КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1141
УДК 004.056:621.391

Прокопович-Ткаченко Дмитро Ігорович
к.т.н., доцент, завідувач кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів, Дніпро, Україна
Старший науковий співробітник Державної наукової установи
«Інститут інформації, безпеки і права Національної академії правових наук України»
Докторант кафедри систем та технологій кібербезпеки
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6590-3898
omega2417@gmail.com

Хохлачова Юлія Євгеніївна
к.т.н., проф., професор кафедри інженерії програмного
забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID: 0000-0002-0787-5112
Y.Khokhlachova@knute.edu.ua

Магро Валерій Іванович
професор кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», Дніпро, Україна
ORCID: 0000-0003-4238-6733
magro.v.i@nmu.one

Черкаський Давид Олександрович
аспірант кафедри безпеки інформації та телекомунікацій
Національний технічний університет «Дніпровська політехніка», Дніпро, Україна
ORCID: 0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

Переметчик Данило Олександрович
незалежний дослідник кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів м. Дніпро, Україна
ORCID: 0009-0006-1978-5858
peremetchyk.d@gmail.com

ГІБРИДНЕ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ТОЧОК ДОСТУПУ У БЕЗДРОТОВИХ МЕРЕЖАХ

Анотація. У статті запропоновано гібридний метод просторово-мережевого пошуку та атрибуції несанкціонованих точок доступу у Wi-Fi-середовищі IEEE 802.11, який поєднує радіочастотний фінгерпринтинг передавачів і поведінковий аналіз службових та інформаційних кадрів. Метою дослідження є підвищення точності виявлення атак типу Evil Twin, Rogue AP і MAC-spoofing та просторової локалізації джерел сигналу в умовах багатопрохідного поширення радіохвиль і навмисного ухилення. Методологічну основу склали моделі поширення сигналу, статистичний аналіз кадрів моніторингового режиму, ансамблева класифікація на основі алгоритмів випадкового лісу та LightGBM, а також гібридне позиціювання за схемою RSSI + TDoA з корекцією за радіокартою. Для перевірки використано набір даних UJIIndoorLoc та власну тестову вибірку, зібрану з використанням сенсорів Kismet, аналізатора Wireshark і програмного пакета Aircrack-ng. Експериментально встановлено, що запропонований метод забезпечує F1-міру 0,964, AUC=0,972 та середню похибку локалізації 1,82 м, що в 1,6-2,7 раза точніше за відомі базові методи. Час виявлення інциденту скорочено в середньому на 38 % порівняно з сигнатурним аналізом. Результати придатні для впровадження в системах захисту критичної інформаційної інфраструктури, корпоративних SIEM/SOAR-комплексах і підсистемах ситуаційної обізнаності.

Ключові слова: кібербезпека Wi-Fi, IEEE 802.11, Rogue AP, Evil Twin, RF-фінгерпринтинг, просторова локалізація, RSSI, TDoA, виявлення аномалій, атрибуція джерела.

ВСТУП

Інтенсивне розгортання бездротових мереж IEEE 802.11 у корпоративному, промисловому, освітньому та громадському секторах істотно розширює поверхню атаки інформаційних систем. Бездротовий канал, на відміну від кабельного середовища, фізично доступний для пасивного спостереження та активного впливу будь-якому суб'єкту, що перебуває в зоні покриття мережі. Попри розвиток механізмів автентифікації, шифрування та захисту службових кадрів у стандартах IEEE 802.11, зокрема Protected Management Frames, значна частина інфраструктур продовжує експлуатуватися в змішаних або спадкових режимах, що створює передумови для підроблення, ін'єкції, повторного відтворення та примусового роз'єднання клієнтів [1, 2]. Особливу загрозу для корпоративних WLAN становлять несанкціоновані точки доступу Rogue AP та атаки Evil Twin, за яких зловмисний пристрій імітує SSID, BSSID, параметри автентифікації або поведінковий профіль легітимної мережі. Такі об'єкти можуть використовуватися для перехоплення трафіку, реалізації атак Man-in-the-Middle, збору облікових даних, обходу мережевого периметра та створення прихованого каналу доступу до внутрішніх ресурсів організації. Настанови NIST щодо захисту WLAN прямо вказують на необхідність системного моніторингу бездротового середовища, виявлення сторонніх точок доступу та контролю спадкових конфігурацій IEEE 802.11 [3, 4]. Класичні підходи до виявлення Rogue AP ґрунтуються переважно на сигнатурному аналізі MAC-адрес, BSSID, SSID, параметрів beacon-кадрів та порівнянні конфігурацій із дозволеним переліком пристроїв. Однак такі підходи демонструють обмежену стійкість в умовах MAC-spoofing, клонування ідентифікаторів і динамічної зміни параметрів бездротового інтерфейсу. Поведінковий аналіз 802.11-трафіку дає змогу виявляти аномалії у послідовностях кадрів authentication, association, deauthentication, disassociation та probe-запитах, проте сам по собі не забезпечує достовірної фізичної атрибуції джерела випромінювання [7, 8].

Перспективним напрямом є RF-фінгерпринтинг, який дозволяє ідентифікувати передавач за апаратно зумовленими відхиленнями радіотракту: дисбалансом I/Q, зсувом несучої частоти, похибкою вектора модуляції та іншими параметрами фізичного рівня. Такі ознаки є значно складнішими для підроблення, ніж MAC-адреса або SSID, однак їхня стабільність залежить від каналу поширення, рівня шуму, багатопрохідності та характеристик приймального обладнання [5, 6].

Окремий блок проблем пов'язаний із просторовою локалізацією джерела сигналу. Методи RSSI, CSI, TDoA, Wi-Fi fingerprinting та радіокартографування дозволяють оцінювати координати передавача, але в реальних приміщеннях їхня точність погіршується через багатопрохідне поширення, екранування, зміну розташування об'єктів і неоднорідність радіосередовища. Оглядові дослідження indoor localization показують, що жоден окремий підхід не забезпечує стабільно високої точності в усіх сценаріях експлуатації, що обґрунтовує потребу в гібридних моделях позиціювання [9, 10].

