КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1315
УДК 004.056.5:004.8:621.391

Лобан Георгій Антонович
Аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0003-4862-8729
heorhii.loban.asp.2025@lpnu.ua

Луковський Тарас Ігорович
к.т.н., доцент кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

ВИЯВЛЕННЯ REPLAY/RELAY АТАК У БЕЗДРОТОВИХ СИСТЕМАХ ЗАСОБАМИ RF-FINGERPRINTING ТА SDR

Анотація. У статті проведено систематизацію методів виявлення атак типу Replay та Relay у бездротових системах на основі радіочастотного відбитка (RF-fingerprinting) сигналу з використанням програмно-визначених радіоприймачів (SDR). Показано, що атаки повторного відтворення й ретрансляції сигналу зберігають коректність даних на протокольному рівні, тому виявлення таких атак можливе лише за рахунок аналізу фізичних апаратних артефактів передавача – зсуву несучої частоти, дисбалансу IQ-компонентів, нелінійності підсилювача потужності та характеристик перехідного процесу. Проаналізовано механізми Replay-атак (повторне відтворення раніше перехопленого сигналу) та Relay-атак (ретрансляція сигналу в реальному часі без його модифікації) на прикладі систем безключового доступу автомобілів, NFC/RFID та вузькосмугових IoT-протоколів (EV1527, Zigbee, LoRa). Виконано порівняльний аналіз придатності поширених SDR-платформ (RTL-SDR V3, HackRF One, ADALM-PLUTO, USRP B210) для задач захоплення IQ-відліків з метою фінгерпринтингу. Запропоновано узагальнену архітектуру системи виявлення, що поєднує SDR-приймач, модуль попередньої обробки сигналу, екстрактор RF-відбитка та блок прийняття рішення на основі порівняння з еталонною базою відбитків. Розроблено узагальнений алгоритм виявлення Replay/Relay атаки, що не потребує модифікації протоколу зв'язку і застосовний незалежно від типу криптографічного захисту даних. Аналіз результатів, наявних у літературі, показує, що підходи на основі RF-fingerprinting дозволяють відрізняти оригінальний сигнал від повтореного чи ретрансльованого з точністю, що сягає 90-99 % залежно від протоколу та умов експерименту.

Ключові слова: радіочастотний відбиток, RF-fingerprinting, Replay-атака, Relay-атака, Software-Defined Radio, SDR, безключовий доступ, автентифікація фізичного рівня, Інтернет речей, зсув несучої частоти, IQ-дисбаланс.

ВСТУП

Атаки типу Replay та Relay посідають особливе місце серед загроз бездротовим системам саме тому, що вони не порушують криптографічний протокол як такий. У випадку Replay-атаки зловмисник перехоплює легітимний сигнал і відтворює його повторно в момент, коли це вигідно атакуючому; у випадку Relay-атаки сигнал ретранслюється в реальному часі між віддаленими точками, створюючи в системи хибне враження про фізичну близькість легітимного пристрою [4, 6]. В обох сценаріях пристрій-приймач отримує коректно сформований, а в багатьох випадках і правильно підписаний або зашифрований пакет даних, тому суто протокольні механізми автентифікації – коди доступу, що змінюються (rolling code), часові мітки, криптографічні підписи – не мають формальних підстав відхилити такий сигнал як підроблений [6].

Найбільш показовим прикладом практичної небезпеки таких атак є системи безключового доступу автомобілів (Passive Keyless Entry, PKES). Продемонстровано, що ретрансляція сигналу між ключем та автомобілем дозволяє відкрити й завести транспортний засіб навіть тоді, коли фізична відстань між

ключем і автомобілем сягає кількох десятків метрів, незалежно від використовуваного протоколу чи стійкості криптографічного захисту [4]. Аналогічна проблема характерна для NFC/RFID-систем контролю доступу та безконтактних платежів, де ретрансляція сигналу через проміжний канал зв'язку дозволяє обійти захист без розкриття криптографічного ключа [7].

Історично основним напрямом протидії Relay-атакам є протоколи обмеження відстані (distance bounding), що вимірюють час проходження сигналу між пристроями для оцінки верхньої межі відстані [5]. Однак практична реалізація таких протоколів ускладнена вимогами до точності вимірювання часу на рівні наносекунд, а огляд сучасних атак і захисних механізмів для автомобільних систем безключового доступу показує, що розроблені варіанти протоколів неодноразово демонстрували вразливість до більш витончених атак [6]. У зв'язку з цим дедалі більшої актуальності набуває альтернативний, фізичний рівень захисту – ідентифікація пристрою за унікальними апаратними особливостями його передавача (RF-fingerprinting), який не залежить від коректності даних чи часових характеристик протоколу [1, 2, 3].

Незважаючи на значний обсяг досліджень з RF-fingerprinting як методу ідентифікації пристроїв загалом [2, 3], питання систематизації підходів саме до задачі виявлення Replay/Relay атак розроблене фрагментарно, здебільшого в межах окремих застосувань – виявлення NFC-релею [7] або ретрансльованих сигналів автомобільних систем дистанційного керування [8] – без єдиної методологічної основи та узагальненої ролі SDR-приймачів у побудові подібних систем. Це зумовлює актуальність даного дослідження.

