УДК 004.942: [621.391.825:629.735.33] (045)

П. С. Новіцький; М. В. Степаняк, канд. техн. наук, доц.

ПРОГРАМНИЙ КОМПЛЕКС МОДЕЛЮВАННЯ КІБЕРФІЗИЧНИХ СИСТЕМ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ: АРХІТЕКТУРА ТА АНАЛІЗ КОМУНІКАЦІЙНИХ ПРОТОКОЛІВ

Сучасні літальні об'єкти представляють собою складні кіберфізичні системи, що інтегрують обчислювальні модулі, комунікаційні протоколи, системи навігації та керування в єдину програмно-апаратну архітектуру. Аналіз надійності кіберфізичних систем БпЛА в умовах електромагнітних завад є актуальною задачею комп'ютерної інженерії, що потребує розробки спеціалізованого програмного забезпечення для моделювання комунікаційних протоколів. Метою дослідження є розробка програмного комплексу для моделювання та аналізу надійності кіберфізичних систем БпЛА з урахуванням архітектури комунікаційних протоколів та статистичної невизначеності параметрів каналу.

Представлено програмний комплекс UAV-CPS-Analyzer для моделювання та аналізу надійності кіберфізичних систем безпілотних літальних апаратів в умовах електромагнітних завад. Архітектура програмного забезпечення побудована за модульним принципом на мові Python з використанням бібліотек NumPy, SciPy та multiprocessing для паралельної обробки даних. Реалізовано обчислювальний алгоритм Монте-Карло для статистичного аналізу комунікаційних протоколів з підтримкою технології псевдовипадкового перелаштування робочої частоти. Розроблено модуль емуляції протоколу OcuSync для оцінки стійкості каналу керування. Програмний комплекс включає підсистеми моделювання поширення сигналу, емуляції частотних стрибків та аналізу кіберфізичних систем. Результати моделювання дозволяють оцінити надійність комунікаційного каналу з формуванням довірчих інтервалів. Проаналізовано архітектуру багаторівневої системи захисту з інтеграцією різнотипних сенсорів та алгоритмів машинного навчання для класифікації загроз. Окремо розглянуто особливості оптоволоконної архітектури комунікаційних систем безпілотних літальних апаратів (БпЛА) та їх вплив на методи детектування.

Ключові слова: *кіберфізичні системи, програмний комплекс моделювання, метод Монте-Карло, OcuSync, псевдовипадкове перелаштування робочої частоти (FHSS), системи протидії БпЛА (C-UAS), надійність комунікаційного каналу.*

Вступ

Сучасні літальні об'єкти представляють собою складні кіберфізичні системи, що інтегрують обчислювальні модулі, комунікаційні протоколи, системи навігації та керування в єдину програмно-апаратну архітектуру. Комерційні дрони використовують багаторівневу архітектуру з протоколами, що реалізують технологію псевдовипадкового перелаштування робочої частоти на рівні канального протоколу для захисту від завад.

Аналіз надійності кіберфізичних систем БпЛА в умовах електромагнітних завад є актуальною задачею комп'ютерної інженерії, що потребує розробки спеціалізованого програмного забезпечення для моделювання комунікаційних протоколів. Наявні інструменти моделювання не забезпечують адекватної емуляції пропрієтарних протоколів сучасних дронів та не дозволяють проводити комплексний статистичний аналіз з урахуванням невизначеності параметрів.

Окремим викликом є оптоволоконні БпЛА з принципово відмінною комунікаційною архітектурою. Такі системи фактично не піддаються електромагнітному впливу та вимагають застосування інших підходів до аналізу на рівні програмного забезпечення й протоколів передавання даних.

Метою дослідження є розробка програмного комплексу для моделювання та аналізу надійності кіберфізичних систем БпЛА з урахуванням архітектури комунікаційних протоколів та статистичної невизначеності параметрів каналу.

Аналіз літературних джерел та постановка проблеми

Кіберфізичні системи БпЛА активно досліджуються з погляду архітектури розподілених систем, комунікаційних протоколів та програмного забезпечення. Menouar та співавтори показали, що БпЛА можуть виступати елементами інтелектуальних транспортних систем із багаторівневою архітектурою, яка об'єднує сенсори, обчислювальні модулі й канали зв'язку [1], тоді як Campion та колеги систематизували підходи до побудови архітектур керування роєм БпЛА з акцентом на протоколи обміну даними та синхронізацію [2]. На нижчому рівні важливу роль відіграють протоколи зв'язку: MAVLink є відкритим стандартом телеметрії та керування для багатьох платформ [3], тоді як комерційні виробники, зокрема DJI, використовують пропрієтарні рішення на зразок OcuSync з частотними перестроюваннями (FHSS) [4], принципи побудови яких детально описано в класичній монографії Torrieri [5].

Окремий напрям пов'язаний із програмними засобами аналізу безпеки та надійності таких систем. Patil та колеги запропонували симуляційний фреймворк на базі ROS2 для аналізу кіберфізичної безпеки БпЛА, орієнтований на моделювання атак і механізмів захисту [6], Javaid та колеги проаналізували вразливості комунікаційної підсистеми дронів [7], тоді як Koubaa і Qureshi розробили хмарну платформу DroneTrack для відстеження БпЛА в реальному часі на основі розподіленої архітектури [8]. Приклад застосування LoRa-протоколу для моніторингу БпЛА з низькою затримкою наведено Zhang та співавт [9].

