ЗАСТОСУВАННЯ СИСТЕМИ ПОЗИЦІОНУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ АБОНЕНТІВ БЕЗПРОВІДНОЇ МЕРЕЖІ WI-FI

Василенко Т.О., Никитюк О.О.

Кафедра комп'ютерної радіоінженерії та систем технічного захисту інформації,
Харківський національний університет радіоелектроніки,
Україна

E-mail: tetiana.vasylenko@nure.ua
oleksandr.nykytiuk@nure.ua

Abstract

The task of ensuring security is complex, so its solution requires auxiliary analysis methods, an expanded set of features considered for detecting unauthorized access, and features specific to wireless Wi-Fi networks. To address this problem, the present work proposes to examine local positioning (indoor localization) methods and to develop a monitoring system based on one of these methods. Experimental studies were carried out, including creation of a radio map for a 116 m² room with 93 reference points. It was shown that signal level is practically independent of the positions of doors and windows in the room. An analysis of attack organization principles against wireless networks demonstrated that taking location into account makes it possible to detect man-in-the-middle attacks, user impersonation (subscriber fraud) and rogue access points, as well as to localize the source of jamming.

За даними [1], у 2022 році значна частина українських компаній зіткнулася з економічними злочинами та шахрайством протягом останніх двох років. У більшості випадків шахрайство здійснювалося самими працівниками організацій. Відкритість і простота підключення до бездротових мереж, які стрімко впроваджуються повсюдно, можуть суттєво спрощувати завдання зловмисникам. Сам принцип бездротової передачі створює можливість для несанкціонованих підключень, причому стандартні засоби захисту [2, 3] часто не забезпечують належного рівня безпеки.

З огляду на численні недоліки та вразливості, що дозволяють шкідливим впливам успішно обходити системи захисту інформації, актуальними є дослідження, спрямовані на комплексне забезпечення безпеки із використанням додаткових параметрів аналізу для виявлення несанкціонованого доступу та ідентифікації зловмисника.

Огляд різних методів виявлення місцяположення [4-8] показав, що найефективнішим є метод радіовідбитків (Fingerprinting) [9]. Він базується на побудові радіокарти в приміщенні та передбачає дві стадії реалізації. На першому етапі здійснюється збирання інформації про RSSI від кількох опорних точок базових станцій (щонайменше трьох) і формування бази даних цих значень разом із планом приміщення. Потужність сигналу від доступних точок доступу Wi-Fi має бути прив'язана до локальних або глобальних координат об'єкта. Другий етап полягає у постійному моніторингу RSSI користувацьких пристроїв та порівнянні отриманих значень з базою даних для пошуку збігів або найближчих відповідностей. Такий метод забезпечує високу точність визначення місцезнаходження за умови своєчасного оновлення та актуалізації радіокарти.

Для експериментального дослідження на основі методу RSSI було обрано житлове приміщення у приватній забудові площею 116 м². На рис. 1 представлено схему будинку із зазначенням місць встановлення трьох точок доступу, що формують зону контролю.

Точки доступу було розміщено в межах зони покриття на різних висотах і позиціях, що дозволило отримати більш точну інформацію про розташування пристроїв, які при інших конфігураціях могли б виглядати однаково віддаленими від різних передавачів. Перед початком вимірювань було проведено радіообстеження приміщення для оптимального підбору робочих каналів та налаштування потужності передавачів у зоні дії мережі.

Результати показали, що використання трьох точок доступу забезпечує стійке покриття площі близько 116 м². У роботі застосовувався маршрутизатор TP-LINK Archer AXE75 із такими основними

характеристиками: робоча частота 5,240 ГГц, коефіцієнт підсилення антени 5 dBi та потужність передавача 27 dBm. Як приймальний пристрій використовувався смартфон Xiaomi POCO F6.

Оптимальним рішенням для дослідження було б використання трьох однакових маршрутизаторів, проте через наявність лише одного пристрою експеримент проводився по черзі з різними його розташуваннями. Встановлені параметри роботи: канал 42 з центральною частотою 5210 МГц і шириною смуги 80 МГц (діапазон 5180–5260 МГц).

