КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1279
УДК 004.056.53:004.7.057.4

Банах Роман Ігорович
Доктор філософії, доцент кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка», Львів, Україна
ORCID: 0000-0001-6897-8206
roman.i.banakh@lpnu.ua

ВИЯВЛЕННЯ АТАКИ EVIL TWIN НА БЕЗДРОТОВІ МЕРЕЖІ СТАНДАРТУ IEEE 802.11 В УМОВАХ ЩІЛЬНОЇ ЗАБУДОВИ

Анотація. Розглянуто проблему виявлення атак типу Evil Twin на бездротові мережі стандарту IEEE 802.11 в умовах щільної міської забудови з монолітно-каркасними залізобетонними конструкціями, що суттєво послаблюють радіосигнал у діапазонах 2.4 та 5 ГГц. У сценарії повного клонування точки доступу зловмисник копіює як ідентифікатор мережі, так і апаратну адресу легітимного пристрою, що унеможливлює застосування класичних методів детекції, які базуються на аналізі ідентифікаторів керуючих кадрів. Запропоновано метод виявлення, що використовує мережу з чотирьох розподілених у приміщенні Wi-Fi-сенсорів для безперервного вимірювання індикатора потужності прийнятого сигналу легітимної точки доступу та аналізує геометричні співвідношення між сенсорами. Метод поєднує два незалежні детектори – детектор парних залишків S(t), що базується на статистичній моделі різниць потужності сигналу між усіма парами сенсорів і чутливий до тривалих порушень просторового патерну послаблення сигналу, а також імпульсний детектор на основі z-оцінки кожного сенсора відносно його калібрувальної норми, який реагує на короткі локально-сильні відхилення тривалістю 2-5 хвилин. Подальша класифікація імпульсних інтервалів за магнітудою піка z-оцінки дозволяє розділити сильні зовнішні атаки від нормальної людської активності всередині приміщення. Експериментальна перевірка проведена на наборі з 40 розмічених атак з використанням чотирьох типів антен, розташованих ззовні бетонної будівлі. Метод досяг 60% повноти та 85.7% точності на рівні окремих атак, та 100% повноти на рівні сесій атак (груп з десяти послідовних атак для кожної антени). Розроблений підхід не потребує спеціалізованого обладнання, працює зі стандартними Wi-Fi-чіпсетами та може бути впроваджений у наявну інфраструктуру для захисту об'єктів критичної інфраструктури.

Ключові слова: Атака Evil Twin; бездротові мережі; IEEE 802.11; Wi-Fi; RSSI; статистична детекція аномалій; захист бездротових мереж; ослаблення радіосигналу; сенсорна мережа.

ВСТУП

Постановка проблеми. Бездротові мережі стандарту IEEE 802.11 (Wi-Fi) стали основним способом доступу до корпоративних інформаційних ресурсів, систем керування технологічними процесами та об'єктами критичної інфраструктури. Поряд із цим, відкритий характер радіоканалу робить такі мережі вразливими до широкого спектру атак на канальному та фізичному рівнях, серед яких одну з найбільш загрозливих позицій займає атака типу Evil Twin (ET), метою якої є створення зловмисником фальшивої точки доступу, що видає себе за легітимну. Внаслідок успішної атаки клієнтські пристрої підключаються до контрольованої зловмисником інфраструктури, що відкриває можливості для перехоплення даних, атак типу man-in-the-middle (MITM), впровадження шкідливого коду та збору облікових записів.

Існуючі підходи до детекції цієї атаки переважно ґрунтуються на виявленні відмінностей між фальшивою та легітимною точками доступу, а саме різниця в MAC-адресі, параметрах захищеного з'єднання, часі формування beacon-кадрів, часі формування beacon-кадрів, особливостях коливань тактового генератора, тощо. Проте у сценарії повного клонування, коли зловмисник із належним обладнанням повністю копіює як ідентифікатор мережі (англ, Service Set Identifier, SSID), так і апаратну адресу (англ. Basic Service Set Identifier) легітимного пристрою, а також відтворює тип та параметри криптографічного захисту, ідентифікаційний рівень детекції стає принципово непридатним, оскільки для клієнта і навіть для інших мережних пристроїв обидві точки виглядають ідентичними.

Окремою складністю стає середовище щільної міської забудови з монолітно-каркасними залізобетонними конструкціями, що типово для багатоповерхових офісних та урядових будівель.

Сталебетонні стіни вносять значне послаблення сигналу на робочих частотах Wi-Fi (2.4 та 5 ГГц), що ускладнює як саму атаку ззовні, так і її детекцію всередині приміщення. Слабкі або частково заглушені сигнали від передавача, який проводить атаку, можуть бути нерозрізнимі від фонового шуму, природної варіації середовища або від руху людей у приміщенні. Таким чином, виникає потреба у методах детекції, які залишаються чутливими навіть у разі, коли зловмисний сигнал знаходиться на межі рівня шуму, та одночасно є стійкими до хибних спрацювань через нормальну активність у приміщенні.

Аналіз останніх досліджень і публікацій. Проблема безпеки бездротових мереж стандарту IEEE 802.11 залишається актуальною попри впровадження сучасних протоколів захисту. Зокрема, у роботі [1] показано вразливості Dragonblood у протоколі WPA3 та EAP-pwd, оскільки навіть найновіші стандарти не забезпечують абсолютного захисту, особливо проти атак, що оперують на канальному та фізичному рівнях. Це обумовлює потребу в незалежних від криптографічного рівня методах виявлення зловмисної активності.

Питання детекції атак ET досліджувалося авторським колективом протягом останніх років. У роботі [2] запропоновано підхід до перехоплення метаданих Wi-Fi пристроїв зловмисників з метою їхньої просторової локалізації, що заклало основу для подальшого розвитку методів аналізу радіосередовища. У роботі [6] розроблено метод виявлення ET атак на основі моделі класифікації методом найближчих сусідів (англ. K-Nearest Neighbors, KNN), що використовує статистичні ознаки потужності сигналу (англ. Received Signal Strength Indicator, RSSI); у роботі [9] цей підхід було розширено застосуванням підходу data mining для виявлення атак за патернами поведінки потужності сигналу. Однак ці роботи зосереджувалися переважно на ідентифікації вторгнень.

Інші дослідники також пропонували різноманітні підходи. У роботі [3] представлено ефективну схему виявлення атак ET на основі аналізу взаємодій клієнт-точка доступу. У [4] Yang та ін. розробили активний клієнто-сторонній метод детекції з використанням статистичних технік порівняння часу відгуку. Laurendeau та Barbeau у [5] запропонували використання гіперболічної кластеризації позицій на основі вимірювань RSSI для виявлення інсайдерських атак, що концептуально близько до використання просторової інформації RSSI.

Окремий напрямок становлять методи на основі машинного навчання. У роботі [7] застосовано згорткові нейронні мережі (англ. Convolutional Neural Network, CNN) для класифікації ET атак за патернами Wi-Fi трафіку. У дослідженні [8] автори продемонстрували можливість використання ML-моделей для блокування небезпечних запитів у мережі, що є дотичним напрямком захисту бездротових систем. Спільною рисою цих робіт є залежність від великих обсягів розмічених даних, що ускладнює перенесення моделей між різними середовищами розгортання.