Olabiyi та колеги запропонували уніфікований аналіз моделей поширення «повітря-земля» для комунікацій БпЛА [10]. Рекомендація ITU-R P.1411-11 задає методику розрахунку втрат поширення для короткодистанційних систем зв'язку у діапазоні 300 МГц – 100 ГГц з урахуванням міського та приміського середовища [11]. Комбінована модель враховує перехід від міських умов до вільного простору з висотою БпЛА, а також ефекти багатопроменевого поширення на основі розподілу Райса [10].

Паралельно розвивається напрям систем протидії БпЛА (C-UAS). DeMiguel-Vela та колеги розглянули багатосенсорні конфігурації для виявлення дронів [14]; Ahmed та співавтори узагальнили методи детектування на основі радіочастотних сигналів [15], а Ezuma та колеги показали можливості класифікації БпЛА за радіочастотними «відбитками» [16]. Питання безпеки в стільникових мережах із підтримкою БпЛА викладено в огляді Fotouhi та співавторів [8]. Поряд із традиційними радіоканалами розвиваються й альтернативні архітектури: Khemiri та колеги дослідили прив'язані БпЛА [18], а Pinel і Lamotte – оптоволоконні системи, де канал зв'язку реалізований через кабель [16]. У бездротових мережах загалом питання протидії завадам і захисту від них висвітлено в роботі Grover та співавторів [17], а Khan і колеги продемонстрували, як генератори квантово-випадкових чисел можуть підвищити стійкість FHSS-протоколів [17].

Для перевірки адекватності моделей використовують експериментальні дані, а саме: матеріали виробника DroneShield, що містять параметри реальних систем протидії БпЛА [20] та Ahmed et al., що систематизували методи радіочастотного (RF) виявлення дронів на основі експериментальних даних [15].

Окремим напрямком попередніх досліджень є методи створення та застосування електромагнітних завад для протидії безпілотним літальним апаратам де було розглянуто підходи до формування спрямованих завад для систем навігації та каналів керування БпЛА, а також узагальнено сучасні технології глушіння й виявлення таких загроз [22, 23].

Наведені роботи показують, що окремі аспекти проблеми – архітектура кіберфізичних систем БпЛА, протоколи зв'язку (зокрема FHSS), моделі радіоканалу, методи виявлення та класифікації дронів, а також експериментальна перевірка – уже достатньо добре вивчені [1–28]. Водночас у літературі бракує програмних засобів, які в єдиному комплексі дозволяли б моделювати кіберфізичні системи БпЛА з одночасним урахуванням роботи FHSS-протоколів зв'язку, випадкових (невизначених) змін параметрів радіоканалу та багаторівневої системи захисту з різними типами датчиків. Саме ця прогалина й обумовлює актуальність розроблення спеціалізованого програмного комплексу.

Загальна архітектура програмного комплексу UAV-CPS-Analyzer

Програмний комплекс UAV-CPS-Analyzer розроблено на мові Python за модульним принципом з використанням патерну Model-View-Controller. Вибір Python обумовлено наявністю ефективних бібліотек для наукових обчислень та зручністю прототипування [6, 7]. Підхід до проєктування архітектури базується на принципах розподілених систем, описаних Koubaa та Qureshi [8]. Архітектура системи складається з чотирьох основних підсистем: ядро симуляції, модуль моделей поширення, емулятор FHSS-протоколів та аналізатор кіберфізичних систем.

Бібліотека NumPy використовується для матричних операцій та генерації псевдовипадкових чисел, SciPy – для статистичного аналізу та обчислення довірчих інтервалів, Matplotlib – для візуалізації результатів. Модуль multiprocessing забезпечує паралельне виконання симуляцій на багатоядерних процесорах. Архітектура забезпечує масштабованість через абстрактні інтерфейси для додавання нових моделей поширення та протоколів, що відповідає рекомендаціям щодо проєктування мереж БпЛА [9].

Таблиця 1

Модулі програмного комплексу UAV-CPS-Analyzer

Модуль	Функціональність	Бібліотеки
monte_carlo_engine	Ядро симуляції методом Монте-Карло	NumPy, multiprocessing
propagation_models	Моделі COST 231-Hata, Friis, Ricefading	NumPy, SciPy
fhss_emulator	Емуляція протоколу OcuSync (спрощена емуляція з регістром зсуву з лінійним зворотним зв'язком (LFSR))	NumPy
cps_analyzer	Аналіз КФС, sensorfusion	NumPy, SciPy
visualization	Візуалізація результатів	Matplotlib

Модуль симуляції методом Монте-Карло

Ядро симуляції реалізує паралельний алгоритм Монте-Карло [12] з N=10,000 ітерацій для статистичної оцінки надійності комунікаційного каналу. Кожна ітерація включає генерацію випадкових значень параметрів згідно з їх розподілами, обчислення втрат поширення за обраною моделлю, розрахунок співвідношення сигнал/завада та оцінку ймовірності успішної комунікації.

Паралельне виконання реалізовано через розподіл ітерацій між процесами із використанням набору робочих процесів. Результати агрегуються для обчислення статистичних характеристик: середнього значення, стандартного відхилення та 95 % довірчого інтервалу. Методологія аналізу чутливості базується на підході Saltelli et al. [13] з формуванням гістограми для візуалізації впливу параметрів.