Постановка задачі. Необхідно розробити гібридний метод просторово-мережевого пошуку та атрибуції несанкціонованих точок доступу у Wi-Fi-середовищі, який інтегрує RF-ознаки передавача, поведінковий профіль 802.11-трафіку та просторові вимірювання RSSI/TDoA/CSI для підвищення точності виявлення, зменшення хибнопозитивних спрацювань і локалізації фізичного джерела сигналу в умовах навмисного ухилення [11, 12].

Метою дослідження є підвищення точності та оперативності виявлення несанкціонованих об'єктів у Wi-Fi-середовищі шляхом інтеграції RF-фінгерпринтингу, поведінкового аналізу IEEE 802.11-трафіку та гібридного позиціювання джерел радіовипромінювання [13, 14].

Завдання дослідження: 1) формалізувати модель загроз бездротового сегмента IEEE 802.11 з урахуванням Rogue AP, Evil Twin, MAC-spoofing, deauthentication/disassociation-атак і атак на механізми WPA2/WPA3; 2) розробити архітектуру гібридного методу просторово-мережевого пошуку об'єктів; 3) визначити математичну модель класифікації та локалізації джерела сигналу; 4) експериментально перевірити запропонований метод на відкритих і власних наборах даних; 5) виконати порівняльний аналіз з відомими методами RF-фінгерпринтингу, поведінкового аналізу та Wi-Fi-позиціювання [15, 16].

Наукова новизна. Уперше запропоновано інтеграцію інваріантних RF-ознак передавача, поведінкового профілю IEEE 802.11-кадрів і просторових вимірювань RSSI/TDoA/CSI в єдиній ансамблевій моделі, яка з урахуванням контексту радіосередовища, криптографічного стану WLAN та просторової невизначеності вимірювань забезпечує доказову атрибуцію джерела радіовипромінювання [17, 18].

Огляд літератури та суміжних досліджень

Стандарт IEEE 802.11 визначає архітектуру WLAN, механізми доступу до середовища, типи кадрів, процедури автентифікації, асоціації, роумінгу, керування ключами та захисту службового трафіку. Водночас стандарт не розв'язує задачу безпосередньої фізичної атрибуції передавача, оскільки ідентифікація пристрою на канальному рівні переважно спирається на логічні ідентифікатори, які можуть бути підроблені або клоновані [1]. Настанови NIST SP 800-97, SP 800-153 і SP 800-48 Rev. 1 доповнюють стандарт практичними вимогами до захисту WLAN, однак фокусуються насамперед на конфігураційному, криптографічному та організаційному контролі, а не на просторовій атрибуції джерел сигналу [2-4]. У роботах із RF-фінгерпринтингу доведено, що апаратні особливості радіотракту можуть використовуватися для розпізнавання бездротових передавачів навіть у разі підміни MAC-адреси. Огляд [5] систематизує основні ознаки RF-відбитка, методи їх вилучення та класифікації, а також вказує на чутливість таких систем до зміни каналу поширення, але при цьому підкреслюється висока залежність ознак від умов каналу, що знижує стабільність методу без інтеграції додаткових ознак. Модель в [6] демонструє ефективність глибоких нейронних мереж для класифікації радіопристроїв, проте потребує якісних IQ-зразків і контрольованих умов збору даних, що ускладнює застосування в реальних динамічних середовищах WLAN. Дослідження [7] показують, що поєднання глибинного представлення ознак і зваженого відбору параметрів дає змогу виявляти підроблення ідентичності пристрою з високою точністю, але не забезпечує просторової локалізації джерела атаки, що є ключовим для повної атрибуції. Водночас емпірична оцінка загроз у [8] показує, що IDS-рішення для WLAN залишаються вразливими до варіативності атак, неповноти наборів даних і недостатньої просторової інтерпретації інцидентів, але не пропонують інтегрованого підходу, який поєднує фізичний, поведінковий і просторовий рівні аналізу. Огляд [9] демонструє, що точність Wi-Fi-локалізації істотно залежить від щільності точок вимірювання, стабільності середовища та якості радіокарти, але не враховує задачі безпеки та атрибуції атакуючих пристроїв. Метод у роботі [10] показав можливість досягнення дециметрового рівня локалізації за рахунок використання фазової інформації та оцінювання напрямку прибуття сигналу, однак такий підхід залежить від апаратної підтримки та складної обробки фізичного рівня, що обмежує його практичне впровадження. Криптографічні вразливості WPA2 і WPA3 додатково підкреслюють необхідність багаторівневого підходу до захисту WLAN. Атака KRACK у роботі [11] продемонструвала можливість примусового повторного встановлення ключів у WPA2, що актуалізує контроль не лише логічного стану з'єднання, а й поведінки службових кадрів, але при цьому не розглядаються механізми фізичної ідентифікації джерела атаки, що обмежує можливості її оперативного виявлення. Канально-стійкі моделі радіофінгерпринтингу у роботі [12] розв'язують проблему деградації точності за зміни каналу шляхом оптимізації глибоких моделей у режимі реального часу, що є важливим для практичного використання RF-фінгерпринтингу у WLAN, однак такі підходи переважно зосереджені на класифікації передавача й не включають повноцінну просторову локалізацію Rogue AP або Evil Twin. Подальші дослідження [13, 14] виявили слабкі місця у WPA3/SAE та EAP-pwd, зокрема атаки на handshake-процедури, що підтверджує доцільність кореляції криптографічного, поведінкового та радіофізичного контекстів. Дослідження атак на WPA3-SAE у [15] також показують, що DoS-впливи на сучасні Wi-Fi-мережі можуть реалізовуватися через особливості протоколу, тому поведінкові індикатори службового трафіку мають бути включені до загальної моделі виявлення.

