УДК 004.056.5

О. О. Руснак
А. А. Шиян

СИСТЕМА ВЕРИФІКАЦІЇ WI-FI ТОЧОК ДОСТУПУ НА ОСНОВІ АНАЛІЗУ ЧАСОВИХ ХАРАКТЕРИСТИК ТА DEVICE FINGERPRINTING

Вінницький національний технічний університет

Анотація

У роботі розглянуто підхід до верифікації Wi-Fi точок доступу на основі багатокритеріального аналізу часових і логічних характеристик мережевого трафіку. Запропоновано використовувати міжінтервальні затримки службових кадрів, дисперсію джиттера, RSSI, номери послідовності кадрів і структуру інформаційних елементів як основу цифрового відбитка пристрою. Спроєктовано модульну архітектуру програмної системи, що поєднує пасивне захоплення кадрів, вилучення метаданих, математичний співпроцесор, логічну верифікацію та підсистему прийняття рішень. Обґрунтовано використання ковзного вікна, нормалізації часових рядів, зваженої евклідової відстані та локального сховища еталонних профілів для виявлення атак Rogue AP та Evil Twin.

Ключові слова: Wi-Fi, IEEE 802.11, Rogue AP, Evil Twin, Device Fingerprinting, IAT, джиттер, RSSI, цифровий відбиток, верифікація точки доступу.

Abstract

The paper considers an approach to Wi-Fi access point verification based on multi-criteria analysis of timing and logical characteristics of network traffic. Inter-arrival time of management frames, jitter variance, RSSI, frame sequence numbers, and information element structure are proposed as the basis of a device fingerprint. A modular software architecture is designed, combining passive frame capture, metadata extraction, a mathematical coprocessor, logical verification, and a decision-making subsystem. The use of a sliding window, time-series normalization, weighted Euclidean distance, and local storage of reference profiles is substantiated for detecting Rogue AP and Evil Twin attacks.

Keywords: Wi-Fi, IEEE 802.11, Rogue AP, Evil Twin, Device Fingerprinting, IAT, jitter, RSSI, device fingerprint, access point verification.

Вступ

Бездротові мережі стандарту IEEE 802.11 є важливою частиною корпоративної та побутової інформаційної інфраструктури, однак відкрита природа радіоефіру створює умови для пасивного перехоплення, ін’єкції службових кадрів, розгортання несанкціонованих точок доступу та атак типу Evil Twin. Особливу небезпеку становить те, що зловмисник може відтворити логічні ідентифікатори мережі, зокрема SSID, BSSID і параметри безпеки, тому перевірка лише адресних або сигнатурних ознак не забезпечує достатньої стійкості [1-4].

Перспективним напрямом є використання Device Fingerprinting, тобто формування цифрового відбитка пристрою на основі ознак, які складніше підробити програмно. До таких ознак належать часові характеристики передавання кадрів, джиттер, поведінка лічильників послідовності, зміни RSSI та структура інформаційних елементів службових кадрів [5-9]. У реальних умовах жодна з цих ознак не є абсолютно стабільною, тому актуальним є саме комплексне поєднання декількох незалежних параметрів у єдиній моделі верифікації.

Метою роботи є проєктування підходу до верифікації Wi-Fi точок доступу на основі аналізу часових характеристик та ідентифікації пристроїв методом Device Fingerprinting, а також обґрунтування архітектурних, алгоритмічних та інформаційних рішень для виявлення підроблених вузлів бездротової інфраструктури.

Результати дослідження

У межах розробленого підходу Wi-Fi точка доступу розглядається як джерело потоків службових кадрів, поведінка якого визначається не лише заявленими логічними атрибутами, а й особливостями апаратної платформи та програмного стеку. На відміну від моделей, що спираються тільки на MAC-адресу або SSID, запропонована модель використовує багатовимірний вектор ознак $V = (IAT, \sigma^2IAT, RSSI, Pseq, Flogic)$, де IAT характеризує міжінтервальні затримки, σ^2IAT - рівень джиттера, Pseq - аномальність номерів послідовності, а Flogic - штраф за невідповідність логічних параметрів еталонному профілю [5, 8, 9].

Міжінтервальна затримка визначається як різниця між моментами фіксації двох послідовних службових кадрів від однієї точки доступу: $\Delta t_i = t_i - t_{i-1}$. Далі на ковзному вікні спостереження обчислюються середнє значення μIAT та дисперсія σ^2IAT. Стабільна апаратна точка доступу зазвичай формує більш вузький розподіл

часових інтервалів, тоді як програмна імітація може мати підвищену варіативність через вплив планувальника операційної системи, драйверів і програмного мережевого стеку [5-7].

Другим важливим блоком є аналіз номерів послідовності кадрів. У легітимному обладнанні інкремент лічильника здебільшого підтримується на рівні мікрокоду мережевого адаптера, тому різкі стрибки, повтори або обнулення можуть свідчити про ін'єкцію кадрів чи паралельну роботу програмного імітатора. Для перетворення розривів у числову ознаку доцільно використовувати нормалізований показник Pseq, який зростає зі збільшенням сумарного відхилення між очікуваним і фактичним ходом лічильника.