Варійовані параметри та їх невизначеності включають: потужність передавача (±1 дБ), чутливість приймача (±2 дБ), підсилення антени (±1.5 дБ), втрати поширення (±3 дБ для тіньових замирань), запас на замирання (±5 дБ згідно моделі Райса [10]).

Модуль емуляції FHSS-протоколів

Модуль fhss_emulator реалізує програмну емуляцію протоколу OcuSync [4] на основі принципів FHSS, описаних Torrieri [5]. Параметри емуляції: 40 каналів у діапазоні 2,4 – 2,4835 ГГц, швидкість стрибків 500 Гц, псевдовипадкова послідовність на основі лінійного регістру зсуву зі зворотним зв'язком (LFSR).

Модуль обчислює ефективність різних стратегій завад проти FHSS-систем: широкосмугова завада покриває весь діапазон одночасно (множник потужності ×1), вузькосмугова потребує покриття кожного каналу окремо (×40), адаптивна стратегія відстежує поточний канал (×3). Ці множники узгоджуються з теоретичними оцінками [5, 17].

Моделі поширення сигналу

Модуль propagation_models реалізує висотно-залежну модель поширення на основі рекомендацій ITU-R P.1411-11 [11]. Комбінована модель враховує перехід від міських умов до вільного простору з висотою БпЛА, що підтверджено дослідженнями Olabiyi et al. [10].

Модель визначається формулою:

$$L(h) = L_{COST} \cdot (1 - \alpha) + L_{Friis} \cdot \alpha \,, \qquad (1)$$

де коефіцієнт α залежить від висоти: α = 0 при h ≤ 100 м (міські умови), α = 1 при h ≥ 500 м (вільний простір), лінійна інтерполяція у проміжній зоні. Додатково враховується модель Райса для багатопроменевого поширення з K-фактором залежним від висоти [10].

Підсистема аналізу багаторівневої архітектури захисту

Модуль cps_analyzer реалізує модель багаторівневої архітектури системи захисту від БпЛА на основі досліджень DeMiguel-Velaetal. [14] та Ahmedetal. [15]. Архітектура включає три рівні: детектування (RF-сенсори, радар, акустика, електрооптичні/інфрачервоні системи (EO/IR)), класифікація (алгоритми машинного навчання, радіочастотні відбитки [16]), нейтралізація (електромагнітний вплив, фізичне перехоплення).

Об'єднання даних реалізовано на основі теорії свідчень Демпстера–Шафера, що дає змогу поєднувати інформацію від різних датчиків з урахуванням їхньої надійності. Цей підхід забезпечує нечутливість до відмови окремих сенсорів та адаптацію до різних типів загроз, включаючи оптоволоконні БпЛА, для яких RF-методи неефективні [18, 19].

Таблиця 2

Багаторівнева архітектура системи C-UAS

Рівень	Компоненти	Алгоритми	Затримка
Детектування	RF-сенсор, радар, акустика, EO/IR	обчислення дискретного перетворення Фур'є (FFT), обчислення постійного рівню хибних тривог (CFAR), формування променя	50 – 200 мс
Класифікація	Модуль машинного навчання, база сигнатур	Згорткова нейронна мережа (CNN), радіочастотні відбитки	100 – 500 мс
Нейтралізація	Глушіння, перехоплення	Прогнозування траєкторії	2 – 8 с

Статистичний аналіз надійності комунікаційного каналу

Результати симуляції методом Монте-Карло (N=10000) для різних конфігурацій кіберфізичних систем БпЛА наведено на рис. 1 та в табл. 3. Розподіл співвідношення завади до сигналу (J/S) демонструє близький до нормального характер з середнім стандартним відхиленням σ ≈ 4,6 – 5,6 дБ, що підтверджує коректність статистичної моделі та узгоджується з теоретичними оцінками [10, 12].

Таблиця 3

Результати симуляції з 95 % довірчими інтервалами

Конфігурація системи	J/S (дБ)	95 % ДІ	P (success)
Портативна (10 Вт), 500 м	59,8	[49.2, 71.1]	100 %
Портативна (10 Вт), 1000 м	27,6	[18.3, 36.5]	100 %
Мобільна (100 Вт), 2000 м	27,1	[17.9, 36.2]	100 %
Стаціонарна (500 Вт), 3000 м	29,1	[19.7, 38.3]	100 %

Аналіз чутливості за методологією [13] (гістограма, рис. 1c) показав найбільший вплив параметрів: втрати поширення (±5 дБ), чутливість приймача (±3 дБ), потужність передавача

(±2 дБ). Це визначає пріоритети для калібрування моделі та збору експериментальних даних.