Аналіз останніх досліджень і публікацій. Фундаментальну систематизацію уявлень про фізичну ідентифікацію бездротових пристроїв виконали Danev, Zanetti та Capkun [1], які узагальнили джерела RF-відбитка та розділили їх на дві великі групи – ознаки перехідного процесу (transient-based) та ознаки усталеного режиму (steady-state), а також системно описали типові атаки на самі методи фізичної ідентифікації. Ця робота й дотепер лишається базовою точкою відліку для будь-якої класифікації підходів RF-fingerprinting.

У сучаснішому огляді Xie, Peng, Zhang та ін. [2] систематизовано підходи до RF-fingerprinting саме для пристроїв Інтернету речей, включно з етапами попередньої обробки сигналу, екстракції ознак та класифікації; окрему увагу приділено відкритим проблемам – стабільності відбитків у часі та впливу бездротового каналу на точність ідентифікації. Abbas, Abu Talib, Nasir та ін. [3] у систематичному огляді понад 130 експериментальних робіт за 2010-2023 рр. класифікували підходи за типом ознак, методами фільтрації й алгоритмами класифікації та підтвердили, що моделі глибокого навчання (CNN, RNN) стабільно перевершують класичні методи (SVM, k-NN) на задачах ідентифікації за сирими IQ-відліками.

Значний масив досліджень присвячено застосуванню RF-fingerprinting саме до вузькосмугових IoT-протоколів. Ahmed, Quoitin, Gros та Moeyaert [9] в огляді підходів на основі глибокого навчання для LoRa-пристроїв описують типовий конвеєр, у якому IQ-відліки захоплюються USRP- або HackRF-приймачами, обробляються в GNU Radio і подаються на вхід CNN-моделей; для LoRa-пристроїв такі моделі, навчені на преамбулах сигналу, демонструють точність ідентифікації до 99 % у дротових сценаріях і до 97 % у бездротових умовах. Ці результати прямо стосуються протоколів на кшталт EV1527 та Zigbee, які поділяють з LoRa спільну властивість – обмежену складність модуляції та коротку тривалість корисного сигналу, що робить якість захоплення IQ-відліків критичним фактором точності.

Проєкт ORACLE, описаний у роботі Al-Shawabka та ін. [10], демонструє одну з найбільш масштабних експериментальних реалізацій CNN-based RF-fingerprinting: модель, навчена на сирих IQ-відліках від 16 SDR-передавачів USRP X310 і захоплена приймачем USRP B210, забезпечує точність ідентифікації понад 99 % на частоті Wi-Fi (2,45 ГГц). Водночас автори системно показують, що саме бездротовий канал (багатопроменеве поширення, згасання, доплерівський зсув) є основним джерелом деградації точності RF-fingerprinting при переході від лабораторних до реальних умов – спостереження, критично важливе для задачі виявлення Relay-атак, де сигнал завжди проходить через додатковий ретрансляційний канал. Цю ж проблему безпосередньо розв'язує робота Restuccia, D'Oro, Al-Shawabka та ін. [11]: запропонований підхід DeepRadioID оптимізує параметри радіотракту передавача в реальному часі таким чином, щоб компенсувати спотворення каналу і зберегти стабільність відбитка, що підвищує стійкість ідентифікації саме в динамічних і зашумлених умовах.

Окремий напрям пов'язаний із моделями, здатними працювати з відкритою множиною пристроїв без повного перенавчання. Dhakal, Kandel та Shekhar [12] пропонують Siamese-мережу для автентифікації IoT-пристроїв, що порівнює embedding-вектор невідомого сигналу з базою еталонних відбитків і дозволяє додавати нові авторизовані пристрої без перенавчання класифікатора – властивість, важлива для систем виявлення атак, що експлуатуються тривалий час і повинні підтримувати змінний склад авторизованих пристроїв.

Найбільш дотичними до задачі власне виявлення Replay/Relay атак є дві роботи. Wang, Zou та Zhang [7] безпосередньо застосували RF-fingerprinting для виявлення релею в NFC-системах (стандарт ISO/IEC 14443-A): на SDR-стенді реалізовано дротовий і бездротовий варіанти релейної атаки, а класифікатор, навчений на ATQA-сегментах сигналу, розрізняв оригінальні та ретрансльовані відповіді з точністю близько 99 %, що є прямим експериментальним підтвердженням придатності підходу для задачі, поставленої в цій статті. Quintero, Cuesta та Lopez [8] розв'язують аналогічну задачу для автомобільних систем дистанційного керування (RKE): на основі створеного авторами набору даних KeFRA (оригінальні сигнали та їх ретрансляції з різним підсиленням) навчено класифікатори SVM та VGG-16, які досягли точності розрізнення оригінал/ретрансляція 96,4 % та 95,3 % відповідно, використовуючи лише бюджетний RTL-SDR приймач.