Додаткову роль відіграють RSSI та структура інформаційних елементів. Зміна потужності сигналу не може бути єдиною підставою для висновку, оскільки на неї впливають відстань, перешкоди та положення сенсора. Водночас різке посилення сигналу разом із невідповідністю vendor-specific тегів або порядку інформаційних елементів є суттєвим індикатором підміни обладнання. Тому логічні й енергетичні ознаки застосовуються як допоміжні штрафні компоненти в загальній цільовій функції.

Остаточне рішення щодо автентичності точки доступу пропонується приймати через порівняння поточного вектора ознак з еталонним профілем пристрою. Для цього може використовуватися зважена евклідова відстань D, де вагові коефіцієнти задають важливість окремих метрик. Якщо D перевищує поріг чутливості θ, система класифікує поточний вузол як потенційно підмінений або скомпрометований; якщо відхилення перебуває в межах норми, профіль може м'яко оновлюватися для врахування природних змін середовища [14, 15].

Архітектуру програмної системи доцільно поділити на п'ять функціональних підсистем. Підсистема захоплення кадрів працює в режимі пасивного радіомоніторингу та отримує службові кадри IEEE 802.11 без асоціації з мережею. Підсистема вилучення метаданих виконує декапсуляцію кадру, фіксує часову мітку, BSSID, номер послідовності, RSSI та інформаційні елементи. Математичний співпроцесор обчислює IAT, дисперсію та інші статистичні метрики на ковзному вікні. Модуль логічної верифікації порівнює структуру кадрів із еталонним профілем. Підсистема прийняття рішень агрегує результати та формує вердикт для адміністратора [10-13].

Алгоритмічне забезпечення системи складається з двох послідовних етапів. Перший етап виконує нормалізацію часових рядів: отримання часової мітки, пошук попереднього кадру від того самого джерела, обчислення Δt_i, відсікання граничних викидів і додавання валідного значення до ковзного вікна. Другий етап реалізує багатокритеріальну верифікацію: паралельне обчислення джиттера, аналіз номерів послідовності, перевірку логічних ознак і розрахунок метрики відхилення D. Такий поділ зменшує ризик хибнопозитивних спрацювань у зашумленому радіоефірі та забезпечує передбачуваний час виконання [14, 15].

Інформаційне забезпечення системи має зберігати еталонні цифрові відбитки пристроїв і результати перевірок. У практичній реалізації така структура може бути оформлена як SQLite-таблиця, JSON-файл або локальний кеш профілів. Логічно доцільно виділити реєстр точок доступу, таблицю часових сигнатур і журнал безпекових інцидентів. Реєстр містить BSSID, SSID та службовий статус вузла; таблиця сигнатур зберігає μIAT, σ^2IAT, допоміжні часові й логічні параметри; журнал інцидентів фіксує значення D, поріг θ, час події та вердикт системи [16-18].

Програмна реалізація такого підходу може бути виконана засобами Python із використанням бібліотек для аналізу пакетів, обробки даних і зберігання локальних профілів. Зокрема, Scapy є придатним інструментом для низькорівневого аналізу кадрів, а pandas і NumPy можуть застосовуватися для обчислення статистичних характеристик часових рядів [19, 20].

Таблиця 1 - Узагальнення компонентів системи верифікації Wi-Fi точок доступу

Компонент або ознака	Основне призначення	Очікуваний результат
IAT	Вимірювання інтервалів між службовими кадрами	Базовий часовий профіль точки доступу
Джиттер / σ^2IAT	Оцінювання стабільності часової поведінки	Виявлення програмної імітації або нестабільного вузла
Номери послідовності	Контроль монотонності лічильника кадрів	Фіксація ін'єкцій, стрибків або обнулень
RSSI	Відстеження змін рівня сигналу	Ознака можливої енергетичної підміни
Інформаційні елементи	Перевірка структури службових кадрів	Виявлення невідповідності прошивці або моделі обладнання
Зважена відстань D	Агрегація усіх ознак у єдину метрику	Класифікація вузла як легітимного або підозрілого
Локальний профіль / кеш	Збереження еталонних сигнатур та журналу подій	Підтримка аудиту й подальшого аналізу інцидентів

Висновки

У результаті дослідження обґрунтовано доцільність використання багатокритеріального Device Fingerprinting для верифікації Wi-Fi точок доступу. Запропонований підхід зменшує залежність від легко підроблюваних логічних ідентифікаторів і використовує ознаки, пов'язані з реальною часовою, логічною та енергетичною поведінкою пристрою.

Розроблена модель поєднує міжінтервальні затримки, дисперсію джиттера, RSSI, номери послідовності та структуру інформаційних елементів у єдиному нормалізованому просторі ознак. Використання зваженої евклідової відстані дозволяє кількісно оцінювати ступінь відхилення поточного стану точки доступу від її еталонного цифрового відбитка.