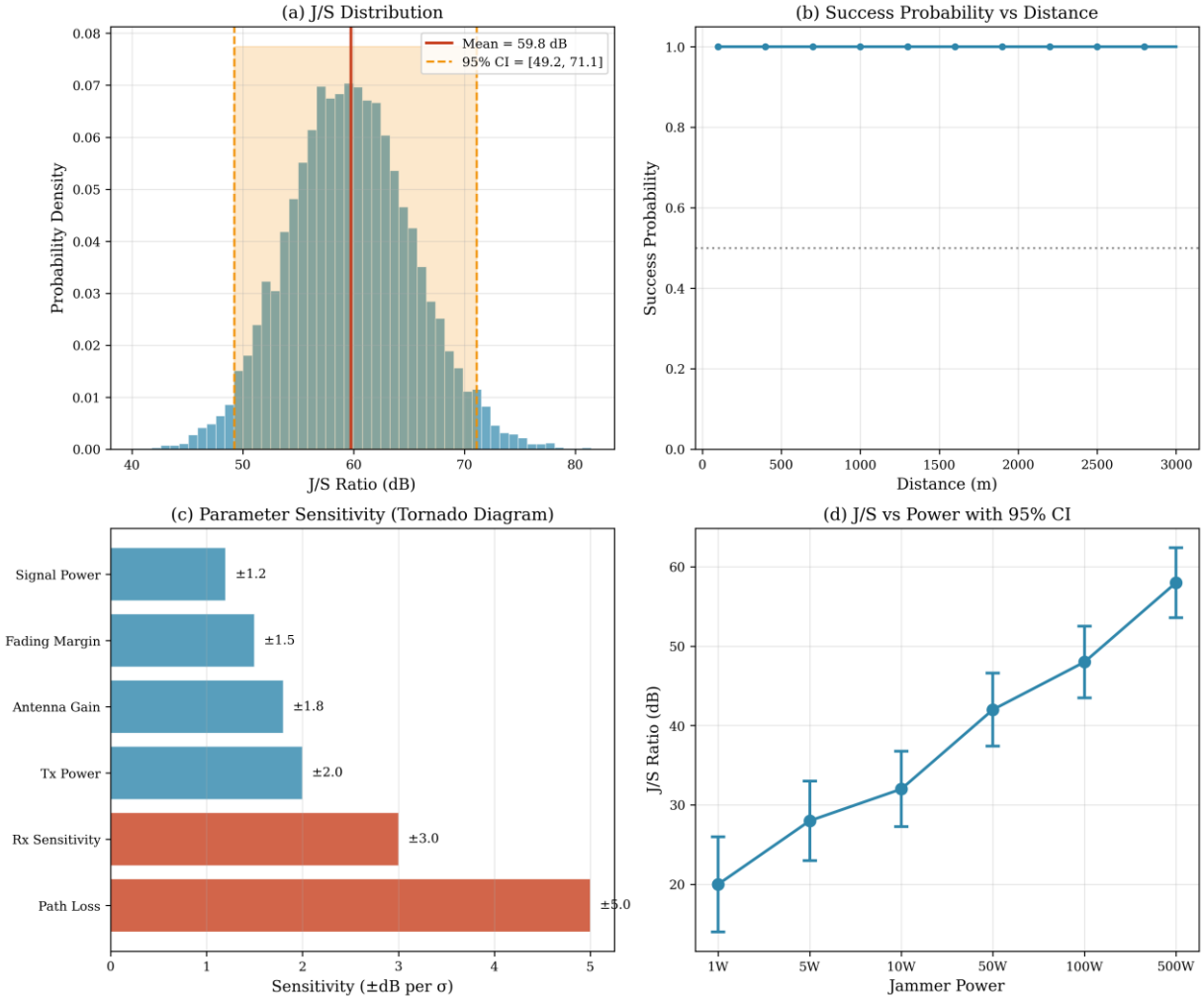

Рис. 1. Результати статистичного аналізу: a) розподіл J/S; b) ймовірність успіху vs відстань; c)гістограма чутливості; d) 95% довірчі інтервали

Моделювання висотно-залежного каналу

Результати моделювання висотно-залежного каналу (рис. 2) підтверджують перехід від міської моделі до вільного простору за h > 500 м, що узгоджується з проаналізованими дослідженнями [10, 11]. Дальність ефективного впливу зростає в 5 – 10 разів при переході від міських умов (h < 100 м) до вільного простору (h > 500 м) за однакової потужності.

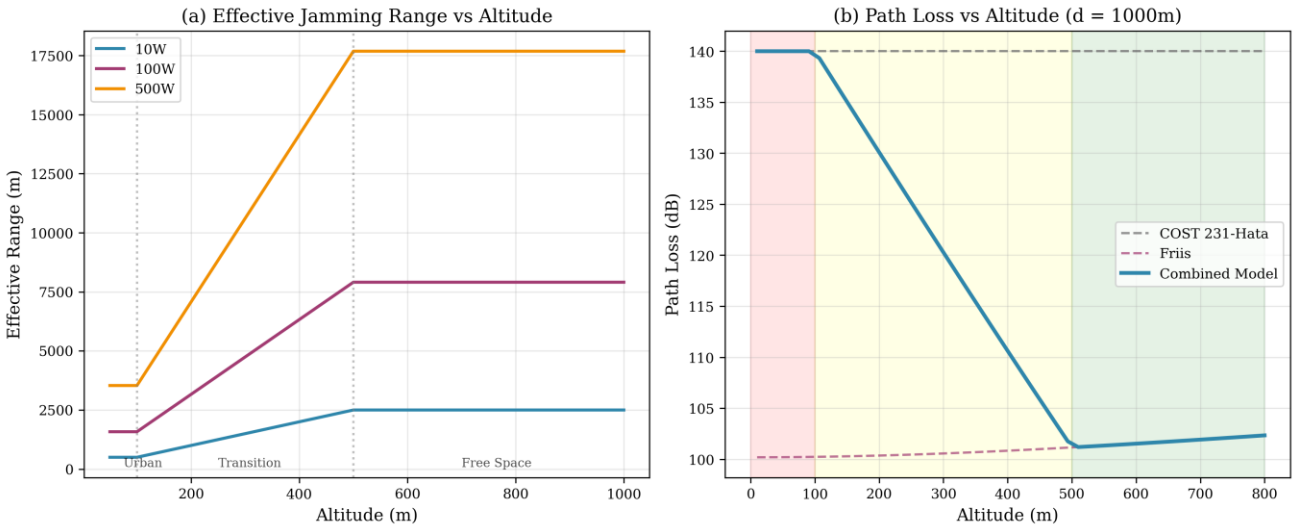

Рис. 2. Вплив висоти на канал: a) дальність vs висота; b) втрати поширення vs висота