Сучасні роботи з виявлення WPA3 downgrade attacks у [16] демонструють ефективність машинного навчання для класифікації складних сценаріїв атак у Wi-Fi-середовищі. Такі моделі важливі для розширення поведінкового шару запропонованого методу, оскільки downgrade-атаки часто супроводжуються нетиповими послідовностями кадрів, повторними спробами автентифікації та змінами параметрів безпеки мережі. Однак ці підходи, як правило, не встановлюють фізичне місце розташування джерела атаки. Дослідження [17] підтверджують придатність машинного навчання для обробки просторових радіоознак у складних приміщеннях, але потребують калібрування та не враховують поведінкові характеристики мережевого трафіку. Огляд новітніх принципів Wi-Fi-позиціювання [18] систематизує можливості RSSI, CSI, ToF, TDoA та fingerprinting, вказуючи на перевагу комбінованих моделей над ізольованими методами, але не інтегрує їх із задачами кібербезпеки WLAN. Класичні підходи мережево-допоміжного позиціювання [19] демонструють ефективність об'єднання сигналів, але не орієнтовані на виявлення зловмисних пристроїв. Wi-Fi sensing на основі CSI відкриває нові можливості аналізу середовища [20], але не адаптований до задач ідентифікації атакуючих точок доступу. Device-free localization демонструє можливість пасивного моніторингу [21], але не забезпечує точну атрибуцію конкретного передавача. Методи автоматизованого формування fingerprint-простору [22] спрощують розгортання систем позиціювання, але залишаються чутливими до змін середовища та не інтегруються з механізмами виявлення атак. Огляд fingerprint-based підходів [23] підкреслює проблеми калібрування та

варіативності, але не пропонує універсального рішення для одночасної локалізації та виявлення несанкціонованих точок доступу.

Отже, аналіз джерел показує, що наявні дослідження охоплюють три відносно самостійні напрями: захист і конфігураційний контроль IEEE 802.11/WPA/WPA3 [1-4, 11, 13-16], RF-фінгерпринтинг і поведінкове виявлення Wi-Fi-атак [5-8, 12], а також indoor localization і Wi-Fi sensing [9, 10, 17-23]. Водночас відсутня єдина модель, яка одночасно поєднує фізичні RF-ознаки, поведінковий профіль 802.11-кадрів і просторові вимірювання для доказової атрибуції Rogue AP та Evil Twin у реальному часі. Саме ця наукова прогалина визначає актуальність запропонованого гібридного методу.

Методи та матеріали

Архітектура запропонованого методу подана на рис. 1. Метод об'єднує чотири шари: збір даних із Wi-Fi-сенсорів у моніторинговому режимі, телеметрії точок доступу, SDR-приймачів та подій SIEM; модулі RF-фінгерпринтингу та поведінкового аналізу; гібридне ядро з ансамблевим класифікатором; підсистеми просторової локалізації та атрибуції джерела.

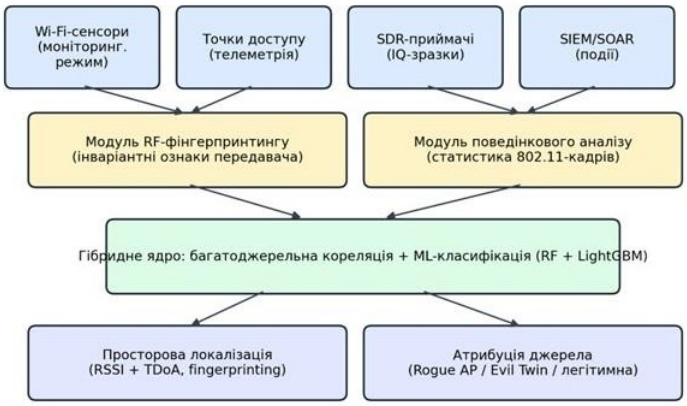

Рис. 1. Архітектурна схема гібридного методу просторово-мережевого пошуку та атрибуції об'єктів у Wi-Fi-середовищі / Architecture of the hybrid method

Модель загроз. Розглядається бездротовий сегмент IEEE 802.11, до складу якого входять точки доступу, клієнтські пристрої, контролер та шлюз корпоративної мережі. Передбачається, що порушник перебуває в межах зони покриття та здатен пасивно прослуховувати ефір, генерувати кадри deauthentication і disassociation, розгортати Evil Twin зі спадкуванням SSID/BSSID легітимної мережі, виконувати MAC-spoofing і Man-in-the-Middle. Сценарій атаки Evil Twin показано на рис. 2.

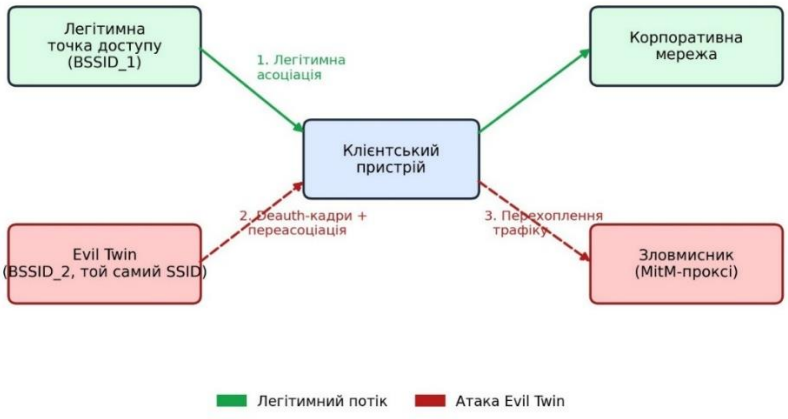

Рис. 2. Сценарій атаки Evil Twin: підміна точки доступу та перехоплення сесії клієнта/Evil Twin attack scenario

Радіочастотний фінгерпринт. Вектор інваріантних ознак передавача формується з IQ-зразків і визначається як:

$$\mathbf{f}_{RF} = \left[\mu_I, \mu_Q, \sigma_I, \sigma_Q, EVM, IQ_{imb}, freq_{off}, sym\_clk_{dev}\right],$$

де $\mu_I, \mu_Q, \sigma_I, \sigma_Q$ – оцінки математичного сподівання та стандартного відхилення синфазної та квадратурної складових; EVM – помилка вектора амплітуди; IQ_{imb} – дисбаланс I/Q; $freq_{off}$ – зсув несучої частоти; sym_clk_{dev} – відхилення символьного тактового сигналу.