Водночас класичний напрям протидії Relay-атакам – протоколи обмеження відстані, закладені у роботі Rasmussen та Capkun [5] та практично скомпрометовані в демонстрації Francillon, Danev та Capkun на десяти моделях автомобілів [4] – на сьогодні системно проаналізовано в огляді Bianchi, Brighente, Conti та Pavan [6], які узагальнили атаки й засоби захисту систем RKE/PKES за період з моменту появи цих систем до 2025 р. і констатували, що жодне з існуючих рішень (distance bounding, UWB-локалізація, аналіз RSSI) не є остаточно надійним самостійно, що підсилює обґрунтованість пошуку додаткового, фізичного рівня захисту.

Таким чином, аналіз літератури дозволяє зробити такі висновки: (1) RF-fingerprinting є теоретично обґрунтованим і експериментально підтвердженим методом фізичної автентифікації [1-3]; (2) для окремих протоколів (NFC, автомобільні RKE) уже продемонстровано практичну здатність RF-fingerprinting відрізняти оригінальний сигнал від ретрансльованого з точністю 90-99 % [7, 8]; (3) бездротовий канал передавання є основним фактором деградації точності, що особливо критично для Relay-атак, які за визначенням додають ретрансляційну ланку [10, 11]; (4) моделі на основі метричного навчання (Siamese-мережі) дозволяють підтримувати змінну множину авторизованих пристроїв без перенавчання [12]; проте (5) відсутня узагальнена, протокольно-незалежна методологія виявлення саме Replay/Relay атак, а також систематизоване порівняння придатності SDR-платформ для розв'язання цієї конкретної задачі.

Метою статті є систематизація методів виявлення Replay/Relay атак у бездротових системах на основі RF-fingerprinting сигналу з використанням SDR-приймачів та розроблення узагальненої, протокольно-незалежної архітектури й алгоритму такого виявлення.

Для досягнення мети сформульовано задачі:

1) проаналізувати механізми Replay- та Relay-атак і визначити, які саме фізичні артефакти сигналу дозволяють їх відрізнити від легітимної передачі;
2) виконати порівняльний аналіз SDR-платформ за критеріями, релевантними для захоплення таких артефактів;
3) запропонувати узагальнену архітектуру системи виявлення;
4) розробити алгоритм прийняття рішення "оригінал / Replay / Relay", застосовний незалежно від протоколу зв'язку;
5) зіставити очікувану ефективність підходу з наявними експериментальними результатами [7, 8].

Новизна дослідження полягає в перенесенні фокусу з задачі ідентифікації пристрою як такої (якою переважно займається література [1-3, 9, 12]) на вужчу й практично гострішу задачу – розрізнення оригінального сигналу та його повторного відтворення чи ретрансляції – та в узагальненні розрізнених протокольно-специфічних результатів [7, 8] у єдину архітектурну модель, не прив'язану до конкретного стандарту зв'язку.

ОСНОВНА ЧАСТИНА

Порівняльний аналіз SDR-приймачів для задач виявлення Replay/Relay атак. Придатність SDR-платформи для виявлення Replay/Relay атак визначається не лише загальною якістю захоплення сигналу, а й специфічними вимогами задачі: необхідністю фіксувати короткочасні артефакти перехідного процесу (для Replay) та вносити мінімальну власну затримку й шум під час прийому (щоб не маскувати артефакти ретрансляції атакуючого при Relay). У табл. 1 наведено порівняння чотирьох найпоширеніших у відповідних дослідженнях платформ.

Таблиця 1

Порівняльна характеристика SDR-приймачів для задач виявлення Replay/Relay атак

Параметр	RTL-SDR V3	HackRF One	ADALM-PLUTO	USRP B210
Частотний діапазон	24 МГц – 1,7 ГГц	1 МГц – 6 ГГц	325 МГц – 3,8 ГГц	70 МГц – 6 ГГц

Розрядність АЦП, біт	8	8	12	12
Макс. швидкість дискретизації, MSPS	3,2	20	61,44	61,44
Орієнтовна вартість, USD	≈ 25–30	≈ 300	≈ 150	≈ 1100
Використання у виявленні Replay/Relay (за літературою)	базовий приймач для дешевого стенду відтворення атаки на RKE [8]	SDR-стенд для реалізації та виявлення NFC-релею [7]	придатний для Siamese-підходу з відкритою множиною пристроїв [12]	еталонна платформа для дослідження впливу каналу на відбиток [10, 11]

Як показано в [8], навіть бюджетний RTL-SDR V3 виявився достатнім для побудови класифікатора, що розрізняє оригінальний і ретрансльований сигнал автомобільного RKE з точністю понад 95 %, оскільки задача відрізнення оригінал/ретрансляція є за своєю природою простішою за задачу ідентифікації конкретного з великої кількості пристроїв – потрібно розрізнити лише два класи, а не десятки. Водночас HackRf One, використаний у [7] для одночасної реалізації та виявлення NFC-релею, дав змогу отримати точність до 99 % завдяки ширшому частотному діапазону, що дозволяє захоплювати сигнал без додаткового підвищення/пониження частоти. USRP B210, як показано в дослідженнях впливу каналу на RF-відбиток [10, 11], залишається кращим вибором тоді, коли потрібно розрізняти не лише "оригінал/підробка", а й компенсувати спотворення від самого каналу передавання – що є прямим підвищенням стійкості до хибних спрацювань.