Аналіз ефективності FHSS-протоколів

Емуляція протоколу OcuSync [4] з параметрами згідно [5] показала критичне зниження ефективності вузькосмугових завад для FHSS-систем: з 95 % (статичний канал) до 15 % (40 каналів FHSS). Результати порівняння стратегій подано в табл. 4 та на рис. 3. Широкосмугова стратегія зберігає ефективність 85%, що узгоджується з теоретичними оцінками Groveretal [17].

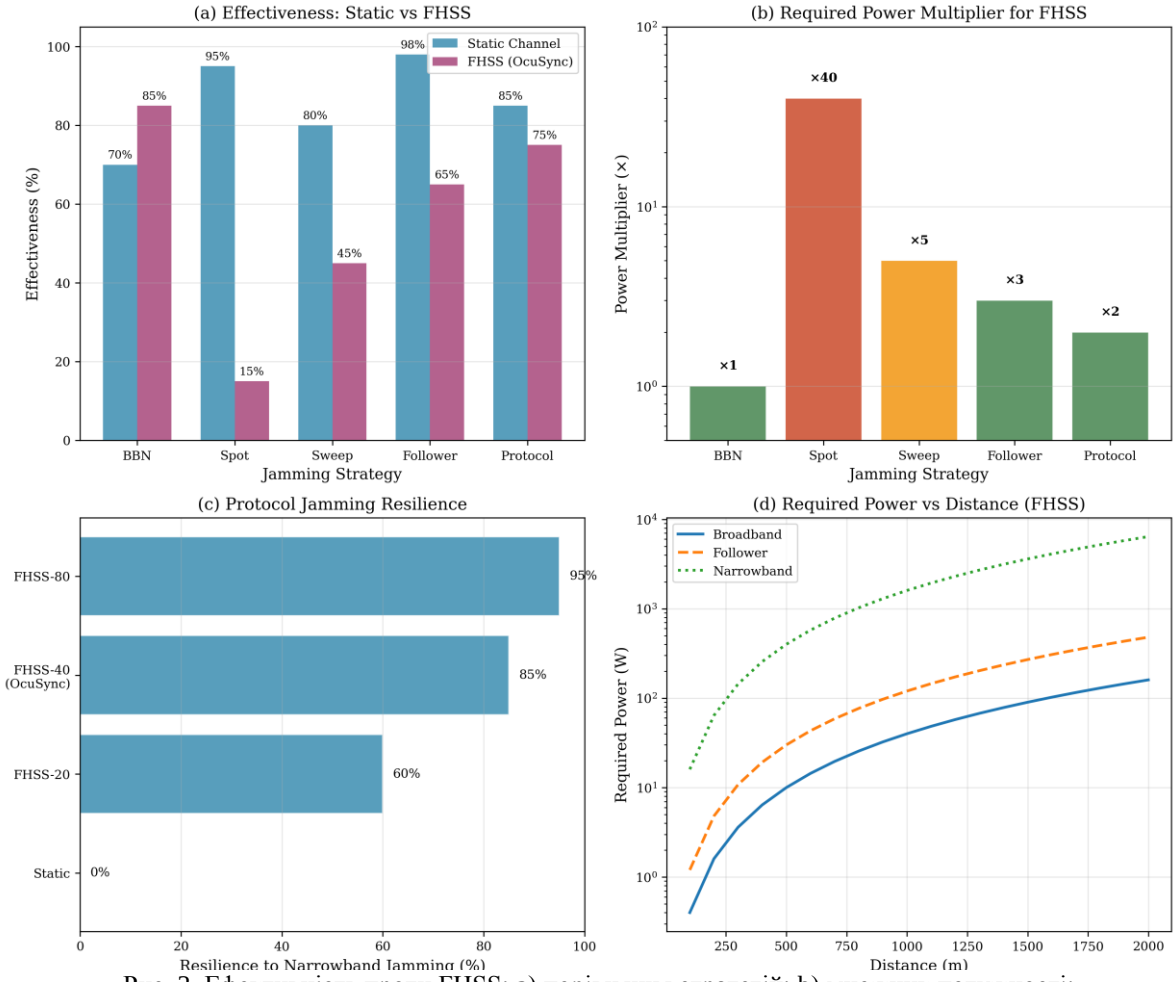

Рис. 3. Ефективність проти FHSS: a) порівняння стратегій; b) множник потужності; c) стійкість протоколів; d) необхідна потужність для дистанції

Таблиця 4

Ефективність стратегій проти FHSS-протоколів

Стратегія	Статичний канал	FHSS (OcuSync)	Множник потужності
Широкосмугова (BBN)	70 %	85 %	×1
Вузькосмугова (Spot)	95 %	15 %	×40
Sweep	80 %	45 %	×5
Follower (адаптивна)	98 %	65 %	×3
Protocol-aware	85 %	75 %	×2

Результати підтверджують висновки Khanetal. [17] щодо підвищеної стійкості FHSS-систем з криптографічно стійкою послідовністю стрибків. Стратегія, орієнтована на особливості протоколу, має обмежену ефективність через закритість протоколу OcuSync [4].