Питання технологій формування діаграми спрямованості (beamforming), які можуть створювати патерни, подібні до ET атак, розглянуто в [10], де описано QoE-орієнтовану оптимізацію band steering. У сучасних роботах [14], [15] показано, що сама технологія beamforming може використовуватися для інтегрованих сенсорно-комунікаційних систем (джиттерів), що відкриває нові можливості для побудови додаткових каналів детекції аномалій.

Мета статті. Метою статті є розробка та експериментальна перевірка методу виявлення атак ET на бездротові мережі стандарту IEEE 802.11 у сценарії повного клонування точки доступу, що функціонує в умовах щільної міської забудови з монолітно-каркасними залізобетонними конструкціями та реалізується на стандартному Wi-Fi-обладнанні без модифікації мережної інфраструктури.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Сформулювати математичну модель просторових співвідношень потужності сигналу між розподіленою мережею Wi-Fi-сенсорів у статичному приміщенні.
2. Розробити алгоритм виявлення аномалій у цій моделі, чутливий як до тривалих, так і до коротких порушень патерну.
3. Запропонувати спосіб розрізнення підозрілих атак від нормальної людської активності всередині приміщення.
4. Провести експериментальну перевірку методу на наборі реальних атак з використанням антен різних типів і характеристик.
5. Оцінити кількісні показники якості методу (повноту і точність) та визначити межі його застосовності.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Індикатор потужності прийнятого сигналу. RSSI – це числова оцінка рівня радіосигналу, який приймається бездротовим адаптером від конкретного передавача, виражена в децибел-міліватах (dBm). Це значення доступне через стандартні механізми мережного стека операційних систем та через

службові кадри IEEE 802.11 (Probe Response, Beacon), що робить його базовою спостережуваною ознакою будь-якої Wi-Fi мережі без необхідності додаткового апаратного забезпечення.

У спрощеній моделі вільного простору потужність прийнятого сигналу описується формулою Фрііса (1).

$$P_R(d) = P_t + G_t + G_r + 20log_{10}\left(\frac{\lambda}{4\pi R}\right) \quad (1)$$

де P_t – потужність передавача, G_t і G_r – коефіцієнти підсилення антен передавача і приймача, d – відстань, λ – довжина хвилі. Для реальних приміщень ця модель доповнюється коефіцієнтом затухання n і втратами на перешкодах (2).

$$P_R(d) = P_R(d_0) - 10nlog_{10}\left(\frac{d}{d_0}\right) - \sum_k L_k \quad (2)$$

де L_k– втрати потужності на k-ій перешкоді (стіна, перекриття, перегородка). Згідно з рекомендацією ITU-R P.2040-3 [16] швидкість загасання радіохвилі в діелектричному матеріалі при $\tan\delta < 0{,}5$ обчислюється за формулою (3).

$$A_{dielectric} = 1636 \cdot \frac{\sigma}{\sqrt{\eta'}} \quad (3)$$

де η'– реальна частина відносної діелектричної проникності, σ – провідність матеріалу (С/м). Для бетону рекомендація наводить параметри $\eta' = 5{,}24$ та $\sigma = 0{,}0462 \cdot f^{0{,}7822}$ С/м, де f– частота в ГГц, що дає (4).

$$A_{dielectric}(f) \approx 33{,}0 \cdot f^{0{,}7822} \quad (4)$$

Підставивши робочі частоти Wi-Fi, отримуємо швидкість загасання приблизно 65,5 дБ/м для 2,4 ГГц та 116,2 дБ/м для 5 ГГц. Для типової бетонної стіни товщиною 20-30 см це відповідає втратам близько 13-20 дБ на частоті 2,4 ГГц та 23-35 дБ на частоті 5 ГГц, не враховуючи додаткових втрат на відбиття на межах “повітря-бетон” (близько 4-6 дБ на дві межі).

У монолітно-каркасних залізобетонних конструкціях наявність арматурної сітки створює додатковий ефект часткового електромагнітного екранування, що збільшує сумарні втрати на 5-15 дБ порівняно з простим бетоном [17]. Таким чином, для зовнішніх стін щільної міської забудови сумарні втрати на проходження сигналу можуть сягати 30-50 дБ на частоті 5 ГГц, що формує специфічні умови дослідження даної роботи. Сигнал пристрою, який здійснює атаку, що надходить з вулиці до внутрішніх сенсорів, опиняється на межі рівня шуму приймачів, а методи детекції повинні зберігати чутливість в цих умовах.

Модель атаки ET та класифікація сценаріїв. Атака ET полягає у створенні зловмисником фіктивної точки доступу, яка імітує легітимну з метою примушування клієнтських пристроїв до підключення. За ступенем імітації можна виділити три класи атак:

1. Базовий клон – збігається лише SSID, інші параметри (BSSID, тип шифрування) відрізняються. Найпростіший для виявлення за допомогою аналізу метаданих [2, 3].
2. Частковий клон – збігаються SSID і BSSID, але можуть відрізнятися параметри захищеного з’єднання, послідовності beacon-кадрів, характеристики апаратного джиттера. Підлягає виявленню методами аналізу часових патернів і характеристик передачі [4].
3. Повний клон – повністю відтворюються SSID, BSSID, тип і параметри шифрування, послідовності керуючих кадрів та, за умови наявності у зловмисника відповідного обладнання, часові характеристики передачі. Класичні методи детекції [3, 4] стають принципово непридатними для цього сценарію.

Ключова інваріантна властивість, яку зловмисник не може клонувати – це фізичне розташування власного передавача. Незалежно від ступеня програмної імітації, радіохвилі від клона поширюються від іншої геометричної точки, ніж від легітимної точки доступу, що неминуче відображається у розподілі потужності сигналу в просторі.

Просторова унікальність радіосигналу в мережі сенсорів. Нехай у приміщенні розгорнуто мережу з N Wi-Fi-сенсорів з фіксованим розташуванням, кожен з яких неперервно вимірює RSSI цільової точки

доступу. У статичному середовищі (відсутність руху людей, переміщення обладнання, температурних змін) вектор виміряних потужностей (5).

$$r(t) = \left(r_1(t), r_2(t), \dots r_N(t)\right)^T \tag{5}$$

де $r_i(t)$ – значення RSSI (dBm), зафіксоване i-м сенсором у момент t; N – кількість сенсорів у мережі; T – операція транспонування. Для рівномірно дискретизованих вимірювань $t = k\Delta t$, де Δt – період опитування сенсорів.

У статичному середовищі (відсутність руху людей, переміщення обладнання, температурних змін) кожна координата $r_i(t)$ поводиться як квазі-стаціонарний випадковий процес з повільною часовою еволюцією та невеликою дисперсією, обумовленою тепловим шумом приймача та мультіпасовим розповсюдженням сигналу. Сам вектор $r(t)$ як такий не є інформативною ознакою – його значення залежать від багатьох випадкових факторів (мікроколивання положення передавача, флуктуації середовища, шум калібрування приймачів). Натомість просторова структура – парні різниці значень між сенсорами (6).

$$d_{ij}(t) = r_i(t) - r_j(t), \quad i, j \in \{1, \dots, N\}, \|i \neq j\| \tag{6}$$

де $d_{ij}(t)$ – різниця потужностей сигналу, виміряних сенсорами i та j в момент t (dB), – визначається виключно геометрією приміщення (відстанями і перешкодами від точки доступу до кожного сенсора) і є унікальним відбитком конкретної конфігурації "точка доступу–сенсори–приміщення". У статичних умовах статистичні характеристики цих різниць задовольняють умову (7).

$$\mathbb{E}\left[d_{ij}(t)\right] \approx const, std[d_{ij}(t)] \ll \left|\mathbb{E}[d_{ij}(t)]\right| \tag{7}$$

де $\mathbb{E}[\cdot]$ – математичне сподівання, $std[\cdot]$ – стандартне відхилення. Тобто середнє значення парної різниці є стабільною величиною, а її варіація мала порівняно з самим значенням.

