УДК 004.7 DOI: 10.31673/2786-8362.2025.025427

Яковець В.П.; Руденко С.В.;
Колесніков О.Е.; Швець Д.М.;
Бойко О.В.

КОНФІДЕНЦІЙНА ПЕРЕДАЧА ДАНИХ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ З ІНТЕГРАЦІЄЮ БПЛА

Yakovets V.P., Rudenko S.V., Kolesnikov O.E., Shvets D.M., Boyko O.V. Confidential data transfer in telecommunications systems with UAV integration. The article examines problems and solutions for ensuring confidentiality in telecommunications systems with integrated unmanned aerial vehicles (UAVs). It analyzes the main threats, such as passive eavesdropping, jamming, DoS/DDoS, GNSS spoofing, MitM, false data injection, ML attacks, and physical capture, as well as their impact on security, privacy, and mission reliability. A multi-level strategy for protecting the physical security of the channel is proposed, using artificial noise, directional beamforming, cooperative suppression, and trajectory and power optimization. The role of MEC/edge in secure offloading and in supporting hardware-based authentication and updates is considered separately. A mathematical formulation of the problem of maximizing the average secrecy rate with kinematic and energy constraints is presented, and practical solution methods (SCA, SDR, stepwise optimization) are described. The paper highlights the "security-delay-energy" trade-offs and provides recommendations for integrating data transmission security and fault tolerance solutions in scalable communication networks with UAV integration.

Keywords: unmanned aerial vehicles, communication confidentiality, artificial noise, trajectory optimization

Яковець В.П., Руденко С.В., Колесніков О.Е., Швець Д.М., Бойко О.В. Конфіденційна передача даних в телекомунікаційних системах з інтеграцією БПЛА. У статті досліджено проблеми та рішення для забезпечення конфіденційності в телекомунікаційних системах із інтегрованими безпілотними літальними апаратами (БПЛА). Проаналізовано основні загрози, такі як пасивне підслуховування, заглушення, DoS/DDoS, GNSS-спуфінг, MitM, ін'єкція фальшивих даних, атаки на ML та фізичне захоплення, а також їхній вплив на безпеку, приватність та надійність місій. Запропоновано міжрівневу стратегію захисту фізичної безпеки каналу за рахунок штучного шуму, напрямленого формування променю, кооперативного пригнічення та оптимізації траєкторії й потужності. Окремо розглянуто роль MEC/edge у безпечному оффлоадингу й у підтримці апаратно-обґрунтованої автентифікації та оновлень. Наведено математичну постановку задачі максимізації середньої швидкості секретної передачі з кінематичними та енергетичними обмеженнями та описано практичні методи розв'язання (SCA, SDR, поетапна оптимізація). Робота підкреслює компроміси «секретність-затримка-енергія» і надає рекомендації щодо інтеграції рішень безпеки передачі даних і відмовостійкості в масштабованих мережах зв'язку з інтеграцією БПЛА.

Ключові слова: безпілотні літальні апарати, конфіденційність зв'язку, штучний шум, оптимізація траєкторії

Вступ

Безпілотні літальні апарати (БПЛА) швидко інтегруються в цивільну та військову інфраструктуру зв'язку, оскільки забезпечують гнучке покриття на великій площі та можливості обчислень на периферії за запитом; водночас їхня залежність від відкритих радіоканалів з лінією прямої видимості та висока мобільність роблять системи з інтеграцією БПЛА вразливими до прослуховування, заглушення, захоплення каналів зв'язку управління та інших атак, що можуть підірвати конфіденційність, безпеку й безперервність надання послуг.

Оскільки самі БПЛА та багато периферійних/IoT-кінцевих пристроїв мають обмежені енергетичні та обчислювальні ресурси, традиційні «важкі» криптографічні механізми часто непридатні, що створює нагальну потребу в легких міжрівневих заходах захисту (зокрема заходах на фізичному рівні, безпечному оффлоадінгу до MEC, легких механізмах автентифікації та механізмах довіри), які збалансовують конфіденційність, затримку та енергоспоживання.