Під час експерименту виявлено вплив орієнтації мобільного пристрою на рівень отриманого сигналу, тому радіокарта формувалася за середнім значенням RSSI, виміряним на висоті 1 м протягом 60 секунд у шести різних положеннях смартфона: у вертикальному положенні (антена вгору та вниз) та горизонтальному (0°, 90°, 180°, 270°). Кожне положення вимірювалося протягом 10 секунд. На рис. 1 наведено 93 опорних точок, до яких віднесено результати проведених вимірювань, наведені в табл. 1.

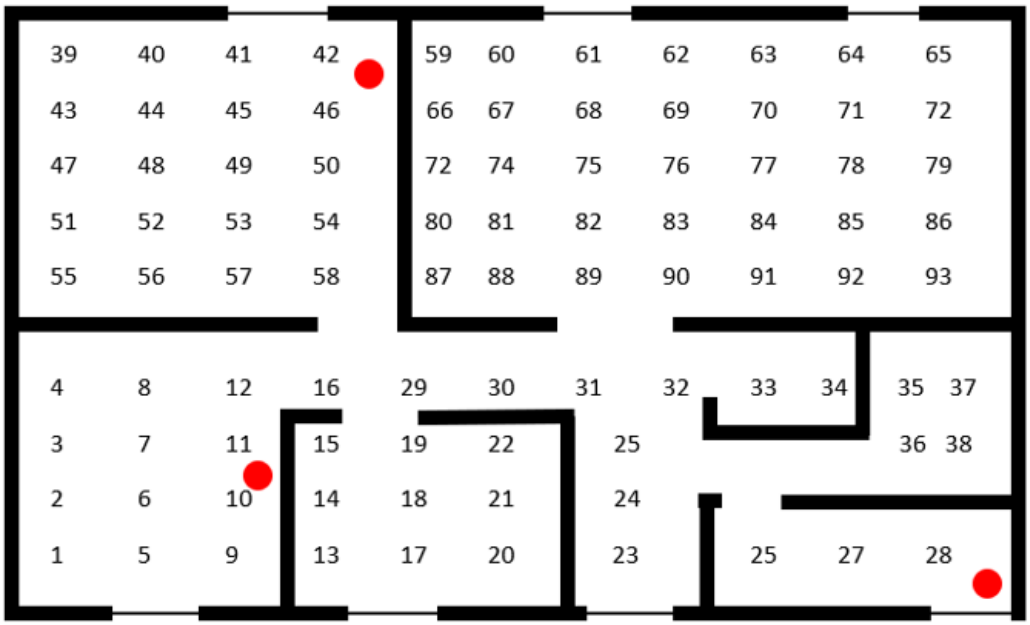

Рис. 1. Схема території, що підлягає захисту, із розташуванням точок доступу

На рис. 2 подано візуалізацію результатів експериментального дослідження поширення Wi-Fi сигналу, яка демонструє обґрунтованість вибору місць розміщення точок доступу. Виміряні значення рівня сигналу в одній і тій же опорній точці для трьох різних передавачів мають помітні відмінності.

Як показує аналіз даних табл. 1, положення дверей та вікон практично не впливають на прийнятий рівень сигналу – зафіксовані відхилення не перевищують 1–2 dBm. Під час формування карти радіовідбитків встановлено, що різниця показників для різних орієнтацій приймача становила від 3 до 10 dBm, причому максимальні розбіжності спостерігалися лише в окремих точках. У більшості випадків різниця вимірювань не перевищувала 5 dBm, що еквівалентно похибці визначення координат близько 2 метрів при застосуванні детермінованого (евклідового) методу позиціонування.

Таким чином, отримана точність позиціонування є порівнянною з рівнем сучасних комерційних систем. Для подальшого підвищення точності можливе збільшення кількості опорних точок та використання методів інтелектуального аналізу даних при обчисленні координат.