Поява другого передавача T' з іншим розташуванням $p' \neq p_{AP}$, де p_{AP} розташування точки доступу, призводить до того, що на кожному сенсорі і приймається сума двох сигналів з різними значеннями послаблення (8).

$$\tilde{r}_i(t) = 10log_{10}\left(10^{r_i^{AP}(t)/10} + 10^{r_i^{T'}(t)/10}\right) + \xi_i(t) \tag{8}$$

де $\tilde{r}_i(t)$ – сумарне (фактично виміряне) значення RSSI на i-му сенсорі при одночасній роботі двох передавачів; $r_i^{AP}(t) = P_{AP} - L_i^{AP}$– значення RSSI від легітимної точки доступу, що визначається потужністю її передавача P_{AP} за вирахуванням сумарних втрат на шляху L_i^{AP} між точкою доступу та i-м сенсором (включаючи геометричне розповсюдження за формулою Фрііса та послаблення на перешкодах); аналогічно $r_i^{T'}(t) = P_{T'} - L_i^{T'}$ гіпотетичне значення RSSI від клона за умови його ізольованої роботи; $\xi_i(t)$ – адитивний гаусівський шум приймача. Структура виразу $10\log_{10}(10^{x/10} + 10^{y/10})$ обумовлена тим, що дві потужності в логарифмічних одиницях (dBm) не можна додавати безпосередньо: фізичне додавання електромагнітних сигналів відбувається на рівні лінійних потужностей (мВт), для чого виконується перехід $P_{[\text{мВт}]} = 10^{P_{[\text{dBm}]}/10}$, сумування лінійних значень і зворотне перетворення.

Оскільки коефіцієнти послаблення L_i^{AP} та $L_i^{T'}$ для двох передавачів з різним просторовим розташуванням є некорельованими функціями положення i-го сенсора (вони визначаються різними траєкторіями розповсюдження, різними наборами перешкод та різними кутами падіння на стіни), парні різниці $d_{ij}(t)$ під дією другого передавача змінюються нелінійно і неоднорідно по парах сенсорів. Цей геометричний інваріант є фундаментальною основою запропонованого методу детекції.

Для скалярної агрегації порушень просторової структури всі парні залишки об'єднуються в єдиний індикатор аномалії (9).

$$S(t) = \sum_{(i,j)\in P} e_{ij}(t)^2, \quad e_{ij}(t) = d_{ij}(t) - \mu_{ij}(t) \tag{9}$$

де $e_{ij}(t)$ – поточний залишок між виміряним значенням пари і її повільною експоненційно-ковзною оцінкою $\mu_{ij}(t)$; $|P| = \binom{N}{2}$ – кількість пар сенсорів. У статичних умовах $S(t)$ знаходиться поблизу нуля; у разі появи другого передавача – стрімко зростає.

Поріг детекції просторової аномалії визначається калібрувальними статистиками за правилом трьох сигм (10).

$$\lambda = (K_\sigma \cdot \bar{\sigma})^2 \cdot |P|, \quad \bar{\sigma} = \frac{1}{|P|} \sum_{(i,j)\in P} \sigma_{ij}^{cal} \tag{10}$$

де K_σ – параметр чутливості (у даній роботі $K_\sigma = 3$); σ_{ij}^{cal} – стандартне відхилення парної різниці (i,j) за калібрувальний період; $\bar{\sigma}$ – усереднене стандартне відхилення по всіх парах. Подія "просторова аномалія" фіксується, коли $S(t) > \lambda$.

Статистичні методи виявлення аномалій у часових рядах RSSI. Для оцінки відхилення поточного значення спостережуваної величини від її норми застосовується класична концепція z-оцінки (11).

$$z_i(t) = \frac{r_i(t) - \mu_i(t)}{\sigma_i} \tag{11}$$

де $\mu_i(t)$ – поточна оцінка середнього (baseline), σ_i – стандартне відхилення в умовах "норми". За правилом трьох сигм, у разі гаусівського розподілу ймовірність $|z| > 3$ становить менше 0,3% що дозволяє інтерпретувати викид цього порогу як статистично значущу аномалію.

Для оцінки $\mu_i(t)$у потоковому режимі використовується експоненційне ковзне середнє (англ. Exponential Moving Average, EMA) (12).

$$\mu_i(t) = (1-\alpha)\mu_i(t-1) + \alpha \cdot r_i(t), \quad 0 < \alpha < 1 \tag{12}$$

де параметр α визначає ефективне вікно спостереження, а отже, ефективна тривалість пам'яті становить приблизно $T_{\text{eff}} = 2/\alpha - 1$ часових кроків. Менше значення α дає більш стабільний, але повільніше адаптивний baseline; більше – швидкий і шумний. Підбір α є компромісом між чутливістю до зміни і стійкістю до шуму.

Для коректної роботи методу необхідна калібрувальна фаза T_{cal} – період заздалегідь відомої "норми", протягом якого оцінюються початкові значення μ_i та σ_i, що використовуються як стартова точка адаптивного процесу та як стабільний знаменник у формулі z-оцінки.

Обґрунтування комбінованої архітектури детектора. Розрізнення сценаріїв "коротка локальна аномалія" і "тривале просторове порушення" вимагає двох взаємодоповнюючих детекторних механізмів, що працюють на різних часових масштабах:

- Геометричний детектор – оперує парними різницями $d_{ij}(t)$, агрегує інформацію по $\binom{N}{2}$ парах, що дає високу чутливість до тривалих стабільних аномалій, але не реагує на короткочасні викиди тривалістю менше характерного часу адаптації EMA.
- Імпульсний детектор – оперує миттєвими відхиленнями $z_i(t)$ окремих сенсорів, реагує на короткі викиди тривалістю від 1-2 хвилин незалежно від їхньої просторової структури.

Спільне застосування обох детекторів забезпечує покриття обох класів аномалій без необхідності компромісного налаштування одного механізму під обидва режими, а додаткова класифікація імпульсних інтервалів за магнітудою піка z-оцінки дозволяє відрізнити сильні зовнішні впливи (атаки) від слабких внутрішніх (наприклад, рух людей).

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження проведено в межах проєкту, що фінансується за грантом Президента України для молодих вчених (докторів філософії/кандидатів наук до 35 років), наданим Національним фондом досліджень України (проєкт № 2025.05/0046), за підтримки Національного університету "Львівська політехніка". Експериментальна перевірка методу здійснена в реальних умовах щільної міської забудови на території одного із корпусів університету.

Експериментальний стенд.

Легітимна точка доступу. Як цільова легітимна точка доступу використано пристрій MikroTik cAP ac (RBcAPGi-5acD2nD-XL) [13] – точку доступу класу enterprise з двома радіомодулями (2,4 ГГц та 5 ГГц), яка широко застосовується в корпоративних мережах. Для експерименту активовано модуль 2,4

ГГц з типовою конфігурацією (WPA2-PSK, фіксований канал). Точка доступу розташована стаціонарно всередині приміщення на висоті близько 2,5 м.