Аналіз останніх досліджень. Дослідження в сфері безпеки зв'язку показують, що доповнення класичної криптографії інформаційно-теоретичними підходами (безпека

© Яковець В.П., Руденко С.В., Колесніков О.Е., Швець Д.М., Бойко О.В. 2025

фізичного рівня, PLS), оптимізацією траєкторії та розподілу ресурсів, а також використанням нових інструментів (машинного навчання, розподілених реєстрів) може суттєво зменшити ризики перехоплення й заглушення, зберігаючи при цьому продуктивність у режимі реального часу, необхідну для критично важливих місій за участю БПЛА. В [1] аналізуються загрози, механізми захисту приватності й аутентифікації, стійкість зв'язку та ефективні стратегії збору/агрегації даних, а також окреслюються перспективні рішення (блокчейн, федеративне/децентралізоване навчання, ШІ, гібридні оптико-RF канали) для надійної та захищеної передачі в БПЛА-системах. В [2] запропоновано гібридну схему захисту для БПЛА-вузлів – кооперативне глушіння на основі точки призначення разом з hybrid-SWIPT для підвищення інформаційної безпеки. В [3] запропоновано модель і захищений протокол для БПЛА-вузлів з SWIPT, виведено SNR приймача/підслуховувача, ймовірність зв'язку та нижні межі рівню секретності. В [4] запропоновано PLS-фреймворк для БПЛА-IRS систем із AN і SWIPT через спільну оптимізацію формування променю БС, позиції дрона та фаз IRS за допомогою DRL (TD3). В [5] запропоновано модель глибокого навчання з підкріпленням на основі комбінованого публічного датасету, що дає істотно кращі показники порівняно зі SVM, Random Forest та RNN для прогнозування й проактивного пом'якшення мульти-крокових кіберзагроз (DoS, Replay, Evil Twin, False Data Injection) у системах зв'язку з інтеграцією супутників та БПЛА. В [6] для підвищення безпеки передачі даних запропоновано робастний алгоритм для multi-AIRS SWIPT з урахуванням джитеру БПЛА. В [7] проведено огляд загроз і вимог безпеки та приватності для БПЛА-систем в 5G (включно з ML-атаками) і проаналізовано сучасні й перспективні рішення – PLS, блокчейн, федеративне навчання та пост-квантову криптографію.

Постановка завдання. Визначити головні види атак на повітряно-наземні канали зв'язку та дослідити заходи щодо забезпечення конфіденційності зв'язку, спеціально адаптовані для систем з інтеграцією БПЛА. Розробити моделі каналу, енергоспоживання і обмежень руху, адекватні для прикладних сценаріїв БПЛА. Розробити ефективні контрзаходи пасивному прослуховуванню на основі штучного шуму та дослідити метод спільної оптимізації траєкторії, висоти та потужності передавача БПЛА-вузла.

Метою роботи є аналіз існуючих загроз для конфіденційності передачі даних в телекомунікаційних системах з інтеграцією безпілотних літальних апаратів та розробка міжрівневих методів забезпечення конфіденційної (секретної) передачі даних з оптимізацією траєкторії та потужності передачі БПЛА-вузлів.

Виклад основного матеріалу дослідження

Пасивне прослуховування (витік інформації). Пасивне прослуховування в системах зв'язку за участю БПЛА відбувається, коли противник безшумно перехоплює повітряно-наземні або повітряно-повітряні передачі, щоб збирати команди керування, потоки з сенсорів, користувацькі дані або результати оффлоадингу обчислень – ризик загострюється через домінуючі канали з лінією прямої видимості, високе відношення сигнал/шум у приймачів і часто обмежені ресурси вузлів.

Оскільки класична end-to-end криптографія може бути занадто «важкою» для БПЛА з обмеженою вагою та енергетично-обчислювальними ресурсами, ефективні заходи убезпечення зазвичай поєднують:

- легкі криптографічні рішення та захищене управління ключами для каналів командно-керування (C2) і передавання даних;
- методи безпеки на фізичному рівні, такі як штучний шум (Artificial Noise – AN), кооперативне/«дружнє» заглушення, напрямлене формування променю (beamforming) та попереднє кодування для багатоантенних передавачів;
- спільну оптимізацію траєкторії, висоти та потужності (або використання ретрансляторів/БПЛА-пригнічувачів) з метою зменшення якості каналу, доступної підслуховувачу;
- засоби виявлення і моніторингу (виявлення аномалій у CSI/RSSI, довірені БПЛА-монітори) разом із безпечними практиками оновлення й супроводу ПЗ для обмеження витоків інформації.

