МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

БАНАХ РОМАН ІГОРОВИЧ

УДК 004.056.53

ДИСЕРТАЦІЯ

УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВТОРГНЕНЬ І СИСТЕМ-ПРИМАНОК У МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

12 «Інформаційні технології»
(галузь знань)

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____/ Банах Роман Ігорович /

Науковий керівник (консультант) Піскозуб Андріян Збігнєвич, к.т.н, доцент

Львів – 2024

АНОТАЦІЯ

Банах Р.І. **Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації». – ІКТА Національний університет "Львівська політехніка" України, Львів, 2024.

Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання із вдосконалення технології виявлення вторгнень та покращення характеристик систем-приманок в мережах стандарту IEEE 802.11, а також покращенню методів деанонімізації зловмисників. Це дасть змогу підвищити ефективність захисту бездротових мереж загального призначення Wi-Fi шляхом застосування системами виявлення вторгнень, які працюють на фізичному та канальному рівнях моделі OSI, та систем-приманок із покращеними характеристиками взаємодії зі зловмисником, що в свою чергу дозволяє задіяти приманку як буфер і отримати більше часу для підготовки захисту виробничих середовищ.

В роботі розроблено концептуальну модель хмарної обчислювальної інфраструктури для взаємодії із системою виявлення вторгнень і системою-приманкою як незалежними зовнішніми елементами мереж стандарту IEEE 802.11 (Wi-Fi). Розроблено метод відслідковування зловмисника за метаданими зібраними з його пристроїв, що дозволяє дізнатись про місця його попереднього перебування та, імовірно, про місце перманентного перебування. Також запропоновано метод оцінки досвідченості зловмисника, на основі якого запропоновано діагностичну модель систем-приманок для мереж стандарту IEEE 802.11, що дає змогу налаштувати систему-приманку згідно з профілем зловмисника, на взаємодію з яким очікується. Окрім того розроблено метод виявлення вторгнень за допомогою збору даних про потужність сигналу і тренування моделі машинного навчання на попередньо зібраних даних, що дозволяє вирізняти атаки з підміни Wi-Fi обладнання на канальному рівні моделі Open Systems Interconnection (OSI).

Об’єктом дослідження є процес аналізу отримання та опрацювання інформації з частотного діапазону, в якому працюють пристрої стандарту IEEE 802.11, де може міститись інформація про атаки та про те хто її здійснював.

Предметом дослідження є технології виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11.

В процесі досліджень використано положення теорії множин, теорію графів, метод кластеризації даних, метод аналізу ієрархій, агрегації та оптимізації даних, методи математичної статистики, кластеризації даних та машинного навчання.

У першому розділі **«Стан та перспективи розвитку технології виявлення вторгнень та систем-приманок у бездротових мережах стандарту IEEE 802.11»** докладно досліджуються основні методи захисту мереж стандарту IEEE 802.11 та їхні недоліки. В цьому розділі надається детальний огляд технології Wi-Fi, її переваги, недоліки та особливості сучасних підходів до впровадження систем виявлення вторгнень та систем-приманок у комп’ютерних мережах даного типу. Також ретельно аналізуються дослідження та публікації, що стосуються актуальності застосування систем виявлення вторгнень та систем-приманок у бездротових мережах стандарту IEEE 802.11. У ході аналізу здійснюється порівняльна оцінка базових механізмів і продуктів, як комерційних, так і продуктів з відкритим вихідним кодом. В результаті дослідження виявлено, що проблеми безпеки мереж IEEE 802.11 мають циклічний характер, оскільки навіть при винайденні нових механізмів захисту і їх впровадженні на серверному обладнанні, вони повинні бути зворотно сумісними з застарілими, вразливими клієнтськими пристроями. Досліджено можливість застосування алгоритмів машинного навчання для покращення виявлення вторгнень у мережах Wi-Fi та розглянуто інтелектуальні підходи до конфігурації систем-приманок з метою уникнення їх виявлення зловмисниками.

У другому розділі **«Концепція побудови систем захисту інформації в бездротових мережах стандарту IEEE 802.11 із застосуванням систем виявлення вторгнень і систем-приманок»** досліджено розвиток систем захисту інформації у бездротових мережах стандарту IEEE 802.11, з фокусом на системи

виявлення вторгнень та системи-приманки. Проведений аналіз виявив, що одним з важливих критеріїв для таких систем є їх толерантність до атак. З цією метою, розроблено життєвий цикл систем захисту, що дозволяє гнучко переналаштовувати їх з урахуванням історичних даних, а також розроблено та проаналізовано моделі потенційних порушників для підприємств. Досліджено можливі демаскуючі ознаки систем захисту, які дозволяють уникнути виявлення їх зловмисниками та позитивно позначитися на безпеці бездротових мереж. На основі цього розроблено концептуальну модель системи захисту інформації з використанням систем виявлення вторгнень та систем-приманок, включно з правилами комунікації між її елементами та використанням обчислювальних платформ для зовнішніх сегментів. Для вирішення проблем масштабованості системи також розглянуто можливість використання хмарних обчислень.

У третьому розділі **«Розроблення та оптимізація моделі системи захисту інформації бездротових мереж стандарту IEEE 802.11 із застосуванням систем виявлення вторгнень і систем-приманок»** розроблено та вдосконалено моделі систем захисту інформації у бездротових мережах стандарту IEEE 802.11 з використанням систем виявлення вторгнень і систем-приманок. Розроблено методику з відслідковування зловмисників, щодо попередніх місць їх перебування, за допомогою аналізу пакетів Probe Request. Представлена діагностична модель системи-приманки для бездротових мереж стандарту IEEE 802.11, зокрема для протоколів бездротової безпеки WPA/WPA2. Вдосконалено методи виявлення вторгнень в мережах IEEE 802.11 за допомогою штучного інтелекту, а саме підміна MAC адреси та «злий двійник», використовуючи алгоритм машинного навчання KNN, в основі якого лежить компактний апаратно-програмний комплекс для моніторингу та аналізу мережевих пакетів у етері. Результати досліджень дозволили покращити виявлення вторгнень та оптимізувати системи захисту інформації у бездротових мережах.

У четвертому розділі **«Покращення механізмів ідентифікації виявлення вторгнень, особи зловмисника та ефективності систем-приманок у бездротових мережах стандарту IEEE 802.11»** досліджено покращення

попередньо розроблених механізмів ідентифікації, виявлення вторгнень та ефективності систем-приманок у бездротових мережах стандарту IEEE 802.11. Виявлено критичні недоліки публічних баз даних, як інструмента для відслідковування зловмисників, визначено підхід до покращення точності геолокації точок доступу за рахунок метрики потужності сигналу, в результаті чого точність виявлення точок доступу зросла з менше ніж 1% до 90% з можливістю подальшого покращення точності. Використовуючи діагностичну модель, надано коефіцієнти для різних механізмів захисту бездротових мереж, що дозволяє підібрати налаштування систем-приманок згідно з профілем зловмисника. Надано результати досліджень з виявлення атаки «злий двійник» де використовувався оригінальний метод агрегації даних і алгоритм машинного навчання KNN. Натренована модель машинного навчання дозволила виявити факти вторгнень у всіх 100% випадків.

У **висновках** дисертаційної роботи наведено основні відкриття та рекомендації, що випливають з результатів досліджень. Подано оцінку ефективності запропонованих рішень у числовому вираженні в умовах їх практичного застосування.

У **додатках** до дисертації долучено короткі програмні коди, в яких описується базовий функціонал програмних засобів, акти впровадження результатів дисертаційної роботи, а також список наукових праць і апробацій автора за темою дисертації.

Ключові слова: виявлення вторгнень, приманки, комп'ютерні мережі, Wi-Fi, IEEE 802.11, машинне навчання, штучний інтелект, аномалії, хмарні обчислення, метадані.

Список публікацій здобувача:

Наукові праці, в яких опубліковано наукові результати дисертації:

1. Дудикевич, В. Б. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв'язку. / Дудикевич, В. Б., Микитин, Г. В., Ребець, А. І., Банах, Р. І. // Сучасна спеціальна техніка, (2014/4), 75-82 сс.

2. Дудикевич В. Б. Інформаційна модель безпеки технологій зв’язку. / Дудикевич В. Б., Хорошко В. О., Микитин Г.В., Банах Р.І., Ребець А.І. // Інформатика та математичні методи в моделюванні 2014 Том 4. – №2. – 137–148 сс.

3. Банах Р. І. Створення концепції захищеної хмарної обчислювальної мережі з використанням систем приманок / Банах Р.І., Піскозуб А.З.,Стефінко Я.Я. // Вісник Національного університету “Львівська політехніка”: Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 74–78.

4. Стефінко Я.Я., Піскозуб А.З., Банах Р.І. Тестування на проникнення з Metasploit і shell скриптами. Вісник Національного університету “Львівська політехніка”: Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 90—93.

5. Банах Р.І. Автоматизація розгортання Wi-Fi точки доступу, як зовнішнього елементу системи приманки. / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Вісник Національного університету «Львівська політехніка». Серія «Автоматика, вимірювання та керування». – 2016. – №852. с. 130–136 сс.

6. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Р.І. Банах, А.З. Піскозуб // Щоквартальне наукове видання «Системи обробки інформації» Випуск 2 (148): Харківський національний університет Повітряних Сил імені Івана Кожедуба, 2017. С. 77-83.

7. Банах Р.І. Оцінка надійності елементів системи-приманки у мережі стандарту IEEE 802.11, як розгалуженої системи зі складним підпорядкуванням. / Банах Р.І., Піскозуб А.З. // Вісник Національного університету «Львівська політехніка». Серія «Автоматика, вимірювання та керування». – 2017. – №880. с. 94–98

8. Р. І. Банах. Визначення параметрів ключа методу автентифікації WPA/WPA2 для системи-приманки мережі стандарту IEEE 802.11 / Р. І. Банах // Радіоелектроніка, інформатика, управління (2018/1). Запорізький Національний технічний університет. с. 110–118.

9. Attackers’ Wi-Fi devices metadata interception for their location identification / Roman Banakh, Andrian Piskozub // Proceedings of the 2018 IEEE 4th

International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018, 2018, pp. 112–116

10. Банах Р.І. Застосування хмарних обчислень для визначення рівня захищеності бездротових мереж стандарту IEEE 802.11. / Банах Р.І., Піскозуб А.З. // Сучасна спеціальна техніка. Науково-практичний журнал №4(67), 2021. с. 5–15.

11. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices / Banakh, R., Piskozub, A., Opirskyy, I. // Advances in Intelligent Systems and Computing, 2019, 754, pp. 468–477

12. Banakh, R., Piskozub, A., Opirskyy, I. 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 (123)) (2023), pp 20–32.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Банах Р. І. Аналіз подій у безпровідних комп'ютерних мережах для автоматизації тестування на проникнення / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем" – Львів, 2015. – 73–74 сс.

2. Банах Р. І. Створення концепції захищеної хмарної обчислювальної мережі із застосуванням систем приманок / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем" – Львів, 2015 – 75–76 сс.

3. Банах Р. Одноплатна робоча станція як компонент системи приманки у безпровідних комп'ютерних мережах. / Банах Р., Стефінко Я. // Захист інформації в інформаційно-комунікаційних системах. Тези доповідей І Міжвузівської науково-практичної конф. студентів і курсантів – Львів, 2015 – С. 6–7.

4. Піскозуб А.З. Тестування на проникнення з допомогою open-source OS Linux і shell скриптів / Піскозуб А.З., Стефінко Я.Я., Банах Р.І. // Матеріали п'ятої науково-практичної конференції FOSS Lviv 2015 (23-26 квітня 2015р.), м Львів – 133–136 сс.

5. Банах Р.І., Тестування на проникнення як механізм аналізу ефективності системи приманки для мережі Wi-Fi. / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Тези доповіді ІІ-ої Міжнародної науково-технічної конференції 24-25 листопада 2016 р. «Інформаційна безпека в сучасному суспільстві» 119с., 79—80 сс.

6. Стефінко Я. "Тестування на проникнення у навчальних лабораторіях з застосуванням контейнеризації" / Стефінко Я., Піскозуб А., Банах Р. // Тези доповідей: Матеріали 8-ї науково-практичної конференції "Інноваційні комп'ютерні технології у вищій школі" . Львів – В-во наук.тов. ім.Т.Г.Шевченка - 2016.- С. 144-151.

7. Banakh R. External elements of honeypot for wireless network / Banakh R., Piskozub A., Stefinko Y. // "Modern Problems of Radio Engineering, Telecommunications, and Computer Science": Proceedings of the XIIIth International Conference TCSET'2016. Lviv-Slavsko, Ukraine February 23 – 26, 2016. Lviv Publishing House of Lviv Polytechnic 2016. 480-482p.

8. Stefinko Y. Manual and Automated Penetration Testing. Benefits and Drawbacks. Modern Tendency» / Yaroslav Stefinko, Andrian Piskozub, Roman Banakh // Modern Problems of Radio Engineering, Telecomunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET'2016 – Lviv-Slavsko, Ukraine, 2016. – 961p. 488-491p.

9. Банах Р. Перспективи розвитку систем приманок для безпровідних мереж / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Інформація, комунікація, суспільство 2016: матеріали 5-ої Міжнародної наукової конференції ІКС-2016, 19–21 травня 2016 року, Україна, Львів, Славське / Національний університет "Львівська політехніка", Кафедра соціальних комунікацій та інформаційної діяльності. – Львів: Видавництво Львівської політехніки, 2016. – С. 30–31.

10. Banakh R. Wi-Fi Honeypot as a service. Conception of business model / Banakh R. // "ENGINEER OF XXI CENTURY": VI INTER UNIVERSITY

CONFERENCE OF STUDENTS, PHD STUDENTS AND YOUNG SCIENTISTS. Bielsko-Biała, Poland December 02, 2016. – 928p. – 59–64 pp.

11. Банах Р.І. Збір та обробка метаданих зловмисника для виявлення імовірних місць його перебування з пристроїв стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // 4-th International Conference on Computational Intelligence (ComInt 2017), Taras Shevchenko National University of Kyiv, May 16-18, 2017. – 197–198 cc.

12. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // Матеріали Міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”: тези доповідей, 20 – 21 квітня 2017 р. – Х.: ХНЕУ імені Семена Кузнеця, 2017. – 92 с. – 27–28 сс.

13. Банах Р.І. Вимірювання потужності сигналу від клієнтських пристроїв в мережах IEEE 802.11 для тренування моделей машинного навчання задля виявлення атак / Банах Р.І., Піскозуб А.З. // Матеріали IX Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем» – Львів : Видавництво Львівської політехніки, 2023. – 185 с. – 53–54 сс.

14. Банах Р.І. Проблематика використання відкритих джерел даних у розслідувані кіберзлочинів у мережах стандарту IEEE 802.11 / Банах Р.І. // Матеріали II Міжнародної наукової конференції «Теорія модернізації в контексті сучасної світової науки», м.Ужгород, 1 березня, 2024р. / Міжнародний центр наукових досліджень. —Вінниця: ТОВ «УКРЛОГОС Груп, 2024.—244с. – 145–147 сс.

SUMMARY

Banakh R. **Improvement of intrusion detection and honeypot technology in IEEE 802.11 networks** – Qualifying scientific work on manuscript rights.

The dissertation for obtaining the scientific degree of Doctor of Philosophy in specialty 125 "Cyber Security". – Lviv Polytechnic National University, Lviv, 2024.

The dissertation is dedicated to addressing the current scientific and practical task of enhancing intrusion detection technology and improving the characteristics of honeypot systems in IEEE 802.11 (Wi-Fi) networks, as well as enhancing de-anonymization methods for intruders. This will increase the effectiveness of protection for general-purpose Wi-Fi networks by applying intrusion detection systems operating at the physical and data link layers of the OSI model, and honeypot systems with enhanced interaction capabilities with intruders, allowing the honeypot to act as a buffer and provide more time for preparing defense mechanisms in production environments.

The study developed a conceptual model of cloud computing infrastructure for interaction with intrusion detection and honeypot systems as independent external elements of IEEE 802.11 (Wi-Fi) networks. A method for tracking intruders based on metadata collected from their devices was developed, enabling identification of their previous locations and, potentially, their permanent location. Additionally, a method for assessing intruder expertise was proposed, based on which a diagnostic model for honeypot systems in IEEE 802.11 networks was developed, allowing customization of the honeypot system according to the profile of the expected intruder interaction. Furthermore, a method for intrusion detection using signal strength data collection and machine learning model training on previously collected data was developed, enabling detection of Wi-Fi equipment substitution attacks at the data link layer of the Open Systems Interconnection (OSI) model.

The research focuses on the analysis of data acquisition and processing in the frequency range where IEEE 802.11 devices operate, which may contain information about attacks and their perpetrators. The research subject is intrusion detection technologies and honeypot systems for IEEE 802.11 networks. The study employs set

theory, graph theory, data clustering, hierarchical analysis, data aggregation and optimization, mathematical statistics, data clustering, and machine learning methods.

In the first chapter, **"State and Perspectives of Intrusion Detection Technology and Honeypot Systems in IEEE 802.11 Wireless Networks"** the primary methods of protecting IEEE 802.11 networks and their drawbacks are thoroughly investigated. This chapter provides a detailed overview of Wi-Fi technology, its advantages, disadvantages, and the peculiarities of modern approaches to implementing intrusion detection systems and honeypot systems in computer networks of this type. Additionally, research and publications relevant to the applicability of intrusion detection systems and honeypot systems in IEEE 802.11 wireless networks are carefully analyzed. The comparative assessment of basic mechanisms and products, both commercial and open-source, is conducted during the analysis. The research reveals that security issues in IEEE 802.11 networks exhibit a cyclical nature, as even with the invention of new protection mechanisms and their deployment on server hardware, they must remain backward compatible with outdated, vulnerable client devices. The possibility of applying machine learning algorithms to enhance intrusion detection in Wi-Fi networks is explored, and intelligent approaches to configuring honeypot systems to evade detection by intruders are considered.

In the second chapter, titled **"Concept of Building Information Security Systems in IEEE 802.11 Wireless Networks Using Intrusion Detection and Honeypot Systems"** the development of information security systems in IEEE 802.11 wireless networks is investigated, with a focus on intrusion detection and honeypot systems. The analysis revealed that one of the essential criteria for such systems is their resilience to attacks. To achieve this, a lifecycle of security systems has been developed, allowing for flexible reconfiguration based on historical data. Additionally, models of potential intruders for enterprises have been developed and analyzed. Investigating potential telltale signs of security systems that enable them to evade detection by malicious actors and positively impact the security of wireless networks. Based on this, a conceptual model of an information security system using intrusion detection and honeypot systems has been developed, including communication rules between its elements and the use of

computational platforms for external segments. The possibility of utilizing cloud computing is also considered to address scalability issues.

In the third chapter, titled **"Development and Optimization of an Information Security System Model for IEEE 802.11 Wireless Networks Using Intrusion Detection and Honeypot Systems"** models of information security systems in IEEE 802.11 wireless networks are developed and optimized using intrusion detection and honeypot systems. The methodology for collecting information about the previous whereabouts of perpetrators through analysis of Dot11ProbeReq packets is extensively examined. A diagnostic model is presented for information security systems in IEEE 802.11 networks, particularly for WPA/WPA2 wireless security protocols. Methods for identifying attacks, such as MAC Spoofing and Evil Twin, are developed and analyzed using the KNN machine learning algorithm. A concept of a compact hardware-software complex for monitoring and analyzing network packets in the ether is presented. A data aggregation method is proposed to reduce the load on the computer network. The research results have improved intrusion detection and optimization of information security systems in wireless networks.

In the fourth chapter, titled **"Enhancement of Intrusion Detection, Attacker Identification, and Honeypot System Efficiency in IEEE 802.11 Wireless Networks"** improvements to previously developed mechanisms for identification, intrusion detection, and the effectiveness of honeypot systems in IEEE 802.11 wireless networks are investigated. Critical shortcomings of public databases are identified, and an approach to improving the accuracy of access point geolocation through signal strength metrics is determined. Using a diagnostic model, coefficients are provided for various wireless network protection mechanisms, enabling the customization of honeypot system settings according to the attacker's profile. A method for detecting Evil Twin attacks with high efficiency and low energy consumption using the KNN machine learning algorithm is developed. It is found that these methods significantly enhance the determination mechanisms for a wide range of attacks in IEEE 802.11 networks (Wi-Fi) and improve their security.

The dissertation **conclusions** present the main discoveries and recommendations arising from the research results. They also provide a numerical assessment of the effectiveness of the proposed solutions in terms of their practical application.

The dissertation **appendices** include brief software codes describing the basic functionality of the software tools, implementation acts of the dissertation results, and a list of the author's scientific works and presentations on the dissertation topic.

Keywords: Intrusion Detection, Honeypots, Computer Networks, Wi-Fi, IEEE 802.11, Machine Learning, Cloud Computing.

The list of author’s publications:

Proceedings where basic scientific results of thesis were published:

1. Dudykevych, V. B., Mykytyn, H. V., Rebets, A. I., Banakh, R. I. (2014). Comprehensive Approach to Language Information Protection in Wireless Communication Technologies. Modern Specialized Equipment, (2014/4), 75-82.

2. Dudykevych, V. B., Khoroshko, V. O., Mykytyn, H. V., Banakh, R. I., Rebets, A. I. (2014). Information Security Model for Communication Technologies. Informatics and Mathematical Methods in Modeling, 4(2), 137–148.

3. Banakh, R. I., Piskozub, A. Z., Stefinko, Y. Y. (2015). Development of a Concept for a Secure Cloud Computing Network Using Honeypot Systems. Bulletin of Lviv Polytechnic National University: Series: Automation, Measurement and Control, 821, 74–78.

4. Stefinko, Y. Y., Piskozub, A. Z., Banakh, R. I. (2015). Penetration Testing with Metasploit and Shell Scripts. Bulletin of Lviv Polytechnic National University: Series: Automation, Measurement and Control, 821, 90–93.

5. Banakh, R. I., Piskozub, A. Z., Stefinko, Y. Y. (2016). Automation of Wi-Fi Access Point Deployment as an External Element of the Honeypot System. Bulletin of Lviv Polytechnic National University: Series: Automation, Measurement and Control, 852, 130–136.

6. Banakh, R. I., Piskozub, A. Z. (2017). Diagnostic Model of a Honeypot System in IEEE 802.11 Wireless Networks. Quarterly Scientific Journal "Information

Processing Systems", Issue 2 (148), Ivan Kozhedub Kharkiv National Air Force University, 77-83.

7. Banakh, R. I., Piskozub, A. Z. (2017). Reliability Assessment of Honeypot System Elements in IEEE 802.11 Networks as a Complex Hierarchical System. Bulletin of Lviv Polytechnic National University: Series: Automation, Measurement and Control, 880, 94–98.

8. R. I. Banakh. Determination of WPA/WPA2 Authentication Method Key Parameters for IEEE 802.11 Network Honeypot System. Radio Electronics, Informatics, Control (2018/1). Zaporizhzhia National Technical University. pp. 110–118.

9. Banakh, R., Piskozub, A. (2018). Attackers' Wi-Fi Devices Metadata Interception for Their Location Identification. In Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018 (pp. 112–116). IEEE.

10. Banakh, R. I., Piskozub, A. Z. (2021). Application of Cloud Computing for Assessing the Security Level of IEEE 802.11 Wireless Networks. Modern Specialized Equipment. Scientific and Practical Journal, Issue 4(67), 5–15.

11. Banakh, R., Piskozub, A., Opirskyy, I. (2019). Detection of MAC Spoofing Attacks in IEEE 802.11 Networks Using Signal Strength from Attackers' Devices. In Advances in Intelligent Systems and Computing (Vol. 754, pp. 468–477).

12. 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 (123)), 20–32.

Proceedings that certify an approvement of thesis materials:

1. Banakh, R. I., Piskozub, A. Z., Stefinko, Y. Y. (2015). Analysis of Events in Wireless Computer Networks for Penetration Testing Automation. In Proceedings of the IV International Scientific and Technical Conference "Information Security and Information Systems Security" – Lviv, 73–74.

2. Banakh, R. I., Piskozub, A. Z., Stefinko, Y. Y. (2015). Development of a Concept for a Secure Cloud Computing Network Using Honeypot Systems. In Proceedings of the IV International Scientific and Technical Conference "Information Security and Information Systems Security" – Lviv, 75–76.

3. Banakh, R., Stefinko, Y. (2015). Single-Board Workstation as a Component of Honeypot System in Wireless Computer Networks. In Information Security in Information and Communication Systems. Abstracts of the 1st Interuniversity Scientific and Practical Conference of Students and Cadets – Lviv, 6–7.

4. Piskozub, A. Z., Stefinko, Y. Y., Banakh, R. I. (2015). Penetration Testing Using Open-Source Linux OS and Shell Scripts. In Proceedings of the Fifth Scientific and Practical Conference FOSS Lviv 2015 (April 23-26, 2015), Lviv, 133–136.

5. Banakh, R. I., Piskozub, A., Stefinko, Y. (2016). Penetration Testing as a Mechanism for Analyzing the Effectiveness of Honeypot Systems for Wi-Fi Networks. In Proceedings of the II International Scientific and Technical Conference on November 24-25, 2016 "Information Security in Modern Society", 119 pp., 79–80.

6. Stefinko, Y. (2016). "Penetration Testing in Educational Laboratories Using Containerization." In Proceedings: Materials of the 8th Scientific and Practical Conference "Innovative Computer Technologies in Higher Education". Lviv: Publishing House of the Taras Shevchenko Scientific Society, pp. 144-151.

7. Banakh, R. (2016). External Elements of Honeypot for Wireless Network. In "Modern Problems of Radio Engineering, Telecommunications, and Computer Science": Proceedings of the XIIIth International Conference TCSET'2016. Lviv-Slavsko, Ukraine, February 23 – 26, 2016 (pp. 480-482). Lviv: Publishing House of Lviv Polytechnic.

8. Stefinko, Y., Piskozub, A., & Banakh, R. (2016). Manual and Automated Penetration Testing: Benefits and Drawbacks. Modern Tendency. In Modern Problems of Radio Engineering, Telecommunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET'2016 – Lviv-Slavsko, Ukraine, 2016 (pp. 488-491). Lviv: Publishing House of Lviv Polytechnic.

9. Banakh, R. Perspectives of Honeypot Systems Development for Wireless Networks. In Proceedings of the Information, Communication, Society 2016: Materials of the 5th International Scientific Conference ICS-2016, May 19–21, 2016, Ukraine, Lviv, Slavske. Lviv: Lviv Polytechnic National University, Department of Social Communications and Information Activities. (pp. 30–31). Lviv: Lviv Polytechnic Publishing House.

10. Banakh, R. Wi-Fi Honeypot as a Service: Conception of Business Model. In "Engineer of XXI Century": VI Interuniversity Conference of Students, PhD Students, and Young Scientists. Bielsko-Biała, Poland, December 02, 2016. (pp. 59–64).

11. Banakh, R. Collection and Processing of Attacker's Metadata for Detecting Probable Locations Using IEEE 802.11 Devices. In Proceedings of the 4th International Conference on Computational Intelligence (ComInt 2017), Taras Shevchenko National University of Kyiv, May 16-18, 2017. (pp. 197–198).

12. Banakh, R. Diagnostics Model of Honeypot System for IEEE 802.11 Wireless Networks. In Proceedings of the International Scientific and Practical Conference "Problems and Prospects of IT Industry Development": Abstracts of Reports, April 20-21, 2017. Kharkiv: Kharkiv National Economic University named after Semen Kuznets, 2017. (pp. 27–28).

13. Banakh, R. Measurement of Signal Strength from Client Devices in IEEE 802.11 Networks for Machine Learning Model Training for Attack Detection / Banakh R., Piskozub A. // Proceedings of the IX International Scientific and Technical Conference "Information Security and Information Systems Security" – Lviv: Lviv Polytechnic Publishing House, 2023. – 185 p. – pp. 53–54.

14. Banakh, R. Issues of Using Open Data Sources in Investigating Cybercrimes in IEEE 802.11 Networks / Banakh R. // Proceedings of the II International Scientific Conference "Theory of Modernization in the Context of Contemporary World Science", Uzhgorod, March 1, 2024 / International Center for Scientific Research. — Vinnytsia: LLC "UKRLOGOS Group, 2024. — 244 p. – pp. 145–147.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Wi-Fi – загальновживана назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалу;

WPA – (англ. Wi-Fi Protected Access) – протокол безпеки для захисту бездротових мереж;

АС – автоматизована система

МАІ – метод аналізу ієрархій (англ. Analytic Hierarchy Process, AHP)

СП – система-приманка

СВВ – система виявлення вторгнень

ШПЗ – шкідливе програмне забезпечення

ТД – точка доступу

PSK – (англ. Pre-Shared key) – ключ, який є попередньо розділений між двома вузлами за допомогою певного безпечного каналу;

AES – (англ. Advanced Encryption Standard) – також відомий під назвою Rijndael – симетричний алгоритм блочного шифрування;

SOHO – (англ. Small office / home office) – назва сегменту ринку, який відноситься до категорії (1 – 10 працюючих);

SSID – (англ. Service Set Identifier) – унікальне найменування бездротової мережі, що відрізняє одну мережу стандарту IEEE 802.11 від іншої.

PKCS – стандарт криптографії з відкритим ключем;

PBKDF2 – (англ. Password-Based Key Derivation Function) – стандарт форматування ключа на основі паролю;

HMAC – (скорочення від англ. hash-based message authentication code) – код перевірки автентичності повідомлень, який використовує хеш функцію.

SHA1 – (англ. Secure Hash Algorithm 1) – алгоритм криптографічного хешування, описаний в RFC 3174.

ВСТУП

Актуальність. Бездротові мережі стали невід'ємною частиною повсякдення як домашніх так корпоративних користувачів надавши свободу пересування під час роботи чи дозвілля. Одними з них є мережі стандарту IEEE 802.11 (Wi-Fi) мережі, які з'явились на ринку відносно нещодавно, та зараз, мабуть, не знайдеться жодного мобільного пристрою, який би не був оснащений модулем Wi-Fi. У випадку передавання даних по радіоканалу, ще не винайдено нічого кращого за радіусом дії і швидкості передачі ніж Wi-Fi та у випадку даної технології платити доводиться безпекою.

Безпека є надважливим аспектом організації обміну інформації будь-якого підприємства. Якщо доступ до дротових мереж можна отримати лише фізично підключившись до порта комутатора чи до мережевої розетки, то підключення до бездротової мережі є набагато простішим, необхідно бути лише у зоні її покриття. Бездротові мережі використовують радіохвилі, які розповсюджуються за законами фізики, і контролювати їх поведінку є не тривіальною задачею.

Поряд із перевагами, які надають мережі Wi-Fi стоять і виклики пов'язані із інформаційною безпекою. За наявності вузько-направленої антени високої потужності, зловмисник може вторгнутись у бездротову мережу на відстанях 2 км і більше, таким чином ускладнюється задача визначення його місцезнаходження.

Завдяки зусиллям постачальників споживчого Wi-Fi обладнання, більшість пристроїв поставляються вже налаштованими за замовчуванням, що дозволяє відразу починати роботу. Та навіть, якщо користувач налаштує маршрутизатор застосовуючи найстійкіші протоколи захисту, така мережа не може вважатись безпечною через велику кількість відомих вразливостей в сучасних протоколах безпеки мереж стандарту IEEE 802.11.

Одним із методів уникнення атак на виробничі середовища є системи-приманки, застосування яких для захисту мереж стандарту IEEE 802.11 є дуже недооціненим.

Є кілька типових робіт про технології виявлння вторгнень і системи-приманки. Проблема покращення системи виявлення вторгнень у бездротові

мережі, а також системи-приманки досліджувалась вітчизняними та зарубіжними вченими, такими як: Тимошик, Дудикевич, Піскозуб, Лі, Жанґ, Форбс, Донґ, Холз, Провос, Рунфу, Ґоел, Аджах. Не зважаючи на велику кількість досліджень у цій сфері досі залишаються невирішені проблеми, такі як: цетралізове управління системами-приманками та системами виявлення вторгнень у бездротових мережах, оцінка рівня захищеності системи-приманки, відслідковування та деанонімізація зловмисників, швидка ідентифікація атак пов’язаних із підміною MAC адрес і клонування ідентифікаторів легітимних пристроїв. Хоч технологія постійно розвивається, і якщо на початковому етапі Wi-Fi мережі були практично беззахисними від атак, то зараз ситуація помітно покращилась. На сучасному етапі розвитку технологій існує маса рішень, які дозволяють зробити бездротову мережу відносно захищеною. Це можуть бути апаратні і/або програмні засоби, платні або безкоштовні рішення, та якщо взяти до уваги розповсюдженість технології Wi-Fi, то для створення безпечного середовища кожен користувач повинен володіти базовими знаннями з адміністрування комп’ютерних мереж та кібербезпеки. Окрім того, в арсеналі рядових користувачів немає інструментів за допомогою яких би вони могли ідентифікувати вторгнення, відводити атаки від власних мереж, а також виявляти особу зловмисника задля заяви про неправомірні дії у відповідні державні органи.

Отже, у зв'язку з необхідністю забезпечення безпеки як корпоративних, так і персональних мереж Wi-Fi, а також відсутністю простих механізмів для вирішення цієї проблеми, виникає науково-практична задача щодо вдосконалення систем виявлення вторгнень та систем-приманок у мережах стандарту IEEE 802.11.

Зв’язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи відповідає науковому напрямку кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка» «Розробка та дослідження методів та створення сучасних засобів захисту інформації в безпровідних мережах». Окремі частини роботи виконано в межах держбюджетної науково-дослідної роботи: «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на

основі глибинних нейронних мереж» (№ держреєстрації 0124U000407), а також межах міжнародного ґранту наданого CRDF Global «Вдосконалення комплексу динамічної автентифікації кінцевих точок засобами машинного навчання та захисту корпоративних мереж від кібератак» (номер ґрантової угоди G-202401-71626).

Мета роботи. Метою дисертаційної роботи є розв’язання науково-практичної задачі із вдосконалення методів виявлення вторгнень в мережах стандарту IEEE 802.11 за допомогою штучного інтелекту, вдосконалення систем-приманок для мереж стандарту IEEE 802.11 шляхом впровадження діагностичної моделі та застосування хмарних обчислень для економії ресурсів, а також розроблення методики відслідковування зловмисників.

Завдання. Дисертаційна робота присвячена вирішенню актуального науково-практичного завдання удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11

Для успішного досягнення мети даної роботи необхідно виконати наступні завдання:

1. Дослідити існуючі механізми захисту технології бездротового зв’язку Wi-Fi та їх вразливості.
2. Дослідити стан та тенденції розвитку існуючих методів виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11.
3. Проаналізувати сучасні дослідження та публікації, що стосуються виявлення вторгнень та систем-приманок у мережах IEEE 802.11.
4. Дослідити життєвий цикл систем-приманок для мере; IEEE 802.11
5. Розробити та проаналізувати модель порушника для мереж стандарту IEEE 802.11.
6. Дослідити можливі демаскуючі ознаки систем-приманок для мереж стандарту IEEE 802.11 на різних рівнях взаємодії з ними.
7. Розробити концептуальну модель системи-приманки та виявлення вторгнень для мережі стандарту IEEE 802.11.
8. Розробити методику відслідковування порушника в мережах IEEE 802.11

9. Розробити діагностичну модель системи-приманки бездротової мережі стандарту IEEE 802.11.

10. Вдосконалити методи виявлення вторгнень в мережах IEEE 802.11 шляхом застосування машинного навчання.

11. Дослідити ефективність розробленої методики з відслідковування зловмисників.

12. Застосувати діагностичну модель системи-приманки для мереж стандарту IEEE 802.11.

13. Проаналізувати результати з удосконалення методу розподіленого підбору ключа доступу до механізму захисту WPA2 у мережах IEEE 802.11.

14. Дослідити ефективність розробленої системи виявлення вторгнень із застосуванням машинного навчання в мережі стандарту IEEE 802.11 шляхом виявлення атаки «злий двійник».

Об'єкт дослідження. Об'єктом дослідження є процеси обробки даних з частотного діапазону, в якому працюють пристрої стандарту IEEE 802.11, де може міститись інформація про атаки та про те хто її здійснював.

Предметом дослідження є технології виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11.

Методи дослідження. Підчас розв'язання поставлених задач, зокрема, при розробленні методу відслідковування зловмисників було застосовано положення теорії множин, теорію графів, метод кластеризації даних. Для розроблення діагностичної моделі системи-приманки та визначення складності її конфігурації застосовано метод аналізу ієрархій. Для визначення атак "злий двійник" та "підміна MAC адреси" було застосовано математичну статистику та машинне навчання і метод кластеризації даних.

Наукова новизна роботи полягає в тому, що:

1. Вперше розроблено концептуальну модель системи захисту інформації із застосуванням систем виявлення вторгнень і систем-приманок для мереж IEEE 802.11 Wireless Honeypot as a Service використовуючи хмарні обчислення, яка на відміну від існуючих підходів до розгортання інфраструктури із системами-

приманками дає можливість покращити характеристики швидкості та гнучкості розгортання цілісної системи захисту інформації для бездротових мереж.