На основі проведеного аналізу для практичної реалізації системи виявлення Replay/Relay атак рекомендовано: RTL-SDR V3 або HackRF One – для прототипування бюджетних рішень або систем контролю доступу на протоколах на кшталт EV1527, де достатньо бінарної класифікації "оригінал/повтор"; ADALM-PLUTO – як збалансоване рішення з підтримкою Siamese-архітектури для систем із відкритою й змінною множиною авторизованих пристроїв; USRP B210 – для сценаріїв із високими вимогами до стійкості проти каналових спотворень, зокрема при значній відстані ретрансляції.

Архітектура системи виявлення. Запропонована архітектура (рис. 1) складається з шести функціональних модулів: (1) SDR-приймач, що захоплює IQ-відліки як від легітимного передавача, так і потенційно від ретрансльованого/повтореного сигналу; (2) модуль попередньої обробки – нормалізація амплітуди, часткова компенсація зсуву несучої частоти (CFO), сегментація інформативних ділянок сигналу; (3) екстрактор RF-відбитка, що перетворює оброблені IQ-відліки на компактний embedding-вектор за принципом, узагальненим у [1, 12]; (4) паралельний модуль аналізу каналу, що оцінює додаткові артефакти, характерні саме для ретрансляції – затримку поширення, зміну співвідношення сигнал/шум, нелінійні спотворення від проміжної апаратури атакуючого [10, 11]; (5) базу еталонних RF-відбитків авторизованих пристроїв; (6) блок ухвалення рішення, що на основі відстані між поточним embedding-вектором і найближчим еталоном, а також показників каналового аналізу, класифікує сигнал як оригінальний, Replay або Relay.

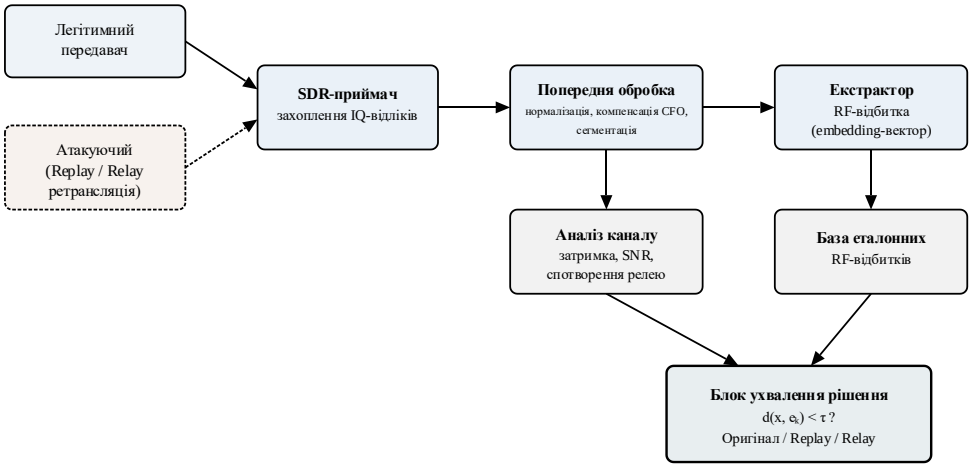

Рис. 1. Архітектура системи виявлення Replay/Relay атак на основі RF-fingerprinting

Ключова архітектурна відмінність запропонованого підходу від класичних систем ідентифікації пристроїв (які відповідають лише на питання "який це пристрій") полягає у введенні окремого каналу аналізу – модуля аналізу каналу (4), що працює паралельно до екстракції відбитка і дозволяє відрізняти два принципово різні сценарії атаки: Replay, за якого відбиток близький до еталона, але сигнал зафіксовано в невідповідний момент часу або з відхиленням часових ознак; та Relay, за якого до відбитка додається додаткова, невластива оригінальному передавачу деградація, внесена ретрансляційною апаратурою атакуючого.

Формалізація задачі виявлення та критерії прийняття рішення. Для формалізації задачі приймемо позначення, узгоджені з підходом до метричного навчання, узагальненим у [1, 12]. Нехай x = {I(n) + jQ(n)}, n = 1, …, L – послідовність IQ-відліків довжиною L, захоплена SDR-приймачем від деякого сигналу (легітимного, повторного або ретрансльованого). Функція екстракції RF-відбитка реалізується як нейромережа f_W(·) із параметрами W, що відображає вхідну послідовність у d-вимірний embedding-вектор:

$$f_W : R^{2\times L} \rightarrow R^d \tag{1}$$

Для двох зразків x_A та x_B міра подібності визначається Евклідовою відстанню між їхніми embedding-векторами:

$$d(A,B) = \|f_W(x_A) - f_W(x_B)\|_2 \tag{2}$$

Пристрій вважається легітимним і відповідним еталону e_k із бази RF-відбитків, якщо:

$$d(x,e_k) = \|f_W(x) - e_k\|_2 < \tau_1 \tag{3}$$

де τ_1 – базовий поріг ідентифікації, визначений на етапі калібрування за FAR/FRR-аналізом [12].