Визначення координат об’єкта можливе також і за межами основної зони контролю, якщо виконати додаткові вимірювання рівнів сигналу на прилеглій території та включити їх до загальної радіокарти. У ситуаціях, коли проведення прямих вимірювань неможливе (наприклад, через обмежений доступ), рівень сигналу може бути спрогнозований аналітично на основі отриманих експериментальних даних та відповідних моделей поширення.

Крім того, локалізація пристрою поза межами захищеної області може здійснюватися за допомогою латераційних (дальномірних) методів. Хоча точність такого підходу є нижчою, наявність сигналу хоча б від однієї або двох точок доступу дозволяє оцінити орієнтовну відстань до об’єкта та напрямок його розташування.

Таблиця 1. Результати вимірювання рівня сигналу

№ точки	ТД1, середній рівень RSSI, dBm		ТД2, середній рівень RSSI, dBm		ТД3, середній рівень RSSI, dBm	
	вікна/двері закриті	вікна/двері відкриті	вікна/двері закриті	вікна/двері відкриті	вікна/двері закриті	вікна/двері відкриті
1	2	3	4	5	6	7
13	-52,6	-51,9	-63,4	-62,6	-58,6	-58,2
14	-53,1	-53,8	-61,1	-61,6	-54,3	-53,9
15	-54,9	-55,4	-57,3	-56,4	-52,0	-51,8
16	-56,4	-56,0	-59,9	-58,1	-59,3	-58,7
17	-57,6	-57,1	-62,4	-61,5	-65,1	-64,3
18	-54,9	-54,6	-56,3	-56,7	-69,5	-69,1
19	-64,7	-64,2	-54,1	-54,0	-68,7	-67,4
20	-64,2	-65,0	-65,3	-64,8	-71,2	-71,0
21	-59,2	-59,6	-57,4	-55,3	-68,9	-69,0
22	-63,2	-61,8	-56,0	-54,4	-65,0	-64,7
23	-68,6	-67,1	-56,4	-55,1	-74,3	-73,6
24	-61,6	-61,4	-57,7	-57,5	-70,1	-69,8
25	-57,9	-57,1	-55,4	-54,9	-67,4	-67,1
26	-70,1	-68,2	-63,7	-62,3	-78,1	-77,4
27	-65,4	-65,5	-64,0	-63,2	-73,7	-73,6
28	-68,7	-67,9	-53,4	-53,6	-71,2	-71,2
29	-57,7	-58,1	-39,4	-39,3	-62,9	-63,0
30	-54,0	-53,3	-41,1	-40,8	-58,7	-58,4
31	-62,9	-62,2	-47,4	-46,2	-54,6	-54,1
32	-56,6	-55,8	-37,6	-37,9	-61,7	-58,4
33	-55,4	-53,1	-36,4	-37,1	-59,4	-58,7
34	-63,7	-61,5	-36,1	-36,3	-51,3	-50,9
35	-67,9	-65,3	-35,4	-35,1	-61,3	-59,8
36	-58,6	-56,1	-35,1	-34,2	-58,3	-57,4
37	-66,7	-63,9	-34,8	-34,5	-54,2	-52,1
38	-68,6	-66,6	-32,7	-32,9	-64,1	-64,5
39	-63,3	-62,8	-30,1	-30,6	-60,7	-58,2
40	-65,1	-63,3	-28,9	-28,1	-55,9	-54,5
41	-48,8	-48,4	-52,4	-52,1	-42,7	-40,6
42	-53,5	-53,2	-47,4	-47,9	-45,2	-44,4
43	-69,5	-69,0	-60,3	-59,7	-64,2	-64,1
44	-64,4	-63,8	-65,1	-64,8	-57,0	-56,8
45	-66,2	-65,7	-66,4	-66,1	-54,8	-54,3
46	-68,7	-68,2	-70,5	-70,3	-61,6	-60,9
47	-62,9	-61,4	-61,8	-61,5	-55,7	-54,7
48	-64,0	-64,3	-66,4	-66,1	-51,2	-51,0
48	-64,0	-64,3	-66,4	-66,1	-51,2	-51,0
49	-67,6	-66,5	-69,7	-69,4	-57,3	-56,8
50	-70,3	-69,4	-63,2	-62,9	-59,4	-59,2
51	-57,1	-56,8	-49,3	-47,6	-39,2	-39,1
52	-60,4	-60,2	-65,3	-65,1	-45,1	-44,9
53	-63,7	-63,5	-72,7	-72,2	-48,4	-48,6
54	-54,4	-54,6	-46	-45,4	-36,3	-36,1
55	-62,1	-62,0	-72,1	-71,7	-34,0	-34,2
56	-64,5	-64,4	-66,8	-66,5	-41,7	-41,4
57	-52,3	-51,8	-49,6	-48,2	-32,4	-32,5
58	-56,1	-56,4	-63,6	-63,4	-30,1	-30,3