Мережа сенсорів моніторингу.

Розгорнуто мережу з N=4 сенсорів моніторингу потужності сигналу, побудованих на базі мікроконтролера Espressif ESP32-C6 [11] – однокристальної SoC з вбудованим Wi-Fi-радіо стандарту IEEE 802.11 b/g/n у діапазоні 2,4 ГГц. Кожен сенсор періодично сканує радіоефір у режимі моніторингу, виконує пасивне прослуховування beacon-кадрів від цільової точки доступу та зчитує значення RSSI з блоку дескриптора пакета (RxControl), що надається SDK Espressif.

Сенсори розташовані у фіксованих точках на периметрі захищеного приміщення (геометрична конфігурація обрана таким чином, щоб забезпечити просторову різноманітність сенсорів стосовно зовнішніх стін, через які потенційно проходитиме зловмисний сигнал). Параметри розгортання:

- Період опитування: $\Delta t_{raw} = 1$с;
- Подальша агрегація: середнє значення RSSI за вікном 1 хв;
- Кількість пар сенсорів: $P| = \binom{4}{2} = 6$.

Платформа збору та зберігання даних. Кожен сенсор передає поточні вимірювання RSSI через локальну Wi-Fi-мережу до сервера, де працює часова база даних InfluxDB [12] – спеціалізоване рішення для роботи з часовими рядами і підтримкою агрегацій, інтерполяцій та запитів мовою Flux. Структура запису:

- Вимірювання: wifi_scan;
- Поле: rssi (тип float, одиниця dBm);
- Мітки: deviceID (ідентифікатор сенсора), ssid (ідентифікатор спостережуваної мережі);
- Часова мітка: UTC, прецизія 1 с.

Подальший аналіз даних виконано мовою Python з використанням бібліотек pandas, numpy та matplotlib [18, 19, 20].

Імітація атаки.

Обладнання для імітації атаки. Для імітації атаки ET використано одноплатний комп'ютер Raspberry Pi 4B із операційною системою RPiOS та USB-адаптер Alfa AWUS036NHA на чіпсеті Atheros AR9271, що підтримує режим монітора та ін'єкцію пакетів, який є стандартним інструментом у дослідженнях безпеки бездротових мереж [21]. Адаптер дозволяє створювати фіктивну точку доступу з повністю контрольованими параметрами (SSID, BSSID, тип шифрування, послідовності beacon-кадрів), що відповідає сценарію повного клонування.

Програмна реалізація атаки виконана з використанням стандартних утиліт пакета aircrack-ng (airbase-ng) та hostapd з налаштуванням, що повторювало параметри легітимної точки доступу MikroTik: ідентичний SSID, скопійований BSSID, той самий тип шифрування WPA2-PSK з аналогічним паролем [22], [23].

Антенне обладнання

Для дослідження залежності якості детекції від характеристик випромінювача застосовано чотири різні зовнішні антени (табл. 1).

Таблиця 1

Характеристики зовнішніх антен у досліді

Назва антени	Тип антени	Підсилення	Діапазон частот
Alfa APA-M25	Панельна спрямована	9 dBi	2,4 ГГц, 5 ГГц
Yagi 16 dBi	Спрямована (хвильовий канал)	16 dBi	2.4 ГГц
Log-periodic 800-6000	Логперіодична широкосмугова	5-7 dBi	0,8-6 ГГц
Alfa 9dBi	Всеспрямована штиркова	9 dBi	2.4 ГГц

Пристрій з якого було імітовано атаки почергово розташовувався зовні будівлі на відстані від 5 до, приблизно 50 метрів. Біло обрано десять навколо будівлі де було встановлено обладнання, що відповідає реалістичному сценарію атаки на корпоративну мережу із прилеглої території (рис. 1).

Як видно з рис. 1 імітація атаки проводилась у десятьох місцях навколо будівлі де знаходиться приміщення, які були визначені як найімовірніші місця для проведення справжньої атаки.

Рис. 1. Схема будівлі, розстановки обладнання, місця імітації атаки

Протокол експерименту.

Експеримент проведений 20 травня 2026 року. Часова структура експерименту наведена у табл. 2.

Таблиця 2

Часовий протокол експерименту

Період	Тривалість	Зміст
07:00 – 10:00	3 год	Калібрувальне вікно – статичне середовище
10:06 – 10:24	18 хв	Підготовка обладнання (присутність двох осіб у приміщенні)
10:37 – 11:52	1 год 15 хв	Сесія 1: атаки з Alfa APA-M25 (10 атак)
12:15 – 13:30	1 год 15 хв	Сесія 2: атаки з Yagi 16 dBi (10 атак)
14:10 – 15:25	1 год 15 хв	Сесія 3: атаки з log-periodic антеною (10 атак)
16:17 – 17:33	1 год 16 хв	Сесія 4: атаки з Alfa 9 dBi (10 атак)

У кожній сесії проведено по 10 окремих атак тривалістю 3 хвилини кожна з інтервалами між атаками 8 хвилин. Загалом за день виконано 40 розмічених атак. Між сесіями приміщення залишалося порожнім (без людей), що забезпечило чистоту експериментальних даних. Точні часові межі кожної атаки фіксувалися у журналі експерименту та зберігалися у вигляді JSON-структури для подальшого автоматизованого зіставлення з результатами роботи детектора.

Протокол експерименту.

Для кількісної оцінки якості детекції використано стандартні метрики бінарної класифікації, адаптовані до часової структури даних.

Повнота (Recall) – частка реальних атак, для яких алгоритм детектора видав попередження (13).

$$\text{Recall} = \frac{|\{a \in \mathcal{A} : \text{detected}(a)\}|}{|\mathcal{A}|} \tag{13}$$

де $\mathcal{A}$ – множина розмічених, підтверджених (ground truth) атак; атака a вважається детектованою, якщо існує інтервал спрацювання I, що перетинається з нею з допуском ±1 хв.

Точність (Precision) – частка інтервалів спрацювання, які відповідають реальним атакам (14).

$$\text{Precision} = \frac{|\mathcal{I}_{\text{TP}}|}{|\mathcal{I}_{\text{TP}}| + |\mathcal{I}_{\text{FP}}|} \tag{14}$$

де $\mathcal{I}_{\text{TP}}$ – інтервали, що перетинаються хоча б з однією атакою з $\mathcal{A}$; $\mathcal{I}_{\text{FP}}$ – інтервали, які не перетинаються з жодною атакою.

Для коректної оцінки введено додаткову множину інтервалів людської активності $\mathcal{H}$ – час, протягом якого в приміщенні були люди (підготовка обладнання у проміжку 10:06-10:24). Інтервали спрацювання, що повністю містяться у $\mathcal{H}$, виключаються з підрахунку як хибнопозитивних (бо алгоритм коректно ідентифікує реальну фізичну активність), так і з підрахунку повноти.

Додатково обчислюються показники на рівні сесій – кількість сесій атак (з чотирьох), у яких алгоритм виявив принаймні одну атаку. Цей показник характеризує практичну цінність методу для

систем моніторингу: навіть часткова детекція сесії дозволяє вчасно оповістити оператора безпеки про підозрілу активність.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Стабільність калібрувальної фази. Тривимірне утворення параметрів алгоритму виконано на калібрувальному вікні $T_{\text{cal}} = [07{:}00,\ 10{:}00]$, протягом якого приміщення залишалося порожнім, а легітимна точка доступу – єдиним джерелом сигналу (рис. 2).
Обчислені статистичні характеристики парних різниць для калібрувального вікна наведено у табл. 3.