2. Вперше розроблено методику відслідковування зловмисників за метаданими, зібраними з їх пристроїв, застосовуючи публічні бази даних геолокації Wi-Fi пристроїв. Розроблено алгоритм з покращеними характеристиками визначення геолокації конкретної точки доступу, який на відміну алгоритму запису інформації за допомогою часових рядів, дозволяє точніше визначити геолокацію Wi-Fi точок доступу, що дає можливість уникнути хибних відображень на карті, а відповідно ідентифікувати попередні місця перебування зловмисників із вищою точністю.

3. Вперше розроблено діагностичну модель системи-приманки для бездротових мереж стандарту IEEE 802.11, яка на відміну від підходів зі "сліпої конфігурації" чи клонування існуючої бездротової інфраструктури дозволяє оцінити рівень захищеності системи-приманки на відповідність до профілю зловмисника, що дає змогу згенерувати конфігурацію системи-приманки для зловмисника з потрібним рівнем підготовки у автоматичному режимі, і відповідно покращити пристосовуваність систем-приманок у бездротових мережах стандарту IEEE 802.11.

4. Вперше розроблено метод виявлення вторгнень із застосуванням машинного навчання, а саме алгоритму K-найближчих сусідів, в якому на відміну від існуючих застосовано оригінальний метод агрегації даних про потужність сигналу, що дає можливість уникнути надлишкового навантаження на комп’ютерні мережі. Розроблений метод дає змогу ідентифікувати атаку «злий двійник» на ранніх стадіях атаки на точки доступу, як елемента мережевої інфраструктури Wi-Fi.

Практичне значення одержаних результатів полягає у можливості їх безпосереднього застосування для підсилення наявних систем виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11 як у корпоративному так і приватному середовищах.

1. Проведено огляд існуючих рішень та реалізацій систем виявлення вторгнень і систем-приманок для комп'ютерних мереж стандарту IEEE 802.11, а також проаналізовано стан сучасних досліджень у цій галузі. За результатами аналізу встановлено, що сучасні системи виявлення вторгнень переважно базуються на сигнатурних методах, а системи-приманки частіше використовуються як інструменти зловмисників. Також визначено, що виявлення зловмисника, який здійснює атаку на бездротову мережу, може становити проблему через його можливе операційне виходження за межі контрольованої зони. Обґрунтовано актуальність науково-практичного завдання дослідження, включаючи розробку методології оцінки захисту систем-приманок та використання штучного інтелекту для поліпшення ефективності систем виявлення вторгнень.

2. Розроблено та проаналізовано моделі порушника у бездротових мережах стандарту IEEE 802.11 для підприємства. Даний аналіз дозволяє краще зрозуміти можливі ризики і розробляти ефективні методи їх протидії. Досліджено можливі демаскуючі ознаки систем-приманок, зокрема їх можливість виявлення на різних рівнях моделі OSI: канальному, мережевому та прикладному, що дозволяє уникнути виявлення систем-приманок зловмисниками і позитивно впливає як на функціонування як систем-приманок, так і на безпеку бездротової мережі Wi-Fi та інших пов'язаних мережевих ресурсів.

3. Розроблено концептуально нову модель системи захисту інформації з використанням систем-приманок, що відповідає сучасним викликам і вимогам безпеки. У цьому контексті описано мінімальний набір елементів, за допомогою яких можна реалізувати таку систему. Регламентовано правила комунікації між їх елементами. Для елементів зовнішнього сегменту системи захисту інформації та системи бездротової мережі запропоновано обчислювальні платформи. Для розв'язання проблем масштабованості розробленої системи також запропоновано використання хмарних обчислень.

4. Досліджено критичні недоліки публічних баз даних з геолокації точок доступу Wi-Fi як інструменту пошуку зловмисника за слідами, залишеними до, під час та після проведення атаки на Wi-Fi інфраструктуру. Такими недоліками

визначено відсутність стандартизації обладнання, яке проводить збір та обробку даних; відсутність валідації даних, які приходять від контриб'юторів; відсутність агрегації даних на основі унікальних екземплярів. Натомість запропоновано методику, яка дозволяє безперервно покращувати точність геолокації знайдених точок доступу за рахунок метрики потужність сигналу, введення поняття унікальності знайдених екземплярів та стандартизації обладнання контрибюторів. Врезультаті вдалось досягти точності у віднайдені унікальних екземплярів з точністю 90—100% на противагу 0.5—1% у публічних базах даних.

5. Розроблено та застосовано діагностичну модель визначено коефіцієнти для усіх наявних механізмів захисту бездротових мереж стандарту IEEE 802.11 (Wi-Fi). Даний підхід дозволяє підібрати налаштування системи-приманки згідно із визначеним профілем зловмисника, що може значно покращити продуктивність у їх застосуванні. Зважаючи на актуальність протоколу захисту WPA2 було розроблено деталізовану діагностичну модель відносно складності подолання його ключа. Для обчислення складності перебору було використано дві різні технології віртуалізації – повна і контейнеризація. Визначено, що контейнеризація є продуктивнішою на 11% за повну віртуалізацію і дозволяє швидко масштабувати ресурси.

6. Розроблено та застосовано модель машинного навчання на основі алгоритму KNN для виявлення атаки "злий двійник" в мережі стандарту IEEE 802.11 (Wi-Fi). Розроблено програмно-апаратний комплекс, що забезпечує моніторинг службових пакетів в етері мережі стандарту IEEE 802.11 з високою ефективністю та мінімальним енергоспоживанням. Завдяки безперервному моніторингу етеру та використанню алгоритмів машинного навчання на зібраних даних моделі вдалося відрізнити легітимні точки доступу від імітованих нелегітимних у 100% випадків. Це свідчить про високу ефективність даного підходу у виявленні атаки "злий двійник". Виявлення цього типу атак є надзвичайно важливим для захисту мереж стандарту IEEE 802.11 (Wi-Fi), оскільки атака "злий двійник" є одним із інструментів у широкому спектрі векторів атак, включаючи атаки на WPA3.

Наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка», зокрема для студентів спеціальності 125 «Кібербезпека» в курсі лекцій з дисципліни «Інформаційно-комунікаційні системи».

Основні результати дисертаційної роботи використано і впроваджено з метою покращення захищеності комп'ютерної мережі та систем в компанії ТзОВ «Інститут інформаційних технологій «Інтелліас», що підтверджено актами впровадження.

Особистий внесок. Усі основні наукові результати, що висвітлено в дисертаційній роботі, аспірант отримав самостійно. Зокрема, в роботі [2] автором проведено аналіз алгоритмів шифрування для технології зв'язку WiMAX, як технології, яка може забезпечити зв'язок між мережами Wi-Fi на великій відстані, на основі чого було розроблено комплексний підхід до захисту мовної інформації в описаних технологіях безпровідного зв'язку. В роботах [9—10] автором було проаналізовано сучасний стан захищеності комп'ютерних мереж Wi-Fi, на основі чого було розроблено діагностичну модель для систем-приманок в мережах стандарту IEEE 802.11. В роботі [13] автором було описано основні характеристики технології Wi-Fi, методи її захисту та нормативно-правове забезпечення, яке стосується даної технології. В роботі [14] здійснено огляд та перспективи розвитку систем-приманок для їх застосування у бездротових мережах. В роботах [43, 50, 79, 81, 89] автором було застосовано практики тестування на проникнення для аналізу ефективності систем виявлення вторгнень та систем-приманок у бездротових мережах. У роботах [44, 69, 74] автором запропоновано методологію для збору інформації про зловмисників, які скоїли атаки на бездротові мережі стандарту IEEE 802.11. В роботах [45, 62—64, 70—71] детально описано концепцію побудови апаратно-програмного комплексу із застосуванням систем виявлення вторгнень, систем-приманок застосовуючи хмарні обчислення та одноплатні комп'ютери. В роботі [59] автором застосовується метод оцінки надійності елементів апаратно-програмного комплексу, як розгалуженої системи зі складним підпорядкуванням. У

роботі [75] автор пропонує застосування хмарних обчислень, як платформи до розв'язання проблеми з визначення рівня захищеності бездротових мереж стандарту IEEE 802.11. В роботі [78] запропоновано принципово новий підхід до вибору ключів WPA/WPA2 для подальшого їх застосування на системах-приманках. В роботах [85, 94] було розроблено метод виявлення атак з підміни MAC адрес та «злий двійник» на основі аналізу потужності сигналу від точок доступу Wi-Fi та від клієнських пристроїв. У роботі [88] автором здійснено аналіз відкритих баз даних, які надають інформацію про точки доступу Wi-Fi, як інструменту для виявлення потенційних місць перебування зловмисника та описано їх недоліки.

Апробація результатів. Основні наукові результати і положення дисертації представлені, доповідались та обговорені на 16-и міжнародних і державних науково-технічних конференціях: I Міжвузівська науково-практична конференція студентів і курсантів «Захист інформації в інформаційно-комунікаційних системах» (м. Львів, 2015 р.), IV Міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем" (м. Львів, 2015 р.), V науково-практична конференція FOSS Lviv 2015 (м. Львів, 23-26 квітня 2015 р.), XIII Міжнародна конференція TCSET'2016 «Modern Problems of Radio Engineering, Telecommunications, and Computer Science» (м. Львів, м. Славсько, 23 – 26 лютого, 2016 р.), XIII науково-практична конференція «Інноваційні комп'ютерні технології у вищій школі» (Львів, 2016 р.), V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2016 р), V Міжнародна наукова конференція «ICS-2016» (Львів, 2016 р.), II Міжнародна науково-технічна конференція «Інформаційна безпека в сучасному суспільстві» (Львів, 2016 р.), VI міжуніверситетська конференція студентів, аспірантів та молодих вчених «ENGINEER OF XXI CENTURY» (Польща, Б'єльсько-б'яла 2016), VIII Міжнародна конференція молодих вчених «Комп'ютерні науки та інженерія» (CSE 2016) (Львів, 2016 р.), 4-а Міжнародна конференція з обчислювального інтелекту «ComInt 2017» (Київ, 2017 р.), Міжнародна науково-практична конференція "Проблеми і перспективи розвитку IT-індустрії" (Харків, 20–21 квітня 2017 р), Міжнародна науково-практична конференція «обчислювальний інтелект (результати, проблеми,

перспективи)» (Київ-Черкаси, 16-18 травня 2017р.), V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем 2017» (Львів, 01–02 червня 2017 р.), IX Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2023 р.).

Публікації. Загальна кількість публікацій за темою дисертації становить 27, з них 11 статей, 9 з яких входять до переліку видань ВАК, 2 проіндексовано міжнародною наукометричною базою даних SCOPUS, 1 проіндексована міжнародними наукометричними базами даних Copernicus та Google Scholar, 1 розділ монографії. 14 тез доповіді, 3 з яких проіндексовано міжнародною наукометричною базою даних SCOPUS.

Структура та обсяг дисертації. Дисертація складається зі вступу та чотирьох розділів що охоплюють 19 підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 190 сторінок, з яких 146 – основний текст, 11 – список використаних джерел (104 найменування), 10 – додатки

РОЗДІЛ 1. СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА СИСТЕМ-ПРИМАНОК У БЕЗДРОТОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

1.1. Огляд існуючих механізмів захисту технології бездротового зв'язку IEEE 802.11 та їх вразливості

У першій версії стандарту IEEE 802.11 не було визначено жодного протоколу для забезпечення безпеки цього типу бездротових мереж. У випадку мереж, де відсутні протоколи безпеки, з'єднання між пристроями встановлюється через передачу двох повідомлень. Цей процес можна розглянути на прикладі двох пристроїв, наприклад, A та B. Пристрій A підтверджує свою ідентичність перед пристроєм B, надсилаючи запит на автентифікацію. Пристрій B, у свою чергу, відповідає на цей запит результатом, який може бути позитивним або негативним. Оскільки не існує жодних критеріїв для перевірки достовірності, автентифікація завершується успішно незалежно від результату. Проте з поширенням мереж IEEE 802.11 (Wi-Fi) виникла гостра необхідність у захисті від несанкціонованого доступу.

За відсутності протоколів бездротової безпеки деякі виробники вирішували проблему захисту, обмежуючи доступ лише за допомогою фільтрації MAC-адрес клієнтських пристроїв. Проте такий підхід не гарантує повного захисту мережі, оскільки зловмисник може змінити MAC-адресу свого пристрою на ту, яка є у списку "білих" адрес на точці доступу, невеликими зусиллями. Загальна кількість можливих MAC-адрес дорівнює 2^{48}, і деякі з них можуть бути відкинуті зловмисником, оскільки ще не всі MAC-адреси пов'язані з виробниками мережевого обладнання. Крім того, існують діапазони MAC-адрес, які не можуть використовуватися клієнтськими пристроями, оскільки відомо, що під час виробництва деяка послідовність адрес була призначена серверному обладнанню. Ці дані можуть стати в пригоді зловмисникам, зменшуючи кількість варіантів при атаках з метою отримання валідної MAC-адреси [1].

Ще один метод, який дозволяв сховати мережу від сторонніх очей, вважалось приховування мережевого ідентифікатора Service Set Identifier (SSID). Для того, щоб отримати доступ до мережі, клієнт при підключенні повинен явно його вказати. Та за наявності спеціального програмного забезпечення зловмисник може отримати дані про SSID точки доступу (ТД), навіть тієї, у налаштуваннях якої встановлений прапорець на функції «не транслювати SSID». Це відбувається тому, що кожен пакет, який відправляється клієнтом до ТД несе в собі інформацію про MAC адресу відправника (клієнта), MAC адресу отримувача (ТД) та SSID отримувача. Для отримання такої інформації зловмиснику всього лиш потрібно перевести мережеву картку у режим моніторингу і увімкнути фільтр пакетів які надходять на ТД із прихованим SSID [2].

Згодом, в специфікації 802.11b був введений протокол бездротової безпеки Wired Equivalent Privacy (WEP), та незадовго після цього в ньому було виявлено велику кількість серйозних вразливостей [3]. Вразливості WEP були виправлені у специфікації стандарту 802.11i [4]. Метою IEEE 802.11i було підвищення таких ключових завдань захисту інформації як цілісність, доступність та конфіденційність. Завдяки процесу автентифікації за допомогою загального ключа (англ. Shared key) автентифікованими можуть бути лише ті клієнти які його знають. Загальний ключ розповсюджується між пристроями за допомогою механізму поза рамками стандарту IEEE 802.11.

У стандарті 802.11 реалізовано два загальні механізми безпеки – Pre-shared key (PSK) та 802.1x. У PSK загальний ключ встановлюється на точці доступу. Взаємна автентифікація здійснюється за допомогою чотиристороннього процесу рукостискання. Зазвичай ключі встановлюються на бездротовий пристрій вручну. Очевидно, що для мереж з великою кількістю клієнтів використання одного й того ж ключа для всіх клієнтів є неефективним, тому для них використовується механізм 802.1x, а PSK використовується у мережах малого чи домашнього офісу (SOHO). Саме про такі мережі буде йтися далі.

Незважаючи на покращення у сфері безпеки, специфікація стандарту 802.11i визначила, що застарілі апаратні засоби стандарту IEEE 802.11 залишалися в

експлуатації протягом тривалого періоду. Програмне забезпечення на таких застарілих пристроях часто використовувало WEP та шифр RC4. З метою уникнення недоліків, пов'язаних із використанням WEP, таких як неправильне керування ключами, колізії вектора ініціалізації та фальсифікація пакетів, у стандарті 802.11i було впроваджено підпротокол Temporal Key Integrity Protocol (TKIP). TKIP функціонує як додатковий шар навколо шифрування WEP, що забезпечує більш складні механізми змішування ключів [5]. Для формування 128-бітного ключа шифрування RC4 використовується тимчасовий ключ (TK), що формується на основі MAC-адреси клієнта, а також вектора ініціалізації. Вектор ініціалізації в TKIP виступає як лічильник послідовності, що допомагає захистити від атак, спрямованих на повторення пакетів.

В рамках TKIP було реалізовано протидію для зменшення ризику фальсифікації та обмеження розголошення інформації про ключ. У випадку підозри на атаку, операції TKIP призупиняються на 60 секунд, а парні ключі генеруються повторно. Такі контрзаходи застосовуються, коли протягом однієї хвилини виявляються два кадри із некоректною цілісністю повідомлення MIC.

Ключ RC4 та вектор ініціалізації, які використовуються в WEP_{SEED}, відносяться до процесу інкапсуляції WEP. WEP використовує ці компоненти для генерації Integrity Check Value (ICV) та шифрування MAC Protocol Data Unit (MPDU) та Message Integrity Code (MIC). Хоча реалізація TKIP є складнішою за WEP, проте MIC є досить вразливим до підробки повідомлень. Тим не менш, він представляє собою кращий рівень захисту, який може бути досягнутий на застарілому обладнанні. Протокол TKIP використовується в рамках протоколу безпеки Wi-Fi Protected Access (WPA).

В табл. 1.1 наведено порівняльні характеристики параметрів безпеки, які вдосконалені при переході від протоколу безпеки WEP до WPA.

Згодом була введена нова версія протоколу безпеки для бездротових мереж WPA, яка базувалась на протоколі CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol).

Таблиця 1.1.

Порівняльні характеристики протоколів безпеки WEP та WPA

Параметр порівняння	WEP	WPA
Шифрування	Використовує слабкий алгоритм шифрування RC4.	Використовує більш сильне шифрування, таке як TKIP (Temporal Key Integrity Protocol) або AES (Advanced Encryption Standard).
Аутентифікація	Використовує просту аутентифікацію WEP ключів.	Використовує більш сильну аутентифікацію, таку як Pre-Shared Key (PSK) або Extensible Authentication Protocol (EAP).
Ключі	Використовує статичні ключі WEP, які менш безпечні.	Використовує динамічні ключі WPA, які змінюються з кожним сеансом або періодично.
Захист зламу	Має відомі уразливості, які роблять його вразливим до та зламу.	Має покращений захист від перехоплення і злому за рахунок використання стійкішого алгоритму шифрування та аутентифікації.

CCMP використовує режим лічильника засобів шифрування AES та CBC-MAC для перевірки автентичності ланцюжка повідомлень. Цей підхід забезпечує конфіденційність і цілісність даних. Відмінною особливістю є те, що алгоритм шифрування AES є значно стійкішим порівняно з RC4, який використовується в WEP та TKIP. Однак AES не може працювати на застарілому обладнанні [6].

В процесі авторизації клієнт отримує доступ до мережі з протоколом безпеки WPA2, після проходження чотиристоронього процесу рукостискання. Однак проблема цього методу полягає в тому, що пакети, які передаються під час цього процесу, можуть бути зловмисно перехоплені будь-якою бездротовою картою, що працює у режимі моніторингу на частотах 2.412 – 2.484 ГГц.

Коли клієнт або ТД готуються до перезавантаження або коли клієнт виходить за межі зони покриття, вони відправляють спеціальний кадр деавтентифікації, який не потребує перевірки автентичності. Це означає, що будь-який пристрій, що працює за стандартом 802.11 і перебуває в зоні покриття певної ТД, може відправити згенерований кадр деавтентифікації, що призведе до отримання пакету рукостискання.

Наявність пакету рукостискання, дозволяє зловмиснику запустити атаку грубої сили на цей пакет, локально на будь-якому комп'ютері перебуваючи на відстані від ТД Wi-Fi чи навіть задовго після перехоплення.

Для ускладнення процесу дешифрування пакету рукостискання рекомендується встановлювати складні паролі. Проте для звичайного користувача бездротової мережі домашнього або невеликого офісу, використання простого пароля є зручнішим варіантом. З метою спрощення процесу авторизації та унеможливлення атак грубої сили на протоколи безпеки WPA/WPA2, був розроблений механізм Wi-Fi Protected Setup (WPS). WPS дозволяє користувачеві майже автоматично отримати доступ до мережі. Проте після введення його в експлуатацію стало відомо, що сам механізм є вразливим до атак грубої сили [7].

Пін-код, який використовується для автентифікації, складається з восьми цифр. При переборі цих цифр можна розглядати дві половини, оскільки при вгадуванні першої половини пін-коду ТД Wi-Fi почне повідомляти про те, що друга половина невірна. Крім того, остання цифра є контрольною сумою перших семи цифр і може бути відновлена за певною формулою. 1.1.

$$f(n) = f\left(\left[\frac{\left[\frac{n}{10}\right]}{10}\right]\right) + 3(n\ mod 10) + \left(\left[\frac{n}{10}\right] mod 10\right) \quad (1.1)$$

Отримавши *f(n)*, можемо отримати контрольну суму (останній символ пін-коду) S_c (1.2).

$$S_c = (10 - f(n) mod 10) mod 10 \quad (1.2)$$

Відповідно до цього, зловмисникові потрібно перебрати всього лиш $10^4 + 10^3$ варіантів [8—10].

На початку 2018 року було оголошено про готовність протоколу бездротової безпеки WPA3. Як і в WPA2, у WPA3 є дві модифікації WPA3-Personal і WPA3-Enterprise. WPA3-Personal вирізняється більш простим вибором паролю, для зручності користувачів і найчастіше використовується в мережах зі сегменту малих або домашніх офісів [11]. Оновлення дозволяє здійснити, так звану одночасну автентифікацію рівних Simultaneous Authentication of Equals (SAE), яка замінила Pre-Shared Keys (PSK) у WPA2-Personal. WPA3-Enterprise як і WPA2-Enterprise призначений для жорсткішого та послідовного застосування протоколів безпеки в корпоративних мережах. В WPA3-Enterprise використовуються ключі сеансу більшого розміру, завдяки чому паролі важче зламати. Ця функція доступна для WPA3-Enterprise, що підтримує 192-бітне шифрування на всій стадії автентифікації, що робить криптографічний інструмент кращим, тобто таким, який посилює конфіденційність даних. У табл 1.2 представлено порівняння протоколів безпеки WPA2 та WPA3.

Як вже було сказано вище, одним із таких покращень є протокол SAE або, як його простіше називають – Dragonfly Handshake. Даний протокол дозволяє відтермінувати вплив атаки, а також робить пароль сильнішим і більш витривалим для компрометації. Також, SAE запобігає віддаленому розшифруванню даних в автономному режимі.

Таблиця 1.2.

Порівняльні характеристики протоколів безпеки WPA2 та WPA3

Параметр порівняння	**WPA2**	**WPA3**	**Покращення WPA3 відносно WPA2**
Обмін ключами	Використовує Pre-Shared Keys (PSK)	Використовує Simultaneous Authentication of Equals (SAE)	Безпечніший ключовий обмін, менше схильність до атак на пароль

Довжина ключа	128, 192 або 256 біт	128, 192 або 256 біт	Аналогічно
Захист від перехоплення	Вразливий до атак з вектором ініціалізації (IV)	Захищений від атак з вектором ініціалізації (IV)	Покращений захист від перехоплення пакетів
Режими безпеки	Режими WPA2-PSK і WPA2-Enterprise	Режими WPA3-Personal і WPA3-Enterprise	Виправлені вразливості та покращені можливості
Конфіденційність	Використовує алгоритм шифрування AES	Використовує алгоритм шифрування AES	Аналогічно
Аутентифікація користувачів	Застосовує процес чотиристороннього рукостискання для PSK і 802.1X	Застосовує Simultaneous Authentication of Equals (SAE) для PSK і 802.1X	Покращена аутентифікація користувачів

В WPA3 замінено протокол WPS на Wi-Fi Device Provisioning Protocol (DPP). DPP – це новий механізм, який дозволяє безпечно додавати нові пристрої до мережі за допомогою QR коду. Також WPA3 підтримує автентифікацію за допомогою Near Field Communication (NFC) – тобто, для автентифікації всього лиш потрібно піднести пристрій до Wi-Fi маршрутизатора. Додано новий розширення під назвою Opportunistic Wireless Encryption (OWE), яке при користуванні спільними ТД отримає кращий захист за рахунок, так званого, неавторизованого шифрування.

Та всього лиш за рік після публікації WPA3, у 2019 році, вже було знайдено перші проблеми у безпеці WPA3-Personal, які можуть дозволити зловмиснику відновити Wi-Fi-паролі, зловживаючи хронометражем або побічним кешем [12]. В опублікованій роботі, яку згодом було названо «Dragonblood», було описано два типи недоліків у WPA3 – перший зі зниженням рейтингу (WPA3 Downgrade) і другий пов’язаний із витоком побічного кешу.

Хоча WPA2 і був вразливим, та це був найбільш безпечний протокол до винайдення WPA3. З 2004 року технологія Wi-Fi здобула величезну популярність, а разом з нею і найбезпечніший протокол того часу – WPA2. На сьогодні мільярди мобільних пристроїв використовують WPA2 і основною проблемою є те, що більшість із них не можуть переключитись на використання WPA3. Для підтримки пристроїв, які були випущені ще до 2018 року, сертифіковані пристрої WPA3 дозволяють роботу, у так званому перехідному режимі. Такий режим дозволяє працювати як з пристроями WPA3-SAE та WPA2.

У роботі [12] дослідники зазначають, що WPA3 Downgrade можуть використати для створення підставної ТД, так званого злого двійника (ЗД), яка підтримує лише WPA2. За допомогою маніпуляцій зі збільшенням потужності сигналу від підставної ТД, зловмисники можуть заставити легітимні пристрої підключатись до цієї ТД. Також у своїй роботі дослідники стверджують, що для атаки «пониження рейтингу» потрібно всього лиш знати SSID атакованої ТД.

Алгоритм кодування пароля в Dragonfly, відомий також як алгоритм "полювання і клювання" (hunting and pecking), використовує умовні гілки. Дослідники стверджують, що у разі, якщо зловмисник зможе визначити, яка умова гілки if-then-else була обрана, то він може встановити, чи був знайдений елемент пароля у конкретній ітерації цього алгоритму. Було виявлено, що якщо зловмисник може виконати непривілейований код на комп'ютері-жертві, то він може використовувати атаку на основі кешу для визначення, яка гілка була активована в першій ітерації алгоритму генерації пароля. Ця інформація може бути використана для проведення атаки методом поділу пароля, що схожа на автономну атаку за словником.

Під час рукостискання Dragonfly використовує певні мультиплікативні групи, алгоритм кодування пароля виконує варіативну кількість ітерацій для його кодування. Кількість ітерацій залежить від MAC адрес ТД і клієнта, а також від пароля. Задля визначення, кількості ітерацій потрібних для кодування пароля, зловмисник може віддалено виконати тимчасову атаку на алгоритм кодування пароля. Відновлена інформація може бути використана для атаки на пароль.

Тож можемо стверджувати, що хоч WPA3 і покращив стійкість мереж Wi-Fi до атак, які були у попередній версії протоколу захисту, та усіх проблем він не вирішив, не в останню чергу через те, що моментальний перехід на WPA3 усіх пристроїв на земній кулі – не можливий.

1.2. Особливості існуючих систем виявлення вторгнень та систем-приманок для мереж стандарту IEEE 802.11

В сучасному цифровому світі існує багато як комерційних систем так і систем з відкритим вихідним кодом, які дозволяють захищатись від різних типів атак на бездротові мережі. У даному розділі проаналізовано особливості існуючих підходів до розроблення систем виявлення вторгнень (СВВ) та систем-приманок (СП). Також, здійснено огляд найпопулярніших продуктів захисту Wi-Fi мереж, які добре себе зарекомендували серед спеціалістів у галузі кібербезпеки.

1.2.1. Особливості існуючих систем-приманок для мереж стандарту IEEE 802.11

СП для бездротових мереж Wi-Fi, відомі також як Honeypots – це спеціально налаштовані вузли або мережи, які використовуються для виявлення і аналізу потенційних загроз і атак в бездротових мережах. Основними задачами СП є:

- Активний аналіз трафіку, що проходить через них. Вони реєструють всі пакети даних і змінюють їх маршрутизацію, щоб спрямовувати трафік через себе. Це дозволяє виявляти і аналізувати навіть ті пакети, які призначені для інших пристроїв.
- Моделювання різних видів атак і вразливостей. Наприклад, допомогою них можна послідовно випробовувати різні паролі для аутентифікації в бездротових мережах і реєструвати всі спроби.
- Збір даних про те, як зловмисники намагаються отримати доступ до мережі. Вони реєструють IP-адреси, способи аутентифікації та іншу інформацію, що допомагає вивчати поведінку зловмисників.
- Виявлення вразливостей в конкретних версіях програмного забезпечення або пристроїв і підтримувати актуальну базу даних про ці вразливості.

- Ізолювання від основної мережі, задля запобігання проникнення зловмисників у реальну мережу.
- Використання більшості доступних каналів та частот для збору даних, що дозволяє отримувати більше інформації про стан бездротового спектра і можливі загрози [13].
- Виявлення потенційних загроз і вдосконалення безпеки мереж.

Важливою характеристикою, яка визначає інтенсивність взаємодії СП і зловмисника, є рівень її інтерактивності. Рівень інтерактивності – це параметр, який характеризує подібність СП до реальної системи. СП за інтерактивністю можна класифікувати на висок-інтерактивні та низько-інтерактивні [14].

Низько-інтерактивні СП (англ. Low Interaction Honeypot Technology) емулюють лише сервіси, які часто використовуються зловмисниками. Такі СП споживають відносно небагато ресурсів, тому декілька віртуальних сервісів можна з легкістю розмістити на одному фізичному комп'ютері. Даний тип СП лише імітує поведінку певних сервісів, які можуть бути цікавими для зловмисників. Низько-інтерактивні СП не дають змогу вивчати поведінку зловмисників, а основним їх завданням є визначення моменту атаки, що допоможе тимчасово відволікти зловмисника від реальної цілі, і розпочати підготовку до протидії. Прикладом такої СП є програмний продукт Honeyd [15].

Високо-інтерактивні СП (англ. High Interaction Honeypot Technology) важко відрізнити від реальних виробничих систем. Такий тип СП дозволяє запускати різні сервіси, на які зловмисники зможуть витрачати час та ресурси. Використовуючи віртуалізацію, на одній фізичній машині може бути розгорнуто велику кількість віртуальних систем, частина з яких може бути приманками. Таким чином, навіть якщо СП буде скомпрометовано, її працездатність можна швидко відновити. Дана технологія дозволяє забезпечити високий рівень безпеки, оскільки її важче виявити. Перевагою високо-інтерактивних СП є використання централізованих рішень по збору і обробці даних з усіх елементів СП. Недоліком є, висока вартість розгортання такого типу СП, та їх обслуговування. Прикладом такої СП є програмний комплекс Honeynet [16].

Робота по створенню СП для стандарту комп'ютерних мереж стандарту IEEE 802.11 активно велась від моменту її виходу на ринок. Нижче описано концепції, проекти та програмне забезпечення, які розроблялись для бездротових мереж Wi-Fi.

Honeyd – це одна з найпотужніших найпопулярніших СП. Програмний код даного продукту є відкритим і підтримується Нілсом Провосом. Honeyd дозволяє створювати індивідуальні рішення, виходячи із задач розробника. За допомогою інтегрованої бази даних мережевих пристроїв, Honeyd дозволяє земулювати підробні сервіси, топологію, та маршрутизацію мережі в бездротовому середовищі. Підробний TCP/IP стек дозволяє ввести в оману такі програмні засоби, як nmap чи xprobe [17—18]. Все це надає вигляд автентичності бездротовій мережі.

Honeyd дозволяє створити сторінку адміністрування Wi-Fi ТД, оскільки після того, як зловмисник проник у мережу, природнім може бути бажання доступитись до її адміністративного ресурсу. Першим, що зробить зловмисник, побачивши форми для заповнення логіну і паролю – це спробує стандартні, які найде у відкритому доступі мережі Інтернет, а у разі невдачі застосує лобову атаку.

Honeyd дає змогу стежити за поведінкою зловмисника, який намагається провести атаку на відкриті сервіси, такі як атаки на протокол SNMP, служби DNS та DHCP, TFTP, чи створити підробні сервіси.

Як і будь-який інший емулятор, Honeyd має власні обмеження. Honeyd очікує на поведінку певного типу і, відповідно реагує на неї в разі її розпізнавання. Таким чином, якщо зловмисник робить щось, що не передбачено конфігурацією або ж самим програмним продуктом, то Honeyd не буде розуміти як реагувати на дану подію і, скоріш за все, відповість повідомленням з помилкою, що може демаскувати СП.

FakeAP – це програмний продукт, який був розроблений компанією Black Alchemy [19–20]. З його допомогою можна генерувати тисячі не справжніх точок доступу стандарту IEEE 802.11 за рахунок маніпуляції полями BSSID та ESSID у кадрі. Цей інструмент може бути використаний для введення в оману зловмисників.

Проте, сьогодні більшість оновлених інструментів, які використовуються зловмисниками, можуть попередити його про те, що знайдена ТД є не справжньою. Це відбувається через те, що аналізатори радіоетеру не ідентифікують трафіку в таких мережах, оскільки його там і немає, а отже таку мережу можна вважати не справжньою.

Wireless Information Security Experiment (WISE) – це перша СП для бездротових мереж стандарту IEEE 802.11, розроблена для збору даних про необережних зловмисників і просто «позичальників» ресурсу [21]. Метою даного проекту був збір даних про не легітимних користувачів, а саме – вивчення методів, специфіки проведення атак та частоти їх проведення. Для розгортання даного проекту використовувалась специфікація стандарту IEEE 802.11b. Даний проект не мав ніякої іншої мети окрім як піддатись атаці. Система детально контролювала усі активності, які відбувались у мережі.

У мережі було 5 точок доступу від компанії Cisco Systems. На деяких із них були навмисно відкриті відомі вразливості. Для того, щоб збільшити імовірність взаємодії зі зловмисником замість стандартних антен, які поставляються виробником, було використано неспрямовані антени з високим коефіцієнтом підсилення, для того, щоб СП була легко досяжною із сусідніх вулиць. Функцію виявлення вторгнень і донесення інформації до кінцевого користувача виконували такі елементи, як сервер журналізації подій та аналізатор трафіку канального рівня в етері. Сервер журналізації подій отримував дані з точок доступу про вихідні з’єднання користувачів. Як і звичайна СП, мережа WISE не мала легітимних користувачів, тому все, що відбувалось в середині було збережено і ретельно вивчено. Даний дослід є цікавий тому, що став першим, на основі якого здійснювавлись дослідження з використання публічних бездротових мереж Wi-Fi і здійснення кіберзлочинів в середині них чи за їх допомогою.

Проект HoneySpot заснований на базі атак, метою яких є втручання в безпечну бездротову мережу [22]. Існує два види HoneySpot – який емулює приватну мережу і той, який емулює публічну мережу. Публічний HoneySpot емулює бездротові мережі загального користування, наприклад, ТД готелів,

аеропортів, кафе, бібліотек та інших публічних місць, де пропонується безкоштовний доступ до мережі Інтернет для своїх клієнтів. HoneySpot для відкритих мереж не пропонує контролю доступу на бездротовому рівні і сфокусований на атаках на рівні IP для відкритих мереж.

HoneySpot забезпечує різні рівні для обидвох сценаріїв. Для публічного доступний лише один рівень, це рівень 0 для відкритих бездротових мереж (з контролем на рівні IP). Для приватного HoneySpot визначено три рівні – 0 для мереж, які захищаються протоколом бездротової безпеки WEP, 1 для мереж, які захищаються протоколом бездротової безпеки WPA і 2 для мереж, які захищаються протоколом бездротової безпеки WPA2. Кожен із рівнів для нас є цікавим з точки зору вивчення дій зловмисників відносно корпоративних мереж. Дана система є корисною тому, що надає можливість комплексного аналізу подій, оскільки володіє такими компонентами, як модуль ТД, модуль моніторингу бездротового доступу, модуль бездротового клієнта, модуль аналізу даних бездротової мережі і опціональний модуль приватної інфраструктури.

1.2.2. Особливості існуючих систем виявлення вторгнення для мереж стандарту IEEE 802.11

СВВ для мереж стандарту IEEE 802.11 (Wi-Fi) спроектовані для виявлення потенційних загроз, аномальних подій та атак у бездротових мережах. Основними задачами СВВ є:

- Моніторинг трафіку та його аналіз на предмет незвичайних або підозрілих пакетів;
- Виявлення атак на основі сигнатурних даних;
- Журналізація подій для перевірки і аналізу подій, зафіксованих в мережі;
- Передавання інформації для систем протидії вторгненням, задля подальшого відбиття атаки.

СВВ є як комерційні так і з відкритим вихідним кодом. Прикладом систем з відкритим вихідним кодом є такі продукти, як Snort та Suricata [23—24]. Дані продукти є найпопулярнішими з числа СВВ з відкритим вихідним кодом, які

підтримують роботу з бездротовими мережами Wi-Fi. Особливостями даних СВВ є те, що вони працюють на багатьох платформах та дають можливість розробникам додавати власні правила для ідентифікації та запобіганню вторгненням.

З числа комерційних продуктів СВВ, які працюють з бездротовими мережами можна відмітити Cisco Meraki Air Marshal, Aruba Wireless IDS [25—26]. І хоч дані продукти прекрасно справляються зі своїми задачами і надають підтримку своїм користувачам, та їх код закритий, що, зазвичай, не дає можливості налаштувати систему під окремі задачі.