Таблиця 1. (продовження)

1	2	3	4	5	6	7
59	-60,0	-61,1	-70,5	-71,1	-35,7	-34,4
60	-66,2	-65,1	-54,4	-55,2	-63,0	-63,2
61	-74,7	-74,2	-59,5	-58,1	-60,9	-61,4
62	-77,1	-76,8	-62,8	-62,2	-66,4	-65,7
63	-68,8	-67,3	-49,1	-49,0	-68,6	-68,1
64	-69,7	-66,5	-59,9	-59,7	-63,9	-63,3
65	-75,6	-74,8	-62,2	-61,2	-72,1	-71,8
66	-73,4	-72,8	-48,4	-47,5	-57,4	-57,1
67	-68,8	-66,9	-56,4	-56,1	-61,4	-61,0
68	-76,8	-75,2	-58,1	-58,7	-67,5	-67,3
69	-73,4	-72,8	-65,7	-65,1	-79,4	-78,8
70	-77,6	-77,3	-62,6	-62,4	-77,2	-76,6
71	-75,5	-72,1	-59,8	-59,2	-74,8	-73,3
72	-79,8	-76,6	-52,6	-51,6	-71,1	-70,1
73	-76,2	-75,7	-68,3	-67,8	-81,4	-81,3
74	-78,1	-78,0	-64,8	-64,1	-78,7	-78,2
75	-79,7	-77,1	-61,1	-60,9	-75,0	-73,1
76	-80,6	-78,2	-55,4	-55,2	-71,8	-69,9
77	-66,2	-65,1	-54,4	-55,2	-63,0	-63,2
78	-74,7	-74,2	-59,5	-58,1	-60,9	-61,4
79	-77,1	-76,8	-62,8	-62,2	-66,4	-65,7
80	-68,8	-67,3	-49,1	-49,0	-68,6	-68,1
81	-69,7	-66,5	-59,9	-59,7	-63,9	-63,3
82	-75,6	-74,8	-62,2	-61,2	-72,1	-71,8
83	-73,4	-72,8	-48,4	-47,5	-57,4	-57,1
84	-75,6	-68,8	-66,9	-56,4	-56,1	-61,4
85	-73,4	-76,8	-75,2	-58,1	-58,7	-67,5
86	-68,8	-73,4	-72,8	-65,7	-65,1	-79,4
87	-76,8	-77,6	-77,3	-62,6	-62,4	-77,2
88	-73,4	-75,5	-72,1	-59,8	-59,2	-74,8
89	-77,6	-79,8	-76,6	-52,6	-51,6	-71,1
90	-75,5	-76,2	-75,7	-68,3	-67,8	-81,4
91	-79,8	-78,1	-78,0	-64,8	-64,1	-78,7
92	-76,2	-79,7	-77,1	-61,1	-60,9	-75,0
93	-75,6	-80,6	-78,2	-55,4	-55,2	-71,8

Розглянемо виявлення основних типів атак та способів реагування за допомогою системи позиціонування.

1. Перехоплення даних. Зловмисник може збирати трафік, перебуваючи поблизу точки доступу. Якщо він знаходиться поза захищеною територією, система визначення координат дає змогу швидко виявити його місцезнаходження та заблокувати діяльність. Якщо ж перехоплення здійснює легітимний користувач зсередини мережі, виявити атаку можна лише за непрямими ознаками – наприклад, нетиповою локацією або підозрілими характеристиками трафіку.