Умова (3) сама по собі розв'язує задачу ідентифікації пристрою, але не розрізняє легітимну передачу від Replay/Relay атаки, оскільки обидва типи атаки можуть за певних умов задовольняти чи не задовольняти цю нерівність з різних фізичних причин. Тому необхідні два додаткові, специфічні для кожного типу атаки критерії.

Критерій Replay. Атака повторного відтворення полягає в тому, що атакуючий передає раніше перехоплений цифровий вміст сигналу за допомогою власного передавального обладнання (наприклад, SDR-передавача), яке фізично відрізняється від оригінального пристрою. Це означає, що навіть при повністю ідентичному бітовому вмісті RF-відбиток повтореного сигналу відповідатиме апаратним характеристикам обладнання атакуючого, а не легітимного пристрою [7]. Формально, якщо payload-послідовність (демодульований бітовий вміст) p(x) збігається з раніше зафіксованою p(x_prev) при високій кореляції:

$$\rho(x,x_{prev}) = corr(p(x),p(x_{prev})) > \tau_{corr} \tag{4}$$

але водночас відбиток не відповідає жодному еталону легітимного пристрою (d(x, e_k) ≥ τ_1 для всіх k), сигнал класифікується як Replay-атака.

Критерій Relay. На відміну від Replay, ретрансляція відбувається в реальному часі й фізично походить від справжнього передавача, тому цифровий вміст і базові часові характеристики протоколу є коректними. Проте проходження сигналу через проміжну підсилювально-ретрансляційну апаратуру атакуючого вносить додаткові, невластиві оригінальному радіотракту спотворення (додаткову нелінійність, власний фазовий шум ретранслятора) [10, 11], а також вимірювану затримку поширення. Введемо нормалізований індикатор аномалії каналу:

$$R(x) = \alpha \cdot \Delta t_{norm}(x) + \beta \cdot \Delta SNR_{norm}(x) + \gamma \cdot [d(x,e_k) - \tau_1]_+ \tag{5}$$

де Δt_norm(x) – нормалізоване відхилення виміряної затримки проходження сигналу від очікуваного для даного сценарію діапазону, ΔSNR_norm(x) – нормалізоване відхилення співвідношення сигнал/шум від типового для легітимної передачі, $[\cdot]_+ = \max(\cdot, 0)$, а α, β, γ ∈ (0, 1), α + β + γ = 1 – вагові коефіцієнти, що калібруються під конкретний протокол і сценарій розгортання. Сигнал класифікується як Relay-атака, якщо:

$$R(x) > \theta \quad \wedge \quad d(x,e_k) < \tau_2 \tag{6}$$

тобто відбиток залишається «впізнаваним» як такий, що походить від відомого пристрою (оскільки апаратна основа сигналу справжня), проте розширений поріг τ_2 враховує додаткову деградацію, внесену ретранслятором, а перевищення каналового індикатора R(x) підтверджує факт ретрансляції.

Підсумкове правило прийняття рішення узагальнює умови (3) – (6):

$$label(x) \in \{\text{Оригінал}, Replay, Relay, \text{Невідомий пристрій}\} \quad (7)$$

- Оригінал, якщо $d(x, e_k) < \tau_1$ і $R(x) \leq \theta$;
- Replay, якщо $d(x, e_k) \geq \tau_1$ і $\rho(x, x\_prev) > \tau\_corr$;
- Relay, якщо $\tau_1 \leq d(x, e_k) < \tau_2$ і $R(x) > \theta$;
- Невідомий пристрій, якщо $d(x, e_k) \geq \tau_2$ для всіх k.

Конвеєр обробки сигналу, що передує обчисленню embedding-вектора f_W(x) і забезпечує формування вхідних даних для формул (1) – (7), подано на рис. 2.

Рис. 2. Конвеєр обробки IQ-сигналу в системі виявлення Replay/Relay атак

Отриманий на виході конвеєра вектор ознак f_W(x) використовується для обчислення відстані (2) та подальшого ухвалення рішення за правилом (7). Компенсація CFO на цьому етапі є частковою: залишковий зсув несучої частоти навмисно зберігається, оскільки сам є інформативною ознакою апаратного відбитка передавача, а не лише завадою, яку слід повністю усунути.

Обговорення результатів та аналіз ефективності підходу. Запропоновані концептуальні основи спираються на систематизацію наявних експериментальних результатів. У табл. 2 зведено дані з джерел, що безпосередньо розв'язують задачу розрізнення оригінал/атака [7, 8], а також результати загальної ідентифікації пристроїв [9, 10], які використано як референс досяжної точності RF-fingerprinting на відповідному обладнанні.