1.3. Аналіз сучасного стану досліджень та публікацій

У роботі [27] Нілсом Провосом подано короткий огляд дизайну та реалізації програмної СП Honeyd, який імітує стек TCP/IP операційних систем для створення віртуальних приманок. Здійснено дослідження відповідно до якого представлено підхід, який дозволяє розрізняти трафік від мережевих вузлів, що проводять сканування мережі за допомогою певного програмного забезпечення. Обмеженням в даному підході є те, що дослідження проводилось лише для провідних комп’ютерних мереж.

У праці [22] Рауль Сілес підсумовує результати дослідження СП для бездротових мереж HoneySpot. В роботі описується архітектурний дизайн HoneySpot, зокрема використання віртуальних мережевих інтерфейсів та можливість імітації різних типів точок доступу. Також надається огляд можливостей цієї системи для виявлення та моніторингу атак у бездротових мережах. Та на жаль, у даній роботі обмежено опис високоінтерактивних можливостей HoneySpot.

У роботі [17] Суен Йек запропонував концепцію, яку було названо «глибокий обман» (англ. Deception-in-Depth). Її особливість полягає в тому, що її архітектура складається з трьох рівнів. На третьому рівні розгортається одну або декілька підробних точок доступу на базі деякого шлюзу. За допомогою таких точок доступу зловмисник зможе розпочати взаємодію з другим рівнем СП. На другому рівні розгортається віртуальна інфраструктура, яка в собі містить велику кількість не

справжніх мережевих вузлів, а саме емуляцію користувацьких робочих станцій, веб серверів, маршрутизаторів та ін., які, своєю чергою, емулюють взаємодію між собою. На першому рівні знаходиться головний керуючий елемент і запускаються усі сервіси СП. Центральною структурою реєстрації атак є система виявлення вторгнень Snort. Snort співпрацює з журналом подій програмного пакету Honeyd. Зібрані мережеві дані можуть підтвердити успішність проникнення у мережу за допомогою зафіксованих та розділених даних, що містить IP адреси, MAC адреси, порти TCP/IP, і протоколи які використовувались у напрямку від джерела до адресата, і навпаки. Недоліком даного підходу можна визначити складність імплементації і велику кількість компонентів, що може призвести до відмови системи. Такий підхід хоч і є доволі надійним та своє застосування може знайти лише у великих корпоративних мережах.

Оцінка захищеності комп'ютерних систем та мереж вимагає великої уваги, особливо ця оцінка набуває цінності, якщо підкріпляється фактичними даними і цифрами [28]. Найбільшої уваги потребують бездротові мережі, оскільки в них важко запровадити контрольовану зону. В роботі [29] запропоновано метод оцінки захищеності бездротових мереж, який базується на методі оцінки ієрархій (MOI, англ. Analytic Hierarchy Process, AHP). Та зі збільшенням кількості елементів у системі збільшується і похибка в оцінці захищеності комп'ютерних мереж. Вплив великої кількості факторів (об'єкти, атрибути і т.д), описаних в роботі [30], не дозволяє отримати точності в результатах. Зрештою, є імовірним виникнення нової вразливості в програмному чи апаратному забезпеченні, що використовуються в АС. Тому, задля досягнення точності в оцінці захищеності необхідно розділяти компоненти у комплексних системах. До прикладу, в бездротових мережах Wi-Fi існує деяка кількість методів захисту, деякі з них можуть використовуватись в комбінації між собою. Кожен з методів має свій час і складність подолання.

Схожу проблему можна спостерігати і у системах, які імітують роботу автентичних систем. Вони функціонують задля відвернення уваги від справжніх систем, а метою їх роботи є збір і обробка інформації про методи та засоби порушників. Види, особливості функціонування, переваги та недоліки, а також

методи інтегрування таких систем в АС, описано в роботі [31]. В роботі [32] описується систематизація методів та засобів аналізу СП в процесі зламу комп'ютерних систем чи мереж і пропонуються рекомендації щодо організації розслідування зламу, вибору засобів та аналізу подій.

Кожна комп'ютерна система володіє певними характеристиками і в кожної є свої вразливості і, відповідно, методи захисту. Не є виключенням і бездротові мережі стандарту IEEE 802.11 [33]. Не вирішеним є і питання створення системи, яка би оцінювала СП на складність подолання її захисту, що би дозволило гнучко підбирати конфігурацію відносно вартості інформації в системі, яка захищається, і очікувань щодо кваліфікованості зловмисника. Така постановка задачі вимагає аналізу вимог щодо системи, що здійснює оцінку, зокрема середовища розгортання та методів взаємодії із СП [34].

Із розвитком технологій мікрочипи стають все меншими, відповідно пристрої, які підтримують стандарт IEEE 802.11, також стають меншими. Популярності набула технологія «інтернет речей» (Internet of Things, IoT). І якщо у розглянутих вище роботах автори розглядали застосування СП і СВВ на серверному обладнанні, то завдяки пристроям IoT попередню обробку даних можна здійснювати на тому ж мережевому обладнанні. В будь-якому IoT пристрої присутній як мінімум один сенсор, дані з якого обробляються і передаються для подальшого відображення чи аналізу. Розробники таких пристроїв використовують різноманітні канали збору інформації, часто досить не очевидні, для того, щоб зробити заміри метрик, які їх цікавлять. Часом, такими сенсорами можуть виступати і мережеві картки Wi-Fi. До прикладу, робота [35] є цікавою в тому плані, що автори представили метод, який дозволяє розрізнити активність людського тіла за допомогою аналізу радіочастотного спектру від присутньої в тій же ж кімнаті Wi-Fi ТД. Як відомо, людське тіло може виступати природньою перешкодою для будь-якого радіо сигналу. Описані підходи в розглянутій роботі дозволяють подивитись на використання сучасних технологій із зовсім іншого боку. Технологія Wi-Fi ніяким чином не призначена для ідентифікації поведінки людини, та за рахунок використання непрямих методів така інформація стає доступною.

Як відомо, то атака «злий двійник» (ЗД) все ще є актуальною через вразливість до неї механізму безпеки WPA2, окрім того, як вже було згадано вище у WPA3 є механізм пониження до WPA2. Окрім того, для здійснення атаки на протокол безпеки WPA3 зловмисник також використає атаку ЗД. Авторами роботи [36] запропоновано алгоритм ідентифікації атаки ЗД на клієнтських пристроях, що однозначно є важливим для клієнтів, адже це може запобігти викраденню їх особистих даних. В корпоративних мережах, де таких клієнтських пристроїв є десятки, за допомогою такого підходу можна створити потужну мережу моніторингу. Та у випадку, якщо якийсь із пристроїв потрапив до мережі зловмисника, то гарантувати оповіщення команди інформаційної безпеки не можливо. Про таку подію зможе дізнатись лише поточний користувач і в цьому випадку доведеться надіятись на його вміння реагувати на інциденти такого плану. У випадку з публічними ТД даний підхід не працюватиме, оскільки клієнти не є постійними і контролю за їх пристроями у власника мережі немає. Досить схожий підхід пропонується у роботі [37], де автори запропонували рішення для виявлення атаки ЗД, базуючись на відмінності MAC-адрес та зовнішніх IP-адрес легітимної та нелегітимної точок доступу. Даний метод виявлення є суто рішенням для клієнтських пристроїв і не залежить від дій адміністратора мережі. Цей підхід дозволяє виявити дублікат ТД та попередити клієнта про імовірну атаку і запропонувати від’єднатись задля убезпечення від інших типів атак на користувацькі пристрої.

В роботі [38] автори пропонують підхід виявлення атаки ЗД за допомогою легковагового алгоритму машинного навчання, а саме Байєсівської класифікації, базуючись на групі службових даних з точок доступу, таких як SSID, MAC-адреса. У випадку, якщо поріг імовірності перевищує 75%, то ТД позначається такою, що може бути нелегітимною. Щоб ідентифікувати нелегітимні ТД, у роботі [39] представлено практичний метод виявлення на стороні клієнта для математичних виявлень атаки ЗД шляхом спостереження за часовою затримкою припинення з’єднання TCP між клієнтом і сервером.

Ще один метод визначення атаки ЗД пропонується у роботі [40]. Алгоритм виявлення атаки базується на перехоплені кадру деавтентифікації з радіоетеру. У випадку виявлення такого кадру СВВ розпочинає пошук точок доступу з однаковими ідентифікаторами. Та пакет деавтентифікації – це лише інструмент пришвидшення перепідключення клієнтських пристроїв до нелегітимної ТД. У випадку, якщо зловмисник намагається залишитись незаміченим, він не буде використовувати цей метод, а всього лиш дочекається кращого моменту, коли сигнал нелегітимної ТД буде сильніший за легітимну для клієнтів.

У роботі [41] автори знову ж таки запропонували підхід активного виявлення атаки ЗД на стороні клієнта, та в даній роботі вони опираються на активні статистичні алгоритми та алгоритми виявлення аномалій.

Усі вищезгадані методи не дозволяють попередити та забезпечити високу ефективність у визначенні атаки ЗД, тож проблема все ще є актуальною. Також більшість із цих підходів зосереджені на визначення атак на клієнтських пристроях, що не завжди є доцільно через затратність у обчисленнях, що окрім всього впливає на час роботи клієнтських пристроїв від автономного живлення.

Однак у роботі [42] авторами пропонується підхід визначення позиціонування вузлів у Wi-Fi мережах на основі алгоритму машинного навчання k-найближчих сусідів (KNN). І хоч розглянута робота не має на меті покращити стан кібербезпеки у бездротових комп’ютерних мережах, та все ж створює засади для покращення питань безпеки як для самих авторів так і для інших дослідників.

1.4. Формування напрямків подальших теоретичних і експериментальних досліджень

Розвиток в галузі виявлення вторгнень і СП для бездротових мереж Wi-Fi є надзвичайно важливим завданням в сучасному світі, де Інтернет-з'єднання стає все більш важливим і розповсюдженим явищем. Зараз Wi-Fi використовується практично в усіх аспектах нашого життя – вдома, на роботі, у громадських місцях, і відповідно до цього зростає і кількість загроз для безпеки мереж.

Розвиток теоретичних досліджень в цій галузі важливий для створення нових та ефективних методів захисту мереж від вторгнень. У зв'язку зі зростанням кількості пристроїв, підключених до мережі Wi-Fi, збільшується ризик вторгнень і кібератак. Нові теоретичні розробки дозволяють розробляти надійніші алгоритми виявлення і реагування на аномальну активність у мережі.

Експериментальні дослідження важливі для практичної реалізації і валідації нових методів і технологій. Вони дозволяють перевірити ефективність і точність СВВ і СП в реальних умовах. Такі дослідження допомагають виявити можливі проблеми та вдосконалити системи до рівня, коли вони можуть бути впроваджені в реальних мережах.

Розвиток цих досліджень сприяє підвищенню рівня обізнаності в галузі кібербезпеки. Інформація про нові загрози і методи їх виявлення стає доступною для спеціалістів і громадськості, що сприяє загальному підвищенню рівня кіберсвідомості і, відповідно, підвищує загальний рівень безпеки.

Нарешті, важливо зазначити, що безпека мереж Wi-Fi має важливе значення для суспільства в цілому. Мережі Wi-Fi використовуються в багатьох критичних системах, таких як медичне обладнання, банківські системи, енергетичні мережі, та багато інших. Вразливості цих мереж можуть мати серйозні наслідки, включаючи втрату конфіденційної інформації та можливість кібератак на критичні інфраструктури. В умовах сучасного ведення бойових дій мережі Wi-Fi дуже часто використовуються військовослужбовцями для передачі оперативної інформації. Тому розвиток досліджень в галузі кібербезпеки бездротових мереж є необхідним для забезпечення безпеки сучасного світу.

1.4.1. Визначення оптимального рівеня захищеності системи приманки для мережі стандарту IEEE 802.11

Задача будь-якої (СП) – піддатись атакам або несанкціонованим дослідженням з боку зловмисників. Це дозволяє вивчити стратегії кіберзлочинців та визначити засоби, за допомогою яких можуть бути нанесені атаки по критичних об'єктах автоматизованої системи (АС). СП фактично є ресурсом, який не несе

жодної користі, крім як відволікання уваги від справжніх, легітимних, інформаційних об’єктів. Під час взаємодії зловмисника з СП, інформація збирається задля подальшого аналізу та обробки [43].

Існує питання стосовно належного налаштування таких систем, зокрема СП, які імітують бездротові мережі стандарту IEEE 802.11, особливо через мобільність їх клієнтів і зазвичай невелику обмеженість контрольованої зони. Неправильна конфігурація СП може стати непотрібним навантаженням в межах цієї системи або навіть загрозою для її нормальної роботи. СП з низьким або відсутнім рівнем захисту може викликати підозру у досвідченого зловмисника, або стати простою мішенню для порушників, які цікавляться лише отриманням доступу до Інтернет-ресурсів. З іншого боку, використання СП з максимальним рівнем захисту також може бути неефективним, оскільки такий підхід перетворює систему на непроникну фортецю для потенційних зловмисників.

Логічно, що у мережах великих корпорацій циркулює інформація, ціна якої значно вища за інформацію, що циркулює у маленьких офісних мережах. В залежності від ціни інформації формується ціна на її захист. Звідси випливає те, що рівень захищеності СП не повинен перевищувати рівень захищеності легітимної системи і бути достатньо привабливим для зловмисника, в той же ж час конфігурація повинна бути такою, щоб не викликати підозри у зловмисника. Дана тема потребує детального розгляду, оскільки розуміння рівня захисту для СП дасть можливість застосовувати їх якомога продуктивніше.

1.4.2. Підходи до організації збору інформації про зловмисника у мережах стандарту IEEE 802.11

Як для користувачів, так і для зловмисників у бездротових мережах характерною є мобільність. Навіть у випадку виявлення атаки, притягнення зловмисника до відповідальності може бути складно виконати. У деяких ситуаціях зловмиснику необов'язково перебувати в зоні покриття більше однієї хвилини, щоб зібрати достатню кількість даних для подальшого дешифрування ключів. [44].

Навіть якщо атака на мережі стандарту IEEE 802.11 ідентифікується, то в кращому випадку її буде всього лиш попереджено. Задля того, щоб притягнути зловмисника до відповідальності, потрібно володіти незаперечними фактами про те, що атаку проводив саме він. На жаль, сьогодні ні один із відомих продуктів не може надати таких даних.

1.4.3. Пошук нових рішень з ідентифікації вторгнень у мережі стандарту IEEE 802.11

Деякі сучасні методи ідентифікації вторгнень є досить неефективними за рахунок помилкових спрацювань або ж не спрацювань у разі, коли атака все ж проводилась. Також система може бути достатньо ефективною, але її потужність повинна бути досить високою, а відповідно це може вплинути на її розміри.

Одним із прикладів неефективного методу ідентифікації вторгнень є метод аналізу послідовності пакетів. Як вже згадувалось, даний метод може допомогти у ідентифікації атаки на протокол бездротової безпеки WEP (Replay Attack) та підміні MAC адреси. Для того, щоб ідентифікувати збій у послідовності кадрів, СВВ повинна створити окремий потік чи процес для кожного клієнта мережі, в залежності від цього вимоги до потужності системи збільшуються лінійно.

Ще однією проблемою є те, що якщо клієнт вийшов із зони покриття системи виявлення вторгнень, то послідовність кадрів буде втрачено, і як тільки клієнтський пристрій повернеться в зону покриття сенсора, то, скоріш за все, він буде ідентифікований як порушник. Послідовність може бути розірвана у випадку, якщо клієнтський пристрій змінить частотний канал мережі. Послідовність буде обнулена у випадку, якщо контролер мережевої картки буде реініціалізований.

1.4.4. Переваги застосування штучного інтелекту у виявленні вторгнень

Штучний інтелект (ШІ) має широке застосування у випадках, коли потрібно провести великий обсяг обчислень для отримання конкретного результату або там, де людське око може пропустити важливі залежності. Особливо актуальним є використання ШІ у мережах IEEE 802.11, де атаки на мережеві ресурси або клієнтів можуть відбуватися в дуже короткий проміжок часу. Використання штучного

інтелекту може ефективно надати інформацію про потенційні загрози на основі аналізу попередньо зібраних даних про функціонування комп'ютерної мережі. Це може дозволити вчасно виявляти та реагувати на аномальну активність та запобігати можливим кібератакам, забезпечуючи високий рівень безпеки та надійності мережі.

1.4.5. Переваги систем із гнучкими підходами до розгортання та підтримки систем-приманок та виявлення вторгнень

Сьогодні існує велика кількість сервісів, які дозволяють віддалено керувати ТД та іншим мережевим обладнанням із хмарного середовища, та ні один із вище описаних продуктів, які реалізують СП чи СВВ, не пропонує такого рівня рішень. На жаль, не існує платформ, які би дозволили збирати інформацію з етеру бездротових мереж Wi-Fi і централізовано її обробляти задля виявлення вторгнень.

Якщо налаштування Wi-Fi ТД не складає значних зусиль для особи з базовими знаннями комп’ютера, то для розгортання СП і СВВ потрібно володіти знаннями в галузі телекомунікацій і інформаційної безпеки. Спрощення розгортання таких систем, централізоване керування елементами та обробка даних, яка не потребує участі кінцевого користувача, можуть значно підвищити рівень захищеності не лише великих корпоративних мереж, але й мереж сегменту домашнього чи малого офісів.

1.5. Висновки до розділу 1

Як відомо, сьогодні не існує жодного методу, який би міг гарантувати повний захист мережі Wi-Fi. Щоб зрозуміти сучасний стан проблем кібербезпеки у бездротових мережах Wi-Fi, у підрозділі 1.1 описано існуючі механізми захисту технології бездротового зв’язку IEEE 802.11 та їх вразливості.

На сьогодні вже існує доволі багато продуктів за допомогою, яких можна виявити вторгнення у комп’ютерні мережі. Менш розповсюдженим є застосування СП в захисних цілях. Окрім того застосування СП все частіше ототожнюються із кіберзлочинами, оскільки існує багато таких інструментів саме для атакувальних цілей. У системах захисту інформації СП і СВВ – це компоненти, які зазвичай

використовуються поряд. Допустимим є використання СВВ без СП, у іншому випадку, а саме використання СП без СВВ – це одна із ознак застосування такої системи у зловмисних цілях. Тому, у підрозділі 1.2 було розглянуто особливості існуючих СВВ та СП для мереж стандарту IEEE 802.11, а саме існуючі рішення, проекти, які колись функціонували, та методи, які дозволяють взаємодіяти зі зловмисниками задля подальшого вивчення методів та засобів проведення атак.

У підрозділі 1.3 здійснено аналіз сучасного стану досліджень і публікацій, що стосується СВВ та СП для мереж стандарту IEEE 802.11. Це є важливим завданням, оскільки ця технологія стає все більш важливою для пересічного користувача, бізнесу та державного сектору. Розвиток технологій Wi-Fi, розширення сфер її застосування, зростання кількості загроз, їх еволюція, розширення та використання Wi-Fi в різних сферах – це фактори, які вимагають постійного аналізу для забезпечення безпеки цих мереж. Аналіз досліджень допомагає визначити нові аспекти і напрямки досліджень, розробити ефективні засоби виявлення і захисту від загроз, та сприяє співпраці в галузі кібербезпеки.

Спираючись на недоліки, описані вище у підрозділі 1.4, сформовано напрямки подальших теоретичних і експериментальних досліджень. При використанні низько-інтерактивних (імітаційних) та не реалістичних емуляцій реальних сервісів та систем, зловмисник, виявивши аномальну поведінку останніх, може викрити дану систему чи мережу та покинути її. При цьому можлива втрата цінних даних та дискредитація подібних систем. А отже, даний вид приманок може принести більше шкоди аніж користі. Також гостро стоїть проблема у ідентифікації персон зловмисників, оскільки при атаках на бездротові мережі вони можуть не взаємодіяти з фізичним обладнанням мереж. Ідентифікація вторгнень у Wi-Fi мережах зазвичай виконується на основі сигнатур, та вони не завжди гарантують 100% ідентифікацію. Застосування ШІ може дещо покращити результати ідентифікації вторгнень. Проблемою є, також, розгортання та обслуговування СВВ та СП для Wi-Fi мереж. У корпоративних мережах використання СВВ є необхідністю, а от в умовах домашніх чи малих офісів сучасні СВВ є невиправданими, не говорячи вже про застосування СП.

Загалом, проблема кібербезпеки Wi-Fi є в тому, що навіть коли винаходяться нові протоколи безпеки, то вони спочатку встановлюються на серверне обладнання, та зазвичай застарілі клієнтські пристрої не готові до взаємодії з ними, і через це виробники змушені створювати перехідні механізми. Таке вже було при переході з WEP на WPA, з WPA на WPA2 та зрештою з WPA2 на WPA3. Все це дозволяє зробити висновок, що дана проблема буде ще дуже довго актуальною, оскільки дослідники в галузі кібербезпеки постійно знаходять шляхи обходу захисту в протоколах безпеки мереж IEEE 802.11 (Wi-Fi), а клієнтські пристрої не оновлюються моментально з виходом нових протоколів. Тому, здавалось би старі атаки, з якими навчились боротись, в нових версіях протоколів безпеки залишаються актуальними і зловмисники цим часто користуються.

Використання СП в бездротових мережах стандарту IEEE 802.11 є дуже недооціненим в аспекті їх застосування в захисних цілях. Ця тенденція має певні передумови, оскільки перед власниками мереж дуже часто постає питання щодо оптимальних налаштувань СП таким чином, щоб вона могла принести максимальну користь, що і робить це проблемою, яку необхідно вирішити.

РОЗДІЛ 2. КОНЦЕПЦІЯ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БЕЗДРОТОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11 ІЗ ЗАСТОСУВАННЯМ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ І СИСТЕМ-ПРИМАНОК

2.1. Розроблення оптимального життєвого циклу систем-приманок для мереж стандарту IEEE 802.11

При застосуванні СП важливим є врахування факторів її життєвого циклу [45]. На рис. 2.1 зображено циклічну послідовність заходів для організації функціонування СП.

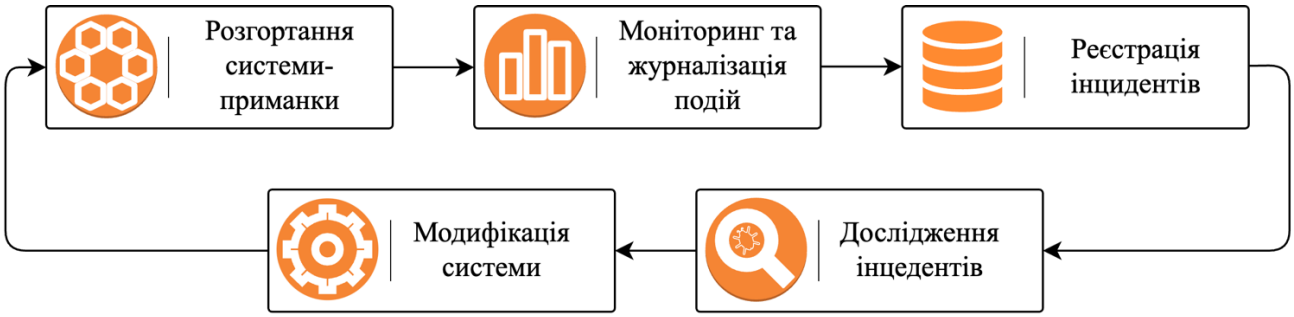


Рис. 2.1. Життєвий цикл систем-приманок

Першим етапом є розгортання СП, під час якого застосовуються конфігурації відповідно до потреб власника системи. Наступним етапом є моніторинг та журналізація подій, в межах якого здійснюється спостереження за показниками СП та запис усіх даних про взаємодію з нею. На третьому етапі відбувається реєстрація інцидентів. Якщо інциденти були зареєстровані, то наступним етапом є їх дослідження. На останньому етапі приймається рішення про ефективність СП і у випадку, якщо система показала себе неефективною то її конфігурація змінюється. Детальніше про життєвий цикл СП буде йтись далі у даному підрозділі.

2.1.1. Розгортання системи-приманок

Першою фазою налаштування СП є розгортання ресурсу, з яким буде взаємодіяти зловмисник. Він включає в себе прийняття рішень відносно:

- виробничих систем, які будуть дублюватись;
- рівня допустимого ризику у мережі;

- активностей, які будуть вивчатись;
- політики мережевої безпеки;
- рівня взаємодії зі зловмисником.

Якість СП полягає у її здатності заманювати і переконувати зловмисників у легітимності системи, яку вони атакують. Велика кількість вразливостей, наявних у мережі може стати маркером, який демаскує СП, а недостатня кількість вразливостей може зменшити шанси СП бути обраною зловмисником для взаємодії з нею. Тому, під час початкового налаштування є необхідним додати кількість вразливостей, поява яких є імовірною у реальній виробничій мережі, яка повинна бути дубльованою. В той же ж момент, широко відомі вразливості, існування яких у виробничій мережі є неможливим через, наприклад, відсутність певного програмного забезпечення, якому властива така вразливість, повинні бути видалені із СП.

Найбільш поширеними атрибутами даної фази є:

1. Сценарій атаки:
    - Атака на канальному рівні
    - Атака на рівні IP (поширена як для провідних, так і для безпровідних середовищ)
2. Модифікація технології IEEE 802.11 (a, b, g, n, ac, w)
3. Політика безпеки мережі:
    - Відкрита;
    - Застосування одного із протоколів бездротової безпеки (WEP / WPA / WPA2 / WPA3);
    - Увімкнення / вимкнення функції швидкого отримання доступу до мережі (WPS)
    - Застосування механізму фільтрування клієнтів за MAC адресами
    - Увімкнення / вимкнення транслювання ідентифікатора мережі (SSID) у етер;

- Використання додаткових серверів автентифікації на базі протоколів 802.1X/EAP.

4. Базові елементи інфраструктури:
    - Модуль бездротової ТД;
    - Модуль провідної інфраструктури;
    - Модуль клієнтського пристрою;
    - Модуль бездротового пристрою.
5. Рівень інтерактивності:
    - Низько-інтерактивна (емульована);
    - Високо-інтерактивна (реальна інфраструктура).

Окрім того, мережа може забезпечувати різний рівень взаємодії на кожному із модулів. Атрибути, які розглядаються у модулях СП:

1. Модуль бездротової ТД:
    - Емульована або реальна;
    - Кількість згенерованих точок доступу (дійсне для емульованих).
2. Модуль провідної інфраструктури:
    - Емульована або реальна;
    - Наявність або відсутність сервісів, які піддаються впливу бездротової мережі (TCP, UDP, ICMP, та ін. А також сервіси на прикладному рівні)
3. Модуль клієнтського пристрою:
    - Емульований або реальний;
    - Тип трафіку між клієнтом і ТД;
    - Вразливості, доступні на рівні операційної системи;
    - Вразливості, доступні на рівні адміністрування програмного забезпечення;
    - Вразливості драйвера бездротової мережі.
4. Модуль бездротового пристрою:
    - Емульований або реальний адміністративний сервер.

Наступною фазою є *моніторинг активностей* спійманого на приманку зловмисника за умови, що він не підозрює, що знаходиться під спостереженням. Дана фаза включає в себе журналізацію міжмодульної взаємодії. Записи про зміну файлів, введення команд, сервіси, до яких здійснювався доступ, все це повинно бути збережено задля подальшої обробки. Для того, щоб мати змогу журналізувати до, під час, після атаки, поряд із приманкою розгортається аналізатор трафіку. Такі програмні рішення як KisMAC чи Kismet у комбінації з аналізатором пакетів, наприклад, TCPDump чи Wireshark забезпечують користувачеві інтерфейс для пасивного моніторингу бездротової мережі [46—49]. Перебуваючи у режимі радіочастотного моніторингу, аналізатори трафіку можуть перехоплювати кадри, не будучи з'єднаними із ТД. Дані з радіо етеру записуються у файли з розширенням *.pcap, та містять в собі дані про незаконні дії зловмисника на канальному рівні. В залежності від потреб аналізатори трафіку можуть бути налаштовані на прослуховування трафіку на тому ж каналі, на якому працює ТД СП, або ж аналізувати трафік і з інших каналів, що дасть змогу оцінити активність вардрайверів (осіб, які здійснюють пошук та реєстрацію точок доступу Wi-Fi) у даній місцевості.

Наступною фазою є *зберігання даних про порушення* у модулях СП. Дана фаза потребує можливості детального розбору даних із попередньої фази. Усі журналізовані дані (*.pcap файли) і системні лог-файли збираються для аналізу на віддаленій локації через провідну чи безпровідну мережу.

Найважливішим етапом, задля якого здійснювалась уся попередня підготовка, є фаза *дослідження*. На даному етапі проводиться аналіз даних, які було зібрано за деякий відрізок часу. У даній фазі проводиться детальний аналіз подій, які відбувались у етері чи в середині СП за допомогою спеціальних інструментів чи аналітиками мануально. У цій фазі можливо віднайти місцезнаходження зловмисника у момент атаки по відношенню до об'єкта бездротового моніторингу та імовірно дізнатись про інструменти (програмне забезпечення, антени, специфікації бездротових карток), які були застосовано під час атаки.

Останньою, та не менш важливою є фаза *модифікації*. Ця фаза випливає з результатів роботи попередніх фаз. Модифікація інфраструктури чи архітектури СП в цілому проводяться в залежності від інформації про вектори атак і виявлених нових методик.

Адміністратор може вирішити збільшити чи зменшити рівень захищеності за допомогою реконфігурації модуля ТД, наприклад, з протоколу бездротової безпеки WPA на WEP, WPA2 чи WPA3.

Більш складні імена користувачів і паролі можуть бути впроваджені для того, щоб уникнути їх вгадування за допомогою лобової атаки, або ж навпаки додавання простих паролів задля того, щоб зловмисник як найшвидше отримав доступ до певного ресурсу. Те ж і з програмним забезпеченням ТД, воно може бути оновлене до останньої версії для уникнення експлуатації відомих вразливостей, або ж застосована стара версія, у якій є наявні добре відомі вразливості.

На етапі модифікації важливою є процедура скидання налаштувань ТД для того, щоб бути впевненим у тому, що конфігурація не була модифікована під час будь-якої із атак.

2.1.2. Моніторинг та журналізація подій

Коли вже всі методи, за допомогою яких зловмисник міг отримати доступ до мережі, вичерпали себе, імовірно, що він застосує метод лобової атаки. Як відомо, лобова атака – це метод вирішення математичних задач, який полягає у послідовного перебору певних даних, з метою з’ясування легітимних. Таким чином, якщо це лобова атака, яка відбувається в режимі онлайн, то ресурс, проти якого проводиться лобова атака, буде негативно відповідати, до поки не отримає легітимні дані. Сучасні комп’ютерні системи володіють можливістю встановлення превентивних методів, наприклад, таких, як поріг невірних введень, перевищивши який, користувач повинен буде зачекати деякий час перед тим, як спробувати ввести дані ще раз. Подібний метод може бути використаний у ідентифікації вторгнень. Наприклад, після *k*-го невірного введення певних даних можна вважати, що проводиться атака грубої сили.

Використання журналу подій у мережах стандарту IEEE 802.11 можна виявити такі види атак:

- Лобова атака на сервер з метою отримати дійсну MAC адресу;
- Лобова атака на сервер з метою отримати прихований SSID мережі за відомою MAC адресою;
- Лобова атака на адміністративні ресурси в середині мережі.

Процес виявлення усіх цих атак є подібним. Візьмемо до прикладу останню. Бувають випадки, коли адміністратори чи власники точок доступу не змінюють стандартний пароль до адміністративної сторінки ТД або до інших ресурсів, які можуть надавати додаткові привілеї. У таких випадках зловмиснику достатньо знайти стандартні реєстраційні дані в мережі Інтернет. Такий ресурс може бути спеціально створеним адміністратором мережі і очікувати на з'єднання з користувачем, який попередньо просканує мережевий діапазон. З'єднання з таким ресурсом буде слугувати маркером атаки [50].

В інших випадках зловмисник буде підбирати пароль самотужки або ж застосує атаку грубої сили. Зазвичай, невдалі спроби користувача отримати доступ до певної сторінки журналізуються в спеціальний файл помилок. Розбираючи такий файл, можна ідентифікувати атаку грубої сили за допомогою встановленого порогу на кількість невірних введень облікових даних користувача.

Якщо зловмисник вже зміг доступитись до мережі, то імовірно він спробує використати цей ресурс для власних потреб. Його метою можуть бути дані користувачів, заволодіння ресурсом чи його використання як плацдарму для подальших атак. Такі атаки можна зауважити за допомогою моніторингу мережі і пошуку аномалій.

Компанія Avenda System у своєму продукті eTIPS [51] запропонувала рішення, яке дозволяє виявити підміну MAC адреси. Метод полягає у безперервному скануванні пристроїв з легітимними MAC адресами за допомогою програмного пакету NMAP. NMAP дозволяє провести сканування пристроїв у мережі і за рахунок їх відгуків – відкритих TCP/UPD портів ідентифікувати платформу і сервіси, які він надає. Якщо у мережі з'являється новий пристрій і

адміністратор ідентифікує його як легітимний, то відбудеться початкова ідентифікація за допомогою NMAP і відповідно отримується так званий відбиток даної системи. Впродовж безперервного сканування система буде націлена на виявлення нелегітимного клієнтського пристрою, MAC адреса якого співпадає з легітимним, але відбитки NMAP не співпадають. Існує дуже мала імовірність, що зловмисник зможе повторити конфігурації легітимного пристрою. Та застосування такого продукту у бездротових мережах є досить не ефективним, оскільки клієнти бездротових мереж здебільшого не виконують ніяких серверних задач, що дозволило би отримати чіткий відбиток такого пристрою. Отже, виявити підміну клієнтського пристрою у бездротовій буде напрочуд важко за допомогою програмного пакету NMAP.

У атаці «людина посередині» (англ. Man-in-the-Middle, MITM) – зловмисник може читати та модифікувати трафік між двома вузлами навіть без їх відома про те, що канал зв’язку між ними є скомпрометованим. В основному дана атака проводиться у мережах Ethernet, а її основою є недоліки протоколу ARP. Це за собою несе створення нової точки входу або оновлення існуючої у динамічній ARP таблиці жертви. Після цього весь трафік буде проходити через робочу станцію зловмисника.

Виявлення атаки MITM є можливим, оскільки дана атака створює багато шуму. Якщо СВВ розташована у середині мережі і через неї не проходить трафік інших вузлів, то вона, як і інші вузли підмережі, отримає повідомлення з ARP запитом від вузла, який би не мав його відправляти. Якщо ж СВВ працює на основному шлюзі підмережі, то вона буде отримувати аномально велику кількість трафіку від одного вузла, і взагалі не отримувати його від інших.

Часто, для того, щоб провести атаку на певний ресурс і не видати місце свого регулярного перебування, зловмисники використовують відкриті ТД у громадських місцях. З мережі, до якої зловмисник має доступ він може провести атаку відмови в обслуговуванні (англ. Denial of Service, DoS) на будь-який віддалений ресурс, який може бути доступним з цієї мережі. Окрім того, що зловмисник може проводити атаку зі своєї робочої станції, він може використати

вразливості клієнтів, які підключені до тієї ж мережі і, за рахунок цього підсилити атаку. Існує декілька модифікацій DoS атак, але найрозповсюдженішою є модифікація, направлена на перевантаження пропускної смуги каналу ресурсу.

Про проведення такої атаки можуть свідчити виявлені широкомовні ICMP Echo Request пакети, пакети у заголовку яких не вказаний зворотний шлях, UDP Echo, Chargen чи Disabled-пакети. Також ідентифікувати таку атаку можна за встановленим порогом пакетів, які надходять від клієнта. Наприклад, такий інструмент як LOIC [52] надсилає велику кількість пакетів до цілі з інтервалом у 0.00005 секунд.

2.1.3. Реєстрація інцидентів

Перший крок – це визначення того, що становить собою інцидент. Інцидент може бути різним – від спроби несанкціонованого доступу на системному рівні і до атаки на мережевий трафік. Для реєстрації інцидентів необхідно розгорнути відповідну систему, яка включає в себе процедури, інструменти та процеси для реєстрації інцидентів. Ця система може бути відокремленою базою даних, журналами подій, спеціалізованим програмним забезпеченням і так далі.

Інциденти можуть бути класифіковані за типом, важливістю, впливом на мережу і іншими факторами. Це допомагає визначити пріоритети і рівні важливості для різних інцидентів.

Будь-який інцидент повинен бути докладно задокументований, включаючи дату і час виявлення, опис події, збережені дані, вплив на систему та іншу інформацію, яка може бути корисною для подальшого аналізу. Інформація про інциденти повинна бути представлена у вигляді звітів для адміністраторів мережі та СП. Події можуть бути вивчені, щоб покращити стратегії безпеки мережі.

2.1.4. Дослідження інцидентів

Метою аналізу є розуміння та ідентифікація загроз та атак, а також розробка стратегій та заходів для їх виявлення та запобігання. Аналіз дій зловмисника в мережах Wi-Fi включає в себе дослідження різних методів та прийомів, які

використовуються для вторгнень, викрадання даних, злому паролів та інших видів кібератак.