Таблиця 3

Статистики парних різниць RSSI за калібрувальний період

Пара (i, j)	$\mathbb{E}[d_{ij}]$, dBm	$\text{std}[d_{ij}]$, dbm
(1, 2)	−11,63	0,41
(1, 3)	−15,10	0,32
(1, 4)	+6,68	0,59
(2, 3)	−3,46	0,25
(2, 4)	+18,31	0,50
(3, 4)	+21,78	0,46

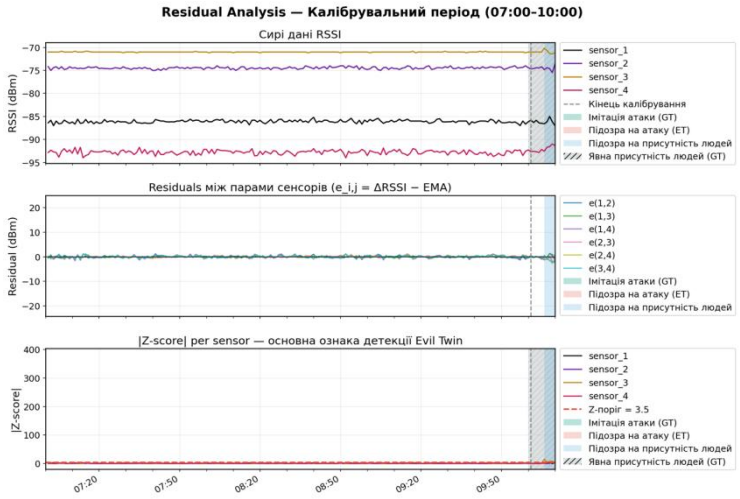

Рис. 2. Стабільність калібрувальної фази (07:00–10:00) – RSSI чотирьох сенсорів, парні залишки $e_{ij}(t)$ та модулі z-оцінок $|z_i(t)|$ у відсутності атак

Середнє стандартне відхилення $\bar{\sigma} = 0{,}42$ dBm; обчислений за формулою (10) поріг індикатора $S(t)$ за формулою (9) становить $\lambda = 9{,}51$.

Загальний перебіг експерименту. Загальна картина роботи методу за весь день експерименту представлена на рис. 3., на якому чітко виділяються чотири кластери зелених міток ground truth, що відповідають чотирьом сесіям атак з різними антенами, а також невелика сіра заштрихована зона у проміжку 10:00 – 10:25, що позначає присутність двох осіб у приміщенні під час підготовки обладнання.

Алгоритм виявив три тривалих інтервали підозри на Evil Twin (зони, виділені червоним кольором), що практично повністю перекривають кластери атак сесій 1, 2 і 3:

- 10:46 – 11:28 (42 хв, пік z = 293 на сенсорі sensor_3) – сесія Alfa APA-M25;
- 12:24 – 13:15 (51 хв, пік z = 311 на сенсорі sensor_3) – сесія Yagi;
- 14:19 – 15:17 (58 хв, пік z = 385 на сенсорі sensor_3) – сесія log-periodic.

Цікавою особливістю є те, що в усіх трьох випадках максимальну реакцію демонструє один і той самий сенсор sensor_3, що очевидно є наслідком його просторового розташування ближче до точки доступу, відповідно і отримував найсильніше значення потужності.

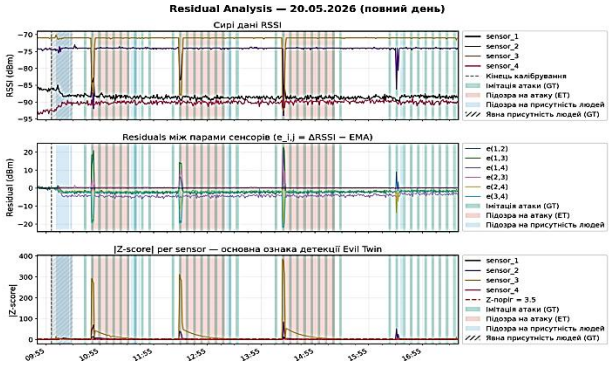

Рис. 3. Загальний перебіг експерименту 20.05.2026 із накладенням інтервалів детекції

Окремо алгоритм виявив шість коротких імпульсних інтервалів меншої магнітуди (зони, виділені синім кольором, відповідають класу “Detected People”), з яких два (тривалістю 15 хв та 2 хв на початку дня) точно збігаються із зафіксованою людською активністю. Кількісні показники якості детекції. Сумарні показники якості детекції за весь експериментальний день наведено у табл. 4.

Таблиця 4

Підсумкові метрики якості детекції

Показник	Значення
Загальна кількість імітаційних атак	40
Детектовано	24
Пропущено	16
Повнота (Recall), окремі атаки	60,0%
Хибні інтервали (False Positives)	1
Інтервали із присутністю людей (виключено)	2
Точність (Precision)	85,7%
Повнота на рівні сесій	4 з 4 (100%)

Розподіл повноти по типах антен представлено у табл. 5.

Таблиця 2

Часовий протокол експерименту

Антена	Детектовано/усього	Повнота	Пік z під час сесії
Alfa APA-M25	6/10	60%	293
Yagi 16 dBi	7/10	70%	311
Log-periodic	8/10	80%	385
Alfa 9 dBi	0/10	0%	4

Особливу увагу звертає різке падіння повноти для антени Alfa 9 dBi порівняно з іншими трьома антенами. Аналіз цієї особливості наведено у наступному розділі.

Загальний перебіг експерименту.

Сесія № 1 із антеною Alfa APA-M25. Перша сесія атак (рис. 4) демонструє характерний для всіх “сильних” сесій патерн.

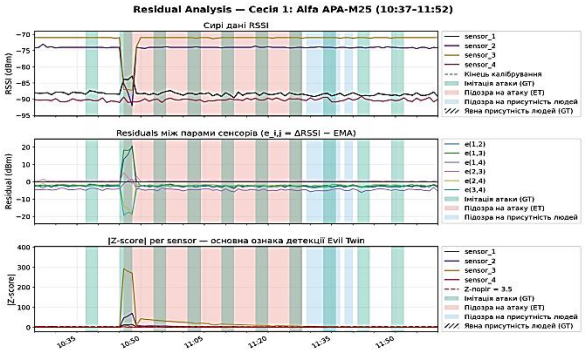

Рис. 4. Результати аналізу відрізку 10:37-11:52 із накладенням інтервалів детекції

У момент початку імітації атаки (приблизно 10:46, на 9 хвилин пізніше від першої позначеної атаки внаслідок необхідності прогріву калібрувальної EMA) спостерігається різкий злам просторової структури сигналу: сенсори sensor_2 і sensor_3 фіксують короткочасний провал потужності легітимного сигналу до -95 dBm (на 13-14 dBm нижче калібрувального рівня), тоді як sensor_4 одночасно показує підйом до – 70 dBm. Така картина типова для колізії beacon-кадрів двох передавачів – клон зловмисника глушить легітимну точку доступу на тих сенсорах, де він приймається сильніше.