Таблиця 2

Порівняння результатів виявлення Replay/Relay атак та загальної ідентифікації пристроїв з літератури

Джерело	Тип задачі	Протокол / сценарій	SDR-платформа	Метод	Точність, %
[7]	Виявлення Relay	NFC (ISO/IEC 14443-A)	SDR-стенд (дротовий/бездротовий релей)	CNN на ATQA-сегментах	≈ 99
[8]	Виявлення Replay	Автомобільний RKE	RTL-SDR	SVM / VGG-16	96,4 / 95,3
[9]	Загальна ідентифікація (референс)	LoRa	USRP / HackRF	1D-CNN на преамбулах	97-99
[10]	Загальна ідентифікація (референс)	Wi-Fi 802.11a	USRP X310 / B210	CNN на сирих IQ	> 99

Аналіз табл. 2 дозволяє зробити такі висновки. По-перше, для задач, що прямо відповідають меті цієї статті – розрізнення оригінал/Relay [7] та оригінал/Replay [8] – точність сягає 95-99 % навіть на бюджетному обладнанні (RTL-SDR), що підтверджує практичну реалізовність запропонованої архітектури без необхідності дорогої SDR-платформи. По-друге, зіставлення з результатами загальної ідентифікації пристроїв [9, 10] показує, що задача "оригінал/атака" (бінарна класифікація) систематично розв'язується не гірше, а часто простіше, ніж задача ідентифікації конкретного пристрою серед десятків [9, 10], оскільки в бінарному сценарії досить надійно відокремити один клас (легітимний відбиток) від решти простору embedding. По-третє, розкид точності між [8] (95-96 %) і [7] (99 %) узгоджується з очікуванням, закладеним у критерій Relay (5)-(6): NFC-релей на близькій відстані вносить більш виражені канальні спотворення (через проміжну апаратуру ближнього поля), тоді як автомобільний RKE-

релей на великій відстані частково компенсує підсиленням сигналу власні спотворення, що ускладнює розрізнення й пояснює дещо нижчу точність. Узагальнений алгоритм ухвалення рішення, що послідовно реалізує критерії (4)-(6) та підсумкове правило (7), подано на рис. 3.

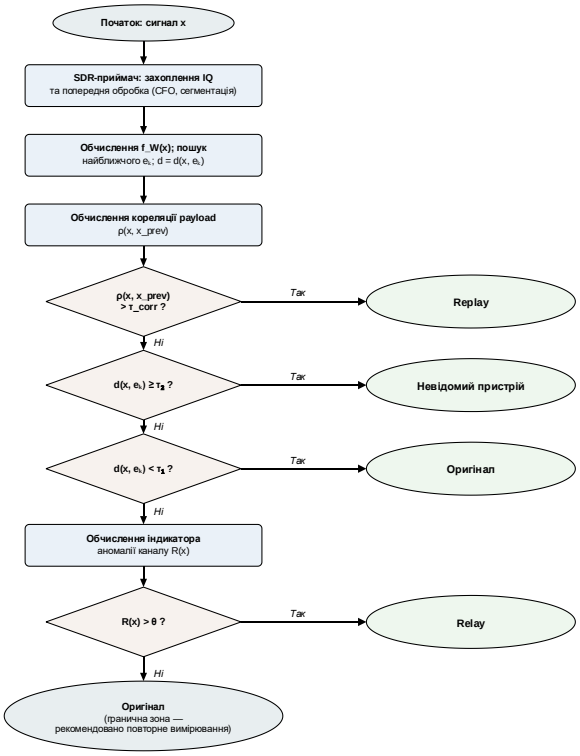

Рис. 3. Алгоритм ухвалення рішення "Оригінал / Replay / Relay / Невідомий пристрій"

Наведений алгоритм послідовно застосовує критерії (4) – (6): спершу перевіряється кореляція payload з раніше зафіксованими передачами (найсильніший і найоднозначніший індикатор Replay), і лише за її відсутності розглядається просторове положення відстані $d(x, e_k)$ відносно порогів τ_1 та τ_2 у поєднанні з канальним індикатором $R(x)$. Такий порядок перевірок мінімізує ризик хибної класифікації Replay-атаки як Relay і навпаки, оскільки ці два типи атак спираються на принципово різні фізичні ознаки – збіг цифрового вмісту для Replay і деградацію каналу для Relay.

Геометричну інтерпретацію порогів τ_1, τ_2 і θ, застосовну після проходження перевірки на Replay, унаочнено на рис. 4.

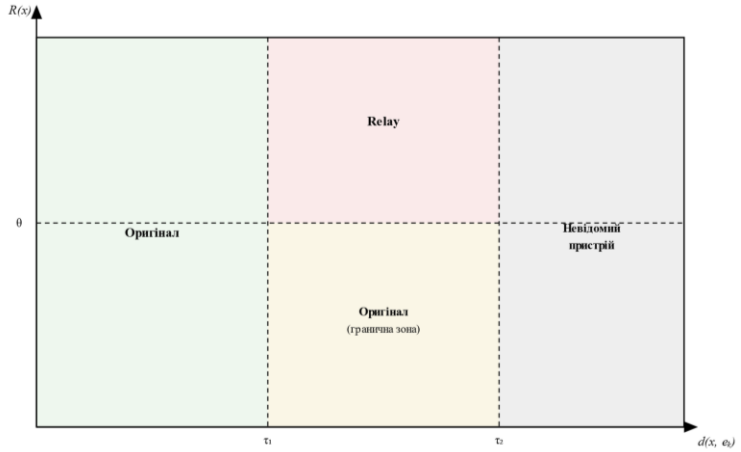

Рис. 4. Області ухвалення рішення у координатах ($d(x, e_k)$, $R(x)$)