2. DoS-атака. Під час атаки відмови в обслуговуванні зловмисник навмисно створює перешкоди у робочому діапазоні точки доступу. Визначення місця генерації сигналу ефективне, якщо джерело розміщується всередині мережі. У випадку віддалених атак локалізація значно ускладнюється.

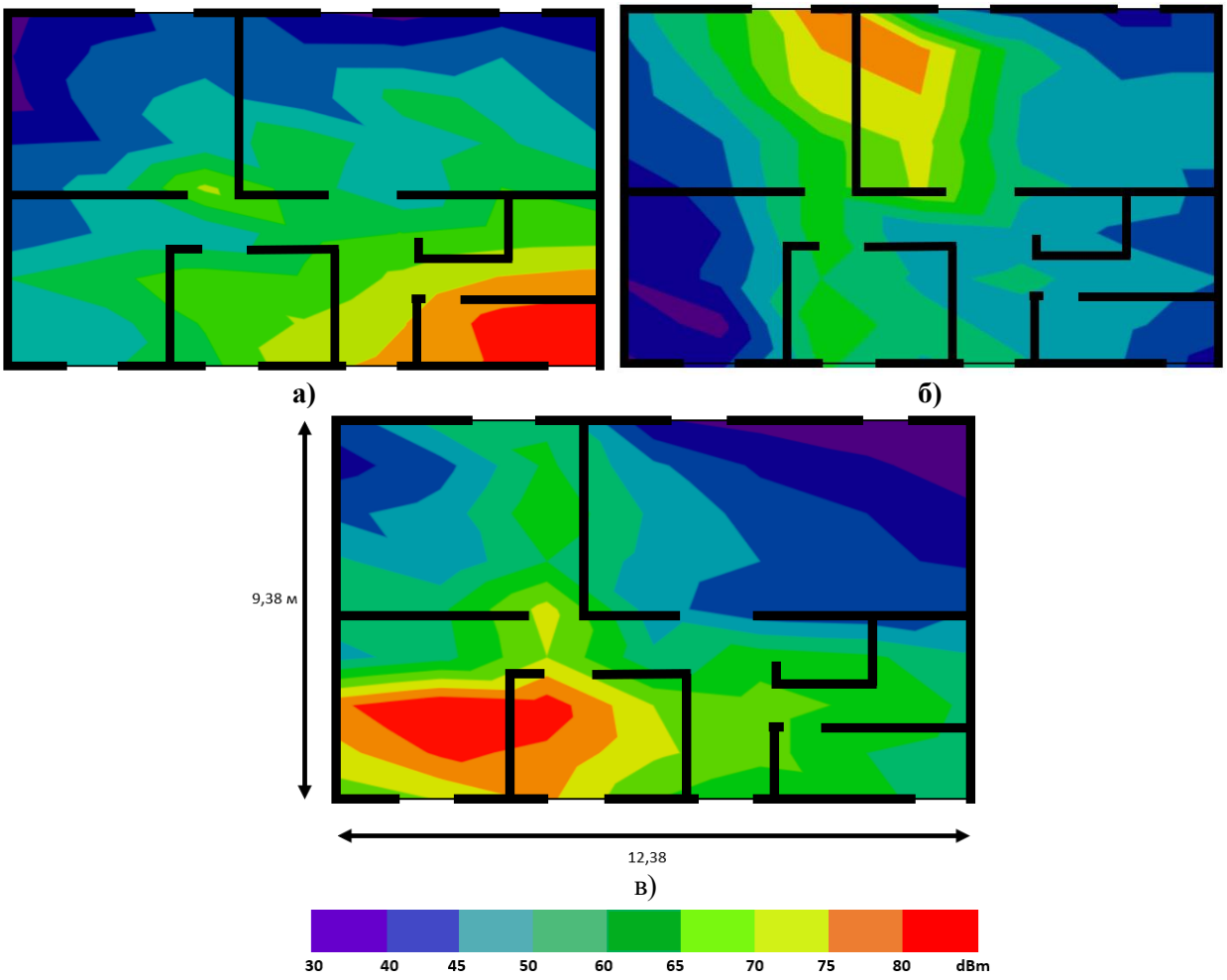

Рис. 2. Карти розповсюдження сигналу за показниками RSSI а) ТД 1; б) ТД 2; в) ТД 3