Залишки $e_{ij}(t)$ синхронно відхиляються від нуля з амплітудою до 20 dBm, а z-оцінка сенсора sensor_3 досягає піка z ≈ 293, що на два порядки перевищує калібрувальний рівень. Після цього спостерігається повільний експоненційний спад z-оцінки, обумовлений адаптацією EMA, протягом якого алгоритм продовжує класифікувати інтервал як підозру на Evil Twin. Усі 10 атак сесії потрапляють у цей інтервал, з яких сім зараховано як детектовані з допуском ±1 хв; три залишилися поза інтервалом через те, що відбулися після того, як EMA вже наздогнала новий рівень.

Також можна побачити хибну ідентифікацію на восьмій точці, де алгоритм хибно ідентифікував атаку як приступність людей у приміщенні.

Сесія № 2 із антеною Yagi 16 dBi. Друга сесія атак повторює патерн першої з ще більш вираженою магнітудою, де пік z-оцінки досягає z=311, тривалість інтервалу спрацювання – 51 хв (рис. 5).

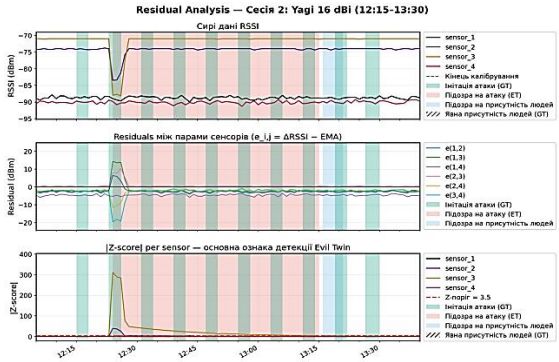

Рис. 5. Результати аналізу відрізку 12:15-13:30 із накладенням інтервалів детекції

Висока спрямованість антени Yagi (16 dBi) забезпечує концентрований радіопотік, що особливо сильно впливає на сенсор sensor_3. Сім з десяти атак цієї сесії потрапили в інтервал спрацювання. Також, один інтервал був хибно ідентифікований як присутність людей у приміщенні.

Сесія №3 із антеною Logperiodic. Третя сесія (рис. 6) показала найвищий пік z-оцінки серед усіх – z = 385, та найбільшу тривалість інтервалу спрацювання (58 хв). Широкосмугова логперіодична антена забезпечила найкращу геометричну ефективність “опромінення” зони сенсорів через зовнішню стіну. В результаті, алгоритмом було виявлено 8 з 10 атак.

На відміну від попередніх двох антен не було хибних спрацювань – не виявлено.

Сесія №4 із антеною Alfa 9 dBi. Четверта сесія (рис. 7) демонструє межу фізичної видимості атаки для застосованої конфігурації сенсорів.

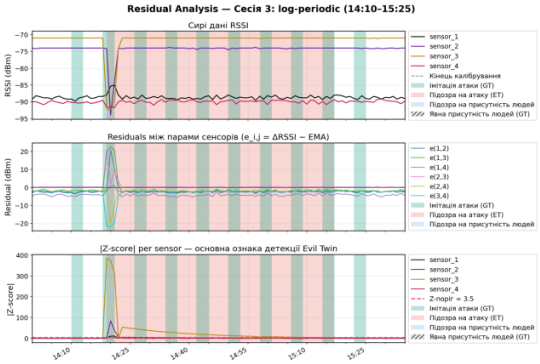

Рис. 6. Результати аналізу відрізку 14:10-15:25 із накладенням інтервалів детекції

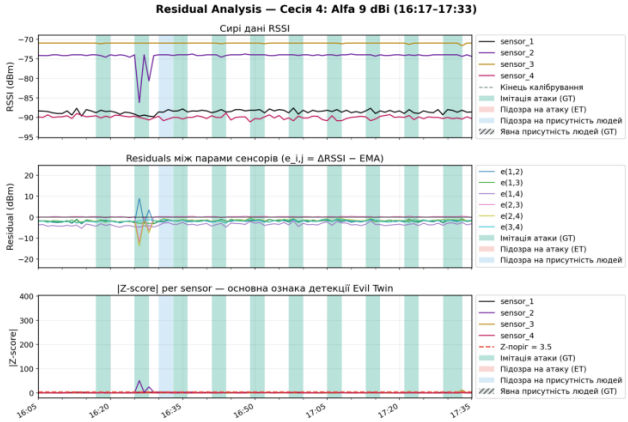

Рис. 7. Результати аналізу відрізку 16:17-17:33 із накладенням інтервалів детекції

Всеспрямована антена Alfa 9 dBi з порівняно невисоким підсиленням, спрямована до периметру через зовнішню залізобетонну стіну, генерує зловмисний сигнал, що на сенсорах знаходиться на рівні теплового шуму приймачів. Візуально на рис. 7 видно ледь помітне відхилення сенсора sensor_2 у моменти атак, але магнітуда відхилення (близько 1-2 dBm) недостатня для впевненого перевищення порогу $Z_{thr} = 3{,}5$ у більшості випадків.

Алгоритм виявив лише одну з десяти атак цієї сесії (інтервал 16:30-16:33 з піком z=4,0), що класифіковано не як ET, а як “Detected People” внаслідок недостатньої магнітуди піка для перевищення порогу $Z_{ET} = 20$.

Цей результат ілюструє фундаментальне обмеження методу, оскільки ефективність детекції лінійно залежить від відношення сигнал/шум на сенсорах, яке у свою чергу визначається фізичними параметрами зовнішнього передавача (потужність, антена) та властивостями огороджувальних конструкцій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі розв’язано науково-прикладне завдання виявлення атак Evil Twin на бездротові мережі стандарту IEEE 802.11 у сценарії повного клонування точки доступу в умовах щільної міської забудови з монолітно-каркасними залізобетонними конструкціями. Запропоновано та експериментально перевірено метод, що базується на статистичному аналізі просторових співвідношень потужності сигналу між розподіленою мережею з чотирьох Wi-Fi-сенсорів і не залежить від ідентифікаційних характеристик точок доступу. Основні наукові та практичні результати дослідження можуть бути узагальнені таким чином:

1. Сформульовано математичну модель просторових співвідношень потужності сигналу між розподіленою мережею Wi-Fi-сенсорів у статичному приміщенні, в якій нормальний стан середовища характеризується стабільними розподілами різниць RSSI між усіма парами сенсорів, а наявність зовнішнього передавача спричиняє детермінований зсув цих розподілів.

2. Розроблено двокомпонентний алгоритм виявлення аномалій, що поєднує детектор парних залишків $S(t)$, чутливий до тривалих порушень просторового патерну послаблення сигналу, та імпульсний детектор на основі z-оцінки кожного сенсора, який реагує на короткі локально-сильні відхилення. Така комбінація забезпечує одночасну чутливість до атак з різною тривалістю та інтенсивністю при єдиному наборі статистичних параметрів.

3. Запропоновано двопорогову класифікаційну схему розрізнення зовнішніх атак від нормальної людської активності всередині приміщення на основі магнітуди піка z-оцінки. Експериментально підтверджено її ефективність: обидва інтервали, спричинені рухом людей, коректно класифіковано як “Detected People” (магнітуди 15,3 та 3,9 при порозі $Z_{\mathrm{ET}} = 20$), що виключило їх з категорії хибнопозитивних спрацювань.

4. Експериментальна перевірка на наборі з 40 розмічених атак з використанням чотирьох типів антен (Yagi 16 dBi, log-periodic, Alfa APA-M25, Alfa 9 dBi) підтвердила працездатність методу: досягнуто 100 % повноти на рівні сесій атак, 60 % повноти на рівні окремих атак та 85,7 % точності. На рівні сесій метод забезпечує повне покриття дослідженого спектра загроз, що є ключовим показником для практичних систем моніторингу безпеки, орієнтованих на оповіщення оператора про факт спроби атаки.