Діаграма унаочнює, що межа τ_1 відокремлює "впевнено легітимну" зону від граничної, у якій остаточне рішення залежить від каналового індикатора R(x): перевищення порогу θ у цій смузі свідчить про фізичну ретрансляцію, тоді як значення нижче θ означає лише природну варіацію каналу в межах, допустимих для оригінального пристрою. Розширений поріг τ_2 формує зовнішню межу, за якою відбиток більше не вважається таким, що належить жодному відомому пристрою.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті виконано систематизацію методів виявлення атак типу Replay та Relay у бездротових системах на основі радіочастотного відбитка сигналу (RF-fingerprinting) з використанням SDR-приймачів. Показано, що обидва типи атак зберігають коректність даних на протокольному рівні, тому їх виявлення можливе лише за рахунок аналізу фізичних апаратних артефактів передавача та каналу поширення сигналу, а не криптографічних чи часових ознак протоколу.

Проведено порівняльний аналіз SDR-платформ (RTL-SDR V3, HackRF One, ADALM-PLUTO, USRP B210) за критеріями, релевантними саме для задачі виявлення Replay/Relay атак, і показано, що навіть бюджетне обладнання забезпечує точність розрізнення "оригінал/атака" на рівні 95-99 % [7, 8].

Запропоновано узагальнену, протокольно-незалежну архітектуру системи виявлення, що поєднує SDR-приймач, модуль попередньої обробки IQ-сигналу, екстрактор RF-відбитка та окремий модуль аналізу каналу, який паралельно оцінює затримку поширення й спотворення, характерні для ретрансляційної апаратури. Формалізовано задачу виявлення як поєднання метричної класифікації в просторі embedding-векторів (для розрізнення відомий/невідомий пристрій) з двома додатковими критеріями – кореляцією payload для Replay та індикатором каналової аномалії для Relay. Розроблено алгоритм ухвалення рішення, що послідовно застосовує ці критерії та класифікує сигнал як оригінальний, Replay, Relay або такий, що належить невідомому пристрою.

Аналіз наявних експериментальних результатів [7, 8] підтверджує практичну реалізовність запропонованого підходу. Водночас слід відзначити обмеження: запропонована архітектура є концептуальною і потребує експериментальної верифікації на єдиному стенді з реальними реалізаціями Replay та Relay атак для конкретних протоколів (EV1527, Zigbee, LoRa), а вагові коефіцієнти α, β, γ та пороги τ_1, τ_2, θ потребують емпіричного калібрування для кожного сценарію розгортання.

Подальші дослідження доцільно спрямувати на: (1) експериментальну перевірку запропонованого алгоритму на лабораторному стенді з HackRF One / ADALM-PLUTO для протоколу EV1527; (2) дослідження стійкості каналового індикатора R(x) до природної мобільності легітимних пристроїв, яка також вносить затримку й варіацію SNR; (3) інтеграцію запропонованого підходу з протоколами обмеження відстані [5, 6] як додаткового, взаємодоповнювального рівня захисту; (4) розширення методики на сценарії з кількома одночасними атакуючими.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. *ACM Computing Surveys, 45*(1), Article 6. https://doi.org/10.1145/2379776.2379782
2. Xie, L., Peng, L., Zhang, J., et al. (2024). Radio frequency fingerprint identification for Internet of Things: A survey. *Security and Safety, 3*, Article 2023022. https://doi.org/10.1051/sands/2023022
3. Abbas, S., Abu Talib, M., Nasir, Q., et al. (2024). Radio frequency fingerprinting techniques for device identification: A survey. *International Journal of Information Security, 23*(2), 1389-1427. https://doi.org/10.1007/s10207-023-00801-z
4. Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2011)*. https://eprint.iacr.org/2010/332
5. Rasmussen, K. B., & Capkun, S. (2010). Realization of RF distance bounding. In *Proceedings of the 19th USENIX Security Symposium* (pp. 389-402). USENIX Association.
6. Bianchi, T., Brighente, A., Conti, M., & Pavan, E. (2025). SoK: Stealing cars since remote keyless entry introduction and how to defend from it. In *Proceedings of the 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec 2025)* (pp. 161-178). USENIX Association.
7. Wang, Y., Zou, J., & Zhang, K. (2023). Deep-learning-aided RF fingerprinting for NFC relay attack detection. *Electronics, 12*(3), Article 559. https://doi.org/10.3390/electronics12030559
8. Quintero, J. C. M., Cuesta, E. P. E., & Lopez, L. J. R. (2023). A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. *Results in Engineering, 19*, Article 101243. https://doi.org/10.1016/j.rineng.2023.101243