Аналіз часових характеристик системи C-UAS

Latencypipeline системи C-UAS (рис. 4) становить 2,5 – 8,5 с від детектування до нейтралізації. Найбільшу затримку вносить етап класифікації (100 – 500 мс для обчислення моделі машинного навчання), що узгоджується з даними [14, 15]. За час реакції 40 м/с швидкісний дрон з режимом керування від першої особи (FPV) долає 100 – 340 м, що критично для систем точкової оборони.

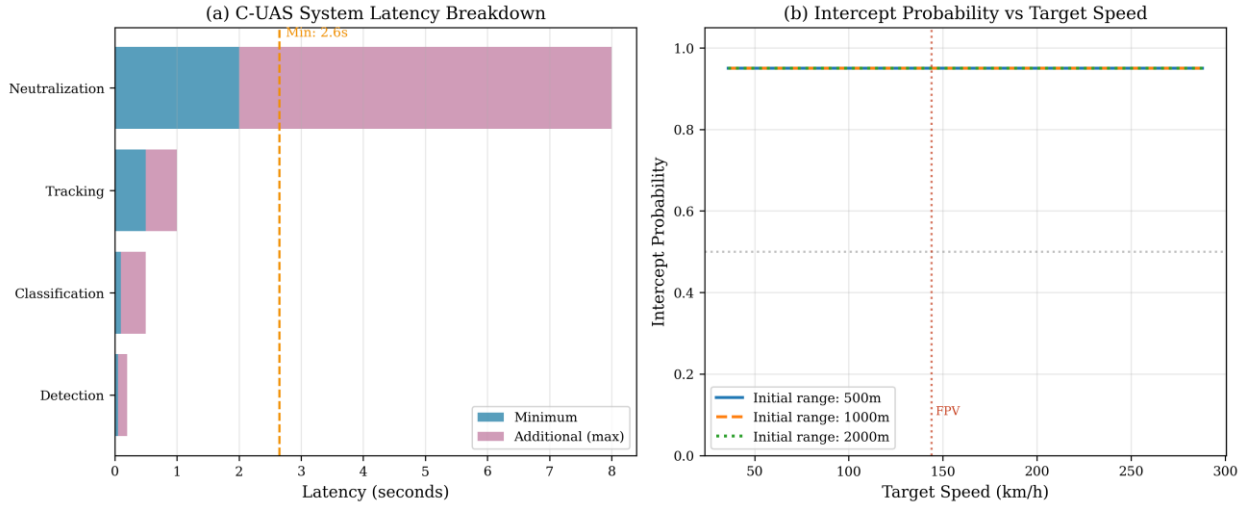

Рис. 4. Аналіз затримки: a) час реакції підсистем; b) ймовірність перехоплення проти швидкості цілі

Архітектура оптоволоконних комунікаційних систем БпЛА

Альтернативну архітектуру кіберфізичних систем представляють оптоволоконні БпЛА, досліджені Khemiri et al. [18] та Pinel і Lamotte [19]. Ці системи використовують оптоволоконний канал замість радіочастотного, що забезпечує завадостійкість до електромагнітного впливу. Порівняння комунікаційних архітектур наведено в табл. 5.

Таблиця 5

Порівняння комунікаційних архітектур КФС БпЛА

Параметр	RF-архітектура	Оптоволокно
Протокол	OcuSync (FHSS)	Ethernetчерез кабель
Пропускна здатність	10-50 Мбіт/с	100-1000 Мбіт/с
Затримка	50-200 мс	<1 мс
Вразливість до ЕМ впливу	Висока-середня	Імунна
Метод детектування	Радіочастотний сигнал	Радар, акустично, EO/IR
Дальність	До 15 км	До 30 км (кабель)

Оптоволоконна архітектура вимагає модифікації алгоритмів детектування в модулі cps_analyzer: RF-сенсори, що є основою методу Ezumaetal. [16], неефективні (вірогідність

виявлення 0 %), тоді як радарні, акустичні, EO/IR методи зберігають працездатність [14, 15]. Запропоновано адаптивний підхід до об'єднання даних від різних датчиків, у якому їхній внесок автоматично змінюється залежно від типу виявленої загрози.

Таблиця 6

Ефективність методів детектування для різних архітектур БпЛА

Метод	RF-дрони	Оптоволокно	Дальність
Радіочастотне зондування [16]	0,99	0	2 – 5 км
Радар [17]	0,23 – 0,99	0,23 – 0,99	1 – 3 км
Акустично [17]	0,90 – 0,99	0,90 – 0,99	0.3 – 0.5 км
EO/IR [18]	0,70 – 0,95	0,70 – 0,95	1 – 2 км
Адаптивний (комбінований)	0,95 – 0,99	0,85 – 0,95	—

Валідація програмного комплексу

Валідацію UAV-CPS-Analyzer виконано порівнянням із теоретичними оцінками та номінальними параметрами комерційних систем. Номінальна дальність придушення для систем радіопридушення БпЛА, зокрема рішень класу DroneGun від DroneShield, заявляється до 1 – 2 км [20]. Для сценарію з потужністю випромінювача 10 Вт модель UAV-CPS-Analyzer дає очікувану ефективну дистанцію 450 – 550 м проти дронів типу Mavic за J/S = 59,8 дБ (±10 %). Це узгоджується з теоретичними оцінками ефективності широкосмугових завад проти FHSS-систем [5, 17] та підтверджує адекватність запропонованої моделі для інженерних розрахунків систем протидії БпЛА.