5. Встановлено межу застосовності методу у вигляді відношення сигнал/шум на сенсорах. Для антен з підсиленням 16 dBi (Yagi) та широкосмугових (log-periodic) метод працює надійно навіть крізь залізобетонні конструкції; для всенаправленої антени 9 dBi частина атак залишається на межі чутливості. Виявлено, що геометрична конфігурація сенсорної мережі є критичним параметром: щонайменше один сенсор має бути розміщений у безпосередній близькості до потенційних напрямків атаки.

Наукова новизна одержаних результатів полягає у запропонованому підході до детекції повного клона точки доступу через спільний аналіз парних залишків і z-оцінок розподіленої сенсорної мережі, що, на відміну від відомих методів, зберігає працездатність в умовах сильного послаблення сигналу та забезпечує автоматичне розрізнення атак і фонової людської активності без потреби в попередньо розмічених навчальних вибірках.

Практичне значення результатів дослідження зумовлене тим, що запропонований метод реалізується на стандартних Wi-Fi-чіпсетах без модифікації мережної інфраструктури і може бути впроваджений у наявні системи захисту об’єктів критичної інфраструктури, державних установ та корпоративних офісів, розташованих у будівлях з монолітно-каркасними залізобетонними конструкціями.

Перспективи подальших досліджень пов’язані з такими напрямками:

1. Підвищення повноти на рівні окремих атак шляхом адаптації параметрів EMA до сценаріїв з короткими атаками (порядку 2-5 хв) для скорочення затримки реакції алгоритму на нову атакуючу подію.
2. Дослідження масштабованості методу для сенсорних мереж більшої щільності та геометричної різноманітності, зокрема для багатоповерхових розгортань і приміщень нерегулярної форми, з оцінкою впливу кількості сенсорів на показники повноти й точності.
3. Розширення на діапазон 5 ГГц та стандарти IEEE 802.11ac/ax/be, де менший радіус дії та більше послаблення сигналу можуть змінити структуру парних залишків і вимагати перегляду статистичних порогів.
4. Інтеграція з технологіями інтегрованого зондування та зв’язку (ISAC) з використанням можливостей beamforming сучасних точок доступу для побудови додаткового каналу детекції аномалій, що дозволить підвищити чутливість методу у сценаріях зі слабким атакуючим сигналом.
5. Розробка адаптивних механізмів калібрування, які автоматично перевизначають референсну норму у відповідь на штатні зміни радіосередовища (переміщення меблів, оновлення мережного обладнання, сезонна варіація вологості будівельних матеріалів), без потреби в ручному переналаштуванні системи.
6. Експериментальна перевірка методу в інших класах будівель – цегляних, дерев’яних, з композитними матеріалами огороджувальних конструкцій – з метою побудови узагальненої таблиці рекомендованих параметрів для різних типів захищених об’єктів.

ПОДЯКА

Дослідження проведено в межах проєкту, що фінансується за грантом Президента України для молодих вчених (докторів філософії / кандидатів наук до 35 років), наданим Національним фондом досліджень України (проєкт № 2025.05/0046), за підтримки Національного університету "Львівська політехніка". Експериментальна перевірка методу здійснена в реальних умовах щільної міської забудови на території університету.

Автор висловлює подяку Національному фонду досліджень України за фінансову підтримку дослідження, а також Національному університету "Львівська політехніка" за надання інфраструктурних та матеріально-технічних ресурсів, необхідних для проведення експерименту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*. IEEE.
2. Banakh, R., & Piskozub, A. (2018). Attackers' Wi-Fi devices metadata interception for their location identification. In *Proceedings of the IEEE 4th International Symposium on Wireless Systems within the International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)* (pp. 112-116). IEEE.
3. Banakh, R., Piskozub, A., & Opirskyy, I. (2023). Devising a method for detecting “evil twin” attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model. *Eastern-European Journal of Enterprise Technologies, 3*(9), 20-32. https://doi.org/10.15587/1729-4061.2023.282131

4. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. (2024). Data mining approach for evil twin attack identification in Wi-Fi networks. *Data*, *9*(10), 119. https://doi.org/10.3390/data9100119
5. Agarwal, M., Biswas, S., & Nandi, S. (2018). An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks. *International Journal of Wireless Information Networks*, *25*(2), 130-145. https://doi.org/10.1007/s10776-018-0396-1
6. Yang, C., Song, Y., & Gu, G. (2012). Active user-side evil twin access point detection using statistical techniques. *IEEE Transactions on Information Forensics and Security*, *7*(5), 1638-1651. https://doi.org/10.1109/TIFS.2012.2207383
7. Laurendeau, C., & Barbeau, M. (2008). Insider attack attribution using signal strength-based hyperbolic location estimation. *Security and Communication Networks*, *1*(4), 337-349. https://doi.org/10.1002/sec.35
8. Tian, Y., Wang, S., & Zhang, L. (2021). Convolutional neural network based evil twin attack detection in WiFi networks. *MATEC Web of Conferences*, *336*, 08006. https://doi.org/10.1051/matecconf/202133608006
9. Korobeinikova, T., & Kravchuk, N. (2025). ML-trained model and method for blocking dangerous queries. In *Proceedings of the Cyber Security and Data Protection Workshop (CSDP 2025)* (Vol. 4042, pp. 1-16). CEUR Workshop Proceedings.
10. Han, Z., Liao, J., Qi, Q., Sun, H., & Wang, J. (2020). Band steering technology based on QoE-oriented optimization in wireless networks. *EURASIP Journal on Wireless Communications and Networking*, *2020*, 1640. https://doi.org/10.1186/s13638-020-1640-9
11. He, Y., Xu, M., Chen, Z., Xiao, F., & Luo, J. (2026). Beamforming-enabled integrated sensing and communication over commodity multi-user Wi-Fi. *IEEE Transactions on Mobile Computing*. Advance online publication. https://doi.org/10.1109/TMC.2026.3672117
12. He, Y., Xu, M., Chen, Z., Xiao, F., & Luo, J. (2025). Beam-Fi: Integrated sensing and communication via MU-MIMO upon commodity Wi-Fi. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *9*, Article 84. https://doi.org/10.1145/3749477
13. International Telecommunication Union. (2023). *Recommendation ITU-R P.2040-3: Effects of building materials and structures on radiowave propagation above about 100 MHz*. ITU. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.2040-3-202308-S!!PDF-E.pdf
14. Stone, W. C. (1997). *Electromagnetic signal attenuation in construction materials* (NISTIR 6055). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.6055
15. MikroTik. (2026). *cAP XL ac (RBcAPGi-5acD2nD-XL)*. https://mikrotik.com/product/cap_xl_ac
16. Espressif Systems. (2024). *ESP32-C6 datasheet*. https://www.espressif.com/sites/default/files/documentation/esp32-c6_datasheet_en.pdf
17. InfluxData. (2026). *InfluxDB: Open-source time series database*. https://www.influxdata.com/
18. The pandas Development Team. (2024). *pandas (Version 2.2)* [Computer software]. Zenodo. https://doi.org/10.5281/zenodo.3509134
19. Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., & Oliphant, T. E. (2020). Array programming with NumPy. *Nature*, *585*(7825), 357–362. https://doi.org/10.1038/s41586-020-2649-2
20. Hunter, J. D. (2007). Matplotlib: A 2D graphics environment. *Computing in Science & Engineering*, *9*(3), 90–95. https://doi.org/10.1109/MCSE.2007.55
21. Alfa Network. (2024). *AWUS036NHA wireless USB adapter*. https://www.alfa.com.tw/products/awus036nha
22. Aircrack-ng Project. (2026). *Aircrack-ng: Wi-Fi network security auditing tools suite*. https://www.aircrack-ng.org/
23. Malinen, J., & contributors. (2026). *hostapd: IEEE 802.11/WPA/WPA2/EAP/RADIUS authenticator*. https://w1.fi/hostapd/