В цьому контексті дослідники та адміністратори мереж мають вивчати та впроваджувати різні техніки та інструменти для виявлення та аналізу аномальних подій у мережі, розробки стратегій безпеки та вдосконалення заходів захисту. Аналіз дій зловмисника є важливою складовою частиною сучасної кібербезпеки та дозволяє підвищити рівень захисту мереж Wi-Fi від потенційних загроз.

Зрозуміти наміри клієнта можна ще на етапі його появи в зоні дії ТД. Службові дані на канальному рівні моделі OSI є відкритими, транслюються у етер і є доступними усім пристроям стандарту IEEE 802.11, які знаходяться у радіусі дії джерела. Таким же ж чином, як зловмисники перехоплюють дані про ТД (частотні канали, на яких вони працюють, методи, які використовуються для захисту та MAC адреси підключених клієнтських пристроїв), можна перехоплювати дані з клієнтських пристроїв, з яких надходять дані. Якщо дані не є притаманними звичайному клієнту, то поведінку можна категоризувати до зловмисної.

Візьмемо до прикладу атаку на ТД, у якої відімкнено надсилання маячків з метою приховання ідентифікатора мережі. Якщо до мережі підключені клієнтські пристрої, то в етері, на канальному рівні зловмисник зможе отримати дані про SSID ТД, пасивно прослуховуючи мережевий трафік, оскільки від клієнтів будуть відправлятись пакети, в яких буде міститись інформація про MAC адресу пристрою, до якого відправляються дані і його SSID. Та зловмисник не зможе отримати такі дані, якщо до ТД з прихованим SSID не буде підключено ні одного клієнта. В такому випадку зловмисник буде зобов’язаний провести перебір за словником відносно ТД.

Ще однією атакою, яку можна виявити в етері, є атака на протокол бездротової безпеки WEP. Мережі, які захищені за допомогою протоколу бездротової безпеки WEP, не мають внутрішнього механізму контролю за кадрами. В результаті кадр може бути підмінений і переданий в мережу пізніше. Ми можемо розпізнати цей вид атаки по перевірці порядкових номерів, які є прив’язані до кожного мережевого кадру. Ці порядкові номери, як правило, допомагають приймальним пристроям сортувати кадри у правильній послідовності і виявляти

відсутні кадри. Порядковий номер допомагає зберегти логіку роботи, але з певних причин, сесія може бути повторена через деякий час. Така різка зміна порядку може вказувати на активну фазу атаки.

Сьогодні найбільш стійким алгоритмом безпеки стандарту IEEE 802.11 є WPA3, та як вже було згадано вище зловмисник може понизити його до WPA2 завдяки перехідному механізму. А як вже відомо, WPA2 є вразливим до ряду атак. Одна із вразливостей полягає в тому, що зловмисник може перехопити кадр з інформацією про рукостискання між клієнтом та ТД. Зловмисник може пасивно сканувати трафік в етері під час підключення клієнта до ТД, отримати даний кадр, і, згодом, його дешифрувати в режимі офлайн. Через те, що даний вид кадрів не проходить перевірку автентичності, зловмисник також може згенерувати такий кадр на своїй робочій станції і відправити його в етер. Та більшість інструментів, які дозволяють провести дану атаку, дозволяють відсилати безліч таких кадрів, для досягнення мети. Велика кількість таких кадрів може привести до відмови в обслуговуванні. Отже, наявність великої кількості кадрів деавтентифікації може послужити маркером виявлення як атаки на протоколи бездротової безпеки WPA/WPA2, так і атаки на відмову в обслуговуванні .

Якщо протоколи бездротової безпеки WPA/WPA2 активовано, то разом з ними може працювати і механізм WPS. Як вже згадувалось, атака на WPS базується на лобовій атаці. Дана атака залишає чіткий слід, оскільки за короткий проміжок часу до ТД надходить велика кількість хибних числових послідовностей, які не відповідають заводському PIN-коду [53].

Усі ці види атак можуть бути ідентифіковані в етері ще до того, як зловмисник успішно завершить одну із них. Таким чином, даний метод дозволяє завчасно зреагувати на атаку і виграти дорогоцінні секунди для відведення атак на не виробничі ресурси.

2.1.5. Модифікація системи

Проведення аналізу ефективності СП є останнім та від того не менш важливим етапом у процесі її використання та підтримки. Цей аналіз допомагає

оцінити, наскільки СП відповідає своїм цілям і завданням, а також виявити її недоліки та можливості для покращення.

Важливо визначити, чи відповідає робота СП цілям безпеки організації. Чи вдалося системі виявити та записати небажану активність? Чи були виявлені потенційні загрози? Аналіз ефективності допомагає виявити недоліки і вразливості СП, які можуть бути використані зловмисниками для обходу захисту.

Іншим важливим аспектом є оцінка того, наскільки ефективно використовуються ресурси, наприклад, обсяги дискового простору та обчислювальні ресурси.

Важливо визначити, скільки хибно позитивних та хибно негативних подій генерує СП. Хибно позитивні можуть виводити персонал на зайву роботу, тоді як хибно негативні можуть пропустити потенційну загрозу. Важливо оцінити, як СП взаємодіє з іншими складовими інфраструктури безпеки, такими як СВВ, антивірусними програмами тощо.

На основі результатів аналізу можна розробити стратегії покращення безпеки мережі та СП. Завершальний етап аналізу ефективності допомагає зрозуміти, як СП функціонує в реальних умовах, і сприяє подальшому її вдосконаленню та адаптації до нових загроз.

2.2. Розроблення та аналіз моделі порушника у бездротових мережах стандарту IEEE 802.11 для підприємства

Розроблення надійної СП є неможливим без визначення категорій потенційних порушників та методів, які вони використовують. Виходячи зі специфіки технології Wi-Fi, задля розробки правильної послідовності кроків у розробці СП для мереж стандарту IEEE 802.11, потрібно визначити модель порушника, яка би адекватно відображала його можливості, щодо можливого втручання у роботу системи.

По суті, модель порушника – це опис його реальних чи теоретичних можливостей, знань про систему, технічної оснащеності тощо. Досліджуючи умови, за яких здійснено порушення, можна зробити висновки про цілі

зловмисника і, відповідно, як покращити процес виявлення вторгнень, так і захист виробничого ресурсу.

2.2.1. Визначення загроз

Виконуючи класифікацію джерел загроз за місцем розташування, вважають, що джерела загроз бувають внутрішні, тобто ті, які виникають усередині підприємства чи організації, та зовнішні – які перебувають поза межами підприємства.

Як відомо, за сутністю прояву, джерела загроз поділяються на три групи:

- Антропогенні – зумовлені діями суб’єкта як умисними, так і ненавмисними;
- Техногенні – ті, що визначаються технократичною діяльністю людини та розвитком цивілізації;
- Стихійні – обставини непереборної сили, тобто такі, які мають об’єктивний та абсолютний характер.

В рамках даної роботи нас будуть цікавити лише антропогенні джерела загроз.

Антропогенні джерела загроз за місцем розташування можна розділити на зовнішні (такі як відвідувачі, представники кримінальних структур, представники зовнішніх технічних і аварійних служб) та внутрішні. Зазвичай внутрішні джерела є висококваліфікованими спеціалістами у галузі розроблення та експлуатації програмного забезпечення, які добре орієнтуються у специфіці діяльності підприємства та структурі автоматизованих систем і мають можливість використовувати штатне обладнання та технічні засоби мережі.

Варто зазначити, що антропогенні загрози є найбільш серйозними та такими, що потребують постійної уваги і аналізу можливих дій, їх наслідків. За результатами досліджень спеціалістів з міжнародних організації у галузі інформаційної безпеки основними джерелами загроз є внутрішні антропогенні джерела загроз, оскільки 75%—85% всіх порушень здійснюються самими

співробітниками підприємств, які мають доступ до АС і лише 15—25% порушень здійснюється сторонніми особами.

Зважаючи на унікальність кожного підприємства та його специфіку, неможливо розробити загальний стандарт або правила для побудови єдиної моделі порушника. Тому при побудові СВВ і СП для бездротових мереж розглянемо наступні категорії порушників:

- Клієнти та відвідувачі;
- Конкуренти;
- Кіберзлочинці;
- Програмісти;
- Оператори (системні адміністратори);
- Адміністрація (керівництво);
- Технічний персонал;
- Працівники яких було звільнено.

Вплив на мережі IEEE 802.11 та захист інформації здійснюється через поля, сигнали та програми в технічних засобах передачі інформації з метою зниження ефективності захисту, створення технічних каналів витоку та порушення цілісності даних шляхом можливої модифікації, руйнування або знищення

Ненавмисні загрози – це вид загроз, який виникає в результаті некомпетентних дій, наприклад, користувач чи адміністратор системи, що не був навчений належним чином, не мають належної документації та не розуміють важливість належних процедур захисту.

Навмисні загрози – вид загроз, який виникає в результаті цілеспрямованих дій з боку порушника. Таких порушників можна поділити на дві категорії: сторонні та втаємничені особи. Наприклад, перехоплення та декодування електромагнітних випромінювань, чи виконання визначеного криптографічного аналізу можуть виконувати лише “висококваліфіковані кіберзлочинці”, які володіють істотним обчислювальним ресурсом, фінансами, часом та персоналом.

2.2.2. Аналіз загроз об’єкта захисту

Як відомо, бездротові мережі Wi-Fi можуть бути доступні не лише в середині контрольованої зони, але й далеко за її межами. Навіть не використовуючи потужних вузьконаправлених антен, зловмисник може сканувати трафік мережі на відстані до 200 метрів. Отже, для даного випадку із системою, яка очікує на взаємодію зі зловмисником, опишемо дестабілізуючі фактори і можливість їх впливу на систему. Такий підхід допоможе в подальшому отримати можливі вектори атак і правильно побудувати вектори захисту виробничих мереж. У табл 2.1 – 2.4 проведено аналіз зовнішніх та внутрішніх дестабілізуючих факторів для АС із використанням мереж стандарту IEEE 802.11 як в межах контрольованої зони так і за її межами.

Як видно з табл. 2.1 та табл. 2.2 – у неконтрольованій зоні загроз доволі небагато, та в порівнянні з дротовими мережами, їх в рази більше, за рахунок того, що радіохвилі непросто і, часто, недоцільно контролювати. Найбільшу небезпеку для функціонування АС несуть загрози від зловмисників, оскільки за допомогою спеціального обладнання вони мають змогу доступитись до АС через бездротові мережі IEEE 802.11. Також не варто забувати про помилки серед персоналу, оскільки неправильна конфігурація обладнання може значно полегшити завдання зловмисникам.

Набагато більше виникає проблем вже в контрольованій зоні (табл. 2.3–2.4). Якщо за межами контрольованої зони зловмисники можуть бачити лише певний службовий трафік мереж стандарту IEEE 802.11, то перебуваючи в контрольованій зоні вони можуть дізнатись про інфраструктуру АС. До прикладу, дізнавшись про модель Wi-Fi обладнання, зловмисник може здійснити пошук їх імовірних вразливостей. Окрім того, отримавши інформацію про обладнання зловмисник може здійснити підміну наявного на власне обладнання, метою якого є перехоплення, модифікації чи знищення даних.

Таблиця 2.1.

Аналіз внутрішніх джерел дестабілізуючих факторів на території радіусом 200 метрів від об’єкту захисту

Тип дестабілізуючих факторів	**Джерела дестабілізуючих факторів**		
	Персонал		
	Адміністрація (керівництво)	**Технічний персонал**	**Інший, не технічний персонал**
Кількісна недостатність	–	–	–
Якісна недостатність	–	–	–
Помилки	–	Не вірне налаштування систем, своєю чергою, може призвести до відмови в обслуговуванні, втрати критично важливих даних. Збільшення потужності мережевого адаптера стандарту IEEE 802.11 може полегшити процес обходу захисту для зловмисника.	–
Злочинні дії	Розповсюдження інформації про точне місце розташування	Розповсюдження інформації про точне місце розташування елементів АС,	Розповсюдження інформації про точне

	елементів АС, модельний ряд пристроїв, технічної документації, тощо.	модельний ряд пристроїв, технічної документації, інформацію про конфігурацію окремих елементів чи АС в цілому	місце розташування елементів АС, модельний ряд пристроїв.
Побічні явища	–	–	–

Таблиця 2.2.

Аналіз зовнішніх джерел дестабілізуючих факторів на території радіусом 200 метрів від об’єкту захисту

Тип дестабілізуючих факторів	**Джерела дестабілізуючих факторів**		
	Зовнішній вплив		
	Відвідувачі	**Кіберзлочинці**	**Працівники, яких було звільнено**
Злочинні дії	–	1. Прослуховування мережі за допомогою програмних або програмно-апаратних аналізаторів 2. Створення завад у радіочастотному діапазоні АС.	–

Побічні явища	–	Активності пов’язані зі збором даних про АС (Елементи соціальної інженерія відносно працівників)	Ненавмисне (вплив збоку соціального інженера) / чи навмисне (з метою збагачення, чи помсти) розповсюдження інформації про точне місце розташування елементів АС, модельний ряд пристроїв.

Таблиця 2.3.

Аналіз внутрішніх джерел дестабілізуючих факторів у контрольованій зоні

Тип дестабілізуючих факторів	**Джерела дестабілізуючих факторів**		
	Персонал		
	Адміністрація (керівництво)	**Технічний персонал**	**Інший, не технічний персонал**
Кількісна недостатність	–	Недостатня кількість інженерів з технічного обслуговування систем, може призвести до не можливості	–

		відслідковувати працездатність і аномалій в АС	
Якісна недостатність	Закупівля неякісного обладнання чи набір некомпетентного персоналу для адміністрування АС	Недостатня кваліфікованість інженерів з технічного обслуговування систем, може призвести до проблем з налаштуваннями і розмежуванням доступу.	–
Помилки	Ненавмисне завантаження шкідливого програмного забезпечення на робочий комп'ютер. Втрата / ненавмисне розповсюдження службової документації, що стосується АС	Не вірне налаштування систем, що, своєю чергою, може призвести до відмови в обслуговуванні чи втрати критично важливих даних	Ненавмисне завантаження шкідливого програмного забезпечення на робочий комп'ютер. Втрата / ненавмисне розповсюдження службової документації, що стосується АС
Злочинні дії	Встановлення закладних пристроїв в АС	Навмисні помилки в налаштуванні систем, що, своєю чергою, може призвести до втрати чи модифікації даних в АС збоку кіберзлочинця	Встановлення закладних пристроїв в АС

Побічні явища	Підключення власних пристроїв, як можуть бути інфікованими шкідливим програмним забезпеченням (ШПЗ), в АС. Навмисне / ненавмисне пошкодження елементів АС	Підключення власних пристроїв, як можуть бути інфікованими ШПЗ, в АС. Навмисне / ненавмисне пошкодження елементів АС	Підключення власних пристроїв, які можуть бути інфікованими ШПЗ, в АС. Навмисне / ненавмисне пошкодження елементів АС

Таблиця 2.4.

Аналіз зовнішніх джерел дестабілізуючих факторів у контрольованій зоні

Тип дестабілізуючих факторів	**Джерела дестабілізуючих факторів**		
	Зовнішній вплив		
	Відвідувачі	**Кіберзлочинці**	**Працівники, яких було звільнено**
Злочинні дії	Розповсюдження інформації про точне місце розташування деяких елементів АС, модельний ряд пристроїв, тощо. Закладання / підміна	Несанкціоноване втручання в роботу АС з метою перехоплення, модифікації, знищення даних.	Встановлення закладних пристроїв в АС в момент коли доступ до контрольованої зони ще не перестав діяти.

	пристроїв АС з метою перехоплення, модифікації, знищення даних.		
Побічні явища	Навмисне / ненавмисне пошкодження елементів АС.	Порушення роботи АС.	Навмисне пошкодження елементів АС.

2.3. Дослідження можливих демаскуючих ознак у приманках

Як відомо, кіберзлочинці і спеціалісти галузі інформаційної безпеки знаходяться у безперервній гонці. Після винайдення технології honeypot ця гонка набула нової форми, оскільки жертвами тепер стають зловмисники.

Хоч СП націлені на те, щоб зібрати доказову базу проти зловмисника і зменшити імовірність атаки на виробничі системи та, як вже було зазначено вище, самі СП через свою недосконаліть замість користі приносять збитки. У кращому випадку приманки можуть ідентифікуватись зловмисниками і покидати їх. У гіршому випадку СП може стати плацдармом для подальших атак на АС.

У даному підрозділі розглянемо можливі демаскуючі ознаки для систем-приманок, які можуть бути застосовані у бездротових мережах.

2.3.1. Виявлення приманки на канальному рівні моделі OSI

Якщо корпоративна ТД налаштована на роботу без використання вразливих механізмів захисту, то це може свідчити про відсутність безпеки такої мережі або ж про можливе застосування СП.

Такий інструмент як FakeAP допомагає розгорнути одну або більше точок доступу. Якщо за допомогою цього інструменту розгорнути одну ТД, то в етері вона не буде відрізнятись від будь-якої іншої, та застосування його таким чином є не доцільно. Здебільшого за допомогою FakeAP розгортають велику кількість точок доступу. Такий підхід дозволяє відволікти зловмисників від справжніх виробничих мереж.

Для того, щоб розгорнути ТД за допомогою FakeAP необхідно вказати наступні дані:

- Канал в етері, на якому буде розгорнута ТД;
- Ім’я ТД, яке відображається в етері.

Також, ТД може бути клонована з існуючої, для цього необхідно вказати ім’я ТД, яку потрібно склонувати. Після цього ТД буде максимально подібною до справжньої.

Велика кількість точок доступу з однаковим ім’ям, але з різними MAC адресами, може свідчити про те, що застосовується певний механізмів розподілу покриття, наприклад Wireless Distribution System (WDS) [54] чи Mesh [55] або про застосування СП. Відрізнити застосування СП, яка генерує безліч несправжніх точок доступу за допомогою одного фізичного пристрою у бездротових мережах стандарту IEEE 802.11, від механізмів розподілу покриття можна за допомогою заміру потужності від усіх точок доступу з однаковим ім’ям. Потужність точок доступу, які працюють в режимі розподілу покриття будуть показувати різні значення, оскільки вони фізично рознесені між собою. Потужність від точок доступу земульованих програмним пакетом FakeAP буде приблизно однаковою. Саме такий прийом може бути використаний зловмисниками для ідентифікації того, що в етері є СП.

2.3.2. Виявлення приманки на мережевому рівні моделі OSI

Після того, як зловмисник опинився в середині мережі, то цілком імовірно, що він продовжить атаку задля отримання доступу до інших ресурсів всередині мережі. Першим кроком, який буде зроблено для досягнення такої мети, буде сканування мережі. Отримавши список мережевих вузлів і сервісів, які на них запущені, зловмисник може перейти до атаки. В такому випадку дії зловмисника будуть журналізуватись.

Сьогодні вже існують сигнатури, які можуть повідомити про взаємодію із СП. У випадку, якщо зловмисник запустить сканер відомих приманок і вони будуть ідентифіковані, то імовірно така система буде одразу ж покинута [56].

Якщо СП представляє собою сервіс, який у реальному середовищі є часто відвідуваним, то звернення до неї обов’язково повинні бути присутніми, в іншому випадку це може стати демаскуючим фактором. Часто, для того, щоб створити ілюзію легітимності СП, запускають різного роду програмні засоби, які генерують мережевий трафік.

У мережевій безпеці існує методика виявлення атак за допомогою аналізу трафіку і пошуку в ньому аномалій. Подібна методика використовується

зловмисниками для виявлення СП у мережах, які вони атакують. Основною проблемою є те, що програмні засоби, які генерують трафік, роблять це одноманітно, без варіацій, що не є притаманним легітимному користувачеві. Тому у випадку зловмисників однією із сигнатур СП може бути ідентифікація одноманітного трафіку [57].

2.3.3. Виявлення приманки на прикладному рівні моделі OSI

Перебуваючи в середині мережі, цілком природньо, що зловмисник захоче заволодіти адміністративним доступом до певної мережевої ланки. У випадку СП для бездротової мережі, як мінімум один мережевий вузол повинен володіти можливістю адмініструвати бездротову мережу.

Як відомо, кожен виробник мережевого обладнання володіє певним діапазоном MAC-адрес, які можуть бути присвоєні його обладнанню. Також, здебільшого, кожен виробник Wi-Fi точок доступу, розробляє власні панелі керування.

ТД з упаковки вже готові до роботи, щоправда зі стандартними налаштуваннями. Особливістю кожного виробника є шаблон, за яким надаються стандартні SSID ТД.

Отже, програмне забезпечення адміністративного ресурсу, SSID ТД і її MAC-адреса повинні відповідати одне одному, оскільки невідповідність може викликати підозру у зловмисника [58].

2.4. Розроблення концептуальної моделі системи захисту інформації із застосуванням систем виявлення вторгнень та систем-приманок

Використання хмарних обчислень для організацій має безліч переваг, які допомагають покращити ефективність, безпеку і адаптивність їхніх інформаційних систем і бізнес-процесів. Використовуючи хмарні обчислення організації можуть уникнути значних витрат на закупівлю, установку та обслуговування власних серверів і обладнання. Вони можуть використовувати інфраструктуру хмарних постачальників, що вже готова до використання. Хмарні постачальники дозволяють миттєво збільшувати або зменшувати обсяги ресурсів в залежності від потреб

організації. Це дозволяє зберігати оптимальну продуктивність і знижувати витрати в той час, коли ресурси не потрібні.

Хмарні обчислення дозволяють використовувати високопродуктивні обчислювальні ресурси та апаратне забезпечення без необхідності чекати на закупівлю та розгортання обладнання. Багато хмарних постачальників мають розгалужені мережі даних та заходи з резервного копіювання, що робить їхню інфраструктуру надійною та стійкою до відмов [59].

Зазвичай постачальники хмарних обчислень беруть на себе обов'язки з оновлення і підтримки інфраструктури, а також забезпечують безпеку, а отже організація може зосередитися на своїх основних завданнях.

Однією із найбільших переваг хмарних обчислень є економія коштів на IT інфрастуктуру. Ці технології дозволяють організаціям платити лише за використані ресурси, що призводить до зменшення витрат порівняно з традиційними інфраструктурними рішеннями.

Представленням будь-якої Інтернет технології, як сервісу є поняття Anything as a Service (XaaS), яке також є синонімом до хмарних обчислень [60]. Найбільш відомими прикладами XaaS є моделі Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

Також існує модель надання послуг в галузі кібербезпеки Security as a Service (SECaaS). Використовуючи модель SECaaS організації чи окремі фізичні особи отримують доступ до різних захисних послуг через мережу Інтернет. Замість того, щоб самостійно встановлювати та підтримувати різні продукти і рішення для захисту своєї інфраструктури і даних, клієнти можуть користуватися послугами кібербезпеки, які надаються віддалено і обслуговуються сторонніми постачальниками.

SECaaS представляє собою модель, у якій постачальник послуг із великими обчислювальними потужностями, який надає послуги інформаційної безпеки, інтегрує свої сервіси у корпоративну інфраструктуру замовника. Такий підхід часто є більш рентабельним, аніж коли доводиться розгортати систему безпеки на своїй стороні. У такій моделі замовнику послуги не потрібно турбуватись про підтримку

системи безпеки, оскільки усі роботи із забезпечення працездатності системи безпеки лежать на постачальникові послуг. В такі сервіси часто входять служби автентифікації, антивіруси, антишпигуни, СВВ та керування подіями безпеки [61—62].

В даному розділі пропонується нова під-концепція SECaaS, із запропонованою назвою «Wireless Honeypot as a Service» (WHaaS). WHaaS – це сервіс, який націлений на забезпечення інформаційної безпеки у діапазоні частот мережах стандарту IEEE 802.11 шляхом розгортання підробних точок доступу і їх постійного моніторингу [63]. Схематичне зображення WHaaS моделі подано на рис 2.2.

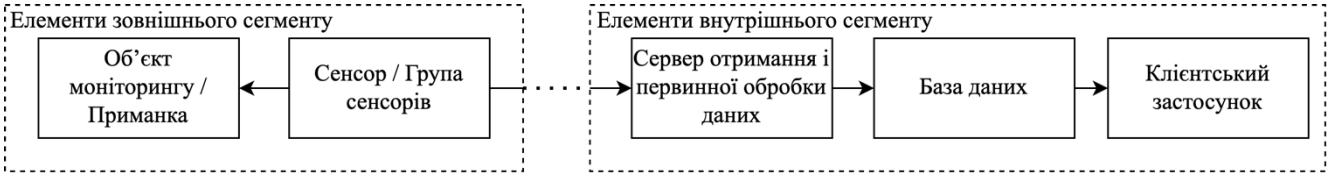


Рис. 2.2. Схематичне зображення моделі Wireless Honeypot as a Service

2.4.1. Елементи моделі Wireless Honeypot as a Service

ТД стандарту IEEE 802.11, які націлені на сегмент малих або домашніх офісів, зазвичай не володіють можливістю виконувати будь-яку іншу роль окрім забезпечення доступу до певного мережевого сегменту. Встановлення будь-якого додаткового програмного забезпечення є дуже складною задачею через архітектурну несумісність або недостатню кількість обчислювальних ресурсів. Wi-Fi сенсором може бути будь-яка робоча станція з інтегрованою або дискретною мережевою картою IEEE 802.11. Для даної мети зручно використовувати одноплатні комп'ютери. Даний тип робочих станцій володіє достатньою кількістю ресурсів для розгортання на них таких операційних систем як Windows чи Linux. Також, із певним типом задач пов'язаних з мережами стандарту IEEE 802.11 можуть справлятись мікроконтролери, які вже мають інтегровані Wi-Fi модулі.

Будь-які два мережеві вузли можуть між собою спілкуватись за умови, якщо вони знаходяться всередині однієї приватної мережі або ж знаходяться у різних мережах, але їм надано публічні IP адреси. Та надання елементам, які задіяні в зборі

і обробці службової інформації, публічної адреси є затратним рішенням, оскільки таких елементів може бути досить багато. Окрім того, доступ до мережевих вузлів ззовні є небезпечним, оскільки вони можуть бути легко атаковані з мережі Інтернет.

Мережі Wi-Fi, у яких немає розподіленого покриття, зазвичай не можуть покрити велику площу. Можливість під'єднання пристрою до мережі сильно залежить від підсилення антени і, якщо говорити про енергоефективні пристрої, то радіус їх дії буде складати до 50 метрів за відсутності завад. Окрім того, задля покращення безпеки може існувати необхідність у покритті площі більшої за контрольовану зону. В такому випадку сенсори можуть бути розташовані між собою на відстані, яка не дозволяє комунікувати між собою. Тож, задля розширення радіусу покриття, у моделі WHaaS, доцільно створити можливість бути фізично підключені до різних мереж, оскільки часом пряма комунікація між сенсорами може бути неможливою.

Для того, щоб забезпечити комунікацію між сенсорами, які можуть бути підключені до різних мереж, вони повинні належати якомусь спільному ресурсу. Такий ресурс можна створити використовуючи віртуальні приватні мережі (VPN). Після підключення до VPN сервера сенсори отримають доступ до всіх елементів мережі і навпаки.

Коли вже зовнішні елементи системи можуть бути доступні в мережі, то можна реалізувати комунікацію з ними за допомогою певного протоколу мережевої комунікації. В залежності від операційної системи, це може бути RDP для Windows та SSH для Unix. Елемент, який здійснює комунікацію і керування з віддаленими елементами далі називатимемо командним центром (КЦ). КЦ дозволить проводити процес встановлення та оновлення програмного забезпечення або виконувати визначені команди на віддалених елементах комплексу. Сценарії можуть бути генеровані відповідно до операційної системи, яка встановлена на той чи інший зовнішній елемент [64].

СВВ є важливою складовою інфраструктури системи захисту інформації на основі моделі WHaaS. Одним з ключових аспектів роботи СВВ є наявність бази даних (БД), яка відіграє важливу роль у функціонуванні цієї системи. БД

використовується для зберігання історії активності в мережі та етері. СВВ отримує дані про мережевий трафік, взаємодію користувачів та активність зловмисників. Ця інформація записується в БД і зберігається для подальшого аналізу. Це дозволяє системі відстежувати зміни в мережевій активності та розпізнавати аномалії.

Важливою задачею БД є те, що вона дозволяє СВВ будувати інтелектуальні моделі здійснення атак та аномальної активності на основі історичних даних. Вона навчається розпізнавати типові сценарії вторгнень і реагувати на них. Також вони використовуються для зберігання інформації задля створення звітів і аналітики щодо безпеки мережі. Це включає в себе виявлення стійких трендів або інцидентів безпеки, що допомагає адміністраторам мережі приймати обґрунтовані рішення щодо покращення безпеки чи модифікації СП.

Після того, як дані було зібрано, необхідно здійснювати їх аналіз. Аналіз даних – це важлива складова будь-якої системи захисту інформації. Основною задачею такого компонента є виявлення відхилень від норми, виявлення аномалій на основі історичних даних, розпізнавання потенційно небезпечних ситуацій на основі сигнатур та ін. Завдяки аналізу даних система захисту може вчасно реагувати на виявлені загрози, приймаючи заходи для їх запобігання або ліквідації. Крім того, аналіз даних допомагає вдосконалювати методи і алгоритми виявлення вторгнень, роблячи систему більш ефективною у виявленні нових та невідомих загроз.

Важливим компонентом будь-якої сучасної системи є ресурс, де користувач чи адміністратор зможе слідкувати за станом системи, налаштовувати її та отримувати сповіщення про певні події. За даний функціонал зазвичай відповідають клієнтські застосунки, розгорнуті на певному сервері. Сервер застосунку – це середовище із програмним додатком, що отримує дані з БД і відправляє їх на користувацький інтерфейс, де користувач може працювати вже з агрегованими даними.

Усі компоненти внутрішнього сегменту повинні забезпечувати безперебійність у наданні послуг, оскільки недоступність VPN сервера чи БД ставить під ризик роботоздатність усієї системи. Найкращу завадостійкість та живучість обчислювальної інфраструктури може забезпечити використання

хмарних обчислень. Хмарні обчислення мають багато переваг, таких як масштабованість, гнучкість, доступність, зменшення витрат та ін.

Отже, зі всього вище сказаного, можемо визначити мінімальний набір елементів для імплементації системи захисту інформації за основі моделі WHaaS:

- Зовнішній сегмент;
  - Сенсори Wi-Fi.
- Внутрішній сегмент;
  - VPN сервер;
  - Сервер командного центру;
  - База даних;
  - Сервер аналізу даних;
  - Сервер застосунку.

2.4.2. Комунікація елементів зовнішнього сегменту моделі WHaaS

Використання VPN сервера дозволяє забезпечити комунікацію між хмарною інфраструктурою, яка повинна знаходитись у приватному мережевому сегменті і сенсорами, які не мають публічних адрес.

VPN серверу повинна бути присвоєна публічна адреса, оскільки він повинен бути доступний з будь-якої точки планети або ж із визначених мереж. Залежно від вибраного VPN сервера повинні бути відкриті визначені TCP/IP порти і закриті усі інші. Потужність VPN сервера визначатиметься кількістю елементів зовнішнього сегменту.

Як тільки будь-який елемент буде підключений до VPN сервера, йому одразу ж стануть доступні усі доступні ресурси приватної підмережі хмарної обчислювальної мережі.

Після того, як зовнішні елементи стали доступні у приватній підмережі хмарної обчислювальної мережі, сенсори матимуть можливість читати і записувати дані в БД. Сенсори безперервно забезпечуватимуть збір даних про події в діапазоні частот IEEE 802.11 і записують їх в БД.

Щоб доступитись до сервера БД необхідно підключитись до мережі за допомогою VPN сервера. Залежно від обраного типу БД, на робочій станції, на якій розгорнута БД повинні бути відкриті визначені TCP/IP порти для комунікації з нею і закриті всі інші. Потужність сервера БД визначається кількістю даних, які надходять на запис.

У кожного програмного продукту є свій цикл життя, що стосується як власних, так і тих, що завантажуються з зовнішніх репозиторіїв. Більшість атак спрямовані на системи з застарілим програмним забезпеченням. Контроль за актуальністю програмних засобів здійснюється через командний центр, де формуються як регулярні, так і нерегулярні команди від користувачів.

Для безпечної взаємодії, на зовнішніх елементах дозволено лише віддалене з’єднання через приватну мережу в середині VPN. Це передбачає відкриття лише визначених TCP/IP портів для комунікації з сервісом, який забезпечує віддалене з’єднання, а всі інші порти TCP/IP повинні бути закриті. Наприклад, для операційної системи Linux таким сервісом є Secure Shell (SSH), який використовує порт 22/TCP.

В момент коли користувач заходить на веб застосунок, сервер додатку розпочинає зв’язуватись із БД. Дані вибираються з БД і після обробки відправляються до користувача.

Коли користувач вирішив виконати нерегулярну команду на сенсорах, перед усім він повинен зайти на користувацький веб-інтерфейс і сформувати свої вимоги. Після підтвердження дані про зміни відправляються на командний центр.

Залежно від обраної комунікаційної платформи, на робочій станції, яка виступає в ролі командного центру, повинні бути відкриті визначені TCP/IP порти, для комунікації з ним і закриті всі решта.

Будь-який хмарний сервіс повинен мати користувацький інтерфейс для представлення та керування інформацією. Для доступу до зібраних і оброблених даних користувач використовує клієнтський інтерфейс, який вибирає дані з бази даних та відображає їх агрегацію. На основі постійно оновлюваних даних з бази,

яку живлять сенсори, сервер обробки даних визначає присутність або відсутність зловмисника у спостережуваному етері.

Представлення найважливіших даних на одній сторінці стало тенденцією у сучасних постачальників хмарних технологій. Такими даними для моделі WHaaS можуть бути:

- Кількість ідентифікованих пристроїв IEEE 802.11;
- Потужність сигналу від точок доступу, які контролюються;
- Виявлені атаки;
- Результати перевірки працездатності зовнішніх елементів.

Концепцію такої сторінки представлено на рис. 2.3.

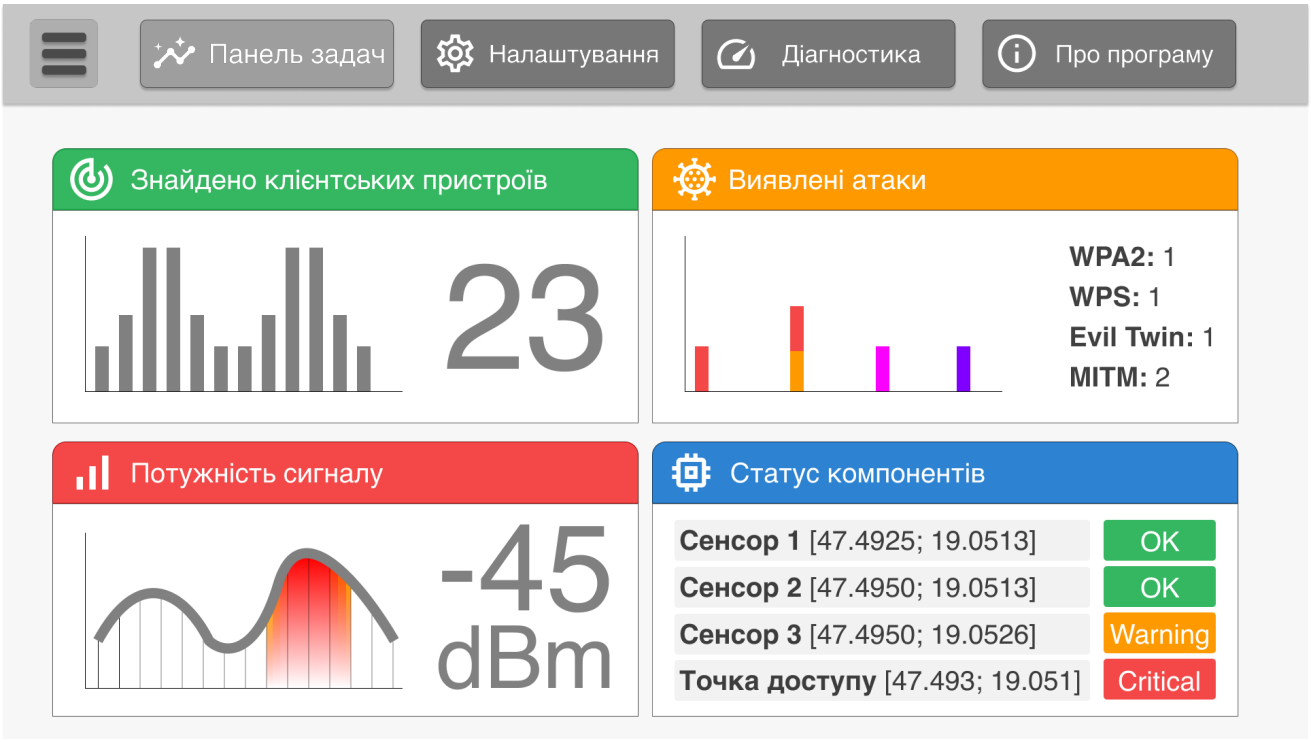


Рис. 2.3. Концепція користувацької веб сторінка моделі WHaaS (панель задач).