Максимізація секретності зазвичай вимагає більшої енергії або призводить до затримок, тому заходи захисту мають оптимізуватися разом з обмеженнями місії.

Заглушення та радіоперешкоди. Зловмисники генерують шум або інтерферуючі сигнали (профілактичне/постійне заглушення, реактивне заглушення або заглушення пілотних/синхронізаційних сигналів) з метою погіршити рівень SINR, порушити телеметрію або унеможливити керування. У разі постійного заглушення супротивник безперервно випромінює високопотужний шум у робочій смузі БПЛА, що «загортає» легітимний сигнал і спричиняє втрату телеметрії або критичних даних місії. Більш витончені атаки включають реактивне заглушення, коли пригнічувач передає лише під час виявлення легітимної активності (для економії енергії та ускладненого виявлення), та заглушення пілотних сигналів, яке спрямовано на канали управління або синхронізації для дестабілізації зв'язку при мінімальній витраті потужності. Наслідки варіюються від деградації сервісу та високого рівня втрати пакетів до повної відмови в обслуговуванні (DoS), що може примусити БПЛА до аварійної посадки або скасування місії.

Контрзаходи поєднують методи на рівні фізичного та канального рівнів (spread-spectrum та FHSS) для ускладнення заглушення, а також використання напрямлених антен і формування променю (beamforming) для скорочення впливу інтерференції. Адаптивне регулювання потужності підтримує стійкість каналу в умовах змінних перешкод. На рівні системи доцільні адаптація траєкторії (фізичний відхід від зон сильного зашумлення), розгортання кооперативних ретрансляторів БПЛА або «дружніх» заглушувачів для відновлення зв'язку чи маскування легітимного сигналу від зловмисників. Сучасні підходи також інтегрують спектральне зондування на основі машинного навчання для виявлення патернів заглушення та оперативного запуску контрзаходів.

Denial-of-Service (DoS). Ці атаки спрямовані на доступність: шляхом «заповнення» каналів управління/керування або інтерфейсів MEC/хмари зловмисник виснажує ресурси або блокує легітимні команди, що призводить до затримок або недоступності сервісів. Приклади атак:

- радіо-/протокольні флуди, які насичують C2-канал або наземне з'єднання (високошвидкісні потоки пакетів або SYN-флуди та скоординовані передавання від багатьох дешевих RF-вузлів);
- атаки на прикладному рівні проти MEC/хмарних сервісів, які обробляють телеметрію або виконують планування польоту (наприклад, ботнет із скомпрометованих IoT-пристроїв чи захоплених наземних станцій може згенерувати величезні навантаження запитів);
- атаки на маршрутизацію/виснаження ресурсів у роях БПЛА або FANET (флуд у таблиці маршрутів, створення фальшивих запитів маршрутизації, що витрачає CPU/пропускну здатність).

Контрзаходи на рівні PHY/MAC – застосовувати spread-spectrum/FHSS, напрямлені антени та різноманітність каналів для зменшення вразливості до точкового насичення. На мережевому рівні – вхідна фільтрація, обмеження пропускної здатності (rate-limiting), SDN-кероване формування трафіку та використання чорних/сірих списків для ослаблення атакуючих потоків. На транспортному/прикладному рівні – вимагати надійної (легкої) автентифікації та перевірки «свіжості» повідомлень, застосовувати challenge-response або обчислювальні пазли там, де доречно, щоб ускладнити обробку фальшивих команд. Контрзаходи на рівні периферії/інфраструктури – розгортати еластичні ресурси MEC, кешування й реплікацію сервісів та виявлення аномалій (статистичні або на основі машинного навчання) для виявлення й пом'якшення розподілених хвильових атак. На системному рівні – проєктувати механізми граціозної деградації та автономії (локальний безпечний режим, watchdog-таймери, заздалегідь налаштовані сценарії відмовостійкої поведінки і альтернативні канали зв'язку, наприклад mesh-мережі або супутникові канали), щоб БПЛА могли продовжувати критичні операції при погіршенні зв'язку. Ці контрзаходи мають компроміси: енерговитрати, затримки та складність реалізації. Тому на практиці оптимально поєднувати легкі, пріоритетні захисні

механізми для С2/телеметрії з масштабованими мережевими оборонними шарами та автономними резервними сценаріями, щоб мінімізувати вплив на місію.