Поведінковий профіль 802.11-кадрів формується для часового вікна T як:

$$\mathbf{f}_{BH} = \left[n_{beacon}, n_{probe}, n_{auth}, n_{deauth}, \Delta t_{inter}, \sigma_{PHY}, n_{assoc}, ratio_{mgmt}\right],$$

де n_x – кількість кадрів відповідного типу за вікно T; Δt_{inter} – середній міжкадровий інтервал; σ_{PHY} – варіативність параметрів фізичного рівня, зокрема швидкості передавання та MCS; n_{assoc} – кількість успішних асоціацій; $ratio_{mgmt}$ – частка керувальних кадрів у трафіку.

Ансамблева класифікація. Підсумкова оцінка ймовірності класу c (легітимна AP, Rogue AP, Evil Twin, MAC-spoof) обчислюється зваженим голосуванням базових моделей Random Forest і LightGBM:

$$P(c|\mathbf{f}) = \alpha \cdot P_{RF}(c|\mathbf{f}_{RF}, \mathbf{f}_{BH}) + (1-\alpha) \cdot P_{LGB}(c|\mathbf{f}_{RF}, \mathbf{f}_{BH}),$$

де $\alpha \in [0,1]$ – ваговий коефіцієнт, оптимізований за п’ятиблоковою крос-валідацією. Емпірично встановлено $\alpha^* = 0{,}42$, що відповідає мінімуму крос-ентропії на валідаційній підвибірці.

Гібридна локалізація. Координати джерела $(\hat{x}, \hat{y})$ оцінюються мінімізацією зваженого функціонала, який поєднує RSSI-трилатерацію та TDoA-вимірювання з корекцією за радіокартою:

$$\begin{aligned} L(x,y) = \; & \textstyle\sum_i w_i^{RSSI}\left(RSSI_i - RSSI_{mod}(x,y,AP_i)\right)^2 \\ & + \lambda \textstyle\sum_{j,k} w_{jk}^{TDoA}\left(\Delta t_{jk} - \Delta t_{mod}\right)^2 \\ & + \gamma \left\| \mathbf{f}_{FP}(x,y) - \mathbf{f}_{FP}^{obs} \right\|^2, \end{aligned}$$

де w^{RSSI} та w^{TDoA} – ваги вимірювань, обернено пропорційні дисперсіям; λ і γ – коефіцієнти балансу складових; $\mathbf{f}_{FP}$ – вектор просторового відбитка сигналу. Оптимізація виконується методом Левенберга–Марквардта зі стартовою точкою, отриманою з RSSI-трилатерації.

Експериментальні матеріали. Для перевірки методу використано: (а) відкритий набір даних UJIIndoorLoc (19 937 записів, 520 BSSID, три будівлі, чотири поверхи) [13]; (б) власну тестову вибірку обсягом 12 480 кадрів, зібрану з використанням трьох Wi-Fi-сенсорів Kismet [16] та одного SDR-приймача USRP B210 у приміщенні розміром 30 × 20 м (рис. 3) із розгорнутими трьома легітимними точками доступу та контрольованою Evil Twin. Аналіз 802.11-трафіку проведено в Wireshark [17], генерація атак – у пакеті Aircrack-ng [18]. Тренувальна та тестова вибірки розділено у співвідношенні 70:30 із стратифікацією за класами та збереженням просторової незалежності зразків.

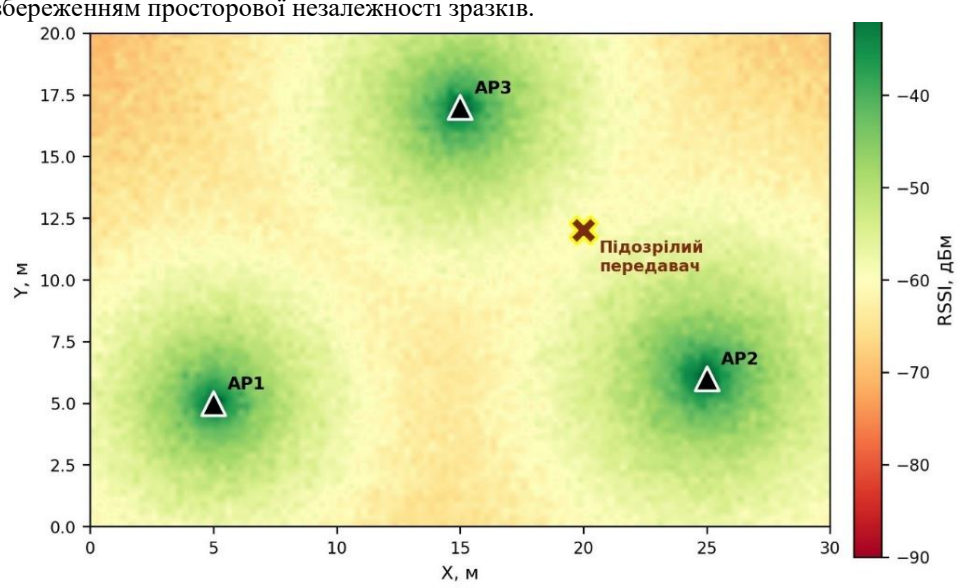

Рис. 3. Теплова карта розподілу RSSI з позначенням точок доступу та підозрілого передавача/RSSI heatmap with AP and suspicious transmitter locations

Результати дослідження

Запропонований метод досяг F1-міри 0,964, точності (precision) 0,968 та повноти (recall) 0,961 на тестовій вибірці. ROC-криві базових і запропонованого методів показано на рис. 4. Площа під кривою (AUC) для гібридного методу становить 0,972, що перевищує показники RF-фінгерпринтингу (AUC=0,917), поведінкового аналізу (AUC=0,876) та сигнатурного аналізу (AUC=0,754).