Запропонована модульна архітектура з підсистемами захоплення кадрів, вилучення метаданих, математичного аналізу, логічної верифікації та прийняття рішень забезпечує розмежування відповідальностей і придатна для подальшої програмної реалізації. Застосування ковзного вікна, фільтрації викидів і локального збереження еталонних профілів підвищує стійкість системи в умовах реального радіошуму.

Практичне значення запропонованого підходу полягає в можливості використання розробленої системи для моніторингу корпоративної Wi-Fi інфраструктури, виявлення Rogue AP та Evil Twin, а також формування журналу подій для подальшого аудиту безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Hsu T.-C., Lin C.-H., Yeh Y.-C. WPFD: Active User-Side Detection of Evil Twins. Applied Sciences. 2022. Vol. 12, No. 16. P. 8088. DOI: 10.3390/app12168088.
2. Lu Q., Li S., Zhang J., Qu H. PEDR: Exploiting phase error drift range to detect full-model rogue access point attacks. Computers & Security. 2022. Vol. 113. P. 102554. DOI: 10.1016/j.cose.2021.102554.
3. Alotaibi A., Elleithy K. Data Mining Approach for Evil Twin Attack Identification in Wi-Fi Networks. IEEE Access. 2024. Vol. 12. P. 14210-14225.
4. Shah S. A., Ahmad M. Convolutional neural network based evil twin attack detection in WiFi networks. MATEC Web of Conferences. 2021. Vol. 336. P. 08006.
5. Mura N., Kurihara T., Shiina K. Recognition of Wi-Fi Devices by Focusing on Inter-Arrival Time and Periodicity of Probe Request Frames. 2023 IEEE 12th Global Conference on Consumer Electronics (GCCE). 2023. P. 1-5. DOI: 10.1109/GCCE59613.2023.10315481.
6. Abdallah S. IoT Device Fingerprinting via Frequency Domain Analysis. Electronics. 2024. Vol. 13, No. 16. P. 3248. DOI: 10.3390/electronics13163248.
7. Djara V. A. D., Andriyana Y., Toharudin T. Potential of Robust Regression Methods in Clock Skew Measurement. Jurnal Ilmu Matematika dan Terapan. 2023. Vol. 16, No. 1. P. 243-252.
8. Wang Z., Zhao H., Li S. A Survey on Cross-Layer Wi-Fi Device Identification: From MAC to Physical Layer. IEEE Communications Surveys & Tutorials. 2024. Vol. 26, No. 1. P. 112-145.
9. Hou W., Wang Y., Zheng Z. Preamble Forgery and Injection in Wi-Fi Networks: Attacks and Defenses. IEEE Transactions on Mobile Computing. 2024. Vol. 23. P. 1-15.
10. Bass L., Clements P., Kazman R. Software Architecture in Practice. 4th ed. Boston : Addison-Wesley Professional, 2021. 416 p.
11. Fowler M. UML Distilled: A Brief Guide to the Standard Object Modeling Language. 3rd ed. Boston : Addison-Wesley Professional, 2003. 208 p.
12. Booch G., Rumbaugh J., Jacobson I. The Unified Modeling Language User Guide. 2nd ed. Boston : Addison-Wesley, 2005. 496 p.
13. Laplante P. A., Ovaska S. J. Real-Time Systems Design and Analysis: Tools for the Practitioner. 4th ed. Hoboken : Wiley-IEEE Press, 2011. 560 p.
14. Box G. E. P., Jenkins G. M., Reinsel G. C., Ljung G. M. Time Series Analysis: Forecasting and Control. 5th ed. Hoboken : Wiley, 2015. 712 p.
15. Aggarwal C. C. Outlier Analysis. 2nd ed. Cham : Springer, 2017. 480 p.
16. Date C. J. An Introduction to Database Systems. 8th ed. Boston : Addison-Wesley, 2003. 1024 p.
17. Codd E. F. The Relational Model for Database Management: Version 2. Reading : Addison-Wesley, 1990. 538 p.
18. Elmasri R., Navathe S. B. Fundamentals of Database Systems. 7th ed. Hoboken : Pearson, 2015. 1280 p.
19. McKinney W. Python for Data Analysis: Data Wrangling with pandas, NumPy, and Jupyter. 3rd ed. Sebastopol : O'Reilly Media, 2022. 544 p.
20. Biondi P. Scapy: Interactive Packet Manipulation Program. 2023. URL: https://scapy.net/ (дата звернення: 28.05.2024).

Руснак Олександр Олегович - студент групи 2КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, , e-mail: rusnak.sana.00@gmail.com

Шиян Анатолій Антонович - к.ф.-м.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: anatoliy.a.shiyan@gmail.com.

Rusnak Oleksandr O. - student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: rusnak.sana.00@gmail.com

Shyian Anatolii A. - Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: anatoliy.a.shiyan@gmail.com