Навіть, якщо зовнішні елементи володіють функцією автоконфігурації, користувач повинен мати можливість задавати конфігурацію на власний розсуд. Окрім того, повинна бути доступна можливість деталізованого моніторингу (рис. 2.4).

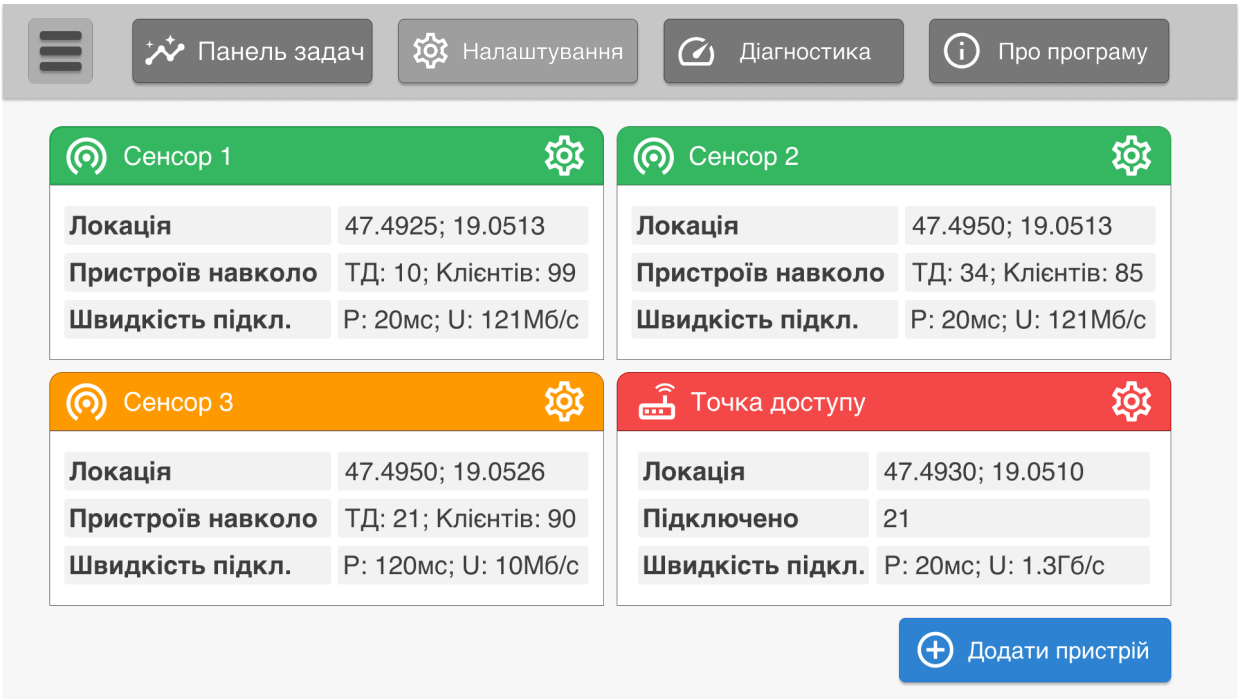


Рис. 2.4. Концепція користувацької веб сторінки моделі WHaaS (панель налаштувань)

Для того, щоб застосувати налаштування вручну, користувач повинен підключитись до користувацької веб сторінки і задати потрібні конфігурації. Після того, як користувач натисне кнопку для застосування змін, дані будуть передані на командний центр, на якому буде згенеровано сценарій для зовнішнього елементу, після чого даний сценарій буде переданий і виконаний на зовнішньому елементі (рис. 2.5).

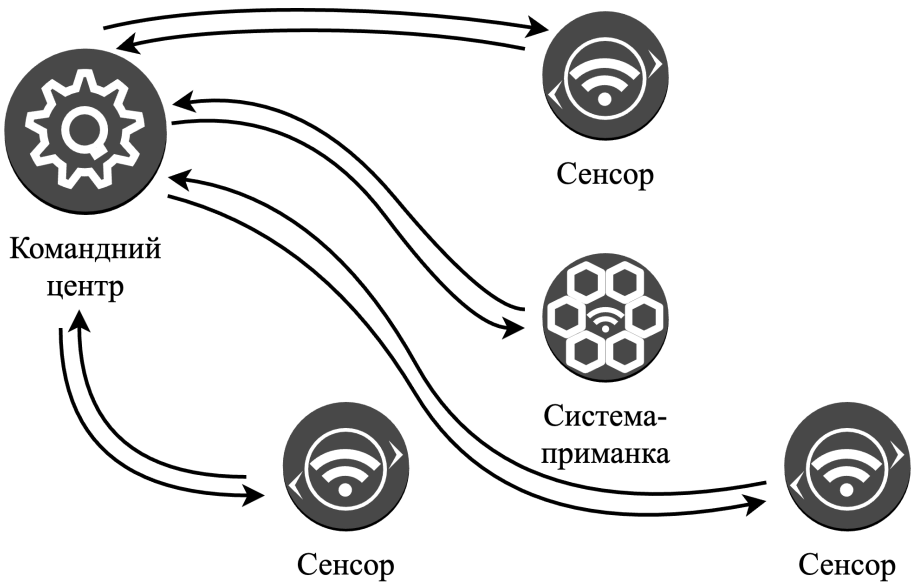


Рис. 2.5. Процес застосування налаштувань на зовнішніх елементах

Загалом, із всього вище сказаного можемо навести загальну архітектуру системи і комунікацію між її елементами (рис. 2.6).

Як можна побачити, на рис. 2.6 існує декілька можливих комунікаційних потоків, за допомогою яких дані циркулюють всередині системи. Перший – процес адміністрування сенсорів. Для цього і адміністратору, і сенсорам необхідно бути підключеними до VPN сервера, що дасть змогу встановити комунікацію з командним центром.

Другий – процес запису даних сенсором у БД. Після встановлення з'єднання із VPN сервером, сенсор отримує доступ до БД, куди може записати сирі дані. Це приводить нас до третього комунікаційного потоку – процесу обробки та аналізу даних. На цьому етапі сирі дані проходять обробку і готуються до відображення на клієнтському застосунку.

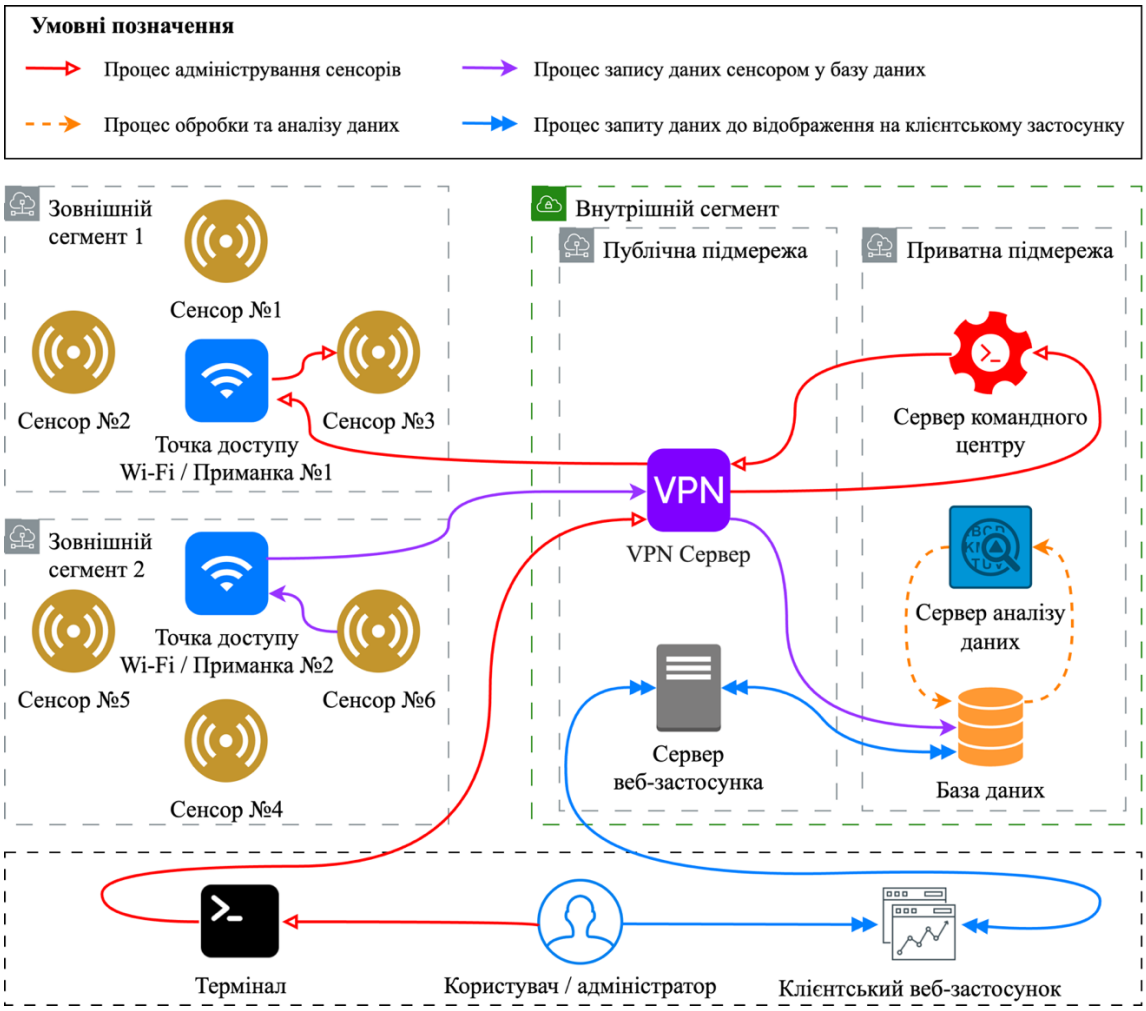


Рис. 2.6. Базові елементи та комунікація елементів системи захисту мереж стандарту IEEE 802.11 на основі моделі WHaaS

Четвертий – процес запиту даних до відображення на клієнтському застосунку. На цьому етапі користувач підключається до сервера веб-застосунка, який знаходиться у публічній підмережі внутрішнього сегменту. Оскільки сервер веб-застосунку знаходиться у публічній підмережі то і доступ до нього може без будь-яких обмежень.

2.4.3. Аналіз та вибір платформи для зовнішніх елементів системи-приманки та системи виявлення вторгнень для мереж стандарту IEEE 802.11

Базові маршрутизатори не можуть відігравати якусь іншу роль окрім надання доступу до певного мережевого ресурсу. Встановлення додаткового програмного забезпечення на маршрутизатор часто є неможливим через архітектурну несумісність або ж недостатню кількість пам’яті. Дану проблему можна вирішити за допомогою будь-якого персонального комп’ютера за наявності безпровідної мережевої карти і таких програмних пакетів як, наприклад, *hostapd* та *isc-dhcp-server,* якщо це стосується операційної системи *Linux* [65—66]. Та використовувати такі комп’ютери недоцільно через великі розміри, ціну та надлишковість обчислювальних ресурсів.

Існує велика кількість платформ, на базі яких можна розгорнути Wi-Fi ТД, СВВ чи СП, прикладом таких платформ можуть бути однопалатні комп’ютери чи навіть мікроконтролери. Вибір платформи залежить від потрібної обчислювальної потужності, розміру чи можливості кастомізації.

На рис. 2.7 зображено одноплатний комп’ютер Raspberry Pi.

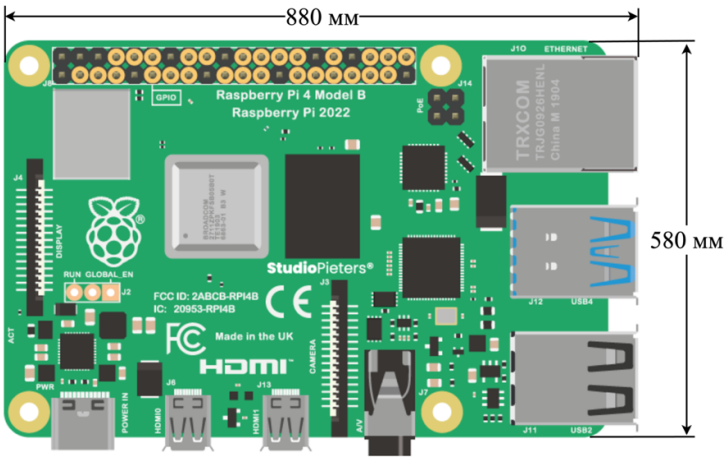


Рис. 2.7. Зовнішній вигляд та розмір одноплатного комп’ютера Raspberry Pi 4

На сьогоднішній день Raspberry Pi пережив вже п’яте оновлення і володіє такими характеристиками, як процесор ARM із тактовою частотою 2,4 ГГц та 2, 4 чи 8 гігабайт оперативної пам’яті. Для зберігання даних використовується Micro-SD накопичувач. На такий комп’ютер може бути встановлено операційні систем Windows або Linux [67].

Одноплатні робочі станції відомі своєю дешевизною та компактністю і не вирізняються значною потужністю, яка, своєю чергою, часто є надлишковою. Тому такі рішення цілком задовольняють проекти, які не передбачають використання значних ресурсів.

Наявний в Raspberry Pi інтегрований адаптер стандарту Ethernet може бути використаний як точка виходу в мережу інтернет, а додатковий безпровідний адаптер – як точка підключення користувачів.

Оскільки одноплатний комп’ютер Raspberry Pi дозволяє на своїй базі розгорнути такі операційні системи як Windows чи Linux, то відповідно на їх основі може бути розгорнута СВВ.

Такий варіант може водночас вирішити проблему додаткового ПЗ на маршрутизаторах, оскільки й сама може виконувати роль маршрутизатора і проблему надлишковості обчислювальних ресурсів.

Існують також і дещо менші за розміром варіанти виконання одноплатних комп’ютерів. До прикладу Raspberry Pi Zero, які володіють меншою потужністю, як от процесор з тактовою частотою 1ГГц та 512 МБ оперативної пам’яті (Рис 2.8).

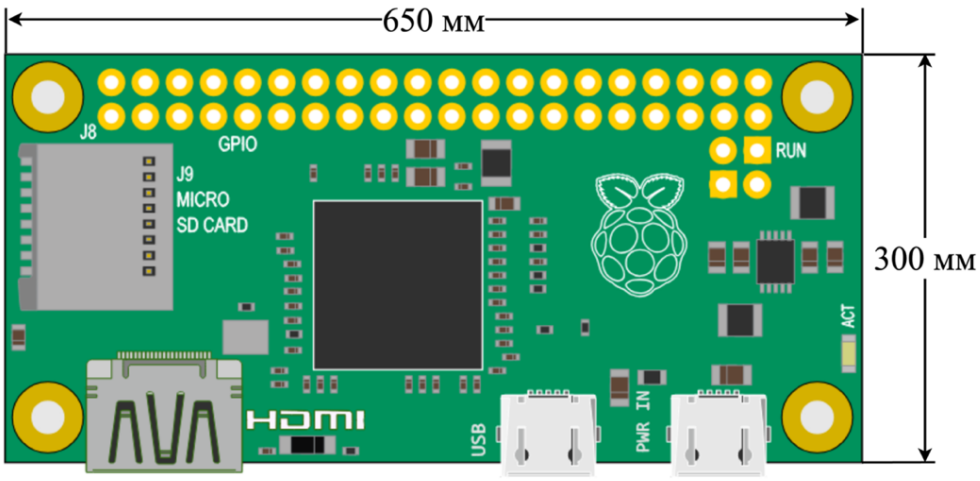


Рис. 2.8. Зовнішній вигляд та розмір одноплатного комп’ютера Raspberry Zero W2

Хоч одноплатні комп'ютери вже можуть вирішити доволі багато проблем з перехопленням інформації і обчисленнями, та для вирішення задач збору інформації з радіо ефіру їх така кількість ресурсів буде надлишковою, окрім того, більшість можливостей операційних систем в задачах виявлення вторгнень і моніторингу задіяні не будуть.

В сучасних IoT пристроях використовуються відносно не великі і дешеві мікроконтролери. Вони дозволяють збирати дані з навколишнього середовища і передавати їх на сервер для подальшої обробки. Деякі сучасні мікроконтроллери сімейства ESP від компанії Espressif Systems вже мають інтегровані Wi-Fi та Bluetooth модулі [68]. На рис 2.9 зображено мікроконтролер ESP32 WROOM із зазначеними розмірами.

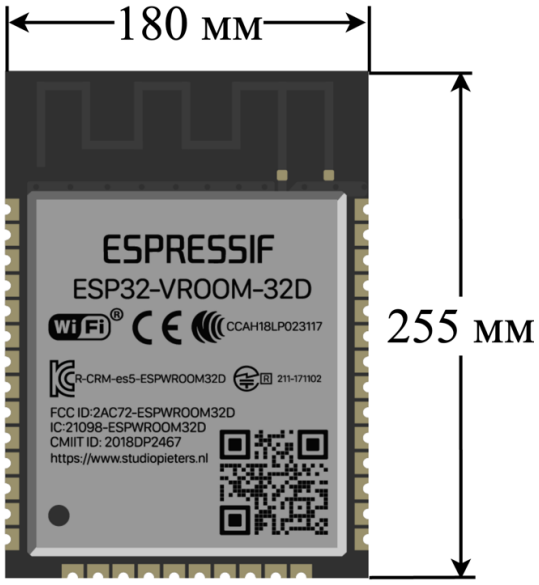


Рис. 2.9. Зовнішній вигляд мікроконтролера ESP32 та його розміри

Мікроконтролери не вимагають наявності операційної системи, що забезпечує їх високу енергоефективність. Програмне забезпечення для них може бути розробленим за допомогою таких мов програмування як C/C++ чи навіть спеціалізованої версії мови програмування Python. Варто врахувати, що при розробці рішення на базі мікроконтролерів ESP необхідно розробляти власну компоновку з електронних компонентів, в залежності від поставлених задач.

У вищеописаній мікро-сервісній архітектурі моделі WHaaS, елементи зовнішнього сегменту потребують окремих обчислювальних одиниць. Якщо і СП,

і сенсори виявлення вторгнень розгорнуті на одному і тому ж типові апаратного забезпечення, то завадостійкість такого комплексу зростає в рази, оскільки елементи зовнішнього сегменту можуть бути взаємозамінними. Наприклад, при відмові одного елементу, командний центр може запустити процес перебудови кластеру і, до прикладу, замінити фунціонал одного із сенсорів ідентифікації вторгнень на приманку. З іншого боку не всі елементи вимагають однакового апаратного забезпечення.

Для створення СП або ТД необхідне апаратне забезпечення із наявним мережевим адаптером Ethernet та Wi-Fi, для організації виходу в мережу Інтернет та можливість підключення клієнтських пристроїв, оскільки необхідно створити імітацію легітимної системи. Отже, такою платформою може бути будь-який одноплатний комп'ютер із можливістю встановлення операційної системи Linux і мережевим адаптеро.

Для створення сенсора, як елемента СВВ в мережах IEEE 802.11 не потрібно ніякого додаткового додаткового обладнання окрім мережевої карти Wi-Fi, оскільки вони працюють в режимі моніторингу. І в таких мікроконтролерах, як ESP32 вже є інтегрований мережевий інтерфейс Wi-Fi, який дозволяє створити ТД, підключитись до мережі чи здійснювати моніторинг. Та на відміну від одноплатних комп'ютерів мікроконтролери володіють значно меншою обчислювальною потужністю, до прикладу, якщо мікроконтролер ESP32 (Додаток 3, файл intercept_beacon_esp32.py) може перехопити близько 10 пакетів-маячків за хвилину від однієї ТД, то одноплатний комп'ютер Raspberry Pi перехоплює близько 600 (Додаток 3, файл intercept_beacon_raspberry.py).

Отже, для вирішення задач з імітації Wi-Fi інфраструктури і виявлення вторгнень оптимальним є застосування одноплатних комп'ютерів.

2.5. Висновки до розділу 2

Доволі важливим критерієм для будь-яких СП є їх толерантність до атак. Толерантність до атаки – це метрика, яку не просто виміряти і ця тема потребує додаткових досліджень, а саме розробки певної діагностичної моделі. У визначення

толерантності до атак повинні бути задіяні компоненти моніторингу, реєстрації подій та аналізу інцидентів. Не менш важливим є можливість до швидкого повторного налаштування СП згідно поставлених задач. Тому, в даному розділі було розроблено та описано життєвий цикл СП для мереж стандарту IEEE 802.11, що дозволить гнучко налаштовувати СП і тим самим застосовувати оптимальні налаштування відносно історичних даних.

Було розроблено та проаналізовано моделі порушника у бездротових мережах стандарту IEEE 802.11 для підприємства. Даний аналіз дозволяє краще розуміти імовірні ризики і відносно них розробляти методи їх протидії.

Також в цьому розділі було досліджено можливі демаскуючі ознаки з СП, а саме можливість виявлення приманки на канальному, мережевому та прикладному рівнях моделі OSI. Визначення демаскуючих ознак дозволять уникнути виявлення СП зловмисниками, що позитивно позначиться як на функціонуванні самих СП так і на безпеці усієї бездротової мережі Wi-Fi та інших пов’язаних мережевих ресурсів.

Розроблено концептуальну модель системи захисту інформації із застосуванням СП, а саме описано мінімальний набір, за допомогою якого можна реалізувати таку систему; регламентовано правила комунікації між елементами даної системи, а саме взаємодію зовнішніх елементів з VPN сервером, взаємодію зовнішніх елементів з БД, взаємодію командного центру із зовнішніми елементами, взаємодію сервера додатку з БД, взаємодію сервера додатку із командним центром, описано приклад взаємодії з користувачем. Для елементів зовнішнього сегменту СП та СВВ запропоновано обчислювальні платформи. Для вирішення проблем із масштабованістю розробленої системи запропоновано використання хмарних обчислень.

Обґрунтоване застосування одноплатних комп’ютерів для організації компонентної бази для зовнішніх елементів інфраструктури на базі моделі WHaaS

РОЗДІЛ 3. РОЗРОБЛЕННЯ ТА ОПТИМІЗАЦІЯ МОДЕЛІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ БЕЗДРОТОВИХ МЕРЕЖ СТАНДАРТУ IEEE 802.11 ІЗ ЗАСТОСУВАННЯМ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ І СИСТЕМ-ПРИМАНОК

3.1. Розроблення методики відслідковування зловмисників

Навіть після виявлення атаки, притягнення зловмисника до відповідальності є не легким завданням, оскільки атака може проводитись поза контрольованою зоною. У випадку з атакою на протоколи бездротової безпеки WPA/WPA2 зловмиснику всього лиш потрібно перехопити один пакет, що займає не більше однієї хвилини. Та особливості стандарту IEEE 802.11, які дозволяють зловмисникам проводити атаки на них можуть допомогти в пошуку пристрою, який брав участь в атаці, що в свою чергу може привести до зловмисника [69].

3.1.1. Особливості пошукових пакетів у стандарті IEEE 802.11, як механізму повторного підключення до мережі

Якщо користувацький пристрій вже був коли-небудь підключений до будь-якої бездротової мережі стандарту IEEE 802.11, то дані про підключення вже залишились на його пристрої. Винятком може бути ситуація коли користувач видалив інформацію про мережу з пристрою або ж в налаштуваннях операційної системи встановив параметр, який забороняє запам’ятовувати налаштування бездротових мереж Wi-Fi.

Така особливість стандарту IEEE 802.11 дозволяє клієнтам з легкістю продовжити роботу з ТД навіть після того, як користувач покинув зону її дії. Це працює через те, що коли клієнтські пристрої не підключені до жодної з мереж, активується режим пошуку відомих йому точок доступу. На пакетному рівні це організовано таким чином, що клієнтські пристрої надсилають пошукові пакети (Probe Request) в мережу і за наявності ТД в радіусі дії пристрою він використовує вже наявні на пристрої дані для авторизації (рис. 3.1).

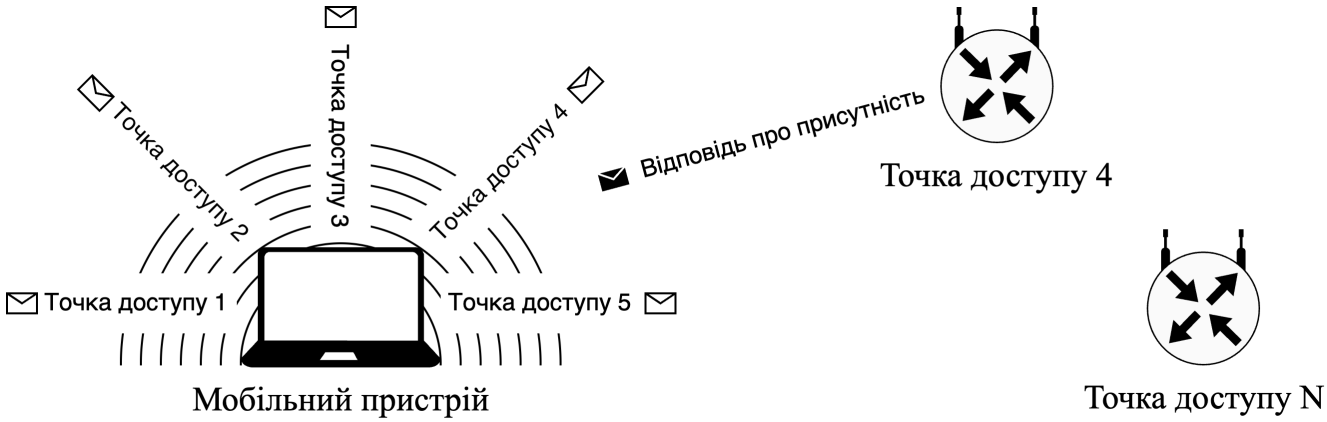


Рис. 3.1. Пошук точки доступу для подальшого підключення за допомогою пошукових пакетів

Якщо ТД відповіла пакетом про присутність (Probe Response) у етері, то відбудеться спроба процесу автентифікації (Рис. 3.2).

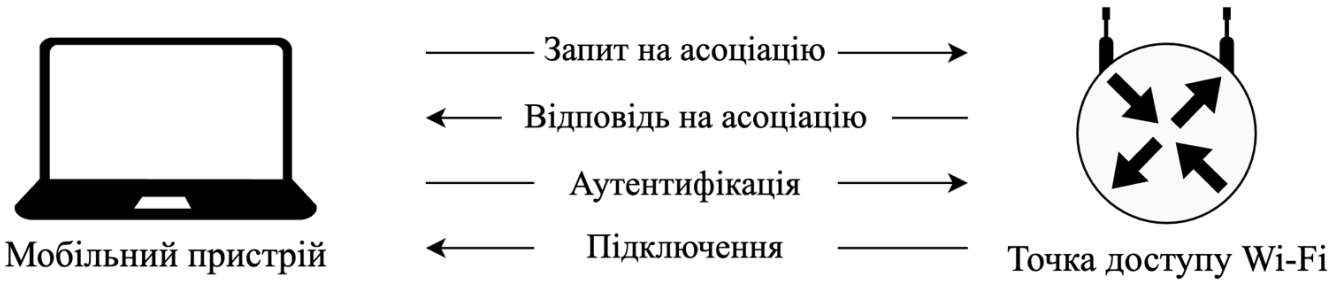


Рис. 3.2. Процес автентифікації на доступ до мережі після відповіді точки доступу про присутність у етері

Щоб побачити пошукові пакети у етері, не потрібно володіти спеціальним обладнанням – необхідно всього лиш активувати режиму моніторингу мережевої картки Wi-Fi. Такою особливістю часто користуються зловмисники для віднайдення ідентифікатора мережі, у випадку якщо він прихований. Клієнтський пристрій надсилає у етер певну кількість пошукових пакетів, після чого зловмисник їх перехоплює і перебирає ідентифікатори при спробах підключення до мережі.

Та варто підмітити, що зловмисники є також користувачами бездротових мереж і зазвичай, навіть у пересічного користувача мережі Інтернет, може бути з собою ще декілька пристроїв, які працюють за допомогою мережі Wi-Fi. Це можуть бути смартфони, розумні годинники та інші IoT пристрої. Коли зловмисники приходять у зону покриття своєї цілі то його пристрої будуть надсилати пошукові

пакети в етер. У кращому випадку для протидії буде ідеально, якщо пристрій, з якого здійснюється атака, вже був підключений до якоїсь бездротової мережі Wi-Fi, у такому випадку окрім виявлення атаки і прив'язки її до пристрою з певною MAC адресою ми отримаємо ще дані про те, до яких мереж зловмисник підключався раніше. Звісно, зловмисник може використовувати, так звану, одноразову операційну систему, яка завантажується із флеш накопичувача і після перезавантаження усі налаштування скидаються. Та як вже згадувалось вище, пристрій атаки з високою імовірністю буде не єдиним пристроєм зловмисника. Таким чином збір пошукових пакетів з інших пристроїв, які було ідентифіковано в тому ж секторі моніторингу, може надати більше інформації про зловмисника (Рис. 3.3).

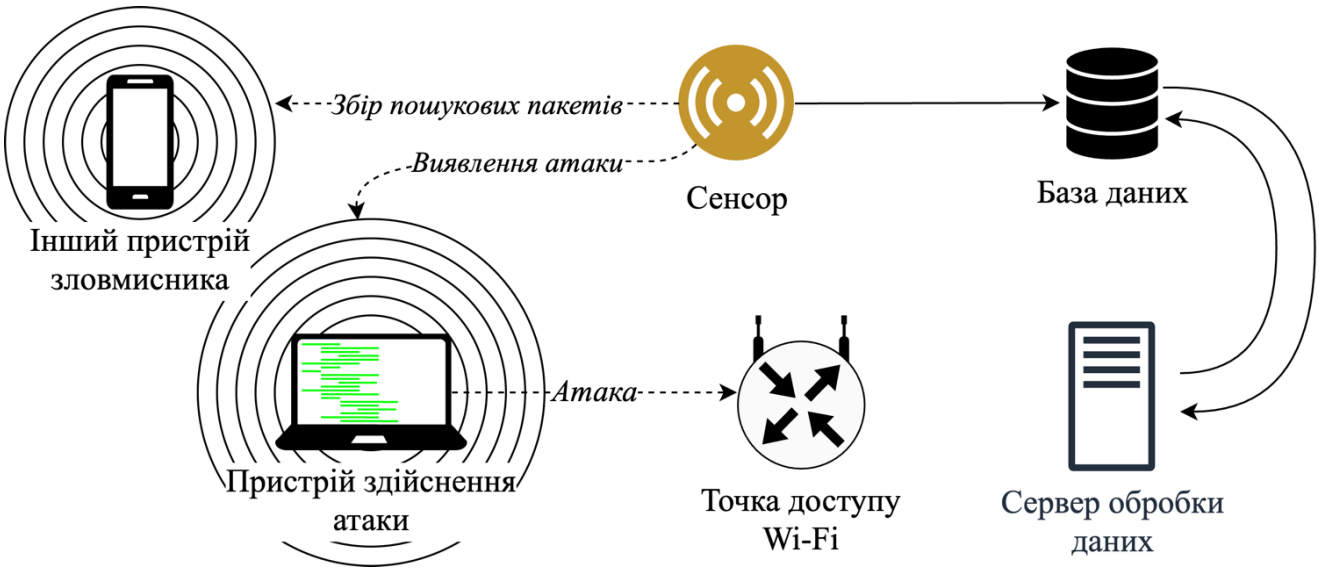


Рис. 3.3. Виявлення пошукових пакетів з пристроїв зловмисника

У запропонованій вище моделі WHaaS для виявлення вторгнень пропонується використання незалежних сенсорів. Через певний канал комунікації сенсор передає службові дані, до яких відноситься інформація про виявлення атак, пристрої, які було ідентифіковано поряд з пристроєм з якого здійснювалась атака, та мережі до яких ці пристрої були раніше підключені [70—71].

3.1.2. Виявлення попередніх місць перебування зловмисника

Wardriving – це діяльність, при якій людина подорожує в автомобілі або іншому транспортному засобі, зазвичай з комп'ютером і спеціалізованою апаратурою, з метою пошуку та ідентифікації бездротових мереж Wi-Fi. Wardriving поєднує дві англійські слова: "ward" (обхід, мандрівка) і "driving" (їзда, водіння), оскільки основна ідея полягає в тому, щоб об'їжджати територію, шукаючи активні Wi-Fi мережі.

Головна мета вищеописаної активності – це знайти та записати інформацію про доступні Wi-Fi мережі, включаючи їхні ідентифікатори (SSID), рівень сигналу, шифрування, геолокацію та інші параметри. Сьогодні існують ресурси, на яких у дослідники діляться такими даними. Одним із таких сервісів є Wireless Geographic Logging Engine (WiGLE) [72]. Сервіс WiGLE – це ресурс для обміну інформацією про ТД Wi-Fi зі всього світу. Користувач може зареєструватись на даному веб ресурсі і завантажити такі дані як GPS координати, SSID, MAC адресу, тип захисту та інші метадані про знайдені ним ТД для обміну цією інформацією з іншими користувачами.

Як було вище згадано, перехоплені пошукові пакети з пристроїв зловмисника можуть містити дані про ті ТД, до яких вони були раніше підключені. Після виявлення атаки такі дані можуть бути передані на сервер обробки даних системи WHaaS. Імена мереж, до яких раніше були підключені пристрої зловмисника, передаються на сервіс wigle.net, який повертає масив з даними про розташування мереж. Однак разом з потрібними даними ми отримуємо велику кількість надлишкової інформації, такої як канал, на якому працює ТД, інше інше, що може збентежити. Після фільтрації ці дані повинні бути відсортовані за локаціями. Це дозволить отримати масив даних з кожної локації, у якій було знайдено ТД з параметрами, що були зібрані з пристроїв зловмисника.

Цілком імовірною є ситуація, що зловмисник приїде з іншого міста або навіть з іншої країни. Та все ж, вищий пріоритет, очевидно, буде мати сектор, в якому знаходиться атакована ТД, навіть якщо в іншій територіальній одиниці буде ідентифіковано більшу кількість точок доступу. Врахування такого фактору є

важливим, оскільки система захисту може знаходитись у місті, яке за розміром менше аніж, наприклад, столиця країни.

Отримавши набір з координат, можна приблизно оцінити відстані між ними, для початку на поточній територіальній одиниці.

Для того, щоб дізнатись приблизну відстань між точками необхідно застосувати формулу обчислення декартової відстані на площині (3.1)

$$d = \sqrt{(\phi_2 - \phi_1)^2 + (\lambda_2 - \lambda_1)^2} \tag{3.1}$$

Де λ – довгота (град.), ϕ – широта (град.).

Після того як відстані усіх точок в територіальній одиниці між собою буде знайдено, необхідно просумувати їх між собою з метою визначення густини розкиду точок доступу (3.2).

$$D = \sum d_i = (d_1 + d_2 + \cdots + d_n) \tag{3.2}$$

Згідно з формулою (3.2) $D \to 0$, оскільки чим ближче між собою розташовані ТД, тим меншим буде значення D. Відповідно, чим менше значення D тим більшою є імовірно того, що визначено територіальну одиницю в якій мешкає зловмисник. Пріоритет зазначено в (3.3).

$$Pr = [D_{min}, \dots, D_{max}] \tag{3.3}$$

На клієнтських пристроях часто залишаються дані про ТД, до яких клієнти лише намагались підключитись, випадковим чином відгадуючи пароль. Опишемо ситуацію: клієнт намагається доступитись до мережі Інтернет і на своєму пристроєві розпочинає пошук всіх можливих точок доступу, які знаходяться поблизу. Декілька з них, забороняють подальшу взаємодію через, наприклад, невдалу авторизацію. В даному випадку, дані, з якими клієнт намагався авторизуватись, вже збереглись на його пристрої, і якщо, в майбутньому, ці ТД будуть ідентифіковані сенсорами, то локації, де вони знаходяться, можна надати високий коефіцієнт імовірності попереднього перебування зловмисника.

Володіючи даними про територіальне розташування точок доступу, які імовірно були відвідані зловмисником, можна створити граф із вагами (кількість знайдених точок доступу) і відстань до СП (рис. 3.4).