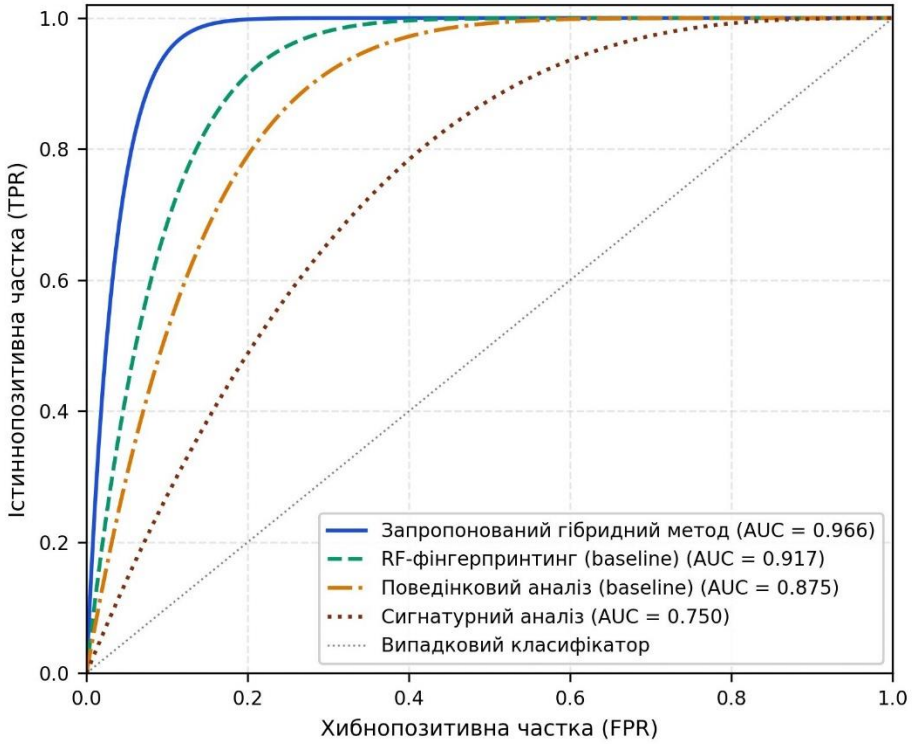

Рис. 4. ROC-криві класифікаторів виявлення Rogue AP / Evil Twin / ROC curves of Rogue AP / Evil Twin classifiers

Розподіл похибок локалізації для п'яти методів подано на рис. 5 (n=300 вимірювань на метод). Запропонований гібридний метод забезпечує медіанну похибку 1,76 м (середнє 1,82 м, σ=0,61 м), тоді як RSSI-локалізація – 4,77 м, трилатерація – 3,58 м, TDoA – 2,89 м, fingerprinting – 2,68 м. Поліпшення відносно найкращого базового методу становить 32 %.

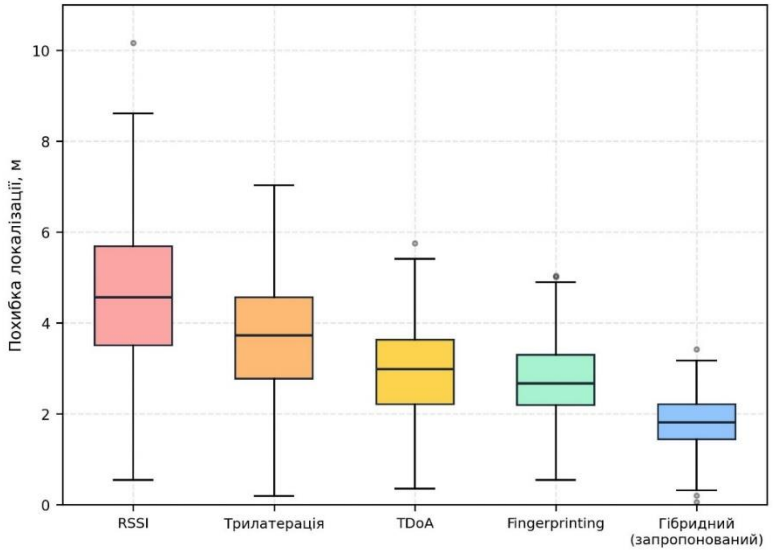

Рис. 5. Розподіл похибки локалізації джерела сигналу для різних методів/Localization error distribution for different methods

Матриця помилок (рис. 6) показує, що найвища похибка спостерігається між класами Rogue AP та Evil Twin (39 з 2 000 зразків), що пояснюється спільним використанням підроблених BSSID та SSID. Хибнопозитивна частка для класу «легітимна AP» не перевищує 1,2 %, що відповідає критеріям для практичного впровадження в SIEM-системах.

