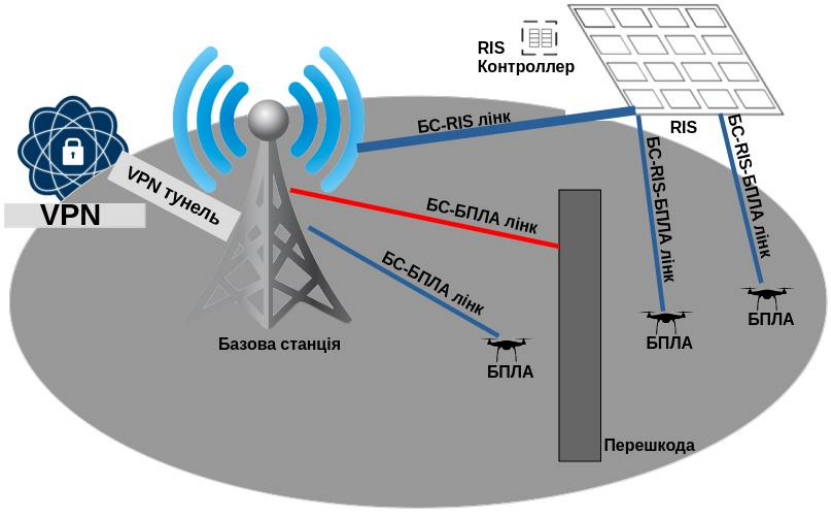

Рис. 2. Інтеграція VPN та RIS у роєві системи БПЛА

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

правильним «ключем» можуть підключитися до VPN. Мережеві пристрої між клієнтом і сервером не можуть отримати доступ до даних або переглянути їх. Основна різниця між HTTPS (SSL/TLS) і VPN полягає в тому, що HTTPS шифрує тільки дані в пакеті, тоді як у VPN весь пакет може бути зашифрований та інкапсульований для створення захищеного «тунелю». Таким чином, VPN надає безпечний спосіб підключення до приватної мережі через незахищену публічну мережу, таку як Інтернет.

Альтернативою VPN є технологія віртуальної локальної мережі (VLAN). Вона дозволяє логічно групувати мережі незалежно від їх фізичного розташування та сегментувати мережу на віртуальні мережі або групи (цю функцію підтримують більшість мережевих комутаторів). Лише користувачі певної групи можуть обмінюватися даними або отримувати доступ до конкретних ресурсів у мережі. Основним протоколом для налаштування VLAN є IEEE 802.1Q, який додає додаткові байти до кожного кадру або пакета, щоб вказати, до якої віртуальної мережі належить пакет.

3. Симуляція використання VPN та RIS у рої БПЛА для оцінки ефективності інтеграції

З масовим поширенням систем БПЛА та різноманітних типів мобільності (автономна, літаюча, транспортна тощо) сучасні мережі повинні враховувати ефект руху, який значно відображається на фізичному рівні залучених пристроїв (доплерівські зсуви, затухання сигналу, втрати на шляху, відбиття, заломлення тощо). Стандартні технології, такі як VLAN і VPN, які спочатку були розроблені для статичних мереж, не адаптовані для ефективного управління мобільністю, тому пропонується рішення комбінованого використання VPN та RIS. Для оцінки ефективності інтеграції VPN та RIS у роєві системи БПЛА було проведено серію симуляцій з використанням сучасних інструментів моделювання мережевих і комунікаційних систем. Метою дослідження було порівняти продуктивність і безпеку роєвої системи з використанням технологій VPN і RIS, а також без них.

Для оцінки ефективності VPN та RIS було розроблено симуляційну модель з використанням програмного забезпечення NS-3 (Network Simulator 3). Вихідня значення параметрів для моделювання:

- кількість БПЛА: від 10 до 100;
- модель руху: Random Waypoint Model;
- швидкість БПЛА: 0-20 м/с;
- розмір зони польоту: 1000м х 1000м х 100м;
- протокол маршрутизації: AODV (Ad hoc On-Demand Distance Vector);
- тип трафіку: UDP з постійною швидкістю передачі даних.