Спуфінг і глушіння GNSS/GPS (атаки на навігацію). Спуфінг і глушіння супутникових систем навігації підривають здатність БПЛА точно знати де вони знаходяться шляхом витіснення корисних супутникових сигналів шумом (глушіння), або підміни їх підробленими сигналами, що повідомляють хибні координати/час (спуфінг). Практичні форми таких атак варіюються від простого широкосмугового глушіння, що змушує приймач втратити фіксацію на GPS, до витонченого «безшовного» спуфінгу, який поступово зміщує БПЛА з курсу без різких сигналів тривоги; також зустрічаються meaconing (відтворення затриманих сигналів), що викликає передбачувані дрейфи, та координовані атаки «спуфінг + підміна даних», що дозволяють обхід геообмежень (geofencing) або приховане захоплення апарата. Наслідки – від погіршення навігації та випадкових відхилень траєкторії до повного відмовлення місії або примусової посадки в контрольованій супротивником зоні. Ефективний захист має багаторівневий характер:

- сигнально-приладові заходи – використання приймачів мультиконстеляційних і багаточастотних систем, антенних решіток для визначення кута приходу (AoA) і формування «нульових» напрямів (null-steering), а також перевірок на основі ефекту Доплера і автономного моніторингу цілісності приймача (RAIM) та тестів на узгодженість SNR/часу для виявлення аномалій;
- злиття даних з датчиків (sensor fusion) – тісне поєднання GNSS із інерційною навігацією (INS/IMU), візуальними методами (optical flow, visual odometry), лідарами або UWB-вимірюванням відстані, щоб навігація плавно переходила на внутрішню оцінку положення (dead-reckoning) при підозрі на ненадійність GNSS;
- аутентифікація PNT – застосування автентифікованих GNSS-сервісів або підсилень PNT (диференційний GNSS, автентифіковані корекції) де можливо;
- операційні та системні заходи – попередньо запрограмовані безпечні режими, перевірка ключових маршрутних точок (waypoint verification), механізми спільного виявлення/звітності про спуфінг/глушіння з боку наземних станцій або «натовпу», а також використання альтернативних каналів (супутниковий зв’язок, наземні маяки) для перехресної перевірки;
- політика та загартування – радіочастотна локація джерел заглушення, укріплене/підписане ПЗ приймача та безпечні ланцюги оновлень, щоб унеможливити допоміжний спуфінг через компрометацію прошивки.

Комбінація надійного виявлення (щоб БПЛА «розумів», що GNSS недостовірний), стійкого злиття сенсорних даних і автономних запасних алгоритмів забезпечує найкращу практичну стійкість як проти грубого глушіння, так і проти тонких спуфінгових атак.

Атаки «людина посередині» (Man-in-the-Middle – MitM), відтворення (replay) та імітація ідентичності (impersonation). Атаки MitM/replay/impersonation спрямовані на порушення довіри між БПЛА та їхніми контролерами шляхом перехоплення, модифікації, повторного відтворення або підробки повідомлень на каналах командно-керуючого зв’язку (С2) та передачі даних. Приклади атак: зловмисний вузол, який «вставляється» між наземною станцією керування (GCS) і БПЛА та пересилає підроблену телеметрію або фальшиві підтвердження (класичний MitM); захоплення та повторне відтворення раніше зафіксованої команди на зліт/точку маршруту, що змушує апарат виконати небажані маневри; wormhole-реле, яке робить вузол нападника «вигідним» маршрутизуючим сусідом; та видавання себе за GCS або БПЛА через підроблені MAC/ідентифікаційні кадри чи сфальсифіковані службові повідомлення для захоплення сесії. Наслідки – втрата керування, витік чутливих даних, відхилення від маршруту або приховане захоплення апарату. Практичні заходи захисту (шарове поєднання):

- сильна взаємна автентифікація і легкі криптографічні зв’язки (наприклад, підписи на основі еліптичних кривих (ECC), ідентифікаційні або безсертифікатні схеми, легкі

онлайн/оффлайн підписи) – щоб лише легітимні вузли могли приєднуватися й обмінюватися ключами;