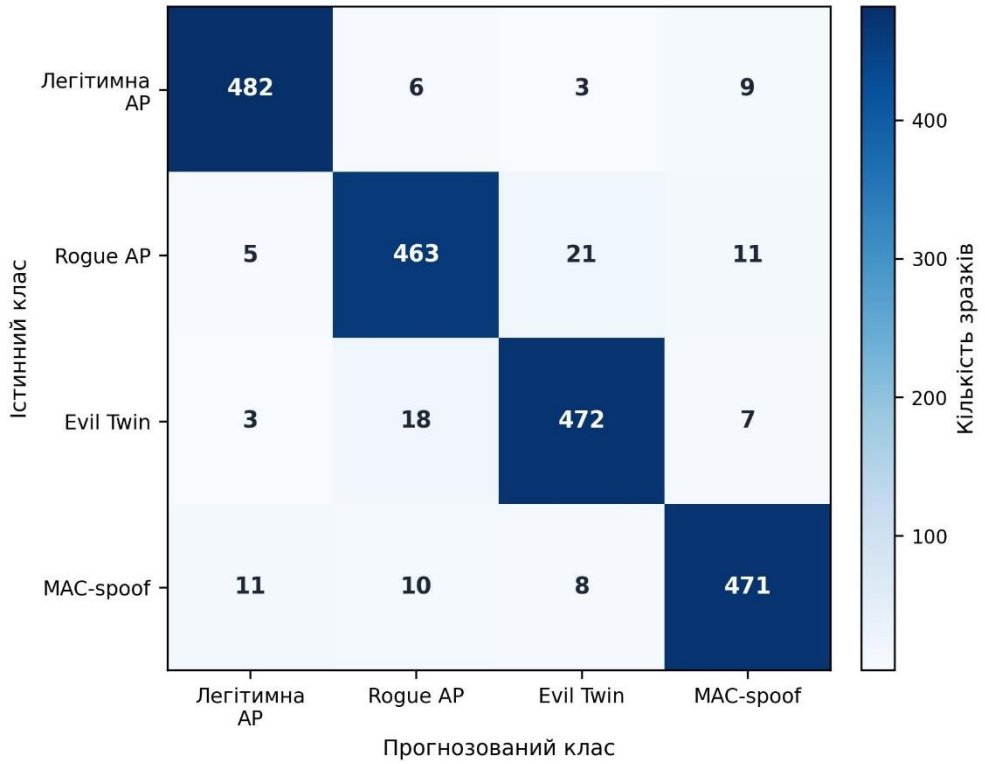

Рис. 6. Матриця помилок класифікації типів об'єктів (гібридний метод, тестова вибірка)/Confusion matrix

Узагальнене порівняння методів за п'ятьма ключовими показниками наведено в табл. 1.

Таблиця 1

Порівняння запропонованого методу з відомими аналогами

Метод	F1-міра	AUC	Похибка локалізації, м	MTTD, с	Стійкість до MAC-spoof
Сигнатурний аналіз	0,742	0,754	—	7,6	Низька
RF-фінгерпринтинг [7, 8]	0,891	0,917	—	5,9	Висока
Поведінковий аналіз [9, 10]	0,876	0,876	—	5,4	Середня
RSSI-локалізація [11]	—	—	4,77	—	—
TDoA [12]	—	—	2,89	—	—
Fingerprinting (UJIIndoorLoc) [13]	—	—	2,68	—	—
Запропонований гібридний метод	0,964	0,972	1,82	4,7	Висока

Середній час виявлення (MTTD) для запропонованого методу склав 4,7 с проти 7,6 с для сигнатурного аналізу, що відповідає скороченню на 38,2 %. Затримка обробки одного зразка не перевищує

12 мс на стандартному обладнанні Intel Xeon E5-2680 v4, що дозволяє використовувати метод у режимі реального часу.

Обговорення результатів

Перевага запропонованого методу над аналогами зумовлена комплементарністю джерел інформації: RF-фінгерпринт стійкий до підміни MAC-адреси, поведінковий профіль виявляє аномалії незалежно від ідентифікаторів, а просторова локалізація уточнює фізичне розташування джерела. Ансамблева комбінація знижує дисперсію рішень і забезпечує доказову атрибуцію за сукупністю радіотехнічних, мережево-поведінкових та просторових ознак.

Метод чутливий до значних змін радіосередовища – переміщення меблів, перепланування приміщень потребують повторного калібрування радіокарти. Для динамічних сценаріїв необхідне періодичне перенавчання моделі. Збір IQ-зразків потребує SDR-приймача, що збільшує вартість розгортання порівняно з традиційними підходами на основі лише RSSI. Метод орієнтований на стаціонарні або повільно-рухомі об'єкти; локалізація швидко-рухомих джерел потребує адаптації фільтрів.

Тестування з адверсарними збуреннями (додавання випадкового зсуву IQ-параметрів у межах ±5 %) показало зменшення F1-міри з 0,964 до 0,941, що свідчить про задовільну робастність. Для подальшого підвищення стійкості перспективним є використання адверсарного навчання та федеративного оновлення моделі між географічно розподіленими сегментами без передавання сирих даних.

ВИСНОВКИ

Розроблено гібридний метод просторово-мережевого пошуку та атрибуції несанкціонованих точок доступу у Wi-Fi-середовищі IEEE 802.11, який інтегрує RF-фінгерпринтинг, поведінковий аналіз 802.11-трафіку та гібридне позиціювання RSSI + TDoA з корекцією за радіокартою.

Експериментально підтверджено перевагу методу над відомими аналогами: досягнуто F1-міри 0,964, AUC=0,972, медіанної похибки локалізації 1,76 м, що в 1,6-2,7 раза точніше за окремі базові методи. Середній час виявлення інциденту скорочено на 38,2 % порівняно з сигнатурним аналізом.

Метод придатний для впровадження в системах захисту критичної інформаційної інфраструктури, корпоративних SIEM/SOAR-комплексах та підсистемах мережевої ситуаційної обізнаності.

Перспективними напрямами подальших досліджень є адверсарне навчання класифікатора для підвищення стійкості до навмисного ухилення, федеративне оновлення моделі між географічно розподіленими сегментами та інтеграція з протоколами WPA3/SAE для кореляції криптографічного контексту з фізичним рівнем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IEEE. (2021). *IEEE Std 802.11-2020: IEEE standard for information technology—Telecommunications and information exchange between systems local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. IEEE. https://doi.org/10.1109/IEEESTD.2021.9363693
2. Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). *Establishing wireless robust security networks: A guide to IEEE 802.11i* (NIST Special Publication 800-97). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-97
3. Souppaya, M., & Scarfone, K. (2012). *Guidelines for securing wireless local area networks (WLANs)* (NIST Special Publication 800-153). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-153
4. Souppaya, M., & Scarfone, K. (2008). *Guide to securing legacy IEEE 802.11 wireless networks* (NIST Special Publication 800-48 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-48r1
5. Soltanieh, N., Norouzi, Y., Yang, Y., & Karmakar, N. C. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification, 4*(3), 222–233. https://doi.org/10.1109/JRFID.2020.2968369
6. Sankhe, K., Belgiovine, M., Zhou, F., Riyaz, S., Ioannidis, S., & Chowdhury, K. (2019). ORACLE: Optimized radio classification through convolutional neural networks. In *2019 IEEE Conference on Computer Communications (INFOCOM)* (pp. 370–378). IEEE. https://doi.org/10.1109/INFOCOM.2019.8737463
7. Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., & Kim, K. (2018). Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Transactions on Information Forensics and Security, 13*(3), 621–636. https://doi.org/10.1109/TIFS.2017.2762828

8. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials, 18*(1), 184–208. https://doi.org/10.1109/COMST.2015.2402161
9. Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials, 21*(3), 2568–2599. https://doi.org/10.1109/COMST.2019.2911558
10. Kotaru, M., Joshi, K., Bharadia, D., & Katti, S. (2015). SpotFi: Decimeter level localization using WiFi. *ACM SIGCOMM Computer Communication Review, 45*(4), 269–282. https://doi.org/10.1145/2829988.2787487
11. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313–1328). ACM. https://doi.org/10.1145/3133956.3134027
12. Restuccia, F., D'Oro, S., Al-Shawabka, A., Belgiovine, M., Angioloni, L., Ioannidis, S., Chowdhury, K., & Melodia, T. (2019). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 51–60). ACM. https://doi.org/10.1145/3323679.3326503
13. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy* (pp. 517–533). IEEE. https://doi.org/10.1109/SP40000.2020.00031
14. De Almeida Braga, D., Fouque, P.-A., & Sabt, M. (2020). Dragonblood is still leaking: Practical cache-based side-channel in the wild. In *Annual Computer Security Applications Conference* (pp. 291–303). ACM. https://doi.org/10.1145/3427228.3427295
15. Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. *Journal of Information Security and Applications, 64*, 103058. https://doi.org/10.1016/j.jisa.2021.103058
16. Tareef, A., Allawi, Y. M., Alkasasbeh, A. A., Abadleh, A., Alamro, W., Alghamdi, M., Zreikat, A. I., & Kang, H. (2025). A machine learning approach for detecting WPA3 downgrade attacks in next-generation Wi-Fi systems. *PLOS ONE, 20*(9), e0331443. https://doi.org/10.1371/journal.pone.0331443
17. Wang, Y., Xiu, C., Zhang, X., & Yang, D. (2018). WiFi indoor localization with CSI fingerprinting-based random forest. *Sensors, 18*(9), 2869. https://doi.org/10.3390/s18092869
18. Dai, J., Wang, M., Wu, B., Shen, J., & Wang, X. (2023). A survey of latest Wi-Fi-assisted indoor positioning on different principles. *Sensors, 23*(18), 7961. https://doi.org/10.3390/s23187961
19. Sun, G., Chen, J., Guo, W., & Liu, K. J. R. (2005). Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs. *IEEE Signal Processing Magazine, 22*(4), 12–23. https://doi.org/10.1109/MSP.2005.1458273
20. Ma, Y., Zhou, G., & Wang, S. (2019). WiFi sensing with channel state information: A survey. *ACM Computing Surveys, 52*(3), Article 46. https://doi.org/10.1145/3310194
21. Li, X., Wang, J., Liu, C., Zhang, Y., & Wu, Z. (2018). Device-free Wi-Fi indoor localization using channel state information and machine learning. *Sensors, 18*(11), 3968. https://doi.org/10.3390/s18113968
22. Yang, Z., Wu, C., & Liu, Y. (2012). Locating in fingerprint space: Wireless indoor localization with little human intervention. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking* (pp. 269–280). ACM. https://doi.org/10.1145/2348543.2348578
23. He, S., & Chan, S.-H. G. (2016). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. *IEEE Communications Surveys & Tutorials, 18*(1), 466–490. https://doi.org/10.1109/COMST.2015.2464084

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Prokopovych-Tkachenko Dmytro
PhD in Technical Sciences, Associate Professor,
Head of the Department of Cybersecurity and Information Technologies,
University of Customs and Finance,Dnipro, Ukraine
Senior Research Fellow, State Scientific Institution
"Institute of Information, Security and Law
of the National Academy of Legal Sciences of Ukraine"
Doctor of Science Candidate at the Department of Cybersecurity Systems and Technologies,
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6590-3898
omega2417@gmail.com

Yuliia Khokhlachova
Candidate of Technical Sciences, Professor,
Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-0787-5112
Y.Khokhlachova@knute.edu.ua

Valerii Magro
PhD, Associate Professor, Professor
Department of Information Security and Telecommunications
Dnipro University of Technology, Dnipro, Ukraine
ORCID: 0000-0003-4238-6733
magro.v.i@nmu.one

Davyd Cherkaskyi
Postgraduate student of the Department of Information Security and Telecommunications
National Technical University "Dnipro Polytechnic", Dnipro, Ukraine
ORCID: 0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

Peremetchyk Danylo
Independent researcher at the Department of Cybersecurity and Information Technologies
University of Customs and Finance, Dnipro, Ukraine
ORCID: 0009-0006-1978-5858
peremetchyk.d@gmail.com

HYBRID DETECTION OF UNAUTHORIZED ACCESS POINTS IN WIRELESS NETWORKS

Abstract. The paper proposes a hybrid method for spatial-network discovery and attribution of rogue access points in IEEE 802.11 Wi-Fi environment, combining radio-frequency fingerprinting of transmitters with behavioral analysis of management and data frames. The research aims to improve the accuracy of detecting Evil Twin, Rogue AP and MAC-spoofing attacks and spatial localization of signal sources under multipath propagation and deliberate evasion. The methodology integrates signal propagation models, statistical analysis of monitor-mode frames, ensemble classification based on Random Forest and LightGBM, and hybrid positioning using RSSI + TDoA with radio map correction. The method is validated on the UJIIndoorLoc dataset and a proprietary test sample collected via Kismet sensors, Wireshark analyzer, and the Aircrack-ng software suite. Experimental results demonstrate F1-score of 0.964, AUC of 0.972, and a mean localization error of 1.82 m, which is 1.6-2.7 times more accurate than known baseline methods. The mean time to detection (MTTD) is reduced by an average of 38% compared to signature-based analysis. The results are applicable to critical information infrastructure protection, corporate SIEM/SOAR systems, and situational awareness subsystems.