Вибрано декілька різних сценаріїв роботи роєвих систем, включаючи міське середовище з високою щільністю забудови, відкриті простори та складні багаторівневі середовища. Вимірювались такі показники, як пропускна здатність мережі, затримка сигналу, енергоспоживання та якість передачі даних. Оцінювались рівень шифрування даних, стійкість до атак на мережу, а також ймовірність перехоплення сигналу та спуфінгу.

Результати симуляцій показали значне покращення продуктивності мережі при використанні RIS у поєднанні з VPN. Зокрема, у сценаріях з високою щільністю забудови RIS дозволили підвищити пропускну здатність мережі на 30-50% завдяки оптимізації маршрутизації сигналу. Використання RIS дозволило зменшити затримку сигналу на 20-35%, що особливо важливо для координації рою в реальному часі. Завдяки спрямованому відбиттю сигналу RIS сприяли зменшенню енергоспоживання на 15-25%, що дозволило дронам працювати довше без дозаправки або підзарядки.

За результатами симуляції встановлено, що впровадження VPN значно підвищило рівень безпеки роєвих систем. Шифрування даних через VPN знизило ризик перехоплення сигналу на 95%, що майже виключило можливість отримання доступу до конфіденційних даних. Поєднання VPN та RIS забезпечило високий рівень стійкості до кібератак, зокрема до атак типу "man-in-the-middle" та спуфінгу, що на 90% зменшило ймовірність успішного вторгнення в мережу. Використання RIS дозволило динамічно перенаправляти сигнал у разі виявлення загрози, що знизило ймовірність перехоплення або блокування комунікацій.

4. Аналіз результатів дослідження

Результати дослідження підтверджують, що інтеграція VPN та RIS у роєві системи БПЛА значно покращує їхню продуктивність та безпеку. Спрямована оптимізація сигналу за допомогою RIS у поєднанні з надійним шифруванням даних через VPN створює комплексне рішення, яке може бути ефективно використане в умовах складних і динамічних середовищ. Значне підвищення пропускної здатності та зниження затримки забезпечують кращу координацію та ефективність рою. Економія енергії дозволяє продовжити тривалість місій без потреби в частих підзарядках.

Високий рівень безпеки робить систему стійкою до кіберзагроз та забезпечує конфіденційність даних.

Крім того, впровадження RIS дозволило значно підвищити стійкість мережі до фізичних перешкод та сигналів-заглушувачів, що особливо важливо в умовах міського середовища з високою щільністю забудови. Це дозволяє забезпечити стабільний зв'язок навіть у складних середовищах, де традиційні методи зв'язку зазнають труднощів. Поєднання VPN та RIS не тільки захищає дані, але й забезпечує їх безперебійне передавання, що критично важливо для успішного виконання складних місій рою БПЛА.

Результати симуляційних досліджень також довели, що використання VPN у поєднанні з RIS дозволяє знизити ризик перехоплення сигналу та інших видів атак на мережу. Це забезпечує додатковий рівень безпеки для військових та цивільних операцій, де захист інформації є критично важливим. Система, що використовує обидві технології, показала високу стійкість до кібератак і надійність, навіть у випадках спроб порушення зв'язку. Важливо також зазначити, що такий підхід сприяє кращому управлінню ресурсами, зокрема оптимізації розподілу каналів зв'язку та зменшенню навантаження на мережу.

Таким чином, отримані результати підтверджують високу ефективність інтеграції VPN та RIS для роєвих систем БПЛА. Використання цих технологій не лише підвищує продуктивність і безпеку, але й сприяє довготривалій та надійній роботі рою в різних умовах. Це відкриває нові перспективи для використання БПЛА в складних кіберфізичних середовищах та забезпечує їхню готовність до майбутніх викликів, пов'язаних із розвитком технологій та зростаючими вимогами до безпеки.