- антиреплей-засоби – одноразові числа (нонси), номери послідовності, часові мітки та перевірки «свіжості» повідомлень, щоб неможливо було повторно використати перехоплені пакети;
- безпечне завантаження та підписування прошивок і стійке управління ключами (бажано делеговане або підтримане МЕС) – щоб запобігти прийому підробленого ПЗ або фальшивих ідентифікацій;
- апаратно закріплена ідентичність (наприклад, PUF – фізично неклоновані функції, або захищені апаратні елементи) – ускладнює імітацію особи та витягування ключів;
- виявлення на основі каналу та поведінки – ідентифікація за відбитком радіочастот/каналу, системи виявлення вторгнень (IDS) і детектори на базі аномалій/машинного навчання для виявлення неочікуваних реле або дублювання маршрутів (wormhole);
- операційна надлишковість – кілька незалежних каналів, резервна наземна станція, запасні автономні режими і механізми відмовостійкості, щоб БПЛА міг відхилити підозрілі команди та забезпечити конфіденційність.

Поєднання легких криптографічних механізмів/автентифікації з антиреплей-примітивами, апаратними «коренями довіри» і моніторингом дає найпрактичніший захист для енергетично й обчислювально обмежених БПЛА. Інші види атак включають:

- *Підміна каналу управління (C2)/захоплення управління.* Якщо канал C2 перехоплено, відтворено або підмінено, нападник може захопити керування польотом (змінити місію, примусово посадити або спричинити катастрофу). Ризик посилюють підроблені або незахищені прошивки та слабка автентифікація.
- *Ін'єкція хибних даних і підміна сигналів датчиків.* Зловмисники подають фальшиві телеметричні дані, маршрутизаційну інформацію або спотворюють покази сенсорів (камери, лідара тощо), що призводить до помилкових рішень або спотворених карт – критично для місій спостереження та картографування.
- *Шкідливе ПЗ, експлуатація прошивки та атаки на ланцюг постачання.* Шкідливий код, вбудований через незахищені канали оновлення або скомпрометовані компоненти, може підривати логіку польоту, викрадати дані або відчиняти бекдори. Тому довіра до постачальника й ланцюга поставок критична.
- *Фізичне захоплення і маніпуляції.* У разі фізичного захоплення БПЛА зловмисник може витягти ключі, модифікувати обладнання або зворотно розробляти системи. Фізична безпека та безпечне зберігання ключів є важливими заходами щодо зменшення ризиків.
- *Атаки на топологію/маршрутизацію у роях (Sybil, wormhole, blackhole).* У мульти-БПЛА мережах нападник може створювати фальшиві ідентичності (Sybil), тунелювати трафік (wormhole) або скидати пакети (blackhole), порушуючи маршрутизацію та співпрацю.
- *Порушення приватності та небажане спостереження.* Зібрані БПЛА зображення, локації та сенсорні дані можуть розкривати чутливу інформацію про людей або операції. Потрібне шифрування збережених і переданих даних, контроль доступу, політики зберігання й видалення, а також правове/операційне регулювання доступу до даних.
- *Атаки на енергетичні ресурси/виснаження батареї.* Примусове багаторазове ініціювання зв'язку, змушування до зайвих маневрів або обчислювальних циклів може швидко виснажити обмежений ресурс енергії.
- *«Adversarial» та «Poisoning» атаки на ML МЕС периферії.* Якщо БПЛА або вузли МЕС використовують ML-моделі (детекція, навігація, ухвалення рішень), зловмисники можуть подавати приманки (adversarial examples) або отруювати навчальні дані/оновлення (poisoning), що призводить до помилкових висновків.

- *Побічні канали та RF-фінгерпринтинг.* Через випромінювання, часові або енергетичні сигнатури нападник може ідентифікувати, відстежувати або вилучати інформацію про БПЛА; натомість зловмисник може спробувати підробити RF-відбиток, щоб видатися легітимним вузлом.
- *Інсайдерські загрози та зловживання обліковими даними.* Компрометація операторів, неправильні налаштування наземних систем або виток облікових даних дозволяють несанкціонований доступ або навмисні зловживання.

Наведені загрози охоплюють пасивні та активні, кібер- і фізичні вектори, а також проблеми на рівні протоколів і машинного навчання; їхні наслідки включають втрату конфіденційності, порушення місії, фізичні пошкодження, порушення приватності та каскадні відмови при залученні MEC/хмари/IoT. Отже, ефективний захист вимагає міжрівневого підходу: поєднання PLS і криптографії, надійної автентифікації, захищених оновлень, стійкої архітектури управління, оптимізації траєкторій і ресурсів та укріплення ML-компонентів.