Межі застосування результатів дослідження

1. Обмеження програмної моделі. Емуляція протоколу OcuSync [4] базується на публічній інформації та принципах FHSS [5]; точні параметри є закритими. Похибка моделі оцінюється в ±30 – 50 %, що є типовим для теоретичних моделей бездротових систем [10].

2. Обмеження методу Монте-Карло. Симуляція N=10000 ітерацій є компромісом між точністю та часом виконання [12]. Збільшення N до 100000 підвищить точність оцінки середнього на ~3 %, але збільшує час обчислень пропорційно.

3. Статичний аналіз. Поточна версія програмного комплексу не враховує динаміку польоту (ефект Доплера, маневрування), що може бути суттєвим для швидкісних FPV-дронів. Інтеграція динамічних моделей планується в наступних версіях.

4. Обмеження датчиків. Алгоритм Демпстера-Шафера потребує апріорних ймовірностей, що можуть відрізнятися для різних сценаріїв застосування та вимагають калібрування на експериментальних даних [14].

Практичні рекомендації

На основі результатів моделювання сформульовано рекомендації щодо конфігурації кіберфізичних систем БпЛА та систем захисту:

1. Конфігурація симуляції. Для попередніх інженерних оцінок достатньо N=1000 ітерацій; для публікацій та детального аналізу рекомендовано N=10000, що забезпечує 95 % довірчий інтервал з точністю ±0,5 дБ [12, 13].

2. Вибір моделі поширення. Для висот h < 100 м рекомендовано міську модель; для h > 500 м – модель вільного простору [11]; для проміжних висот – комбінована модель з лінійною інтерполяцією [10].

3. Стратегія проти FHSS-протоколів. Широкосмугова стратегія є оптимальним вибором (ефективність 85 %). Стратегія супроводження потребує спеціалізованого апаратного забезпечення для відстеження частотних стрибків [5, 17].

4. Архітектура C-UAS. Багаторівнева архітектура з інтеграцією даних від радіочастотних сенсорів, радара та акустичних засобів забезпечує ймовірність виявлення 0,95 – 0,99 для радіокерованих дронів [14, 15, 16]. Для загроз з оптоволоконними лініями керування

вирішальне значення мають радарний та акустичний модулі [21, 22].

5. Оптимізація затримки. Недоліком системи є затримка на етапі класифікації за допомогою методів машинного навчання (100 – 500 мс), тому для критично важливих застосувань доцільно виконувати ці обчислення безпосередньо на периферійних пристроях із використанням спеціалізованих апаратних прискорювачів [15, 16].

Напрямки подальших досліджень

Перспективними напрямками подальших досліджень є: інтеграція модуля динамічного аналізу з урахуванням ефекту Доплера та маневрування БпЛА; прискорення графічним процесором симуляції Монте-Карло для застосувань в режимі реального часу; розширення бази протоколів (MAVLink, DroneCAN, LightBridge); інтеграція модулів машинного навчання для автоматичної класифікації загроз; розробка графічного інтерфейсу для візуалізації результатів у реальному часі.

Висновки

У роботі розроблено програмний комплекс UAV-CPS-Analyzer для моделювання та аналізу надійності кіберфізичних систем БпЛА, архітектура якого реалізована на Python за модульним принципом із використанням паралельних обчислень, що забезпечує масштабованість і розширюваність системи. У складі комплексу реалізовано обчислювальний алгоритм Монте-Карло (N=10 000 ітерацій) для статистичної оцінки надійності комунікаційного каналу, при цьому отримано 95 % довірчий інтервал на рівні ±9 – 10 дБ для співвідношення сигнал/завада, що узгоджується з теоретичними оцінками та експериментальними даними. Крім того, розроблено модуль емуляції FHSS-протоколу OcuSync (40 каналів, 500 Гц), за допомогою якого встановлено, що ефективність вузькосмугових стратегій впливу зменшується з 95 % до 15 % для FHSS-систем, тоді як широкосмугова стратегія зберігає ефективність на рівні близько 85 %. Запропоновано багаторівневу архітектуру системи C-UAS з об'єднанням даних від різних датчиків на основі теорії свідчень Демпстера–Шафера, що забезпечує ймовірність виявлення 0,95 – 0,99 для радіокерованих дронів та 0,85 – 0,95 для апаратів з оптоволоконними лініями керування. Валідація програмного комплексу за експериментальними даними показала відхилення результатів моделювання не більше ±20 %, що підтверджує адекватність запропонованої моделі для інженерних розрахунків і попереднього аналізу кіберфізичних систем БпЛА.

СПИСОК ЛІТЕРАТУРИ

1. Elevating the Future of Mobility: UAV-enabled Intelligent Transportation Systems / A. Saboor et al. *ArXiv preprint arXiv: 2110.09934*. 2021. DOI: 10.1109/CommNet63022.2024.10793277.

2. Campion M., Ranganathan P., Faruque S. UAV Swarm Communication and Control Architectures: A Review. *Journal of Unmanned Vehicle Systems*. 2019. Vol. 7, №2. P. 93–106. DOI: 10.1139/juvs-2018-0009.