3. Глушіння каналу зв'язку. Інтенсивне створення радіоперешкод призводить до повного або часткового порушення роботи мережі. Знання просторового розташування клієнтів та обладнання дозволяє визначити напрямок джерела сигналу та приблизно його локалізувати.

4. Підставна точка доступу. Поява у мережі нового передавача з параметрами, схожими на офіційні, легко відстежується за координатами. Якщо точка розташована поза відомою картою – система може автоматично ідентифікувати її як підозрілу та заблокувати.

5. Зміна даних та несанкціоноване проникнення. Позиціонування корисне, коли зловмисник не є внутрішнім користувачем. Якщо втручання здійснюється авторизованою особою, потрібен додатковий аналіз трафіку для підтвердження порушення.

6. Атака «людина посередині» (Man-in-the-Middle). Сутність атаки полягає у перехопленні та можливій зміні даних між клієнтом і точкою доступу. Виявлення нового джерела сигналу поблизу користувача дозволяє розпізнати атаку та вчасно її припинити.

7. Підміна пристрою (імперсонація). Якщо клієнтський пристрій з'являється у незвичній зоні або змінює характер переміщення, система може автоматично позначити його як ризиковий або заблокувати. Це особливо корисно у випадках викрадення обладнання чи несанкціонованого використання облікових даних.

Висновки

В результаті експериментальних досліджень було запропоновано метод позиціонування який в сукупності зі стандартними методами захисту дозволить виявляти більше атак, специфічних саме для Wi-Fi мереж. Експериментально показано, що похибка визначення місцеположення становить близько ± 2 м при застосуванні детермінованого підходу (на основі евклідової відстані). Це дає підстави

стверджувати про ефективність обраних методів та дозволяє уникнути додаткових фінансових витрат на використання дорогого обладнання.

Література

1. PwC Ukraine. Глобальне дослідження економічних злочинів та шахрайства 2022: результати опитування українських компаній [Електронний ресурс] // 2022. Режим доступу: https://www.pwc.com/ua/uk/survey/2022/pwc-gecs-2022-ukr.pdf.

2. Alkasassbeh A., Al-Haj Baddar K. Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey // Arabian Journal for Science and Engineering. 2023.

3. Hosseini Shirvani M., Akbarifar S. A Survey Study on Intrusion Detection System in Wireless Sensor Network: Challenges and Considerations [Електронний ресурс] // Journal of Electrical, Computer and Electronic Engineering. 2024. Режим доступу: https://jecei.sru.ac.ir/article_2116.html.

4. Niculescu D. Ad hoc positioning system (APS) using AOA // Proceedings of the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. San Francisco, CA, USA. 2003. P. 1734–1743.

5. Youssef M. An asynchronous time-based location determination system // Proceedings of the 4th International Conference on Mobile Systems, Applications and Services, Uppsala, Sweden. 2006. P. 165–176.

6. Cong L. Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems // IEEE Trans. Wirel. Commun. 2002. P. 439–447.

7. Bargshady N. Precise Tracking of Things via Hybrid 3-D Fingerprint Database and Kernel Method Particle Filter // IEEE Sens. J. 2016. P. 8963–8971.

8. Atia M. Dynamic Propagation Modeling for Mobile sers' Position and Heading Estimation in Wireless Local Area Networks // IEEE Wireless Communication Letters. 2012. No. 99. P. 1–4.

9. Bahl P., Padmanabhan V. N. RADAR: An In-building RF-based User Location and Tracking System // IEEE INFOCOM 2000, Tel Aviv, Israel. 2000. P. 775–784.