5. Висновки

У статті проведено детальний аналіз інтеграції технологій VPN та Reconfigurable Intelligent Surfaces (RIS) у роєві системи безпілотних літальних апаратів (БПЛА). Основним результатом дослідження є підтвердження того, що комбінація VPN і RIS дозволяє значно покращити продуктивність, безпеку та стійкість роєвих систем БПЛА в складних і динамічних середовищах.

Інтеграція RIS дозволяє значно покращити якість сигналу, в складних середовищах, що є одним з основних обмежень сучасних бездротових мереж. Використання RIS сприяє зменшенню енергоспоживання, що дозволяє продовжити тривалість місій БПЛА без необхідності частих підзарядок. VPN забезпечує надійне шифрування та захист від кібератак, таких як перехоплення сигналу або спуфінг. Поєднання з RIS створює багатошаровий захист, який суттєво підвищує стійкість системи до загроз.

Використання VPN та RIS дозволяє роєвій системі БПЛА швидко адаптуватися до змін у середовищі та оперативно реагувати на потенційні загрози, що забезпечує стабільність і надійність мережі.

Хоча інтеграція VPN та RIS у роєві системи БПЛА показала високі результати, існує кілька напрямків для подальших досліджень. Подальші дослідження можуть зосередитися на впровадженні RIS у різні типи середовищ і сценаріїв, що дозволить ще більше оптимізувати мережеві комунікації. З огляду на зростаючу складність та агресивність кіберзагроз, підсилених засобами штучного інтелекту (ШІ), вкрай важливо розглянути можливість використання ШІ для захисту кіберактивів роїв БПЛА [17]. Важливо розробити нові алгоритми та методи управління VPN для забезпечення більшої стійкості до зростаючих кібератак і мінімізації затримок у складних мережах. Проведення польових випробувань і експериментів з реальними роєвими системами БПЛА дозволить підтвердити отримані результати та адаптувати їх до практичних умов. Оцінка вартості впровадження та експлуатації технологій VPN та RIS у БПЛА роях може допомогти розробити оптимальні моделі для їх комерційного використання.

Конфлікт інтересів

Автор заявляє, що немає конфлікту інтересів щодо цього дослідження, фінансового, особистого, авторського чи іншого, який міг би вплинути на дослідження та його результати, представлені в статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту

Автор підтверджує, що не використовував технології штучного інтелекту при створенні представленої роботи.

Автор прочитав та погодився з опублікованою версією рукопису

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

Література

1. A robust Internet of Drones security surveillance communication network based on IOTA [Text] / S. Gilani, A. Anjum, A. Khan, M. H. Syed, S. A. Moqurrab, & G. Srivastava // Internet of Things. – 2024. – Article No. 101066. DOI: 10.1016/j.iot.2024.101066.

2. Zemlianko, H. Ensuring Cybersecurity of the Cyber Physical System of Combined Fleets of Unmanned Aerial, Ground and Sea Vehicles [Text] / H. Zemlianko, V. Kharchenko // Integrated Computer Technologies in Mechanical Engineering – 2023. ICTM 2023. Lecture Notes in Networks and Systems. – Springer, Cham, 2024. – Vol. 996. – P. 392-403. DOI: 10.1007/978-3-031-60549-9_29.

3. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems [Text] / M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, & M. A. Debbah // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, iss. 3. – P. 2334-2360. DOI: 10.1109/comst.2019.2902862.

4. Mishra, D. A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements [Text] / D. Mishra, E. Natalizio // Computer Networks. – 2020. – Vol. 182. – Article No. 107451. DOI: 10.1016/j.comnet.2020.107451.

5. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection [Text] / O. Illiashenko, V. Kharchenko, I. Babeshko, H. Fesenko, & F. Di Giandomenico // Entropy. – 2023. – Vol. 25, iss. 8. – Article No. 1123. DOI: 10.3390/e25081123.