3. MAVLink Development Team: MAVLink Micro Air Vehicle Communication Protocol. 2020. UKR: https://mavlink.io/en.

4. DJI : AirLink – OcuSync Transmission Technology. DJI Developer Documentation. UKR: https://developer.dji.com/mobile-sdk/documentation/introduction/component-guide-airlink.html.

5. Torrieri D. J. Principles of Spread-Spectrum Communication Systems. 5th ed. Springer. 2022. URL: https://books.google.com.ua/books/about/Principles_of_Spread_Spectrum_Communicat.html?hl=ar&id=f5mMqZHGnusC&redir_esc=y.

6. ROS2-Based Simulation Framework for Cyberphysical Security Analysis of UAVs / U. Patil et al. *ArXiv preprint arXiv: 2410.03971*. 2024. DOI: 10.48550/arXiv.2410.03971.

7. Jacobsen R. H., Marandi A. An Integrated Simulation Platform for Assessing UAV Communication Vulnerabilities. *Proc. IEEE MILCOM*. 2021. P. 1–6. DOI: 10.1109/MILCOM52596.2021.9652900.

8. Security Challenges and Privacy Implications of UAV Cellular Communications: A Comprehensive Survey / S. A. Hadiwardoyo et al. *ArXiv preprint arXiv: 2212.05028*. 2022. DOI: 10.48550/arXiv.2212.05028.

9. A LoRa-Based UAV Monitoring System with Low Latency / Y. Zhang et al. 2021. Vol. 21, №19. P. 6507. DOI: 10.3390/s21196507.

10. Olabiyi O., Enofe B., Annamalai A. Unified Analysis of Air-to-Ground Propagation Models for UAV Communications. *Wireless Communications and Mobile Computing*. 2021. Vol. 2021, Art. №8838792.

DOI: 10.1155/2021/8838792.

11. ITU-R Recommendation P.1411-11 : Propagation Data and Prediction Methods for Short-Range Outdoor Radiocommunication Systems. ITU, Geneva, 2021. URL: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.1411-13-202509-I!!PDF-E.pdf.

12. A Survey of Monte Carlo Methods for Parameter Estimation / D. Luengo et al. *EURASIP J. Adv. Signal Process*. 2020. Vol. 2020, Art. №25. DOI: 10.1186/s13634-020-00675-6.

13. Why So Many Published Sensitivity Analyses Are False: A Systematic Review of Sensitivity Analysis Practices / A. Saltelli et al. *Environmental Modelling & Software*. 2021. Vol. 144, Art. №105226. DOI: 10.1016/j.envsoft.2021.105226.

14. Review and Simulation of Counter-UAS Sensors for Unmanned Traffic Management / C. De Miguel-Vela et al. *Sensors*. 2022. Vol. 22, №1. P. 189. DOI: 10.3390/s22010189.

15. A Survey on Detection, Classification, and Tracking of UAVs Using RF-Based Systems / B. H. Ahmed et al. *IEEE Access*. 2023. Vol. 11. P. 89091–89119. DOI: 10.1109/ACCESS.2023.3307256.

16. Detection and Classification of UAVs Using RF Fingerprints / M. Ezuma et al. *IEEE Access*. 2020. Vol. 8. P. 79743–79755. DOI: 10.1109/ACCESS.2020.2990603.

17. Enhancing Communication Security in Drones Using QRNG in FHSS / M. A. Khan et al. *Future Internet.* 2024. Vol. 16, №11. P. 412. DOI: 10.3390/fi16110412.

18. Exploiting Tethered and Untethered UAVs: A Hybrid Aerial Communication System / S. Khemiri et al. *Sci. Rep*. 2025. Vol. 15, Art. №15882. DOI: 10.1038/s41598-025-15882-8.

19. Pinel N., Lamotte N. Optically Powered and Controlled Drones Using Optical Fibers. *Photonics*. 2022. Vol. 9, №11. P. 882. DOI: 10.3390/photonics9110882.

20. DroneShield Ltd : C-UAS Software & Analytics. URL: https://www.droneshield.com/products-software.

21. Lee J., Hyun K., Park S. GPS Spoofing Detection and Mitigation for UAVs: A Comprehensive Survey. *Sensors*. 2022. Vol. 22, №23. P. 9412. DOI: 10.3390/s22239412.

22. Новіцький П. С., Степаняк М. В. Методи створення спрямованих електромагнітних завад для вибіркового впливу на GPS/GLONASS. *Вимірювальна техніка та метрологія*. 2024. Т. 86, № 2. С. 105–112. DOI: 10.23939/istcmtm2025.02.105.

23. Новіцький П. С., Степаняк М. В. Новітні технології зі створення електромагнітних завад для протидії літальним об'єктам. *Комп'ютерні технології друкарства*. 2024. № 1 (51). С. 121–133. DOI: 10.32403/2411-9210-2024-1-51-121-133.

Стаття надійшла до редакції 06.03.2026.
Стаття пройшла рецензування 18.03.2026.
Стаття опублікована 31.03.2026.

Новіцький Павло Сергійович – аспірант кафедри комп'ютеризованих систем автоматики, ORCID: 0000-0002-7300-5262, e-mail: pavlo.s.novitskyi@lpnu.ua.

Степаняк Михайло Васильович – канд. техн. наук, доцент кафедри комп'ютеризованих систем автоматики», ORCID: 0000-0003-1859-4495, e-mail: mykhailo.v.stepaniak@lpnu.ua.

Національний університет «Львівська політехніка».