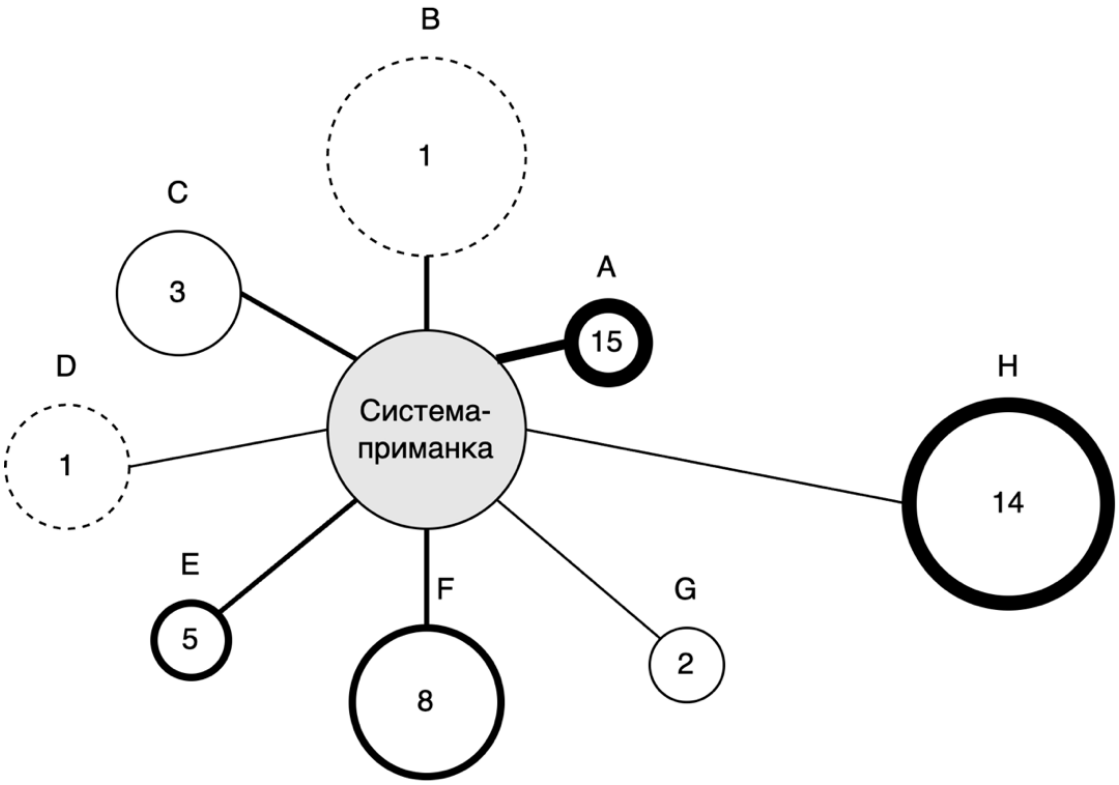


Рис. 3.4. Візуалізація графу територіального розташування точок доступу зібраних з клієнтських пристроїв зловмисника

Додаткова візуалізація графу дозволить зрозуміти, на яких територіальних одиницях варто зосередитись. Товщина лінії з'єднання – це сила зв'язку, під якою розуміється відстань від СП до територіальної одиниці і обчислюється за допомогою тієї ж формули 3.1. Радіус кола – це розмір територіальної одиниці. Товщина лінії обведення кола, як і цифра в середині – говорить про кількість знайдених точок доступу з іменами, зібраними з клієнтського пристрою зловмисника.

Відповідно до рис. 3.4, хоч і вузли E, F, H є доволі імовірними локаціями імовірного перебування зловмисника, та все ж варто зосередити увагу на територіальну одиницю *A*, оскільки вона знаходиться найближче до СП, є малою територіальною одиницею і кількість знайдених точок доступу у ній є найбільшою серед інших. Як вже згадувалось вище, у мегаполісах є велика концентрація точок

доступу Wi-Fi і цілком імовірно, що у деякому великому місті будуть усі ТД, які було ідентифіковані на пристрої зловмисника. Також варто розуміти, що ідентифікатор мережі Wi-Fi не є унікальним, тож імовірні хибні знахідки, особливо у великих територіальних одиницях.

Окрім віддаленості від СП, потрібно зважати на унікальність імен точок доступу, зісканованих з пристрою зловмисника. Наприклад, в локації *H* було знайдено 14 точок доступу із заданим для пошуку іменем і 10 з них є унікальними, а в локації *A* – 15 і унікальними з них є, наприклад, 5. Та існує ще один параметр, який може надати більше інформативності, аніж усі вище описані. Таким параметром є одна точка або група ТД з унікальними іменними ідентифікаторами мережі, які не було знайдено ні в одній територіальній одиниці (рис. 3.5).

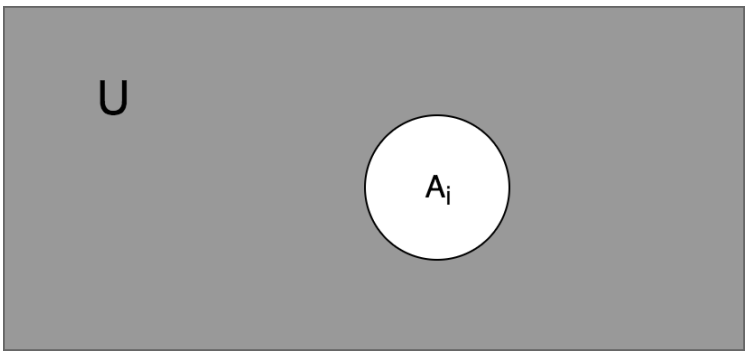


Рис. 3.5. Унікальний елемент в множині значень

Набір з усіх імен точок доступу з усіх локацій – це універсальна множина $U = A \cup B \cup C \cup D \cup E \cup F \cup G \cup H$. Множина, що містить всі елементи універсальної множини без елементу A_i, який в даному випадку є унікальним елементом, називається абсолютним доповненням A_i і позначається як $\overline{A_i}$ або A^C або C_A. Формально: $\overline{A_i} = A_i^C = U - A_i$.

3.2. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11

Підґрунтя для розробки критеріїв діагностичної моделі СП бездротової мережі стандарту IEEE 802.11 базується на оцінці складності обхіду методів їх захисту. Як вже було вказано у попередніх розділах, кожен з методів захисту може

бути компрометований в залежності від навичок та технічного обладнання зловмисника.

ТД, а в нашому випадку СП, яка має недостатній або ж відсутній захист, може легко стати об'єктом атаки для осіб, які мають намір скористатися безкоштовним доступом до Інтернету або ж викликати підозру у досвідчених зловмисників.

3.2.1. Загальна діагностика системи-приманки для мережі стандарту IEEE 802.11

Як вже було зазначено вище – найслабшим із протоколів бездротової безпеки є WEP, а отже його використання ТД імовірно буде сприйматись як помилка з боку адміністратора мережі або наявність в мережі застарілого обладнання.

Певна комбінація факторів може значно знизити ймовірність взаємодії зловмисника з СП. Наприклад, у більшості конфігурацій ТД обов'язково присутній підключений клієнт, без чого атака стає неможливою. Збираючи метадані з діапазону частот 2.401 – 2.483 ГГц за допомогою мережевої картки, що працює в режимі моніторингу, зловмисник може отримати повні або часткові дані про ТД і її клієнтів.

Вразливість, згадана вище, протоколів бездротової безпеки WPA/WPA2 може бути використана лише в разі наявності підключеного клієнта. Винятком є випадок конфігурації з увімкненим механізмом WPS, атака на який не потребує наявності підключеного клієнта, оскільки перебір PIN-коду відбувається відносно лише ТД.

Для здійснення атаки на протоколи бездротової безпеки WPA/WPA2 зловмисникові потрібно отримати спеціальний пакет рукостискання між ТД і клієнтом, який знає ключ до мережі. Цей пакет перехоплюється зловмисником у момент підключення клієнта до мережі.

У випадках конфігурацій, де присутні механізми, такі як прихований SSID, фільтрування MAC адрес або ввімкнений протокол бездротової безпеки WPA2 з вимкненим WPS і відсутні підключені клієнти, ситуація ускладнюється. В таких випадках зловмисникові доведеться очікувати на появу клієнта або розпочинати атаку грубої сили для отримання імені ТД або MAC адреси. Щодо MAC адрес, їх

імовірніше отримати в процесі перебору, оскільки кількість можливих MAC адрес дорівнює 16^6, тоді як для SSID можливі варіанти обмежені лише довжиною рядка від 1 до 32 символів, які можуть бути вибрані з таблиці UTF-8.

Для конфігурації СП з використанням протоколів бездротової безпеки WPA/WPA2 повинен бути встановлений ключ, який може бути віднайдений під час перебору за загальнодоступними словниками. Виробники сучасних маршрутизаторів запроваджують механізм очікування (timeout) після певної кількості невдалих спроб, щоб протидіяти атаці грубої сили на механізм WPS. Такий функціонал може унеможливити доступ зловмисника до СП.

На основі викладених вище даних сформулюємо таблицю істинності комбінацій механізмів захисту бездротових мереж стандарту IEEE 802.11 (табл. 3.1) та побудуємо блок-схему алгоритму дослідження СП на можливість бути атакованою (рис. 3.6).

Таблиця 3.1.

Можливі комбінації механізмів захисту бездротових мереж стандарту IEEE 802.11

№	Open	WEP	WPA	MAC фільтр	Прихований SSID	WPS	Присутність клієнтського пристрою
1	+	-	-	-	-	-	Не є необхідним
2	+	-	-	+	-	-	Необхідна
3	+	-	-	-	+	-	Необхідна
4	+	-	-	+	+	-	Необхідна
5	-	+	-	-	-	-	Не є необхідним
6	-	+	-	+	-	-	Необхідна
7	-	+	-	-	+	-	Необхідна
8	-	+	-	+	+	-	Необхідна
9	-	-	+	-	-	-	Необхідна
10	-	-	+	+	-	-	Необхідна
11	-	-	+	-	+	-	Необхідна
12	-	-	+	+	+	-	Необхідна
13	-	-	+	-	-	+	Не є необхідним
14	-	-	+	+	-	+	Необхідна
15	-	-	+	-	+	+	Необхідна
16	-	-	+	+	+	+	Необхідна

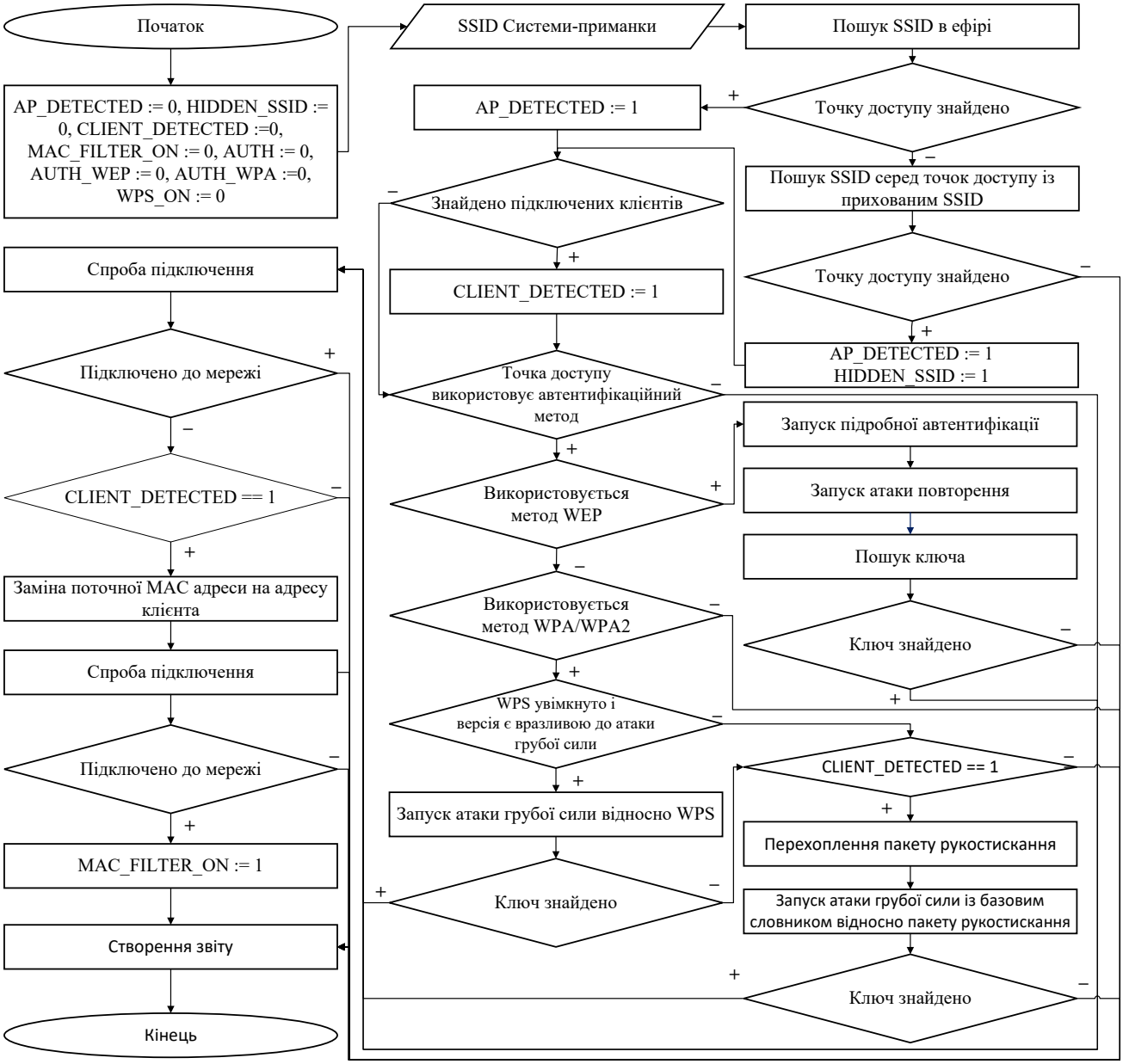


Рис.3.6. Блок-схема алгоритму дослідження системи-приманки на можливість бути атакованою

На рис. 3.6 до уваги не береться механізм захисту мережі WPA3, оскільки існує перехідний механізм для пристроїв, які його не здатні підтримувати, а отже він може бути понижений до WPA2.

Задля оцінки складності подолання умовного захисту СП зробимо їх оцінку за рахунок коефіцієнтів методу аналізу ієрархій, на основі таких критеріїв, як час подолання захисту, наявність відповідного апаратного забезпечення, яке доведеться використати зловмиснику (табл. 3.2).

Таблиця 3.2

Оцінка складності подолання умовного захисту системи-приманки

Оцінковий критерій / Метод захисту	Час подолання	Наявність відповідного апаратного забезпечення	Складності під час проведення атаки
WEP	t ≈ 30 хв.	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Якщо клієнт не підключений до ТД, зловмиснику потрібно провести атаку підробної автентифікації
WPA/WPA2	5 хв > t > ∞	Для реалізації даної атаки необхідно мати мережеву картку за допомогою якої можна відправити пакет деавтентифікації.	Якщо клієнт не підключений до мережі, то атака не може бути здійснена, оскільки перехоплення пакету рукостискання є не можливим. Атака набуває складності із збільшенням кількості символів у ключі і кількості
WPA3	10хв > t > ∞	Справджується все те ж що і для атаки на WPA/WPA2. Окрім того необхідно, щоб перехідний механізм для пристроїв WPA2 був активований (WPA2/WPA3).	Справджується все те ж що і для атаки на WPA/WPA2. У деяких випадках потрібен доступ до пристрою з якого відбувалось підключення до мережі
MAC Фільтрація	1 хв > t > ∞	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Проведення атаки ускладнюється, якщо до мережі не підключені клієнти, в такому випадку потрібно провести атаку грубої сили
Прихований SSID	1 хв > t > ∞	Для реалізації даної атаки достатньо	Проведення атаки ускладнюється, якщо до

		мати базову мережеву картку Wi-Fi	мережі не підключені клієнти
WPS	1 хв > t > ∞	Для реалізації даної атаки достатньо мати базову мережеву картку Wi-Fi	Проведення атаки ускладнюється, або є не можливим у випадку якщо версія WPS > 1

Цей метод дозволяє отримати співвідношення ваг шкал шляхом парних порівнянь з невеликим відхиленням [73—75]. В якості коефіцієнтів використовуються фактичні вимірювання або суб'єктивна думка. На виході отримується співвідношення ваг та індексу узгодженості.

У стандартному виконанні методу аналізу ієрархій оцінка будь-якої групи характеристик здійснюється за допомогою шкали коефіцієнтів від 1 до 9 (таб. 3.3). За допомогою цієї таблиці формується матриця ваги кожного з елементів в порівнянні один з одним (3.4).

$$N = \begin{vmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{12}^{-1} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}^{-1} & a_{2n}^{-1} & \cdots & 1 \end{vmatrix} \quad (3.4)$$

Таблиця 3.3

Шкала оцінки коефіцієнтів у методі аналізу ієрархій

Цифрове значення	Визначення
1	Рівне значення
3	Не значна перевага одного значення над іншим
5	Істотна перевага одного значення над іншим
7	Видима перевага одного значення над іншим
9	Абсолютна перевага одного значення над іншим
2,4,6,8	Середнє судження поміж двох суміжних суджень

На основі табл. 3.2—3.3 зробимо оцінку складності обходу механізмів захисту по відношенню одне до одного.

Таблиця 3.4.

Порівняння складності обходу механізмів захисту точки доступу Wi-Fi

Метод захисту	Коефіцієнт переваги/недоліку	Метод до порівняння
MAC Фільтрація	½	Прихований SSID
	5	WEP
	8	WPA/WPA2
	9	WPA3
	7	WPS
Прихований SSID	2	MAC Фільтрація
	5	WEP
	8	WPA/WPA2
	9	WPA3
	7	WPS
WEP	1/5	Прихований SSID
	1/5	MAC Фільтрація
	6	WPA/WPA2
	9	WPA3
	5	WPS
WPA/WPA2	1/8	Прихований SSID
	1/8	MAC Фільтрація
	1/6	WEP
	4	WPA3
	1/4	WPS
WPA3	1/9	Прихований SSID
	1/9	MAC Фільтрація
	1/9	WEP
	1/4	WPA/WPA2
	1/8	WPS
WPS	1/7	Прихований SSID
	1/7	MAC Фільтрація
	1/6	WEP
	4	WPA/WPA2
	8	WPA3

Для подальшої нормалізації матриці необхідно знайти суми коефіцієнтів для кожного зі стовпців N (3.5).

$$S_i = \sum_{i=1}^{n} a_i = a_{i1} + a_{i2} + \cdots + a_{in} \quad (3.5)$$

Використовуючи суми коефіцієнтів стовпців можна вивести нормалізовану матрицю $|N|$ (3.6)

$$|N| = \begin{vmatrix} \frac{1}{S_1} & \frac{a_{12}}{S_2} & \cdots & \frac{a_{1n}}{S_n} \\ \frac{a_{12}^{-1}}{S_1} & \frac{1}{S_2} & \cdots & \frac{a_{2n}}{S_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}^{-1}}{S_1} & \frac{a_{2n}^{-1}}{S_2} & \cdots & \frac{1}{S_n} \end{vmatrix} \quad (3.6)$$

Просумувавши коефіцієнти кожного рядка нормалізованої матриці і розділивши суму на кількість коефіцієнтів у рядку згідно з формулою (3.7), можна отримати вагу кожного з механізмів захисту.

$$x = \begin{bmatrix} \sum \frac{row_1}{n} \\ \sum \frac{row_2}{n} \\ \cdots \\ \sum \frac{row_k}{n} \end{bmatrix} \quad (3.7)$$

Отже, даний математичний апарат може дозволити оцінити і порівняти з між собою кожен із механізмів захисту. У випадку появи нових механізмів захисту таблиця буде коригуватись, а механізми захисту переоцінюватись експертом. На сьогодні механізм захисту WPA3 є найефективнішим, та все ще найрозповсюдженішим залишається WPA2, тож є необхідність зосередитись на деталізації оцінки цього механізму захисту.

3.2.2. Деталізація оцінки складності обходу умовного захисту системи-приманки із протоколами бездротової безпеки WPA/WPA2

Очікуваним результатом даного дослідження є отримання шкали складності P_k ключа WPA/WPA2 для СП бездротової мережі стандарту IEEE 802.11 для

кінцевого користувача на основі критеріїв a_{ij} матриці N, добутої методом аналізу ієрархій. Результатом правильної конфігурації СП виступають дані тесту t_{BF}, що прогнозує час перебору ключа за допомогою атаки грубої сили. Тест проводиться на основі даних зі словника D, а саме поточного словника d_i, результатом якого є набір $l_i - l_{i-1}$ унікальних ключів $l=\{k_1, k_2, \ldots, k_n\}$, та швидкості перебору ключів S, яка заміряється із певної еталонної системи. Порівнюючи даний метод за допомогою методів повної віртуалізації та віртуалізації на рівні операційної системи, буде вибрано середовище для проведення розподіленої атаки грубої сили, що дозволить знайти оптимальний метод оцінки умовної захищеності СП [76].

Існують дві модифікації даного методу: WPA2 Personal та WPA2 Enterprise. Основна різниця між ними полягає в управлінні ключами шифрування алгоритму AES. У випадку WPA2 Personal ключі зберігаються на кожному окремому пристрої користувача, що зазвичай використовується у мережах домашнього або невеликого офісу (SOHO). Ключ у механізмі WPA2 Personal є однаковим для всіх користувачів. Для корпоративних застосувань використовується динамічний ключ, індивідуальний для кожного користувача. За генерацію пар логін-пароль у WPA2 Enterprise відповідає спеціальний сервер, зазвичай RADIUS.

Протокол WPA2-PSK (Pre-Shared key) дозволяє мобільним пристроям обмінюватись даними з ТД за допомогою методу шифрування AES. У криптографії PSK – це ключ, який попередньо ідентифікується між двома вузлами за допомогою певного безпечного каналу, перш ніж він буде використаний. PSK отримується з ключа, використовуючи стандарт формування ключа на основі паролю PBKDF2 із алгоритмом хешування SHA1 як псевдовипадковою функцією. PSK є 32 байтним (256 бітним), часто відображається у вигляді 64 шістнадцяткових символів.

Стандарт PBKDF2 у свою чергу описується стандартом PKCS#5. У цьому випадку пароль повинен бути довжиною від 8 до 63 символів. Символи конвертуються у машинний код за допомогою таблиці кодування ASCII, а отже у паролі можуть використовуватись лише ці символи.

У PBKDF2 бінарний пароль використовується як ключ до функції HMAC. В якості випадкової додаткової інформації, так званої «солі», використовується

ідентифікатор ТД SSID. Сіль із значенням лічильника використовується для початкового входу в функцію HMAC. Після цього попередні вихідні дані використовуються як вхідні для наступних ітерацій, допоки не буде досягнуто 4096 обчислень HMAC. Зауважте, що хоча алгоритм HMAC може генерувати вихідні дані довільної довжини, у вашому випадку використовується формат з фіксованою довжиною 256 біт. В порівнянні з цим, хеш-функція SHA1 повертає вихідні дані лише 160 біт.

Розуміючи, що вихідні дані функції PBKDF2 використовуються як Pre-Shared Key (PSK), можна визначити PSK як Pairwise Master Key (PMK) безпосередньо у чотиристоронньому процесі рукостискання. (3.8):

$$PSK = PBKDF2(HMAC - SHA1 \mid Passphrase \mid SSID \mid 4096 \mid 256) \qquad (3.8)$$

Паролі, які використовують рядові споживачі сучасного обладнання Wi-Fi зазвичай, є не складними. Це може бути комбінація цифр від одиниці до дев'яти, літери на клавіатурі, які розташовані поряд, чи прості комбінації, як, наприклад дата народження. На сьогоднішній день існує велика кількість згенерованих словників з простими фразами, які використовуються рядовими користувачами. Ці словники доступні в мережі Інтернет або в спеціалізованих операційних системах для тестування на проникнення, таких як Black Arch, ArchStrike, Kali Linux та інші. [77].

Загальна кількість символів, яка може бути використана при створенні ключа дорівнює 95 (Табл. 3.5).

На основі проаналізованих популярних словників, автором формулюються найбільш доцільні комбінації наборів на основі таблиці 3.5 (Табл. 3.6).

Таблиця 3.5.

Символи доступні для задання ключа у протоколах бездротової безпеки WPA/WPA2

№	Набір символів	Кількість символів у наборі	Може використовуватись у словнику, як атомарна одиниця
1	[0-9]	10	+

2	[a-z]	26	+
3	[A-Z]	26	+
4	Спеціальні символи (`~!@#$ %^&*()+-=/|<>[]'".,?:;{})	32	+
5	Пробіл	1	-

Таблиця 3.6.

Комбінація символів на основі табл. 3.5

№	Комбінація символів	Кількість символів у наборі
1	[0-9] + [a-z]	36
2	[0-9] + [A-Z]	36
3	[a-Z] + [A-Z]	52
4	[0-9] + [a-Z] + [A-Z]	62
5	[0-9] + [a-Z] + [A-Z] + спеціальні символи	94
6	[0-9] + [a-Z] + [A-Z] + спеціальні символи + пробіл	95

Для того, щоб отримати доступ до мережі, зловмиснику необхідно перехопити пакет рукостискання і запустити процес дешифрування. Операція дешифрування пароля відбувається за допомогою центрального або графічного процесорів.

Після того, як відбувся перебір за словником і в ньому пароль не було знайдено, очевидно, що потрібно використати наступний словник. Якщо словник залишається тим же за розміром, але збільшується кількість символів для генерації ключів, то цілком доцільним буде виключати комбінації, які вже містяться у попередніх словниках (3.9).

$$D = \sum_{i=1}^{n} d_i = l_i - l_{i-1} \tag{3.9}$$

Де D – загальний словник, d – поточний словник, l – набір ключів у словнику (3.10):

$$l_i = \{k_1, k_2 ... k_n\} \tag{3.10}$$

Де k – ключ.

Якщо базовий словник не містить необхідного ключа, у такому випадку потрібно згенерувати новий словник. Після базового словника очевидно, що

наступним має бути словник, у якому забезпечено мінімальну довжину ключів і найменший набір символів з табл. 3.5. Це може бути словник, який складається лише з цифр. Як видно з формули 3.9, ті ключі, які вже було використано в базовому словнику, не повинні повторно використовуватись.

Якщо було опрацьовано словник, у якому 108 варіантів ключів, згенерованих з мінімального набору символів, ключ не буде знайдено, тоді наступний словник буде згенеровано із кількістю ключів 109 і з тим же ж мінімальним набором символів (тобто, це комбінація символів від 000000000, до 999999999). Для цього потрібно розгорнуто в 10 разів більше обчислювальних ресурсів для пошуку ключів за той же ж час. В іншому випадку, замість збільшення розміру ключа можна збільшувати кількість символів у наборі, тобто змінювати варіанти з таблиці 3.6.

Час, за який буде витрачено на підбір ключа за словником можна визначити за формулою (3.11):

$$t_{BF} = \frac{C_d}{S} \tag{3.11}$$

Де C_d – кількість ключів у словнику, а S – швидкість перебору, отримана за допомогою інструменту aircrack-ng із застосуванням прапорця -*S*.

Для того, щоб обійти захист технології Wi-Fi із протоколом бездротової безпеки WPA2, окрім необхідних знань зловмисник повинен володіти необхідним апаратно-програмним забезпеченням для обчислень. Проведення лобової атаки на пароль здійснюється за рахунок центрального процесора (ЦП), або графічного процесора (ГП). Швидкість роботи ГП у проведенні лобової атаки є значно вищою, але не кожен комп’ютер оснащується дискретною графічною карткою. Для пришвидшення лобової атаки, дана задача може виконуватись розподілено в комп’ютерному кластері.

Рівень захищеності СП, яка імітує певну систему, не повинен бути значно вищим за рівень та можливості зловмисника, який очікується до взаємодії. Тобто, чим складніший ключ, тим потужнішою обчислювальною технікою потрібно володіти.

Перед тим, як обирати наступний словник, система оцінки повинна зробити вибір того критерію, який повинен бути змінений у наступному словнику – довжина ключів чи кількість символів, з яких можуть бути згенеровані ключі. Нами пропонується робити пріоритетним словник, у якому середнім значенням від суми відсоткових співвідношень кількості символів і довжини ключа у наступних словниках є менше з двох варіантів (3.12).

$$P_k = \begin{cases} \frac{x_{k+1} + w_i}{2}, x_{k+1} + w_i < x_k + w_{i+1} \\ \frac{x_k + w_{i+1}}{2}, x_{k+1} + w_i > x_k + w_{i+1} \end{cases} \quad (3.12)$$

Словник, на якому закінчується атака, і буде вважатись точкою для оцінки рівня кваліфікації і технічного оснащення зловмисника.

Даний підхід допоможе якнайшвидше провести оцінку рівня захищеності СП для бездротових мереж, в яких використовуються протоколи бездротової безпеки WPA/WPA2.

Введемо поняття обчислювальної одиниці, якою будемо вважати певний ресурс, який повинен виконати операцію перебору одного словника d_i.

Як вже було згадано, для лобової атаки можна використовувати розподілені обчислення. Сьогодні задля оптимізації використання обчислювальних ресурсів використовуються різні типи комп'ютерної віртуалізації. Серед них повна, часткова, пара-віртуалізація і віртуалізація на рівні ОС. Розглянемо такі два типи віртуалізації як повна віртуалізація і віртуалізація на рівні операційної системи, яка ще також називається контейнеризацією.

Згідно з дослідженнями компанії IBM [78] технологія віртуалізації KVM на операційній системі SUSE Linux Enterprise 11 збільшує споживання ресурсів в загальному на 15%. Також при використанні віртуалізації додаткові витрати у споживанні процесорного часу становлять на 3—4% більше, аніж без застосування віртуалізації.

У технології контейнеризації гіпервізор не використовується, що зменшує навантаження на апаратне забезпечення. Усі контейнери функціонують на базі

лише серверного ядра. Для кожного контейнера створюється своє окреме, ізольоване середовище.

Як вже будо згадано вище, будь-яка технологія ізоляції приносить додаткові витрати. У випадку контейнеризації ці витрати складають від 0.1%–1%, за рахунок того, що використовуються прості перетворення. Наприклад ізоляція PID процесів виконується за допомогою додавання 4-байтного ідентифікатора, який позначає, якому контейнеру належить процес [79].

На рис. 3.7 наведено принципову відмінність між контейнеризацією та віртуалізацією.

а) б)

Рис. 3.7. Схематичне зображення відмінності між а) віртуалізацією та б) контейнеризацією

Для перевірки умовної захищеності СП велике значення має швидкість обробки даних, а отже перевага буде віддаватись технології, яка справляється із задачами перебору за словником швидше.

Задля оцінки складності подолання захисту протоколів бездротової безпеки WPA/WPA2 зробимо його оцінку за рахунок коефіцієнтів методу аналізу ієрархій (MAI) на основі таких критеріїв, як довжина ключа та кількість можливих символів у словнику. Цей метод дозволяє отримати співвідношення на шкалі порівнянь з невеликим відхиленням, як описано в джерелі [73]. Коефіцієнти використовуються на основі фактичних вимірювань або суб'єктивної думки. На виході отримується співвідношення ваг та індекс узгодженості (3.4).

З матриці N знаходяться суми коефіцієнтів для кожного стовпця (3.5), для подальшої нормалізації матриці N (3.6).

Шляхом сумування коефіцієнтів у кожному рядку нормалізованої матриці і поділом отриманої суми на кількість коефіцієнтів у рядку, як показано в формулі (3.7), можна визначити вагу кожного оціненого елемента.

Сума усіх ваг повинна бути рівною 100%, а отже, щоб отримати відсоткове значення складності ключа певної довжини, потрібно додати його вагу до суми попередніх.

3.2.3. Застосування хмарних обчислень для визначення рівня захищеності систем-приманок та бездротових мереж стандарту IEEE 802.11

Існують два основних підходи до проведення тестування на проникнення – з використанням White-Box і Black-Box методів. У випадку White-Box тестування аудитор володіє повним або частковим доступом до інфраструктури та інших компонентів, з якими потрібно взаємодіяти під час тестування [80]. У разі застосування методу Black-Box, аудитор безпеки оцінює мережеву інфраструктуру організації здалеку і не має повного розуміння внутрішніх технологій, що використовуються.

У рамках моделювання поведінки зловмисника ми припускаємо, що всі тести проводяться в режимі Black-Box. Оскільки Pre-Shared ключ шифрується, зловмиснику доступна лише одна можливість – лобова атака на захоплені асоціативні пакети. Це може здатися неефективним, проте варто пам'ятати, що для такого виду атаки не обов'язково бути поруч з ТД. Зловмиснику може вистачити значних обчислювальних ресурсів для атаки грубої сили або перебору за словником. Таким чином, нашою метою є демонстрація реального масштабу загрози для будь-якої організації.

Також важливо зазначити, що для перехоплення пакета рукостискання зловмиснику не обов'язково чекати, доки до мережі підключиться новий пристрій. Деякі бездротові адаптери, за використання нестандартних драйверів, можуть надсилати в мережу реасоціативні пакети, що призведе до переривання мережевих з'єднань та ініціації нового обміну ключами між клієнтами та ТД. У такому випадку для перехоплення необхідних пакетів зловмиснику потрібно, щоб до мережі був

підключений хоча б один клієнт. Для успішної атаки зловмиснику необхідно знаходитися близько до ТД, щоб його адаптер та антена мали достатньо потужності для посилання пакетів деасоціації та перехоплення пакетів рукостискання.

В межах даної роботи було розроблено програмно-апаратний комплекс, що моделює дії потенційного зловмисника [81]. На рис. 3.10 зображено умовну схему компонентів та взаємодію між модулями комплексу, що здійснюють перехоплення та дешифрування ключів для мереж, що працюють з протоколом бездротової безпеки WPA2-PSK стандарту IEEE 802.11.

Перед початком операцій з комплексом необхідно встановити пристрій для моніторингу радіочастотного ефіру та перехоплення пакетів на місці, де рівень сигналу від мережі та її клієнтів є достатнім для здійснення перехоплення [82]. Мінімальний рівень сигналу зазвичай становить приблизно -90dBm. Після встановлення та активації перехоплювача, з центру управління можна відправляти команди, наприклад, за допомогою SMS-повідомлення, яке активує процедури перехоплення пакетів рукостискання (крок 1 на рис. 3.10).

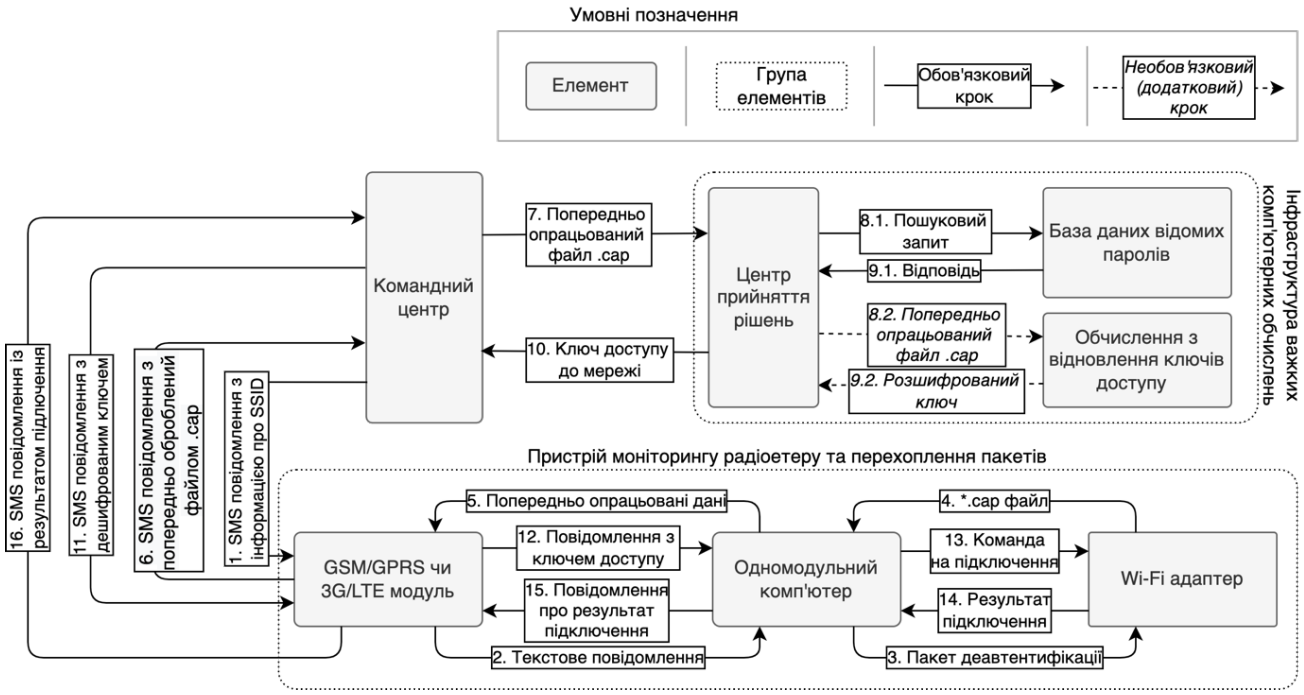


Рис. 3.10. Умовна схема і порядок комунікації між модулями комплексу перехоплення і дешифрування ключа

Таке повідомлення може включати дані про ТД, з якої необхідно перехопити пакети рукостискання, тип перехоплення (активний за допомогою пакетів деавтентифікації або пасивний) тощо. Після цього перехоплювач переходить у режим сканування. Інформація з такого повідомлення передається на GSM/GPRS модуль і негайно потрапляє на комп'ютер для подальшої обробки (крок 2 на рис. 3.10). Wi-Fi адаптер переводиться в режим моніторингу з налаштуваннями, що дозволяють фільтрувати всі інші дані з радіочастотного ефіру (крок 3 на рис. 3.10).