6. Interference Analysis for UAV Connectivity over LTE Using Aerial Radio Measurements [Text] / I. Kovacs, R. Amorim, H. C. Nguyen, J. Wigard, P. Mogensen // IEEE 86th Vehicular Technology Conference (VTC-Fall). – Toronto, ON, Canada, 2017. – P. 1-6. DOI: 10.1109/VTCFall.2017.8287891.

7. Певнев, В. Кібербезпека безпроводових смарт-систем: канали втручань та радіочастотні вразливості [Текст] / В. Певнев, В. Торяник, & В. Харченко // Радіоелектронні і комп'ютерні системи. – 2020. – № 4. – С. 79-92. DOI: 10.32620/reks.2020.4.07.

8. EuroDRONE, A European UTM Testbed for U-Space [Text] / V. Lappas, G. Zoumponos, V. Kostopoulos, H. Y. Shin, A. Tsourdos, M. Tantarini, D. Shmoko, J. Munoz, N. Amoratis, A. Maragkakis, T. Machairas, & A. Trifas // International Conference on Unmanned Aircraft Systems (ICUAS 2020). – Athens, Greece, 2020. – P. 1766-1774. DOI: 10.1109/ICUAS48674.2020.9214020.

9. Donenfeld J. A. WireGuard: Next Generation Secure Network Tunnel [Video] / A. J. Donenfeld // Youtube. – 2020. – Available at: https://www.youtube.com/watch?v=88GyLoZbDNw (accessed: 12.05.2024).

10. Reconfigurable Intelligent Surfaces (RIS); Technological challenges, architecture and impact on standardization [Text] // ETSI GR RIS 002 v1.1.1. – F-06921 Sophia Antipolis Cedex - FRANCE, 2023. – 33 p. – Available at: https://www.etsi.org/deliver/etsi_gr/RIS/001_099/002/01.01.01_60/gr_RIS002v010101p.pdf. (accessed: 13.05.2024).

11. Koulianos, A. Blockchain Technology for Secure Communication and Formation Control in Smart Drone Swarms [Text] / A. Koulianos, & A. Litke // Future Internet. – 2023. – Vol. 15, iss. 10. – Article No. 344. DOI: 10.3390/fi15100344.

12. Aljehani, M. Multi-UAV tracking and scanning systems in M2M communication for disaster response [Text] / M. Aljehani, & M. Inoue // IEEE 5th Global Conference on Consumer Electronics. – Kyoto, Japan, 2016. – P. 1-2. DOI: 10.1109/GCCE.2016.7800524.

13. Locke, J. Can Drones Be Hacked, Tracked, and Used to Carry Passengers? [Electronic resource] / J. Locke // DIGI International. – 2023. – Available at: https://www.digi.com/blog/post/can-drones-be-hacked-tracked-and-carry-passengers (accessed 14.05.2024).

14. Reconfigurable Intelligent Surfaces: A signal processing perspective with wireless applications [Text] / E. Björnson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti, & E. de Carvalho // IEEE Signal Processing Magazine. – 2022. – Vol. 39, No. 2. – P. 135-158. DOI: 10.1109/msp.2021.3130549.

15. Security and Privacy Issues of UAV: A Survey [Text] / Y. Zhi, Z. Fu, X. Sun, & J. Yu // Mobile Networks and Applications. – 2019. – Vol. 25, No. 1. – P. 95-101. DOI: 10.1007/s11036-018-1193-x.

16. Enhancing Wireless Networks with Attention Mechanisms: Insights from Mobile Crowdsensing [Electronic resource] / Y. Yang, H. Du, Z. Xiong, D. Niyato, A. Jamalipour, & Z. Han // arXiv. – 2024. – Article No. 2407.15483v1. – P. 1-9. – Available at: https://arxiv.org/html/2407.15483v1 (accessed: 14.05.2024).