Дизайн штучного шуму (AN) для запобігання пасивному прослуховуванню. В статті розглядається наступна модель системи штучного шуму: один легітимний користувач, один прослуховувач і MISO-передавач. Нехай передавач БПЛА має N_t антен, легітимний Користувач і Підслуховувач мають по одній антені. У заданий момент часу складні сигнали, що приймаються в основній смузі, є:

$$y_b = h^H x + n_b,$$
$$y_e = g^H x + n_e,$$

Де $h \in \mathbb{C}^{N_t}$ вектор каналу БПЛА→Користувач, і $g \in \mathbb{C}^{N_t}$ це БПЛА→Підслуховувач, та $n_b, n_e \sim CN(0, \sigma^2)$ є рамками шуму. Переданий вектор x несе інформаційний промінь та штучний шум:

$$x = ws + z$$

Де s – інформаційний символ з $\mathbb{E}[|s^2|] = 1$, $w \in \mathbb{C}^{N_t}$ – вектор формування променю для інформаційного сигналу, $z \sim CN(0, Q_z)$ – вектор штучного шуму з коваріацією $Q_z \succcurlyeq 0$. Обмеження загальної потужності передачі:

$$tr(ww^H) + tr(Q_z) \leq P_{tot}.$$

SINR та рівень секретності. Миттєвий SNR Користувача (при розгляді AN як шуму):

$$SNR_{\text{к}} = \frac{|h^H w|^2}{h^H Q_z h + \sigma^2}$$

Миттєвий SNR Підслуховувача:

$$SNR_{\text{п}} = \frac{|g^H w|^2}{g^H Q_z g + \sigma^2}$$

Миттєва швидкість секретності (біт/с/Гц) може бути виражена як різниця між пропускною здатністю зв'язку з Користувачем і пропускною здатністю, яку мав би Підслуховувач:

$$R_s = [\log_2(1 + SNR_{\text{к}}) - \log_2(1 + SNR_{\text{п}})]^+.$$

Якщо різниця від'ємна, вона вважається нульовою. Якщо Користувач має одну антену, а AN-генератор розміщений у нульовому просторі h^H (набір передавальних сигналів, які невидимі для Користувача), то $h^H Q_z h = 0$ і SNR Користувача відповідно спрощується – це часто використовувана конструкція, коли доступна повна CSI Користувача.

Цілі проектування (типові форми оптимізації). Максимізація миттєвої швидкості секретності:

$$\max_{w, Q_z} R_s$$
За умови: $tr(ww^H) + tr(Q_z) \leq P_{tot}$
$$Q_z \succcurlyeq 0.$$

Ця проблема в цілому є неконвексною, тому стандартними підходами до вирішення можуть бути: SDR (напіввизначена релаксація), SCA (послідовне конвексне наближення) або альтернативна оптимізація. Формулювання розподілу потужності (простий скалярний розподіл) через поділ загальної потужності P_{tot} на інформаційну потужність P_s і потужність AN P_a:

$$w = \sqrt{P_s}u, \qquad \|u\| = 1,$$
$$tr(Q_z) = P_a, \qquad P_s + P_a \le P_{tot}$$

Практичний дизайн: вибрати u як MRT до Користувача, $u=h/\|h\|$, і вибрати Q_z щоб генератор був в Null(h^H) у випадку якщо CSI Користувача ідеальний, або був ізотропним на доповнювальному підпросторі, якщо SCS Підслуховувача невідомий. Потім оптимізувати скаляр P_s (еквівалентно P_a) щоб максимізувати R_s.

Спільна оптимізація траєкторії, висоти та потужності. В нашій моделі передачі ми дискретизуємо місію на N часових інтервалів Δt. Інтервали індексуються як n=1,…,N. 3D-положення БПЛА в інтервалі n: $q[n]=(x[n],y[n],h[n]) \in \mathbb{R}^3$ (висота $h[n]$ є явною). Позиція легітимного Користувача на землі: $q_b = (x_b,y_b,0)$, позиція Підслуховувача: $q_e=(x_e,y_e,0)$, яка може бути невідомою/стохастичною в надійних варіантах. БПЛА має N_t передавальних антен. Вектор формування променю в інтервалі n – $w[n] \in \mathbb{C}^{Nt}$, коваріація AN – $Q_z[n] \succeq 0$, потужність передачі – $P_{tx}[n]=\|w[n]\|^2+\mathrm{tr}(Q_z[n])$. P_{max} – максимальна потужність передачі на інтервал, потужність шуму на приймачах – σ^2. β_0 – величина втрат на трасі на одиничній відстані; показник втрат на трасі α (часто α=2 для LoS/вільного простору). Відстань від БПЛА до приймача – $k \in \{b,e\}$:

$$d_k[n] = \|q[n] - q_k\|_2.$$

Детермінована (LoS-домінуюча) модель каналу (в якій один комплексний коефіцієнт підсилення ігнорується або нормалізується до β_0):

$$h_k[n] = \sqrt{\frac{\beta_0}{d_k[n]^\alpha}}\,\widetilde{h_k}[n],$$

Де $h_k[n]$ – вектор маломасштабного завмирання з одиничною нормою (може бути встановлений на 1 для детермінованого LoS). Для приймачів з однією антеною слід використовувати скаляр $h_k[n] = \sqrt{\frac{\beta_0}{d_k[n]^\alpha}}$.

Що стосується SNR/швидкості секретності на інтервал (передавач MISO, Користувач/Підслуховувач з однією антеною), для ясності припустимо, що обоє мають одну антену (узагальнення MIMO є аналогічним). SNR Користувача в інтервалі n:

$$SNR_к[n] = \frac{|h_к[n]^H w[n]|^2}{h_к[n]^H Q_z[n] h_к[n] + \sigma^2}$$

SNR Підслуховувача в інтервалі n:

$$SNR_п[n] = \frac{|h_п[n]^H w[n]|^2}{h_п[n]^H Q_z[n] h_п[n] + \sigma^2}$$

Миттєва швидкість секретності в інтервалі n:

$$R_s[n] = [\log_2(SNR_к[n]) - \log_2(1 + SNR_п[n])]^+$$

Таким чином, мету можна підсумувати як максимізацію середньої за часом швидкості секретності:

$$\overline{R}_s = \frac{1}{N}\sum_{n=1}^{N} R_s[n]$$

Обмеження щодо мобільності, кінематики та енергії є надзвичайно важливими для формулювання задачі спільної оптимізації з метою максимізації середньої швидкості секретності. Максимальна швидкість $V_{\max}$:

$$\|q[n+1] - q[n]\|_2 \le V_{max}\Delta t, \qquad n = 1, \dots, N-1$$

Висотні обмеження:

$$h_{min} \le h[n] \le h_{max}, \qquad \forall n$$

Обмеження початкової та кінцевої точки маршруту:

$$q[1] = q_{init}, \qquad q[N] = q_{final}$$

Рушійну силу та загальний енергетичний баланс E_{tot} можна сформулювати за допомогою загальної моделі рушійної сили $P_{\text{prop}}(v[n])$, яка походить від функції швидкості $v[n] = \|q[n+1]-q[n]\|/\Delta t$. Таким чином, обмеження енергії:

$$\sum_{n=1}^{N}\Big(P_{tx}[n]+P_{prop}(v[n])\Big)\Delta \mathrm{t} \le E_{tot}$$

Загальна спрощена модель, яка враховує кубічний опір: $P_{prop}(v)=c_1v^3+c_2$. Обмеження потужності передачі на інтервал:

$$P_{tx}[n] \le P_{max}, \qquad \forall n$$

Обмеження спектральної щільності потужності за коваріації штучного шуму:

$$Q_z[n] \succcurlyeq 0, \qquad tr(Q_z[n]) \le P_{a,max}[n]$$

Цільова величина є неконвексною за рахунок обмежень (дробні співвідношення SNR, логарифмічна різниця та зв'язок $q[n]$ з коефіцієнтами посилення каналу), але кінцева задача оптимізації з максимізацією середньої швидкості передачі секретної інформації може бути сформульована наступним чином:

$$\max_{\{q[n],w[n],Q_z[n]\}} \frac{1}{N}\sum_{n=1}^{N}[\log_2(1+SNR_b[n])-\log_2 1+SNR_e[n]]^+$$

$$\text{За умови: } \|q[n+1]-q[n]\| \le V_{max}\Delta t,\ n=1,\dots N-1,$$

$$h_{min} \le h[n] \le h_{max}, \qquad \forall n,$$

$$\sum_{n=1}^{N}\Big(\|w[n]\|^2+tr(Q_z[n])+P_{prop}(v[n])\Big)\Delta t \le E_{tot},$$