Після виявлення необхідного пакету рукостискання комп'ютер отримує файл з розширенням .cap (крок 4 на рис. 3.10). Дані з файлу .cap підготовлюються комп'ютером для подальшого надсилання через канал GSM (крок 5 на рис. 3.10), після чого вони передаються до командного центру (крок 6 на рис. 3.10). Командний центр подальше надсилає опрацьований файл формату .cap на центр прийняття рішень (крок 7 на рис. 3.10), який в свою чергу розпочинає пошук в базі даних вже відомих паролів (крок 8.1. на рис. 3.10). У випадку, якщо ключ не було знайдено на попередньому етапі, центр прийняття рішень створює кілька віртуальних комп'ютерів в хмарному середовищі та передає файл .cap для проведення подальшої лобової атаки (крок 8.2 на рис. 3.10). Після успішного виявлення ключа він передається на центр прийняття рішень (кроки 9.1, 9.2 на рис. 3.10), звідки повертається назад на командний центр (крок 10 на рис. 3.10).

Командний центр генерує SMS повідомлення з паролем доступу до визначеної ТД і відправляє його на GSM/GPRS модуль перехоплення (крок 11 на рис. 3.10). Дані з GSM/GPRS модуля передаються на одномодульний комп'ютер (крок 12 на рис. 3.10). Комп'ютер формує команду для підключення до мережі Wi-Fi (крок 13 на рис. 3.10). Незалежно від того, чи вдале це підключення, комп'ютер отримує результат від мережевої карти (крок 14 на рис. 3.10). Цей результат обробляється комп'ютером, формується повідомлення, яке в результаті передається на GSM/GPRS модуль (крок 15 на рис. 3.10). Дані про результат надсилаються на командний центр (крок 16 на рис. 3.10). У випадку позитивного результату від перехоплення (крок 14 на рис. 3.10), командний центр вимикає обчислювальні потужності і переходить в режим очікування або знову запускає весь процес у разі

негативної відповіді. При наступній спробі перехоплення пакету рукостискання між тим же клієнтом і ТД діяти не буде, оскільки ймовірно, що раніше перехоплений пакет був недійсним, тобто не містив правильного ключа доступу до ТД.

Середовища, які зберігають дані про вразливості певних систем, часто стають об'єктом атак зловмисників, оскільки успішна атака на одну ланку може дати доступ до інформації про вразливості інших систем або навіть до обчислювальних ресурсів за потребою [83—84]. На рис. 3.11—3.12 показана архітектура ланки важких обчислень на базі хмарного провайдера Amazon Web Services (AWS). Як показано раніше на рис. 3.10, остання ланка комплексу включає елементи, які відповідають за обчислення ключів. Логічно розмістити такі ресурси в приватних сегментах мережі для уникнення доступу з Інтернету. Однак, якщо цим елементам потрібен доступ до Інтернету, вони можуть використовувати шлюзи перетворення мережевих адрес (NAT Gateway), розташовані в публічних сегментах віртуальної приватної мережі. Таким чином, запити будуть направлені через шлюз доступу до Інтернету (рис. 3.11).

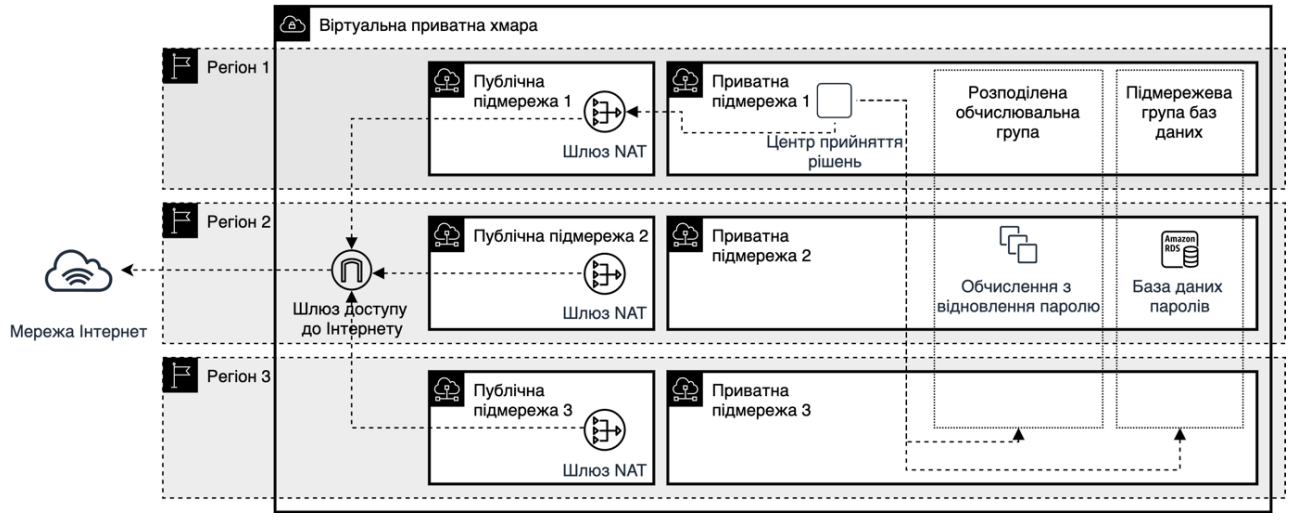


Рис. 3.11. Архітектура віртуальної приватної хмари та приклад виходу її елементів у мережу Інтернет

Найбільш безпечний доступ до елементів з мережі Інтернет можна забезпечити за допомогою технології віртуальних приватних мереж (Virtual Private Network (VPN)) (рис. 3.12).

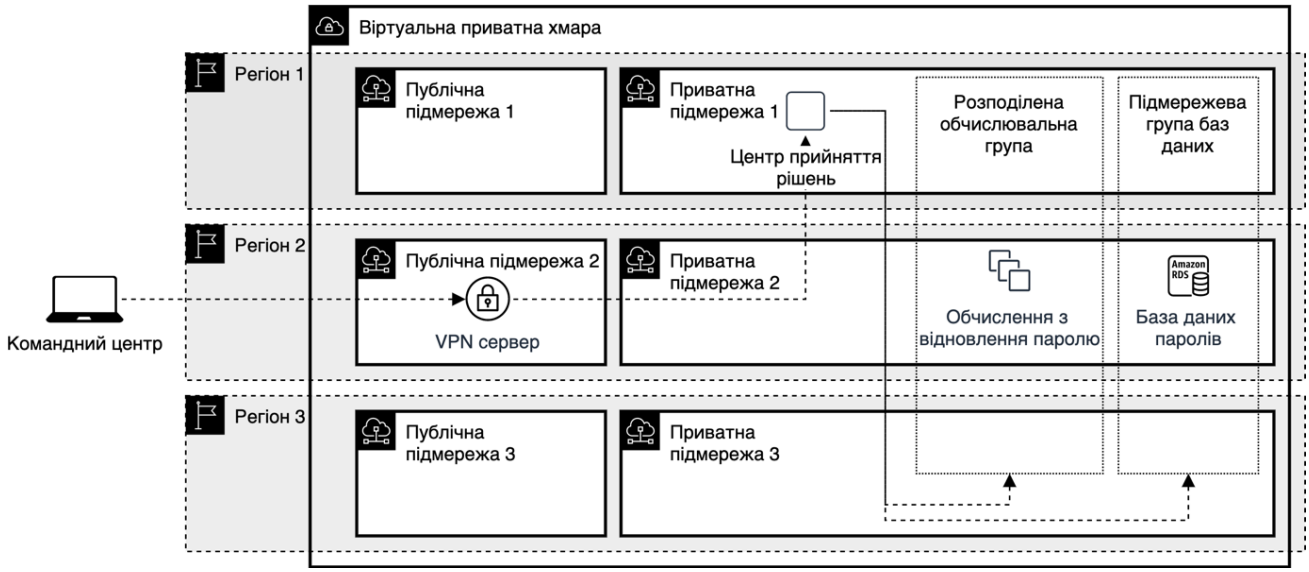


Рис. 3.12. Архітектура віртуальної приватної хмари та приклад комунікації командного центру з її елементами

VPN сервер, розташований у публічному сегменті, очікує з'єднання, і коли до нього підключається клієнт, надається мережева конфігурація, яка дозволяє клієнту спілкуватися з тими ж вузлами мережі, що і VPN сервер. Після цього, у даному випадку, командний центр може безперешкодно взаємодіяти з ресурсами віртуальної приватної хмари.

3.3. Вдосконалення методів виявлення вторгнень в мережах IEEE 802.11 за допомогою систем штучного інтелекту

В першій версії стандарту IEEE 802.11 не було задекларовано ні одного протоколу бездротової безпеки. Одним із механізмів, який дозволяв забезпечити захист від сторонніх користувачів, була фільтрація клієнтів за MAC адресою. Хоч виробники мережевого обладнання постійно додають нові механізми захисту, та все ще не існує жодного, який би повністю гарантував захищеність мережі та її клієнтів.

Кожен пристрій, який належить до сім’ї стандартів IEEE 802.1x володіє унікальними ідентифікаторами, які присвоюються виробниками. Такі ідентифікатори дуже зручно використовувати для того, щоб фільтрувати доступ клієнтських пристроїв. У випадку коли фільтрування за MAC адресою активовано, клієнти, MAC адреса яких не занесена в список дозволених, не зможуть

підключитись до мережі. Та в арсеналі зловмисників існує інструментарій, який дозволяє обійти механізм фільтрування за MAC адресою, а підміна MAC адреси виявляється лише під час розслідувань.

3.3.1. Специфіка MAC адрес в мережах Wi-Fi

Як вже згадувалось вище, за замовчуванням кожен клієнтський пристрій Wi-Fi зберігає дані про мережі до яких був підключений. Це є наслідком того, що клієнтські пристрої повторно підключаються зразу ж після того як з'являються в зоні покриття точок доступу. Ця функція робить життя користувачів простішим, оскільки їм не потрібно кожного разу вводити дані для автентифікації. Та основною проблемою є те, що велика кількість метаданих про мережі, до яких був підключений клієнт, може бути перехоплена і оброблена зловмисниками. Такі метадані доступні у відкритому виді на канальному рівні моделі OSI.

Якщо клієнтський пристрій підключений до будь-якої мережі, він буде активно передавати дані до ТД і отримувати від неї. Звичайно, в своїй більшості ці дані є зашифрованими, але такі адміністративні дані, як, наприклад, MAC адреса ТД і клієнта, канал ТД, протокол бездротової безпеки ТД та ім'я ТД (SSID), є доступними для перегляду, якщо мережева карта переведена в режим моніторингу. У випадку, якщо клієнт не підключений до жодної мережі, дані про SSID, до яких клієнт був підключений, можуть бути доступними, оскільки клієнтський пристрій безперервно знаходиться в їх пошуку.

Для зловмисника є природнім використання адміністративних даних та інших метаданих для проведення атак на клієнта і на інфраструктуру в цілому.

У випадку, якщо зловмиснику відома MAC адреса клієнта і SSID ТД до якої клієнт підключений, він може склонувати ТД з тією ж MAC адресою та SSID, але без будь-якого протоколу бездротової безпеки навіть, якщо на легітимній точці доступу він використовувався. Збільшення потужності сигналу підробної ТД і DoS атака може допомогти зловмиснику відключити клієнта з легітимної ТД і підключити до клонованої ним ТД. Така атака отримала назву "Злий двійник" (англ. Evil Twin).

В іншій модифікації вищеописаної атаки, зловмисник створює клон ТД і перенаправляє усі клієнтські запити на фішингову сторінку, на якій клієнта просять ввести пароль для того, щоб нібито підтвердити його автентичність. Після того, як клієнт ввів пароль, зловмисник його одразу ж отримає, а сервер, який забезпечував сервіс “злого двійника” буде зупинений.

Якщо клієнтський пристрій не підключений до жодної ТД, то він буде активно шукати мережі, до яких був раніше підключений. На канальному рівні моделі OSI, цей процес може бути ідентифіковано зловмисником. Використовуючи дані з клієнтських пристроїв, зловмисник може створити підробні ТД.

Допоки легітимний клієнт і зловмисник підключені до однієї і тієї ж мережі, другий може перехоплювати і/або модифікувати трафік першого.

3.3.2. Проблеми пов’язані з безпекою відносно MAC-адрес та їх вирішення

Швидкий розвиток будь-якої технології часто приносить проблеми пов’язані з безпекою, які не так просто замітити на початкових фазах. Після того, як базова технологія отримала велику кількість функціональних особливостей, які вже отримали розповсюдження серед користувачів, виправлення проблем пов’язаних з безпекою можуть вплинути на працездатність в цілому. Такий підхід може принести незручності як для виробників так і для кінцевих користувачів.

Мережі IEEE 802.11 дозволяють своїм користувачам підключатись до мереж автоматично після того, як вони вже були авторизовані. Уявімо, що ця функціональність буде заборонена з метою забезпечення безпеки. Перш за все, кожен клієнт буде змушений авторизуватись кожен раз як захоче скористатись будь-якою із точок доступу. Механізм WDS чи інший сітковий механізм розподіленого доступу до мережі, стане безкорисним, оскільки при пересуванні між ТД користувач буде змушений щоразу авторизуватись.

3.3.3. Розроблення методу ідентифікації атак з підміни MAC адреси та «злий двійник»

Перед тим, як сенсори зможуть ідентифікувати позиціонування і поведінку клієнтів вони повинні ідентифікувати позиціонування одне одного. Основною

проблемою є те, що в режимі моніторингу сенсори не можуть ідентифікувати одне одного, оскільки в даному режимі вони не можуть передавати дані. Таким чином перед тим як запустити режим моніторингу кожним сенсором повинен бути сформований спеціальний кадр, який буде відправлено сусіднім сенсорам. Використовуючи модель WHaaS після того як сенсори розставлені по місцях, повинна бути натиснута умовна кнопка, після чого розпочнеться процес обміну службовими даними. Окрім цього, такі кадри не можуть бути створені за певним шаблоном для того, щоб уникнути створення сигнатур для зловмисників, які вже знають існування такої СП і СВВ, і принципу, за яким відбувається синхронізація між сенсорами [85].

Враховуючи вищесказане, пропонується наступний метод синхронізації, що ґрунтується на створенні синхронізаційних пакетів в командному центрі моделі WHaaS. Коли командний центр отримує запит від користувача, він розпочинає підготовку даних для сенсорів. Наприклад, це можуть бути маячки, що використовуються ТД для повідомлення клієнтів про свою присутність, або пошукові пакети, які використовуються клієнтськими пристроями для пошуку мереж, до яких вони підключені. На наступному етапі командний центр розсилає дані, що є унікальними для кожного сенсора. Зовнішні елементи отримують список команд і відповідно до черги надсилають у етер дані, які їм відповідають з певним, випадково визначеним інтервалом. Паралельно з процесом надсилання своїх даних, сенсори прослуховують етер і за фільтром з отриманого раніше списку даних ідентифікують сусідів. Якщо зовнішній елемент отримав дані від свого сусіда, він має негайно передати ідентифікатор елемента, сигнал якого він отримав, і потужність його сигналу. В кінці процесу синхронізації кінцевий користувач отримує карту з розташуванням елементів комплексу і має підтвердити чи заперечити правильність її побудови.

Якщо метод ідентифікації зовнішніх елементів базується на передаванні маячків, як це робить будь-яка ТД, то слід застосувати додаткове маскування, оскільки автентичність ТД може бути визначена за допомогою її MAC-адреси. База даних MAC адрес виробників може бути використана для уникнення підозри з боку

зловмисника, щодо ідентичності системи, яку він планує атакувати. Перші 24 біти MAC адреси можуть розповісти зловмиснику про виробника пристрою, який він ідентифікував в етері. Також, поряд з MAC адресою може бути застосовано стандартний SSID.

Для того, щоб ідентифікувати сусідів, достатньо перехопити лише один кадр з етеру, та це також може бути маркером для зловмисника. Отже, ще одним параметром, який повинен генеруватись випадковим чином є число кадрів, які будуть передані в етер.

3.3.4. Приклад інфраструктури з еталонним покриттям системи виявлення атак пов'язаних з підміною MAC адреси для мереж IEEE 802.11

Представимо, що об'єкт, який повинен бути під моніторингом, знаходиться у приміщенні, яке має форму ідеального квадрату. Для того, щоб досягти кращого покриття потрібно розмістити сенсори рівновіддалено одне від одного. Зобразимо таку схему за ідеальних умов (рис. 3.13)

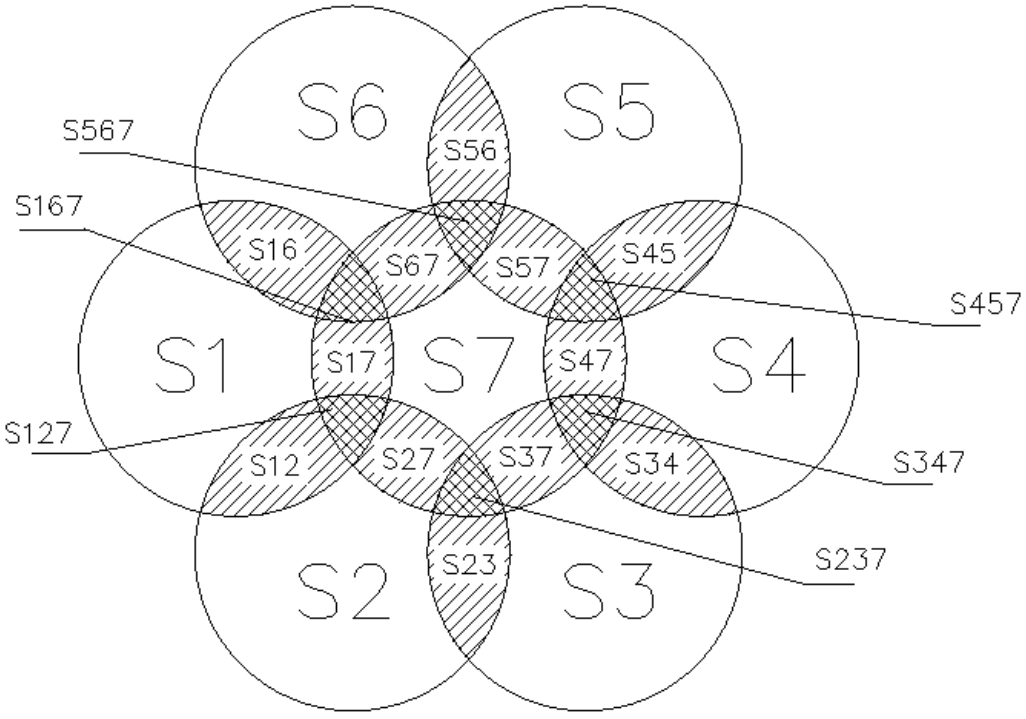


Рис. 3.13. Приклад розміщення сенсорів системи виявлення вторгнень для мережі IEEE 802.11

Для зображеної вище схеми буде справедливою таблиця істинності представлена в табл. 3.9.

Таблиця 3.9.

Таблиця істинності для схеми зображеної на рисунку 3.10

Ідентифікатор сенсора	***S1***	***S2***	***S3***	***S4***	***S5***	***S6***	***S7***
S1		+	–	–	–	+	+
S2	+		+	–	–	–	+
S3	–	+		+	–	–	+
S4	–	–	+		+	–	+
S5	–	–	–	+		+	+
S6	+	–	–	–	+		+
S7	+	+	+	+	+	+	

Схематичне зображення покриття СВВ, зображеного на рис. 16, є простим прикладом того, як метод ангуляції може допомогти у визначенні вторгнень. Якщо відомо про те, що користувач має знаходитись у зоні дії 3-х визначених сенсорів, а в зоні дії інших не повинен бути, то такий процес може допомогти у виявленні зловмисника, наприклад, якщо поява клієнтського пристрою в етері зафіксована сенсорами, в зоні дії яких він не повинен з’являтись. Та викликом буде ситуація при якій зловмисник скористається, наприклад вузьконаправленою антеною і потужність його сигналу не вийде за сенсори, в межах яких він повинен працювати, то така атака не буде виявлена.

3.3.5. Застосування машинного навчання у вивчені поведінки користувачів мереж IEEE 802.11 і подальшого виявлення вторгнень

Сьогодні не існує методу, який може допомогти ідентифікувати атаку MAC spoofing в мережах IEEE 802.11. Та дана проблема може бути частково вирішена за допомогою машинного навчання.

Кожен клієнтський Wi-Fi пристрій має свій унікальний денний шлях, який залежить від його власника. В іншому випадку пристрій може бути статично розміщений, наприклад, це може бути маршрутизатор. Отже, відносно точок доступу і клієнтських пристроїв повинні бути застосовані різні підходи.

Якість і стабільність сигналу залежить від великої кількості зовнішніх факторів. На сигнал ТД можуть негативно впливати, наприклад, сусідні ТД, які працюють на тому ж частотному каналі, побутові електричні прилади, міжкімнатні

стіни та меблі. На рис. 3.14 проведено моделювання потужність сигналу зі схемою з рис. 3.13.

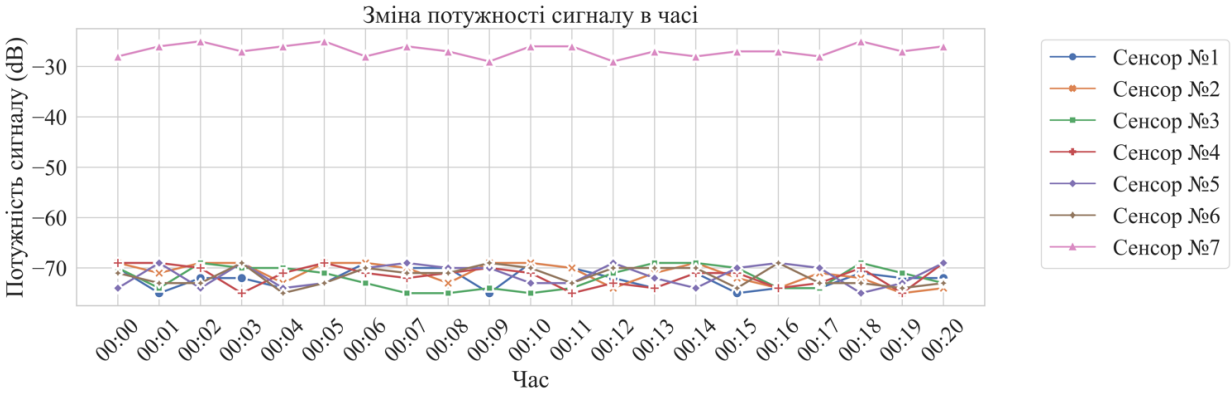


Рис. 3.14. Варіація сили сигналу легітимного пристрою Wi-Fi, представлена в часі

На рис. 3.14 видно, що потужність сигналу з сенсора №7 значно перевищує інші, що може бути ознакою перебування клієнтського пристрої у безпосередній близькості до вище згаданого сенсора. Відповідно, потужність сигналу пристрою за яким здійснюється спостереження, на усіх інших сенсорах стабільний і рівновіддалений від сенсора біля якого знаходиться цей пристрій.

В атаці “злий двійник”, зловмисник створює ТД, яка за основними реєстраційними даними дублює легітимну. У звичайного користувача створена зловмисником ТД не викличе жодної підозри. Та існує висока імовірність того, що навіть, якщо ТД буде ідеально склонована, вона фізично перебуватиме в іншому місці. Це означає, що потужність сигналу такої ТД буде принципово іншою. На рис. 3.15. зображено сигнатуру появи «злого двійника».

Рис. 3.15. Варіація сили сигналу легітимного і появи нелегітимного пристроїв Wi-Fi

Як видно з рис. 3.15, хоч потужність сигналу від легітимного пристрою збережена на сенсорі №7, та у проміжку між десятою та одинадцятою часовими точками на сенсорі №4 зростає потужність сигналу від спостережуваного пристрою.

Розташування точок доступу є здебільшого стаціонарним. Це свідчить про те, що імплементація навчання систем штучного інтелекту на потужності сигналів Wi-Fi точок доступу є досяжною ціллю, оскільки нейронну мережу чи класифікатор не потрібно часто перенавчати.

На відміну від точок доступу, вивчення клієнтської поведінки є набагато важчим завданням, оскільки клієнтські пристрої з’являються і зникають разом зі своїми власниками. Наведемо перелік метаданих, які можуть бути застосовані у вивченні поведінки клієнта, для уникнення атаки MAC spoofing та ін.:

Визначення часу коли клієнтський пристрій з’являється і зникає у зоні покриття. Дуже важливо знати звичну поведінку клієнтського пристрою, до прикладу час коли клієнтський час з’являється і зникає із зони покриття. Для прикладу, опишемо типову поведінку працівника умовного підприємства. Працівник з понеділка по п’ятницю приходить о 9 годині ранку в офіс, покидає його о 13:00 і повертається о 14:00, залишається на робочому місці до 18:00 і покидає робоче місце до наступного ранку. Звичайно ж людина не може приходити точно в один і той же ж час кожного дня і слідувати одній і тій же ж моделі поведінки через вплив інших людей і факторів, але володіючи такими даними можна дуже легко ідентифікувати аномальну поведінку. Прикладом аномальної поведінки може бути поява клієнта в зоні покриття, наприклад, у ніч суботи.

Виявлення вузьконаправленої або іншої потужної антени. Якщо всі або майже всі сенсори ідентифікують сигнал від клієнтського пристрою деякого клієнта, найбільша потужність сигналу виявляється сенсорами розташованими на деякому зовнішньому краю інфраструктури, і потужність поступово зменшується в протилежному напрямку, це може свідчити про можливу атаку, коли зловмисник використовує вузьконаправлену антену (рис. 3.16).

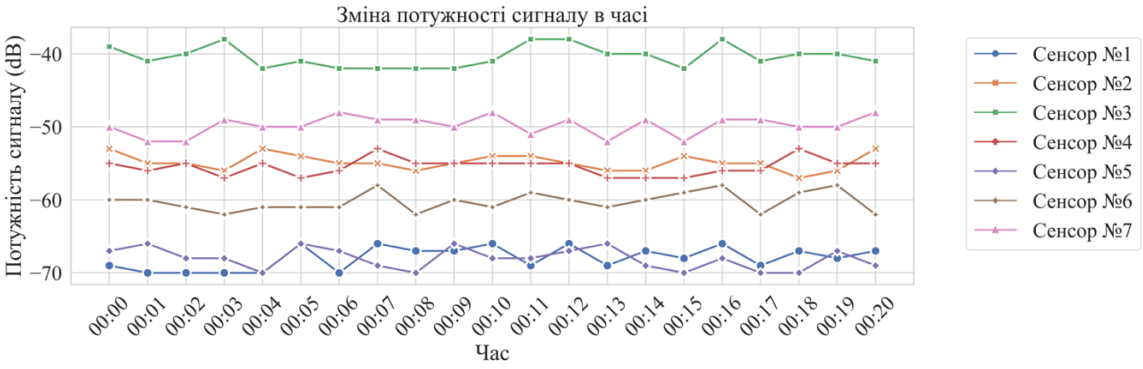


Рис. 3.16. Варіація сили сигналу клієнтського Wi-Fi пристрою нападника (зі спрямованою антеною) представлено в часі

На основі описаного сценарію і схеми розміщення сенсорів з рис. 3.13, на рис. 3.16 зображено варіацію сили сигналу потенційного зловмисника з направленою антеною. З рис. 3.16 видно, що найвища потужність зафіксовано сенсором №3, далі сенсорами №7, №2, №4 та №6, що відповідає наскрізному розповсюдженню потужності сигналу.

Ідентифікація дубльованої MAC адреси у зоні покриття. Якщо у зоні покриття з'являється ще один пристрій з MAC адресою, яка вже в певний момент зареєстрована у мережі, то це може свідчити про атаку. На основі вищеописаного сценарію і інфраструктури з рисунку 3.13, на рисунку 3.17 зображено варіацію сили сигналу потенційного зловмисника, який розпочав атаку MAC Spoofing поряд з уже зареєстрованим в мережі клієнтом.

Рис. 3.17. Виявлення підміни MAC адреси у мережі Wi-Fi з системою виявлення вторгнень моделі WHaaS

Інтерпретувати рисунок 3.17 можна так: перший сенсор, який ідентифікував клієнта був сенсор №3 як свідчить зміна потужності сигналу (часовий проміжок

між 0:00 і 0:03). Згодом рух вектор руху змінюється в сторону сенсора №7, який є сусіднім до сенсора №3, що свідчить про природність руху по зоні покриття (часовий проміжок між 0:03 і 0:06). Тоді, окрім сенсорів №3 та №7 клієнтський пристрій стає ідентифікуватись сенсором №2. Від сенсора до сенсора пристрій змінює своє місцезнаходження і о 0:17 сенсор №1 і №5, які не є сусідніми виявляють сигнали з пристроїв з однаковою MAC адресою.

Виявлення клієнтського пристрою у місці, де він однозначно не повинен бути. Якщо будівля, мережа в які повинна бути захищена, є великою, то імовірно, що там повинно бути розмежування доступу до певних приміщень. Виявлення клієнтських пристроїв у не звичних для них місцях (місцях які покриті зоною дії певних сенсорів) можуть свідчити про присутність зловмисника, який фізично зайняв зручне для нього місце або про зловмисні дії з боку персоналу.

Виявлення атаки MAC Spoofing за пошуковими пакетами з клієнтських пристроїв. Кожен клієнтський пристрій Wi-Fi, який вже був підключений до якоїсь кількості бездротових мереж буде здійснювати їх пошук за допомогою спеціальних пошукових пакетів. Це означає, що кожен клієнтський пристрій буде мати свій власний список точок доступу, пошук яких буде активно проводитись. У всякому разі, навіть якщо зловмисник змінить MAC адресу свого пристрою на адресу легітимного, він буде надсилати пошукові пакети зі значеннями, не притаманними легітимному пристрою, або не надсилати їх взагалі. Такі активності можуть слугувати маркером атаки.

3.3.6. Застосування машинного навчання для виявлення вторгнень у мережі стандарту IEEE 802.11

В даному розділі вже було наведено приклад сигнатур які можуть вказувати на цілий ряд атак із підміни пристроїв Wi-Fi в етері за допомогою аналізу потужності сигналу. Та будувати систему захисту від атак в мережах Wi-Fi базуючись лише на сигнатурних правилах є великим викликом для адміністратора мережі, оскільки будь-які зміни в приміщенні будуть вносити свої корективи у

потужність сигналу від ТД до користувацького пристрою чи сенсора, який здійснює моніторинг.

Існує доволі багато різних підходів до реалізації моделей машинного навчання, це може бути навчання з вчителем чи без вчителя. Якщо говорити про навчання з вчителем, то воно зазвичай потребує менших обчислювальних потужностей для навчання моделі.

Оскільки дані, зібрані з ефіру, можуть містити певні шуми, тобто рівень сигналу від ТД може бути часом не стабільний, то для аналізу даних у даній роботі було вирішено застосовувати алгоритм класифікації k-найближчих сусідів (KNN). KNN класифікує отриману точку даних на основі її близькості до інших точок даних у навчальному наборі. У даному випадку, тренування моделі можна застосувати відносно максимальної, мінімальної середньої потужностей сигналу, також потужності сигналу, яка найчастіше з'являлась.

Щоб обчислити відстань між двома точками даних, використовується метрика відстані. Зазвичай використовувані метрики відстані включають евклідову відстань, манхеттенську відстань і відстань Мінковського [86].

У тренування нашої моделі за метрику відстані було взято метод Мінковського. Метрика Мінковського є узагальненою формою інших метрик відстані, таких як евклідова відстань і манхеттенська відстань. Відстань Мінковського порядку p між двома точками визначається за формулою (3.13):

$$D(x,y) = \left[\left(\sum_{i=1}^{n}|x_i - y_i|^p\right)^{\frac{1}{p}}\right] \tag{3.13}$$

де x та y – це дві точки даних із n ознаками, p – параметр, який визначає порядок метрики відстані, а $D(x,y)$ — відстань Мінковського між x і y.

При $p = 1$ метрика Мінковського зводиться до манхеттенської відстані, а при $p = 2$ – до евклідової. Загалом, більше значення p призводить до сильнішого акценту на більших відмінностях між значеннями ознак і слабшого акценту на

малих відмінностях. Для тренування моделі порядок метрики відстані було присвоєно 2, а отже метрика відстані еквівалентна евклідівській відстані (3.14).

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \tag{3.14}$$

Серед K найближчих сусідів підраховується кількість точок даних, які належать кожному класу. Клас із найбільшою кількістю найближчих сусідів призначається невидимій точці даних. Значення K визначає кількість найближчих сусідів та може бути обране на основі експерименту. У нашому K експериментальним методом було обрано значення 3.

Голосування за більшістю: коли знайдено K найближчих сусідів, точці даних призначається клас із більшістю найближчих сусідів. Якщо K – непарне число, клас із найбільшою кількістю найближчих сусідів є більшістю. Якщо K є парним числом, мажоритарний клас визначається шляхом розгляду значень найближчих сусідів по відношенню до точки даних [87].

У математичних термінах більшість голосів можна виразити за допомогою 3.15.

$$y = majority(y_1, y_2, \dots, y_K) \tag{3.15}$$

де $y_1, y_2, \dots, y_K$ – це мітки класу K найближчих сусідів, а більшість $(y_1, y_2, \dots, y_K)$ повертає мітку класу, яка найчастіше зустрічається серед K найближчих сусідів.

Послідовність процесу класифікації зображено на рис. 3.18.

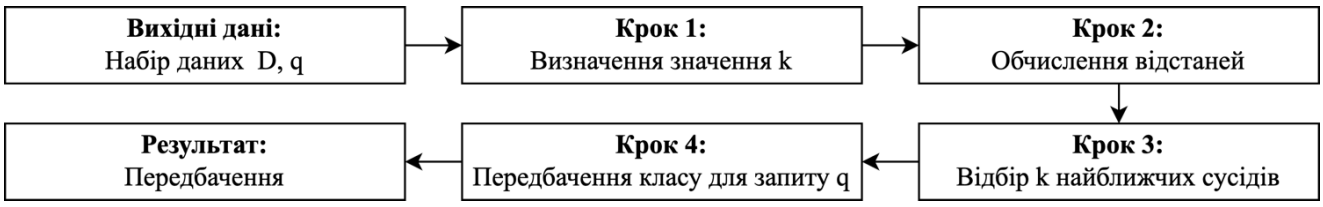


Рис. 3.18. Послідовність процесу класифікації за допомогою KNN

Представимо короткий опис процесу класифікації представленого на рис. 3.18:

- Блок вхідних даних представляє вхідні дані для алгоритму KNN, який складається з набору даних D, що складається з n точок даних $(x_1, y_1) \dots (x_n, y_n)$ і точки запиту q.
- Крок 1 передбачає встановлення значення k, яке визначає, скільки найближчих сусідів враховувати під час прогнозування.
- Крок 2 передбачає обчислення відстані між точкою запиту q і кожною точкою даних у наборі даних D.
- Крок 3 передбачає вибір k точок даних із набору даних D, які мають найкоротшу відстань до точки запиту q.
- Крок 4 передбачає підрахунок кількості точок даних у вибраному наборі, які належать до кожного класу, і вибір класу, який має найбільшу кількість, як прогнозований клас для точки запиту q.
- Блок вихідних даних представляє вихід алгоритму KNN, який є прогнозованим класом для точки запиту q.

На рис. 3.19 зображено компонентну схему програмно-апаратного комплексу для виявлення вторгнень в мережі стандарту IEEE 802.11, за допомогою алгоритмів машинного навчання.

Рис. 3.19. Схема роботи та елементів програмно-апаратного комплексу визначення атаки «злий двійник»

Цілісна система складається з трьох шарів. Перший – рівень збору інформації. Цей рівень складається з трьох компонентів – пристрій для збору даних, агрегатор даних та база даних на основі часових рядів. Задачею даного рівня є виключно збір даних. Другий – рівень аналізу даних. Цей рівень складається із сховища даних підготовлених до навчання, обчислювального середовища для навчання та компонента безперервної інтеграції та доставки моделі машинного навчання. Третій – рівень прикладного рівня. Цей шар складається балансира навантаження веб трафіку, застосунку, який оперує натренованою моделлю і БД, яка зберігає дані про виявлені атаки.

Робота комплексу організована наступним чином: на першому етапі сенсори збирають дані. Після збору і агрегації дані записуються в базу даних на основі часових рядів. В момент, коли достатня кількість даних зібрана, вона направляється у сховище даних для тренування моделі машинного навчання, після чого відбувається тренування моделі. Далі, натренована модель доставляється на серверний застосунок.

Після процесу збору, навчання і доставки артефактів, компоненти з рівня збору інформації встановлюються в сторожовий режим роботи, метою якого є моніторинг рівня сигналу і його звірка даних із моделлю. У випадку необхідності можна викликати режим повторного збору і дотренування чи перетренування моделі.