17. Veprytska, O. Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining [Electronic resource] / O. Veprytska, V. Kharchenko // 5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2024), March 28, 2024, Khmelnytskyi. – 2024. – P. 1-19. – Available at: https://ceur-ws.org/Vol-3675/paper26.pdf. (accessed: 14.05.2024).

References

1. Gilani, S. M., Anjum, A., Khan, A., Syed, M. H., Moqurrab, S. A., & Srivastava, G. A robust Internet of Drones security surveillance communication network based on IOTA. *Internet of Things*, 2024, article no. 101066. DOI: 10.1016/j.iot.2024.101066.

2. Zemlianko, H., & Kharchenko, V. Ensuring Cybersecurity of the Cyber Physical System of Combined Fleets of Unmanned Aerial, Ground and Sea Vehicles, *Integrated Computer Technologies in Mechanical Engineering – 2023. ICTM 2023. Lecture Notes in Networks and Systems*, Springer, Cham, 2024, vol. 996, pp. 392-403. DOI: 10.1007/978-3-031-60549-9_29.

3. Mozaffari, M., Saad, W., Bennis, M., Nam, Y. H., & Debbah, M. A. Tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, iss. 3, pp. 2334-2360. DOI: 10.1109/comst.2019.2902862.

4. Mishra, D., & Natalizio, E. A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements. *Computer Networks*, 2020, vol. 182, article no. 107451. DOI: 10.1016/j.comnet.2020.107451.

5. Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., & Di Giandomenico, F. Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. *Entropy*, 2023, vol. 25, iss. 8, article no. 1123. DOI: 10.3390/e25081123.

6. Kovacs, I., Amorim, R., Nguyen, H. C., Wigard, J., & Mogensen, P. Interference analysis for UAV connectivity over LTE using aerial radio measurements. *IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, Canada, 24–27 September 2017, 2017, pp. 1-6. DOI:10.1109/VTCFall.2017.8287891.

7. Pevnev, V., Torianyk, V., & Kharchenko, V. Kiberbezpeka bezprovodovykh smart-system: kanaly vtruchan′ta radiochastotni vrazlyvosti [Cyber security of wireless smart systems: channels of intrusions and radio frequency vulnerabilities], *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4, pp. 79-92. DOI: 10.32620/reks.2020.4.07. (In Ukrainian).

8. Lappas, V., Zoumponos, G., Kostopoulos, V., Shin, H., Tsourdos, A., Tantarini, M., Shmoko, D., Munoz, J., Amoratis, N., Maragkakis, A., Machairas, T., & Trifas, A. EuroDRONE, A European UTM Testbed for U-Space. *International Conference on Unmanned Aircraft Systems (ICUAS 2020)*, Athens, Greece, 1–4 September 2020, pp. 1766-1774. DOI: 10.1109/ICUAS48674.2020.9214020.

9. Donenfeld, J. A. *WireGuard: Next Generation Secure Network Tunnel*. YouTube. 2020. Avaiable at: https://www.youtube.com/watch?v=88GyLoZbDNw (accessed: 12.05.2024).

10. *Reconfigurable Intelligent Surfaces (RIS); Technological challenges, architecture and impact on standardization*. ETSI GR RIS 002 v1.1.1. F-06921 Sophia Antipolis Cedex - FRANCE, 2023. 33 p. Available at: https://www.etsi.org/deliver/etsi_gr/RIS/001_099/002/01.01.01_60/gr_RIS002v010101p.pdf. (accessed: 13.05.2024).

11. Koulianos, A., & Litke, A. Blockchain Technology for Secure Communication and Formation Control in Smart Drone Swarms. *Future Internet*, 2023, vol. 15, iss. 10, article no. 344. DOI: 10.3390/fi15100344.

12. Aljehani, M., & Inoue, M. Multi-UAV tracking and scanning systems in M2M communication for disaster response. *IEEE 5th Global Conference Consumer Electronics*, Kyoto, Japan, 2016, pp. 1-2. DOI: 10.1109/GCCE.2016.7800524.