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

Roman Banakh
PhD, Associate Professor
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0001-6897-8206
roman.i.banakh@lpnu.ua

EVIL TWIN ATTACK DETECTION IN IEEE 802.11 WIRELESS NETWORKS IN DENSE URBAN ENVIRONMENTS

Abstract. The paper addresses the problem of detecting Evil Twin attacks on IEEE 802.11 wireless networks in dense urban environments with monolithic reinforced concrete construction, which significantly attenuates radio signals in the 2.4 and 5 GHz bands. In a full access point cloning scenario, the attacker copies both the network identifier and the hardware address of the legitimate device, making classical detection methods based on the analysis of management frame identifiers inapplicable. A detection method is proposed that uses a network of four indoor Wi-Fi sensors to continuously measure the received signal strength indicator of the legitimate access point and analyzes the geometric relationships between sensors. The method combines two independent detectors – a pair-wise residual detector S(t) based on a statistical model of signal power differences across all sensor pairs, sensitive to sustained violations of the spatial signal attenuation pattern, and an impulse detector based on the z-score of each sensor relative to its calibration baseline, which reacts to short, locally strong deviations lasting 2-5 minutes. Subsequent classification of impulse intervals by peak z-score magnitude allows separation of strong external attacks from regular human activity inside the room. Experimental validation was performed on a labeled set of 40 attacks using four types of antennas placed outside the concrete building. The method achieved 60% recall and 85.7% precision at the individual attack level, and 100% recall at the attack session level (groups of ten consecutive attacks per antenna). The developed approach does not require specialized hardware, operates on standard Wi-Fi chipsets, and can be deployed within existing infrastructure to protect critical infrastructure facilities.

Keywords: Evil Twin attack; wireless networks; IEEE 802.11; Wi-Fi; RSSI; statistical anomaly detection; wireless network security; radio signal attenuation; sensor network.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Vanhoef, M., & Ronen, E. (2020). Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*. IEEE.
2. Banakh, R., & Piskozub, A. (2018). Attackers' Wi-Fi devices metadata interception for their location identification. In *Proceedings of the IEEE 4th International Symposium on Wireless Systems within the International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)* (pp. 112-116). IEEE.
3. Banakh, R., Piskozub, A., & Opirskyy, I. (2023). Devising a method for detecting “evil twin” attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model. *Eastern-European Journal of Enterprise Technologies, 3*(9), 20-32. https://doi.org/10.15587/1729-4061.2023.282131
4. Banakh, R., Nyemkova, E., Justice, C., Piskozub, A., & Lakh, Y. (2024). Data mining approach for evil twin attack identification in Wi-Fi networks. *Data, 9*(10), 119. https://doi.org/10.3390/data9100119
5. Agarwal, M., Biswas, S., & Nandi, S. (2018). An efficient scheme to detect evil twin rogue access point attack in 802.11 Wi-Fi networks. *International Journal of Wireless Information Networks, 25*(2), 130-145. https://doi.org/10.1007/s10776-018-0396-1
6. Yang, C., Song, Y., & Gu, G. (2012). Active user-side evil twin access point detection using statistical techniques. *IEEE Transactions on Information Forensics and Security, 7*(5), 1638-1651. https://doi.org/10.1109/TIFS.2012.2207383
7. Laurendeau, C., & Barbeau, M. (2008). Insider attack attribution using signal strength-based hyperbolic location estimation. *Security and Communication Networks, 1*(4), 337-349. https://doi.org/10.1002/sec.35
8. Tian, Y., Wang, S., & Zhang, L. (2021). Convolutional neural network based evil twin attack detection in WiFi networks. *MATEC Web of Conferences, 336*, 08006. https://doi.org/10.1051/matecconf/202133608006

9. Korobeinikova, T., & Kravchuk, N. (2025). ML-trained model and method for blocking dangerous queries. In *Proceedings of the Cyber Security and Data Protection Workshop (CSDP 2025)* (Vol. 4042, pp. 1-16). CEUR Workshop Proceedings.
10. Han, Z., Liao, J., Qi, Q., Sun, H., & Wang, J. (2020). Band steering technology based on QoE-oriented optimization in wireless networks. *EURASIP Journal on Wireless Communications and Networking, 2020*, 1640. https://doi.org/10.1186/s13638-020-1640-9
11. He, Y., Xu, M., Chen, Z., Xiao, F., & Luo, J. (2026). Beamforming-enabled integrated sensing and communication over commodity multi-user Wi-Fi. *IEEE Transactions on Mobile Computing*. Advance online publication. https://doi.org/10.1109/TMC.2026.3672117
12. He, Y., Xu, M., Chen, Z., Xiao, F., & Luo, J. (2025). Beam-Fi: Integrated sensing and communication via MU-MIMO upon commodity Wi-Fi. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 9*, Article 84. https://doi.org/10.1145/3749477
13. International Telecommunication Union. (2023). *Recommendation ITU-R P.2040-3: Effects of building materials and structures on radiowave propagation above about 100 MHz*. ITU. https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.2040-3-202308-S!!PDF-E.pdf
14. Stone, W. C. (1997). *Electromagnetic signal attenuation in construction materials* (NISTIR 6055). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.6055
15. MikroTik. (2026). *cAP XL ac (RBcAPGi-5acD2nD-XL)*. https://mikrotik.com/product/cap_xl_ac
16. Espressif Systems. (2024). *ESP32-C6 datasheet*. https://www.espressif.com/sites/default/files/documentation/esp32-c6_datasheet_en.pdf
17. InfluxData. (2026). *InfluxDB: Open-source time series database*. https://www.influxdata.com/
18. The pandas Development Team. (2024). *pandas (Version 2.2)* [Computer software]. Zenodo. https://doi.org/10.5281/zenodo.3509134
19. Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., & Oliphant, T. E. (2020). Array programming with NumPy. *Nature, 585*(7825), 357–362. https://doi.org/10.1038/s41586-020-2649-2
20. Hunter, J. D. (2007). Matplotlib: A 2D graphics environment. *Computing in Science & Engineering, 9*(3), 90–95. https://doi.org/10.1109/MCSE.2007.55
21. Alfa Network. (2024). *AWUS036NHA wireless USB adapter*. https://www.alfa.com.tw/products/awus036nha
22. Aircrack-ng Project. (2026). *Aircrack-ng: Wi-Fi network security auditing tools suite*. https://www.aircrack-ng.org/
23. Malinen, J., & contributors. (2026). *hostapd: IEEE 802.11/WPA/WPA2/EAP/RADIUS authenticator*. https://w1.fi/hostapd/

Отримано редакцією журналу / Received: 04.03.26
Прорецензовано / Revised: 15.03.26
Схвалено до друку / Accepted: 25.06.26