$$\|w[n]\|^2+tr(Q_z[n]) \le P_{max}, \qquad Q_z[n] \succcurlyeq 0,$$

$$q[1]=q\_init, q[N]=q\_final.$$

Це підкреслює необхідність використання консервативних моделей руху або виміряних кривих «потужність-швидкість» для реалістичного розрахунку енергоспоживання та дотримання обмежень безпеки (зони заборони польотів, уникнення зіткнень) як лінійних/опуклих обмежень, де це можливо. Якщо БПЛА має одну антену (без нульового простору) – виникає необхідність в кооперативних пригнічувачах або оптимізації лише траєкторії.

Висновки

У роботі проведено системний аналіз загроз інформаційній безпеці в телекомунікаційних системах із інтеграцією безпілотних літальних апаратів (БПЛА) та розглянуто сучасні підходи до забезпечення конфіденційної передачі даних у таких мережах. Доведено, що висока мобільність, домінування каналів із лінією прямої видимості, обмежені енергетичні ресурси й обчислювальні можливості роблять БПЛА особливо вразливими до широкого спектра кіберфізичних атак – від пасивного прослуховування й заглушення до підміни навігаційних сигналів, атак «людина посередині» та отруєння моделей машинного навчання на периферії.

Для підвищення рівня конфіденційності запропоновано багаторівневий підхід, який поєднує технології безпеки фізичного рівня з використанням штучного шуму (Artificial Noise), формування променю (beamforming) та кооперативного заглушення з метою зниження якості каналу потенційного перехоплювача без шкоди для легітимного користувача. Додатково розглянуто задачу спільної оптимізації траєкторії, висоти та потужності передачі, що дозволяє максимізувати середню швидкість секретної передачі даних з урахуванням кінематичних та енергетичних обмежень БПЛА.

Список використаної літератури:

1. Poorvi J., Kalita A., Gurusamy M. Reliable and Efficient Data Collection in UAV based IoT Networks. IEEE Communications Surveys & Tutorials. 2025. P. 1. URL: https://doi.org/10.1109/comst.2025.3550274.

2. Secrecy Analysis and Optimization of UAV-Assisted Communications With Hybrid SWIPT and Cooperative Jamming / G. K. Pandey et al. IEEE Journal on Miniaturization for Air and Space Systems. 2025. P. 1. URL: https://doi.org/10.1109/jmass.2025.3568592.

3. Yang S., Ma H. Security Performance Analysis of Full-Duplex UAV Assisted Relay System Based on SWIPT Technology. Applied Sciences. 2024. Vol. 14, no. 12. P. 4987. URL: https://doi.org/10.3390/app14124987.

4. Secure and energy-efficient transmission in UAV-assisted intelligent reflecting surface networks / J. Xue et al. Scientific Reports. 2025. Vol. 15, no. 1. URL: https://doi.org/10.1038/s41598-025-17852-y.

5. Khosravian E., Denghan M. Cyber Risk Prediction for UAVs in Space-related Missions using Deep Reinforcement Learning. Journal of Space Science and Technology. 2025. Vol 15, no. 1. P. 1-15. URL: https://doi.org/10.22034/jsst.2025.1527.

6. Aerial IRS-Assisted Secure SWIPT System With UAV Jitter / T. Cheng et al. IEEE Transactions on Green Communications and Networking. 2024. P. 1. URL: https://doi.org/10.1109/tgcn.2024.3366539.

7. Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review / M. A. Khan et al. IEEE Transactions on Network and Service Management. 2024. P. 1. URL: https://doi.org/10.1109/tnsm.2024.3487265.

Автори статті

Яковець Всеволод – аспірант, старший викладач, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0002-3866-8017

Руденко Сергій – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0002-9499-3025

Колесніков Олексій – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0003-3552-9721

Швець Дмитро – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0007-9059-7064

Бойко Олег – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0001-3761-7528

Authors of the article

Yakovets Vsevolod – postgraduate, senior lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0002-3866-8017

Rudenko Serhiy – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0002-9499-3025

Kolesnikov Oleksiy – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0003-3552-9721

Shvets Dmytro – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0007-9059-7064

Boyko Oleg – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0001-3761-7528