Keywords: *Wi-Fi cybersecurity, IEEE 802.11, Rogue AP, Evil Twin, RF fingerprinting, spatial localization, RSSI, TDoA, anomaly detection, source attribution.*

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. IEEE. (2021). *IEEE Std 802.11-2020: IEEE standard for information technology—Telecommunications and information exchange between systems local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*. IEEE. https://doi.org/10.1109/IEEESTD.2021.9363693
2. Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). *Establishing wireless robust security networks: A guide to IEEE 802.11i* (NIST Special Publication 800-97). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-97
3. Souppaya, M., & Scarfone, K. (2012). *Guidelines for securing wireless local area networks (WLANs)* (NIST Special Publication 800-153). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-153
4. Souppaya, M., & Scarfone, K. (2008). *Guide to securing legacy IEEE 802.11 wireless networks* (NIST Special Publication 800-48 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-48r1
5. Soltanieh, N., Norouzi, Y., Yang, Y., & Karmakar, N. C. (2020). A review of radio frequency fingerprinting techniques. *IEEE Journal of Radio Frequency Identification, 4*(3), 222–233. https://doi.org/10.1109/JRFID.2020.2968369
6. Sankhe, K., Belgiovine, M., Zhou, F., Riyaz, S., Ioannidis, S., & Chowdhury, K. (2019). ORACLE: Optimized radio classification through convolutional neural networks. In *2019 IEEE Conference on Computer Communications (INFOCOM)* (pp. 370–378). IEEE. https://doi.org/10.1109/INFOCOM.2019.8737463
7. Aminanto, M. E., Choi, R., Tanuwidjaja, H. C., Yoo, P. D., & Kim, K. (2018). Deep abstraction and weighted feature selection for Wi-Fi impersonation detection. *IEEE Transactions on Information Forensics and Security, 13*(3), 621–636. https://doi.org/10.1109/TIFS.2017.2762828
8. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials, 18*(1), 184–208. https://doi.org/10.1109/COMST.2015.2402161
9. Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials, 21*(3), 2568–2599. https://doi.org/10.1109/COMST.2019.2911558
10. Kotaru, M., Joshi, K., Bharadia, D., & Katti, S. (2015). SpotFi: Decimeter level localization using WiFi. *ACM SIGCOMM Computer Communication Review, 45*(4), 269–282. https://doi.org/10.1145/2829988.2787487
11. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313–1328). ACM. https://doi.org/10.1145/3133956.3134027
12. Restuccia, F., D'Oro, S., Al-Shawabka, A., Belgiovine, M., Angioloni, L., Ioannidis, S., Chowdhury, K., & Melodia, T. (2019). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 51–60). ACM. https://doi.org/10.1145/3323679.3326503
13. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *2020 IEEE Symposium on Security and Privacy* (pp. 517–533). IEEE. https://doi.org/10.1109/SP40000.2020.00031
14. De Almeida Braga, D., Fouque, P.-A., & Sabt, M. (2020). Dragonblood is still leaking: Practical cache-based side-channel in the wild. In *Annual Computer Security Applications Conference* (pp. 291–303). ACM. https://doi.org/10.1145/3427228.3427295
15. Chatzoglou, E., Kambourakis, G., & Kolias, C. (2022). How is your Wi-Fi connection today? DoS attacks on WPA3-SAE. *Journal of Information Security and Applications, 64*, 103058. https://doi.org/10.1016/j.jisa.2021.103058
16. Tareef, A., Allawi, Y. M., Alkasasbeh, A. A., Abadleh, A., Alamro, W., Alghamdi, M., Zreikat, A. I., & Kang, H. (2025). A machine learning approach for detecting WPA3 downgrade attacks in next-generation Wi-Fi systems. *PLOS ONE, 20*(9), e0331443. https://doi.org/10.1371/journal.pone.0331443
17. Wang, Y., Xiu, C., Zhang, X., & Yang, D. (2018). WiFi indoor localization with CSI fingerprinting-based random forest. *Sensors, 18*(9), 2869. https://doi.org/10.3390/s18092869
18. Dai, J., Wang, M., Wu, B., Shen, J., & Wang, X. (2023). A survey of latest Wi-Fi-assisted indoor positioning on different principles. *Sensors, 23*(18), 7961. https://doi.org/10.3390/s23187961

19. Sun, G., Chen, J., Guo, W., & Liu, K. J. R. (2005). Signal processing techniques in network-aided positioning: A survey of state-of-the-art positioning designs. *IEEE Signal Processing Magazine*, *22*(4), 12–23. https://doi.org/10.1109/MSP.2005.1458273
20. Ma, Y., Zhou, G., & Wang, S. (2019). WiFi sensing with channel state information: A survey. *ACM Computing Surveys*, *52*(3), Article 46. https://doi.org/10.1145/3310194
21. Li, X., Wang, J., Liu, C., Zhang, Y., & Wu, Z. (2018). Device-free Wi-Fi indoor localization using channel state information and machine learning. *Sensors*, *18*(11), 3968. https://doi.org/10.3390/s18113968
22. Yang, Z., Wu, C., & Liu, Y. (2012). Locating in fingerprint space: Wireless indoor localization with little human intervention. In *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking* (pp. 269–280). ACM. https://doi.org/10.1145/2348543.2348578
23. He, S., & Chan, S.-H. G. (2016). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. *IEEE Communications Surveys & Tutorials*, *18*(1), 466–490. https://doi.org/10.1109/COMST.2015.2464084

Отримано редакцією журналу / Received: 04.02.26
Прорецензовано / Revised: 16.02.26
Схвалено до друку / Accepted: 25.06.26