13. Locke, J. *Can Drones Be Hacked, Tracked, and Used to Carry Passengers?* DIGI International, 2023. Available at: https://www.digi.com/blog/post/can-drones-be-hacked-tracked-and-carry-passengers (accessed 14.05.2024).

14. Björnson, E., Wymeersch, H., Matthiesen, B., Popovski, P., Sanguinetti, L., & De Carvalho, E. Reconfigurable Intelligent Surfaces: A signal processing perspective with wireless applications. *IEEE Signal Processing Magazine*, 2022, vol. 39, iss. 2, pp. 135-158. DOI: 10.1109/msp.2021.3130549.

15. Zhi, Y., Fu, Z., Sun, X., & Yu, J. Security and Privacy Issues of UAV: A Survey. *Mobile Networks and Applications*, 2019, vol. 25, no. 1, pp. 95-101. DOI: 10.1007/s11036-018-1193-x.

16. Yang, Y., Du, H., Xiong, Z., Niyato, D., Jamalipour, A., & Han, Z. Enhancing Wireless Networks with Attention Mechanisms: Insights from Mobile Crowdsensing. *arXiv*, 2024, article no. 2407.15483v1, pp. 1-9. Available at: https://arxiv.org/html/2407.15483v1 (accessed: 14.05.2024).

17. Veprytska, O., & Kharchenko, V. Analysis of AI powered attacks and protection of UAV assets: quality model-based assessing cybersecurity of mobile system for demining. *5th International Workshop on Intelligent Information Technologies and Systems of Information Security (IntelITSIS'2024)*, March 28, 2024, Khmelnytskyi, 2024, pp. 1-19. Available at: https://ceur-ws.org/Vol-3675/paper26.pdf. (accessed: 14.05.2024).

Надійшла до редакції 15.05.2024, розглянута на редколегії 15.08.2024

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

USING VPNS AND RIS TO ENSURE COMMUNICATION SECURITY IN DYNAMIC UAV SWARM NETWORKS: INTEGRATION PATHS, RESOURCE ALLOCATION, AND SIMULATION RESULTS

Ruslan Demura

The **subject of this paper** is the integration of virtual private networks (VPN) and Reconfigurable Intelligent Surfaces (RIS) technologies into swarm systems of unmanned aerial vehicles (UAVs). The **goal** is to investigate the possibilities of improving the performance and security of UAV swarm systems using VPNs for data encryption and protection, as well as RIS for optimizing signal routing in complex environments. The **tasks** to be solved are: to analyze existing approaches to ensure the security and performance of networks in UAV swarm systems, evaluating the effectiveness of VPN and RIS integration in various swarm scenarios, such as urban environments with high building density, open spaces, and complex multi-level environments, and conducting simulation studies to compare the performance and security of UAV swarm systems with and without VPN and RIS. The **methods** used are modeling and simulation of network and communication systems using NS-3 (Network Simulator 3). The simulation includes various scenarios of UAV swarm systems, which allows us to compare the impact of VPN and RIS on communication efficiency. The following **results** were obtained: the integration of VPN and RIS into UAV swarm systems can significantly improve network performance, reduce signal delays, increase energy efficiency, and ensure a high level of data security. Simulation studies have demonstrated that VPN provides reliable data protection and reduces the risk of interception, while RIS optimizes signal transmission in complex environments, improving the overall swarm efficiency. **Conclusions**. The results demonstrate that the integration of VPNs and RIS into UAV swarm systems is a promising approach to ensure the security and efficiency of communications in a dynamic environment. The results indicate the need for further research to improve these technologies, particularly in the field of adaptation to new threats and energy efficiency.

Keywords: unmanned aerial vehicles; swarm systems; virtual private networks; reconfigurable intelligent surfaces; network security; signal optimization.

Демура Руслан Іванович – магістр кібербезпеки, асистент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Ruslan Demura – Master of Cybersecurity, Assistant at the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine.
e-mail: r.i.demura@csn.khai.edu, ORCID: 0009-0003-2248-2565.