9. Ahmed, A., Quoitin, B., Gros, A., & Moeyaert, V. (2024). A comprehensive survey on deep learning-based LoRa radio frequency fingerprinting identification. *Sensors, 24*(13), Article 4411. https://doi.org/10.3390/s24134411
10. Al-Shawabka, A., et al. (2020). Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications* (pp. 646–655). IEEE. https://doi.org/10.1109/INFOCOM41043.2020.9155259
11. Restuccia, F., D'Oro, S., Al-Shawabka, A., et al. (2019). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 51-60). Association for Computing Machinery. https://doi.org/10.1145/3323679.3326503
12. Dhakal, R., Kandel, L., & Shekhar, P. (2025). Radio frequency fingerprinting authentication for IoT networks using Siamese networks. *IoT, 6*(3), Article 47. https://doi.org/10.3390/iot6030047

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Loban Heorhii Antonovych
PhD Student, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0003-4862-8729
heorhii.loban.asp.2025@lpnu.ua

Lukovskyy Taras Ihorovych
PhD, Associate Professor, Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

DETECTION OF REPLAY/RELAY ATTACKS IN WIRELESS SYSTEMS USING RF-FINGERPRINTING AND SDR

Abstract. This paper systematizes methods for detecting Replay and Relay attacks in wireless systems based on radio-frequency fingerprinting (RF-fingerprinting) of the signal using Software-Defined Radio (SDR) receivers. It is shown that both attack types preserve data correctness at the protocol level, so their detection is only possible through analysis of physical hardware artifacts of the transmitter and propagation channel rather than cryptographic or timing protocol features. A comparative analysis of SDR platforms (RTL-SDR V3, HackRF One, ADALM-PLUTO, USRP B210) relevant to Replay/Relay detection is performed. A generalized, protocol-independent detection architecture is proposed, combining an SDR receiver, an IQ preprocessing module, an RF-fingerprint extractor, and a channel-analysis module that evaluates propagation delay and relay-induced distortions in parallel. The detection task is formalized as metric classification in embedding space combined with two additional criteria – payload correlation for Replay and a channel-anomaly indicator for Relay. A decision algorithm is developed that classifies a signal as original, Replay, Relay, or belonging to an unknown device. Analysis of available experimental results confirms the practical feasibility of the proposed approach, with reported accuracy of 95-99% for original/attack discrimination on both budget and high-end SDR hardware.

Keywords: radio frequency fingerprint, RF-fingerprinting, Replay attack, Relay attack, Software-Defined Radio, SDR, keyless entry, physical-layer authentication, Internet of Things, carrier frequency offset, IQ imbalance.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Danev, B., Zanetti, D., & Capkun, S. (2012). On physical-layer identification of wireless devices. *ACM Computing Surveys, 45*(1), Article 6. https://doi.org/10.1145/2379776.2379782
2. Xie, L., Peng, L., Zhang, J., et al. (2024). Radio frequency fingerprint identification for Internet of Things: A survey. *Security and Safety, 3*, Article 2023022. https://doi.org/10.1051/sands/2023022
3. Abbas, S., Abu Talib, M., Nasir, Q., et al. (2024). Radio frequency fingerprinting techniques for device identification: A survey. *International Journal of Information Security, 23*(2), 1389-1427. https://doi.org/10.1007/s10207-023-00801-z
4. Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2011)*. https://eprint.iacr.org/2010/332
5. Rasmussen, K. B., & Capkun, S. (2010). Realization of RF distance bounding. In *Proceedings of the 19th USENIX Security Symposium* (pp. 389-402). USENIX Association.
6. Bianchi, T., Brighente, A., Conti, M., & Pavan, E. (2025). SoK: Stealing cars since remote keyless entry introduction and how to defend from it. In *Proceedings of the 3rd USENIX Symposium on Vehicle Security and Privacy (VehicleSec 2025)* (pp. 161-178). USENIX Association.
7. Wang, Y., Zou, J., & Zhang, K. (2023). Deep-learning-aided RF fingerprinting for NFC relay attack detection. *Electronics, 12*(3), Article 559. https://doi.org/10.3390/electronics12030559
8. Quintero, J. C. M., Cuesta, E. P. E., & Lopez, L. J. R. (2023). A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. *Results in Engineering, 19*, Article 101243. https://doi.org/10.1016/j.rineng.2023.101243

9. Ahmed, A., Quoitin, B., Gros, A., & Moeyaert, V. (2024). A comprehensive survey on deep learning-based LoRa radio frequency fingerprinting identification. *Sensors, 24*(13), Article 4411. https://doi.org/10.3390/s24134411
10. Al-Shawabka, A., et al. (2020). Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications* (pp. 646–655). IEEE. https://doi.org/10.1109/INFOCOM41043.2020.9155259
11. Restuccia, F., D'Oro, S., Al-Shawabka, A., et al. (2019). DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. In *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 51-60). Association for Computing Machinery. https://doi.org/10.1145/3323679.3326503
12. Dhakal, R., Kandel, L., & Shekhar, P. (2025). Radio frequency fingerprinting authentication for IoT networks using Siamese networks. *IoT, 6*(3), Article 47. https://doi.org/10.3390/iot6030047

Отримано редакцією журналу / Received: 28.01.26
Прорецензовано / Revised: 07.02.26
Схвалено до друку / Accepted: 24.09.26