3.4. Висновки до розділу 3

Виявлення та реагування на події в бездротових мережах стандарту IEEE 802.11 є завданням, яке вимагає значних зусиль і складається не лише з простих кроків. Використовуючи базову специфіку стандарту IEEE 802.11 у підрозділі 3.1 запропоновано методику зі збору інформації про попередні місця перебування зловмисників. Даний підхід базується на аналізі пакетів Dot11ProbeReq з пристроїв, які здійснювали атаку або перебували у безпосередній близькості до них, а відповідно можуть належати зловмиснику. Дана методика значно розширює можливості дослідників кіберзлочинів, оскільки така інформація може розширити

доказову базу проти кіберзлочинця. Окрім того, методика дає можливість деанімізувати власника пристроїв, які були присутні в місці у якому здійснювалась атака. Запропоновано метод із визначення територіальної одиниці, в якій зловмисник може перебувати.

В розділі 3.2 розроблено загальну діагностичну модель для СП для мереж стандарту IEEE 802.11, проведено уточнення діагностичної моделі для протоколів бездротової безпеки WPA/WPA2, як до одного із найбільш захищеного, та на даний момент, найпопулярнішого механізму захисту. Запропоновані різноманітні конфігурації, які визначені у таблиці 3.1, включають в себе варіанти з 4 по 8, які враховують ймовірність наявності застарілого обладнання у мережі. Варіант 9 стосується ключа, який можна виявити у базових словниках для атаки грубою силою. Варіант 13 вказує на ймовірність неправильної конфігурації або неможливості вимкнути вразливий протокол WPS на точці доступу. Наведені шаблони конфігурацій дозволять збільшити імовірність взаємодії зловмисника із СП.

Особа яка атакує певну систему в будь-який момент може вирішити, що подальше продовження атаки є не доцільним, через час, який йде на дешифрування ключа, чи коштів, які вже вкладені в обчислювальну потужність.

Найпростішим варіантом з якого починають зловмисники – це використовувані ключі, що найбільше використовуються користувачами. Такими ключами може бути інформація, яка несе в собі якусь логіку, наприклад, дані про саму ж ТД, її власника чи місце, де вона знаходиться. Тому очевидно, що атаку варто починати зі словника, який містить в собі таку інформацію.

Якщо у базовому словнику ключа не буде знайдено, то для обробки буде взятий найпростіший словник, згенерований лише з цифр від 0 до 9, довжина ключів в якому не перевищуватиме 8 символів. Процес підбору словника буде виконуватись до моменту, поки ключ не буде знайдений. Відповідно, чим складніший словник – тим більший ресурс буде виділено для пошуку ключа, і тим вищою буде оцінка захищеності умовного захисту СП. Найскладнішим буде

словник, ключі якого генеруються з 95 різних символів таблиці ASCII, а довжина його складає 63 символи.

Власники бездротового обладнання Wi-Fi нечасто встановлюють складні паролі на доступ до мережі, і цим користуються зловмисники. Тому логічно, що атака не буде розпочата зі словника, у якому ключі є довжиною 63 символи. Складність ключа певної довжини буде дорівнювати сумі коефіцієнта його ваги з усіма попередніми. Відповідно до цього можемо вивести шкалу складності подолання протоколу бездротової безпеки WPA2 для розміру ключа. Виключенням з правил може бути випадок, якщо зловмисник знає довжину ключа.

В підрозділі 3.3 та на прикладі інфраструктури, розгорнутої в приміщенні з ідеальним покриттям, було вдосконалено метод виявлення вторгнень в мережах стандарту IEEE 802.11. Розроблено метод ідентифікації атаки з підміни MAC адреси та ЗД, а також запропоновано метод визначення атаки ЗД за допомогою алгоритму машинного навчання KNN. Для цього, до використання запропоновано алгоритм машинного навчання з вчителем KNN, який добре підходить для вивчення потужності сигналів від легітимних точок доступу та подальшого виявлення вторгнень. На відміну від сигнатурних методів виявлення вторгнень, даний метод дозволяє точніше виявляти атаки ЗД у випадку, якщо зловмисник створює точну копію ТД копіюючи ідентифікатор ТД та її MAC адресу, оскільки сигнатури дозволяють виявляти атаки за рахунок ідентифікації ідентичної ТД із відмінною MAC адресою.

Крім того, було розроблено концепцію компактного та енергоефективного апаратно-програмного комплексу для реалізації моніторингу та аналізу службових мережевих пакетів у етері та збереження даних на основі часових рядів. Для зменшення навантаження на комп’ютерну мережу і враховуючи обмежену обчислювальну здатність комплексу, було запропоновано метод агрегації даних, який забезпечує швидку передачу даних. Даний комплекс дозволив зібрати і організувати велику кількість даних від легітимних та імітованих нелегітимних точок доступу, які в подальшому було використано для тренування моделі машинного навчання.

РОЗДІЛ 4. ПОКРАЩЕННЯ МЕХАНІЗМІВ ІДЕНТИФІКАЦІЇ ВИЯВЛЕННЯ ВТОРГНЕНЬ, ОСОБИ ЗЛОВМИСНИКА ТА ЕФЕКТИВНОСТІ СИСТЕМ-ПРИМАНОК У БЕЗДРОТОВИХ МЕРЕЖАХ СТАНДАРТУ IEEE 802.11

4.1. Дослідження в межах розробки методики з відслідковування зловмисника

Об’єктом дослідження виступав пристрій, який попередньо був підключений до більше ніж десятка публічних та приватних мереж Wi-Fi. Основною метою було здійснити перехоплення пошукових пакетів від даного пристрою і віднайти можливі місця попереднього перебування власника клієнтського пристрою. Саме дослідження дозволить проаналізувати на скільки точною є інформація від публічних БД про геолокацію точок доступу Wi-Fi.

4.1.1. Визначення недоліків публічної бази даних WiGLE в умовах досліду

Одночасно і перевагою і недоліком публічних платформ для пошуку геолокації Wi-Fi точок доступу є те, що дані на них може завантажувати будь-хто. З одного боку це дозволяє зібрати більше інформації, з іншого – постає питання до якості цих даних [88]. Також дані не можуть бути перевірені чи верифіковані власниками таких платформ. Користувачі, які завантажують дані збираються і обробляються користувачами не стандартизованими методами і за допомогою різних програмно-апаратних комплексів, що призводить до похибок при запитах до БД. В даному дослідженні було використано публічну БД про геолокацію точок доступу WiGLE, оскільки це БД із найбільшою кількістю даних, оскільки сервіс зберігає історичні дані починаючи з 2001 року.

Обмеженням платформи WiGLE на даний момент є те, що інформація про кожну ТД може записуватись кожної мілісекунди і кожен такий запис вважатиметься унікальним, але вибрати агреговані дані лише по конкретній точці доступу в незалежності від часу – неможливо. Це все говорить про те, що записів про одну і ту ж ТД може бути на стільки великою, що навіть в такому місті як, наприклад, м. Львів пошук однієї ТД може зайняти не один тиждень. Оскільки пакет Dot11ProbeReq не передає інформацію про MAC адресу, а лише

ідентифікатор SSID, то шукати доводиться лише за одним параметром і унікальність даних у такому випадку ставиться під питання.

Одним із записів, які було віднайдено із пристрою, який імітував пристрій зловмисника був запис про ТД із ідентифікатором Tenda_716370, локація якого була завідомо відомою. Даний ідентифікатор мережі був вибраний серед інших, як такий, у якому є випадковий набір цифр і існує висока імовірність того, що він буде унікальним у визначеній територіальній одиниці.

На площі приблизно 2 кілометри квадратних сервіс, після першого запиту, БД WiGLE повертає більше 100 унікальних записів після першого запиту про ТД з ідентифікатором Tenda_716370, що є доволі сумнівним результатом. Після більше ніж 20 тис. запитів до сервісу, унікальних точок доступу з досліджуваним ідентифікатором вже стало 135. І за умови валідності даних, це говорить про те, що вибір даних і агрегація лягають на плечі інженера-дослідника (рис. 4.1).

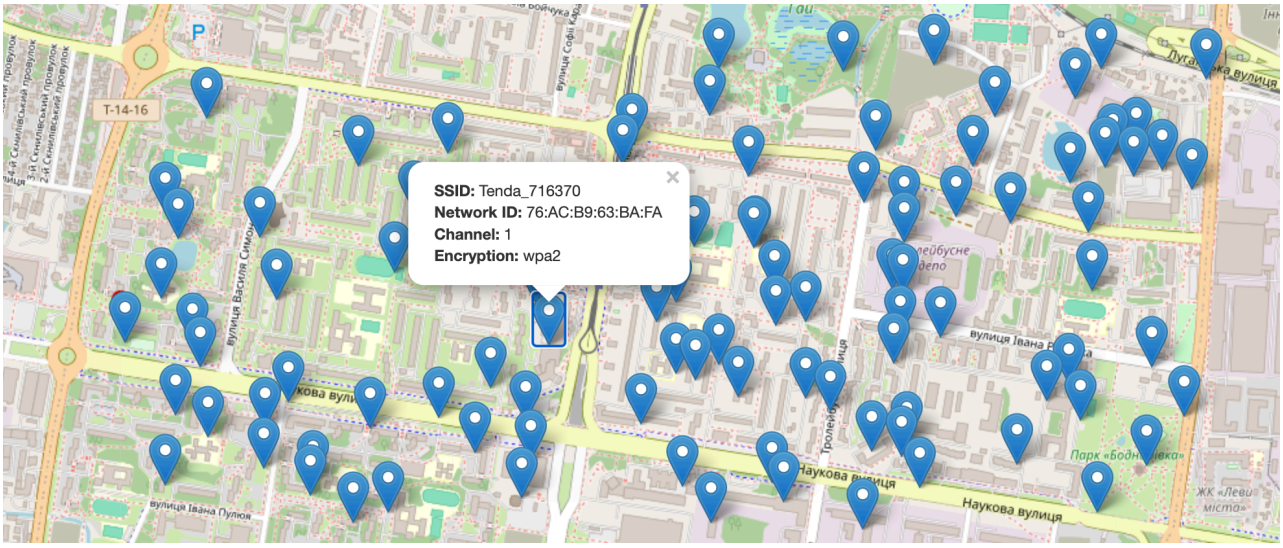


Рис. 4.1. Візуалізація даних отриманих з бази даних WiGLE про точку доступу з ідентифікатором Tenda_716370

Якщо взяти до уваги те, що дослідник не має інформації про MAC адресу, то таку інформацію можна прирівняти до шуму, фільтрація якого також вимагає значних обчислювальних та людських ресурсів.

Візуалізація даних на рис. 4.1 може також свідчити про проблему із стандартизацією користувацького обладнання, яке використовується для збору

інформації або про їх невалідність. А якщо взяти до уваги те, що дослідник не має інформації про MAC адресу, то імовірність визначення геолокації попередніх місць перебування зловмисника прямує до нуля. Для платформи WiGLE і схожих сервісів, важливо аби у користувача був GPS модуль та мережева карта Wi-Fi. Проте, ніяким чином не робиться аналіз того, якого типу антену Wi-Fi адаптера використовує користувач і яка в неї потужність або на скільки точним є GPS модуль.

Оскільки перехопивши з пристрою зловмисника пакети Dot11ProbeReq ми можемо знати лише один параметр – це ідентифікатор мережі SSID, то інформація про локацію ТД з визначеним іменем повинна бути на стільки точною, на скільки це можливо. Оскільки БД WiGLE повернула доволі багато даних про ТД з іменем Tenda_716370 на території площею у 2км, то валідність таких даних варто піддати сумніву.

4.1.2. Верифікація даних отриманих з бази даних WiGLE та застосування методу наближення на основі потужності

Оскільки валідність отриманих даних є сумнівною, з’явилась необхідність провести дослід із пошуку точок доступу із ідентифікатором Tenda_716370 в межах досліджуваної території. Для того, щоб покращити точність геолокації точок доступу з’явилась необхідність у створенні власного програмного забезпечення.

Для перехоплення пакетів було використано бібліотеку Scapy, яка не має альтернативи у опрацюванні мережевих пакетів на мові програмування Python. Логіка програми полягає у безперервному моніторингу етеру. У випадку якщо програма натрапляє на пакет з даними, які містять шар Dot11ProbeReq, то такий пакет надходить на подальше опрацювання. Кожну унікальну MAC адресу, яка буде знайдена записується у словник, в якому MAC адреса – це ключ, а значенням є список унікальних імен (SSID) точок доступу, які були присутні у пакетах Dot11ProbeReq і мають відношення до MAC адреси клієнтського пристрою. Базовий функціонал сценарію на мові програмування python3 наведено у додатку Б, файл beacon_intercept.py

Дані було зібрано на визначеній території площею близько 2км^2 за допомогою комп’ютера із додатковим GPS модулем та мережевою картою Alfa AWUS036NHA, яка може працювати в режимі моніторингу (рис. 4.2).

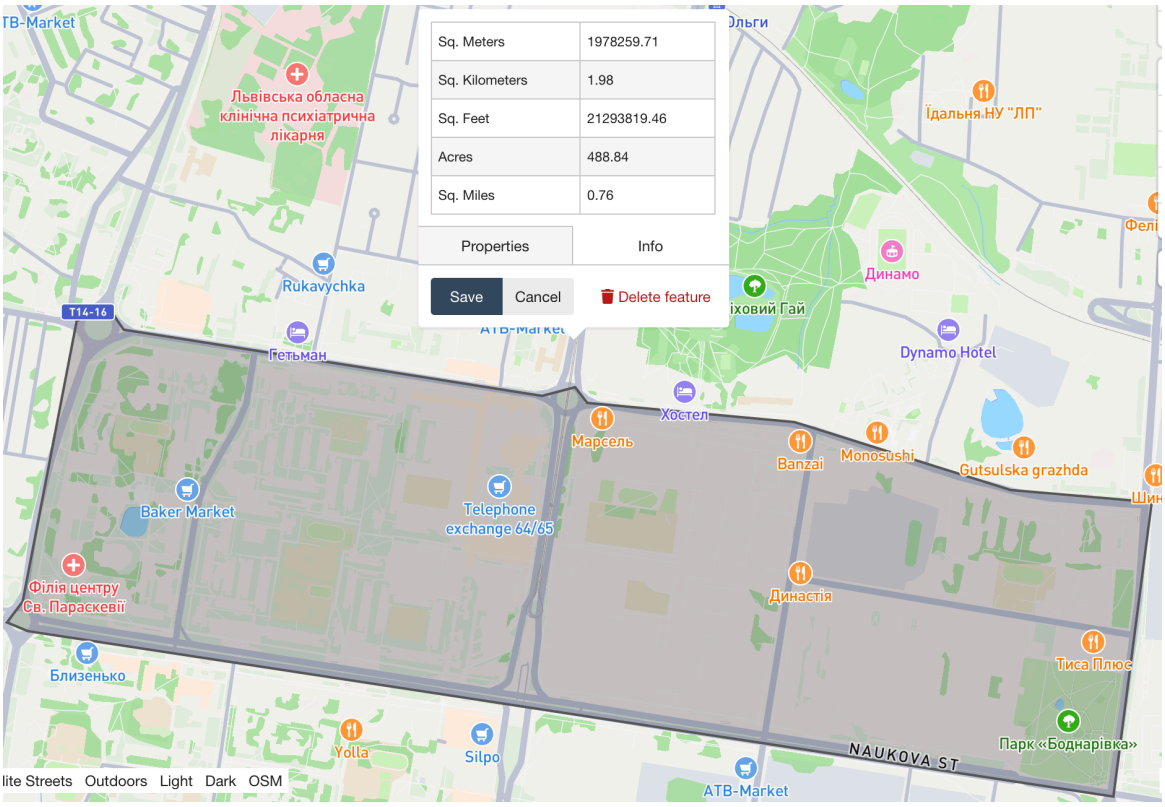


Рис. 4.2. Територія на якій здійснювався пошук точки доступу Tenda_716370 у сервісі WiGLE

Використання GPS модуля для даної задачі є обов’язковим, оскільки при виявленні нової ТД необхідно записати поточні координати. Мережева карта Alfa AWUS036NHA була вибрана, оскільки вона є виносною, а антена на ній може бути замінена в залежності від потреб, зрештою, для даної задачі може бути використана будь-яка інша мережева карта, яка може працювати в режимі моніторингу.

Виходячи з необхідності покращення точності геолокації точок доступу, було розроблено власний алгоритм для пошуку точок доступу Wi-Fi за допомогою якого в подальшому було здійснено збір інформації (рис. 4.3).

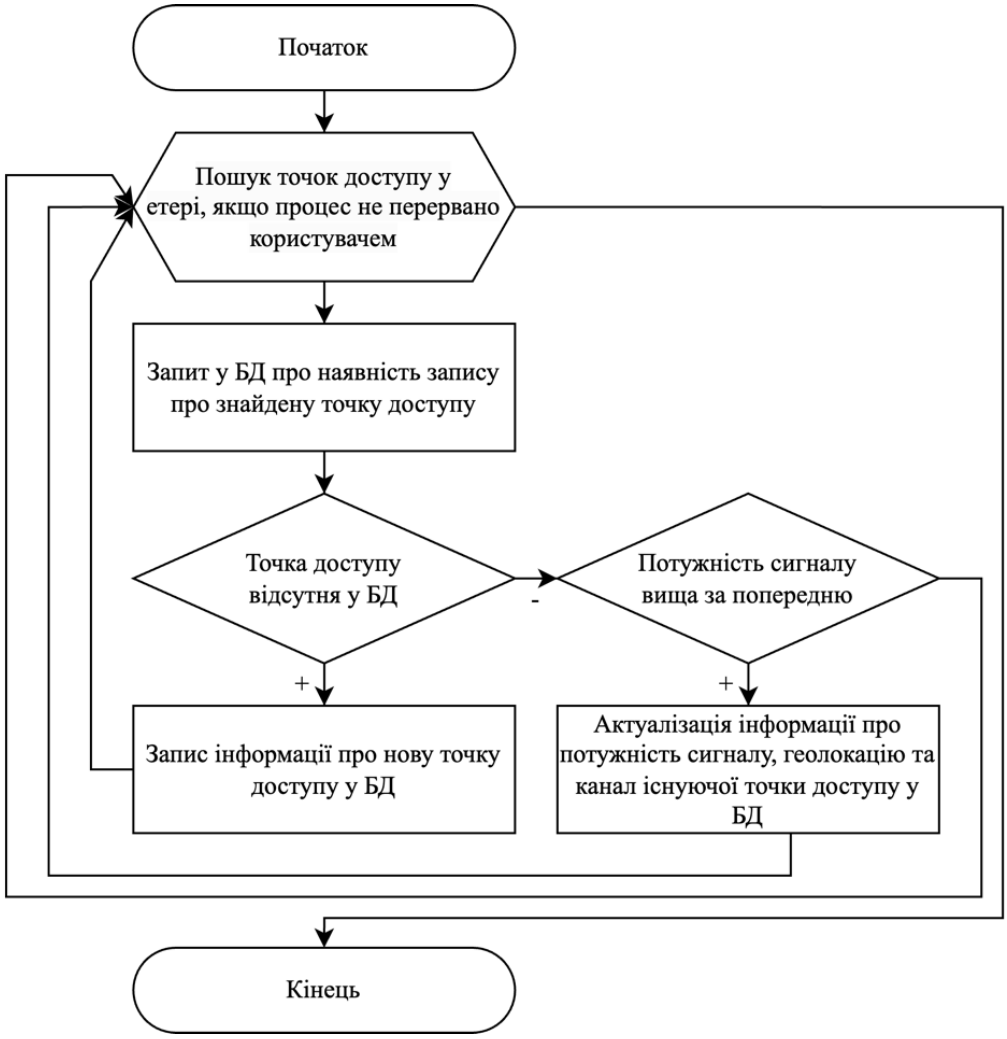


Рис. 4.3. Алгоритм збору і агрегації даних про геолокацію точок доступу Wi-Fi

Даний алгоритм дозволяє здійснювати збір і агрегацію даних по відношенню до точок доступу, які несуть унікальну інформацію. Кожній точці доступу присвоюється унікальний ідентифікатор (uuid), на основі її MAC адреси та ідентифікатора SSID (код функціоналу представлено у додатку Б, файл generate_uuid.py). Якщо інформація про ТД з’являється вперше, то дані про її MAC-адресу, SSID, потужність сигналу, канал та геолокацію записуються у локальну БД.

У випадку якщо дані про ТД вже наявні у БД то інформація про потужність сигналу, канал та геолокацію перезаписуються лише у випадку, якщо потужність сигналу є вищою за попередню. Таким чином застосовуючи метод наближення на основі потужності вдається досягти точності у виявленні позиції потрібного ресурсу.

Врезультаті розроблений підхід, по тому ж периметру (рис. 4.2), дозволив зібрати інформацію про 17037 точок доступу, з яких 13950 записів є не пошкодженими (такими, де GPS модуль отримував дані з супутника). Також було знайдено дублікати мереж із однаковим SSID, що може бути причиною того, що ТД належать одній системі і працюють у режимі сітки або мати однакову назву і належати різним власникам (рис 4.4).

```
sqlite> SELECT * FROM location_data LIMIT 10;
50:d4:f7:ac:f6:4c|Struk|-80|1|49.7855425|24.0251378333333
d4:da:21:5f:de:a6|Peremoha|-63|1|49.7854881666667|24.0250241666667
da:da:21:5f:de:a6|<hidden>|-66|1|49.7855065|24.0244428333333
b0:95:75:26:fb:ee|TP-Link_FBEE|-64|1|49.7854295|24.0245796666667
b0:4e:26:a2:b1:f2|ARKA|-83|1|49.7851281666667|24.0246595
14:eb:b6:ad:54:c7|TWINS|-83|2|49.7854361666667|24.0245905
00:31:92:b9:8f:f6|str115v-97|-75|3|49.7855601666667|24.0245703333333
74:4d:28:4e:c6:44|R I M|-80|3|49.7853183333333|24.0246308333333
06:31:92:b9:8f:f6|<hidden>|-68|3|49.785696|24.0244365
50:ff:20:2f:05:28|Stealth|-33|3|0.0|0.0
sqlite> SELECT COUNT(*) FROM location_data;
17037
sqlite> SELECT COUNT(*) FROM location_data WHERE latitude != 0.0 AND longitude != 0.0 ;
13950
sqlite> SELECT COUNT(DISTINCT ssid) FROM location_data;
12393
sqlite> SELECT COUNT(DISTINCT ssid) FROM location_data WHERE latitude != 0.0 AND longitude != 0.0;
10355
```

Рис. 4.4. Аналіз зібраних даних з радіоетеру про геолокацію Wi-Fi точок доступу

Для візуалізації даних на карті було використано проект OpenStreetMap, який є безкоштовним і розповсюджується за ліцензією Open Database License. На рис. 4.5 візуалізовано усі виявлені ТД на заданій територіальній одиниці.

Рис. 4.5. Візуалізація даних про Wi-Fi точки доступу на карті

Програмний код візуалізації мовою розмітки гіпертексту наведено у додатку Б у файлі visualization.html. До візуалізації було додано фільтрацію за параметром SSID, та проміжками широти та довготи. Отже можемо ввести ідентифікатор, на проміжку, який нас цікавить і порівняти точність публічної БД WiGLE зібраних даних із актуальними даними зібраними за допомогою представленого підходу (Рис. 4.6).

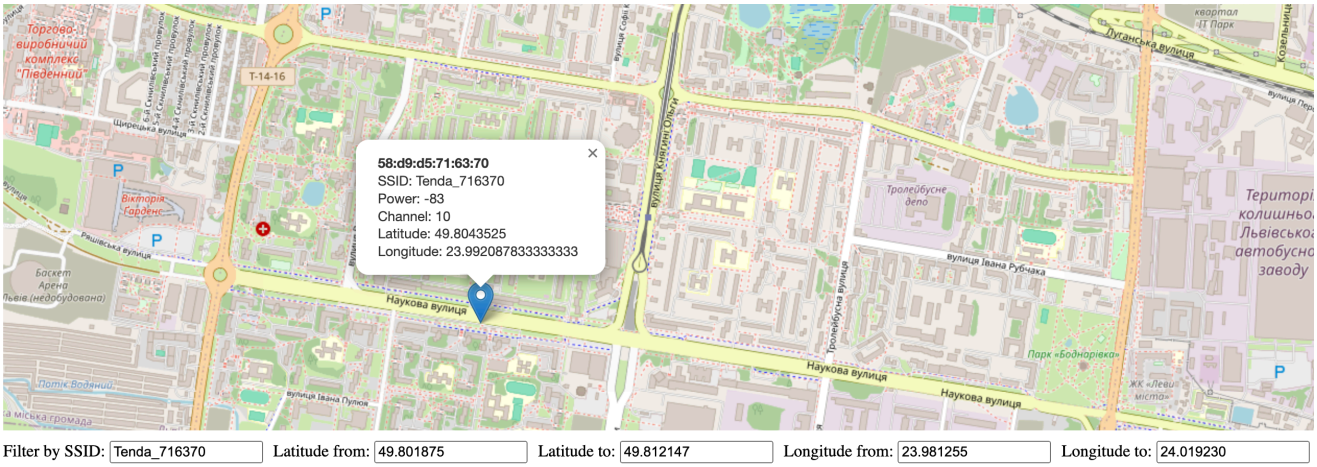


Рис. 4.6. Пошук конкретної точки доступу і її візуалізація на карті

З рис. 4.6 можемо бачити, що ідентифікатор бездротової мережі Tenda_716370 є унікальним для досліджуваного периметра розміром у 2км^2. Якщо порівнювати дані отримані з публічної БД WiGLE (рис. 4.1), з наявними, то можемо бачити, що отримати точні координати місцезнаходження конкнетного пристрою навіть на невеликій площі доволі важко. Отже, можемо зробити висновок, що агрегація даних і метод наближення на основі потужності дозволяють отримати точнішу геолокацію шуканого пристрою.

4.2. Застосування діагностичної моделі системи-приманки для бездротових мереж стандарту IEEE 802.11

На основі формули 3.4 та таблиці 3.4 знайдемо матрицю ваг кожного з елементів по відношенню одне до одного:

$$N = \begin{vmatrix} 1 & 2 & 1/5 & 1/8 & 1/9 & 1/7 \\ 1/2 & 1 & 1/5 & 1/8 & 1/9 & 1/7 \\ 5 & 5 & 1 & 1/6 & 1/9 & 1/6 \\ 8 & 8 & 6 & 1 & 1/4 & 4 \\ 9 & 9 & 9 & 4 & 1 & 8 \\ 7 & 7 & 5 & 1/4 & 1/8 & 1 \end{vmatrix}$$

Знайдемо суми коефіцієнтів для кожного зі стовпців для подальшої нормалізації матриці *N* (3.5).

$$S_1 = 1 + \frac{1}{2} + 5 + 8 + 9 + 7 = 30.5$$

$$S_2 = 2 + 1 + 5 + 8 + 9 + 7 = 32$$

$$S_3 = \frac{1}{5} + \frac{1}{5} + 1 + 6 + 9 + 5 = 21.4$$

$$S_4 = \frac{1}{8} + \frac{1}{8} + \frac{1}{6} + 1 + 4 + \frac{1}{4} = 5.7$$

$$S_5 = \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \frac{1}{4} + 1 + \frac{1}{8} = 1.71$$

$$S_6 = \frac{1}{7} + \frac{1}{7} + \frac{1}{6} + 4 + 8 + 1 = 13.45$$

Відповідно до формули 3.6 знайдемо нормалізовану матрицю |N|:

$$|N| = \begin{vmatrix} \frac{1}{30.5} & \frac{2}{32} & \frac{1/5}{21.4} & \frac{1/8}{5.7} & \frac{1/9}{1.71} & \frac{1/7}{13.45} \\ \frac{1/2}{30.5} & \frac{1}{32} & \frac{1/5}{21.4} & \frac{1/8}{5.7} & \frac{1/9}{1.71} & \frac{1/7}{13.45} \\ \frac{5}{30.5} & \frac{5}{32} & \frac{1}{21.4} & \frac{1/6}{5.7} & \frac{1/9}{1.71} & \frac{1/6}{13.45} \\ \frac{8}{30.5} & \frac{8}{32} & \frac{6}{21.4} & \frac{1}{5.7} & \frac{1/4}{1.71} & \frac{4}{13.45} \\ \frac{9}{30.5} & \frac{9}{32} & \frac{9}{21.4} & \frac{4}{5.7} & \frac{1}{1.71} & \frac{8}{13.45} \\ \frac{7}{30.5} & \frac{7}{32} & \frac{5}{21.4} & \frac{1/4}{5.7} & \frac{1/8}{1.71} & \frac{1}{13.45} \end{vmatrix} = \begin{vmatrix} 0.033 & 0.062 & 0.009 & 0.022 & 0.065 & 0.011 \\ 0.016 & 0.031 & 0.009 & 0.022 & 0.065 & 0.011 \\ 0.164 & 0.156 & 0.047 & 0.029 & 0.065 & 0.012 \\ 0.262 & 0.25 & 0.28 & 0.175 & 0.146 & 0.297 \\ 0.295 & 0.281 & 0.421 & 0.702 & 0.585 & 0.595 \\ 0.23 & 0.219 & 0.234 & 0.044 & 0.073 & 0.074 \end{vmatrix}$$

Просумувавши коефіцієнти кожного рядка нормалізованої матриці і розділивши суму на кількість коефіцієнтів рядка за допомогою (3.7) і отримаємо вагу кожного з механізмів захисту.

$$x = \begin{bmatrix} \frac{0.033 + 0.062 + 0.009 + 0.022 + 0.065 + 0.011}{6} \\ \frac{0.016 + 0.031 + 0.009 + 0.022 + 0.065 + 0.011}{6} \\ \frac{0.164 + 0.156 + 0.047 + 0.029 + 0.065 + 0.012}{6} \\ \frac{0.262 + 0.25 + 0.28 + 0.175 + 0.146 + 0.297}{6} \\ \frac{0.295 + 0.281 + 0.421 + 0.702 + 0.585 + 0.595}{6} \\ \frac{0.23 + 0.219 + 0.234 + 0.044 + 0.073 + 0.074}{6} \end{bmatrix} = \begin{bmatrix} 0.034 \\ 0.026 \\ 0.079 \\ 0.235 \\ 0.48 \\ 0.146 \end{bmatrix}$$

Відповідно до матриці x отримуємо коефіцієнти для кожного із механізмів захисту. Фільтрування за MAC адресою дорівнює 0,034; приховування ідентифікатора ТД (SSID) за рахунок вимкнення функції розсилання маячків у відкритий етер рівне 0,026; протокол бездротової безпеки WEP рівний 0,079; протоколи бездротової безпеки WPA/WPA2 дорівнює 0,235; WPA3 дорівнює 0.48; WPS дорівнює 0,146.

На основі отриманих коефіцієнтів у результаті обчислень за методом оцінки ієрархій, ми можемо оцінити складність обхідних заходів для кожної комбінації механізмів захисту ТД стандарту IEEE 802.11, додавши ці коефіцієнти на відрізку від 0 до 1.

Оскільки увімкнений механізм WPS лише погіршує захищеність ТД, комбінація цього механізму з протоколами бездротової безпеки WPA2 буде відрізнятися за різницею коефіцієнтів, а саме:

$$WPA2 - WPS = 0.235 - 0.146 = 0.089$$

Для того щоб зацікавити зловмисників – захист на точці доступу однозначно повинен бути присутнім, але таким чином, щоб його можна було з відносно не великими зусиллями подолати.

4.3. Аналіз результатів з удосконалення методики розподіленого підбору ключа доступу до механізму захисту WPA2 у мережах IEEE 802.11

У виведенні базового словника для лобової атаки було використано ресурс операційної системи Kali Linux. Kali Linux – це операційна система сімейства Linux, яка базується на дистрибутиві Debian, є безкоштовною і знаходиться у

вільному доступі. Прямим призначенням даної операційної системи є тестування на проникнення. Але окрім тестувань власних систем не виключено, що такі операційні системи можуть використовуються зловмисниками для атак [89].

В межах проведення досліду було проаналізовано словники, які поставляються з операційною системою Kali Linux, і знаходяться у директорії /usr/share/wordlists. Дані словники фільтруються таким чином, щоб з них виключались усі слова-комбінації які менші за 8 символів, і ті, які не складаються із символів системи кодування ASCII цілком. Дані словники інтегруються в один, з якого виключаються не унікальні слова-комбінації (Лістинг 4.1).

Лістинг 4.1. Виведення базового словника для проведення лобової атаки на пакет рукостискання протоколів бездротової безпеки WPA/WPA2 у операційній системі Kali Linux

```
cat dirbuster/*.txt fern-wifi/* rockyou.txt fasttrack.txt metasploit/*.lst
metasploit/*.txt | grep ........ | grep -P -v "[^[:ascii:]]" | sort --unique
```

Звичайно ж кожне тестування залежить від типу апаратного забезпечення, конфігурації програмного забезпечення. У цьому дослідженні було досліджено швидкість обчислення ключа для протоколу бездротової безпеки WPA2 з попередньо перехопленого пакету «рукостискання».

Дослід проводився у контейнері віртуальної машини CoreOS, якій було виділено 1 Гб оперативної пам'яті і одне ядро процесора Intel Core i5-4590 з тактовою частотою 3.3 ГГц.

Попередньо було здійснено тестування за допомогою команди aircrack-ng –S, яка дозволяє здійснити замір швидкості лобової атаки у співвідношенні ключів за секунду.

Після виконання команди з лістингу 4.1 і підрахувавши кількість ключів, отримуємо значення C_d = 9801317.

Замір швидкості лобової атаки на двох різних підходах, віртуалізації і контейнеризації було проведено по 10 разів, результати представлено у табл. 4.1, а також візуалізовано на рис. 4.7.

Таблиця 4.1

Заміри швидкості перебору ключів за словником

Спроба / Тип віртуалізації	1	2	3	4	5	6	7	8	9	10
Повна віртуалізація (ключів/секунду)	922	956	954	955	927	911	949	947	933	912
Контейнеризація (ключів/секунду)	1053	1038	1038	1041	1031	1032	1038	1038	1054	1036

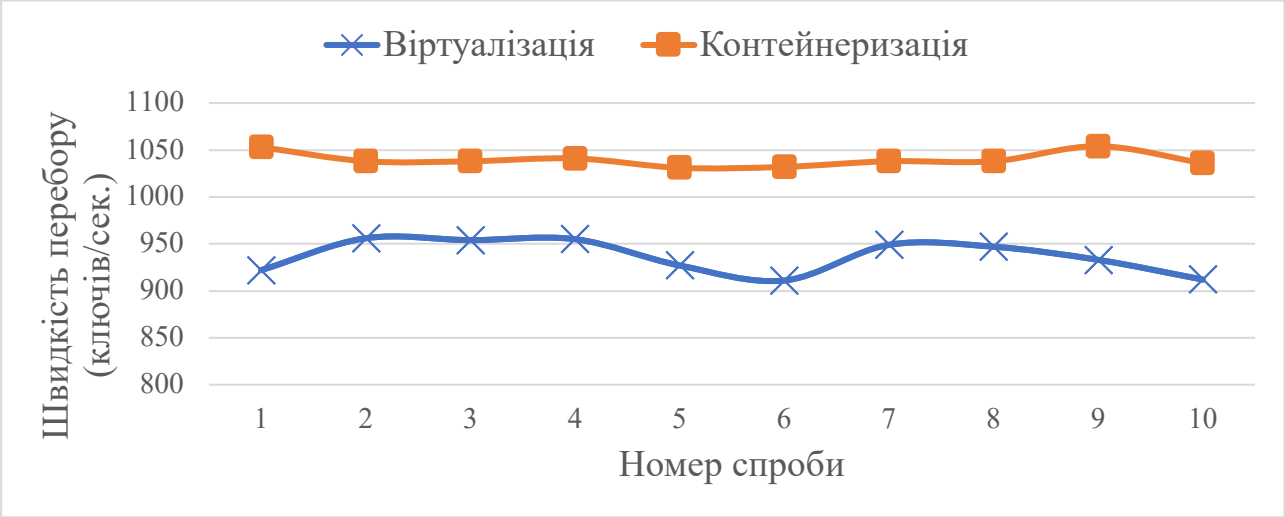


Рис. 4.7. Візуалізація порівняння швидкості перебору ключів за допомогою віртуалізації і контейнеризації

Обчислимо середню швидкість для віртуалізації:

$$\overline{S_V} = \frac{922 + 956 + 954 + 955 + 927 + 911 + 949 + 947 + 933 + 912}{10} = 936{,}6$$

Обчислимо середню швидкість для контейнеризації:

$$\overline{S_V} = \frac{1053 + 1038 + 1038 + 1041 + 1031 + 1032 + 1038 + 1038 + 1054 + 1036}{10} = 1039{,}9$$

Володіючи даними про кількість ключів у базовому словнику і швидкість з якою опрацьовуються ключі можемо скористатись формулою (3.11) і знайти приблизний час за який буде здійснено перебір усього базового словника.

$$t_{BF} = \frac{9801317}{1039{,}9} \approx 9425\text{сек} \approx 2\text{год } 37\text{хв}$$

Якщо ж у базовому словнику ключ не буде знайдено, то пошук ключа буде розпочато із восьмисимвольного словника. Як вже було згадано вище, WPA2 дозволяє задати ключ довжиною від 8 до 63 символів, що еквівалентно 56 варіантам довжини ключа. Це означає, що кількість варіантів буде збільшено в десятеро при переході на наступний словник, а отже й потужності буде затребувано в десятеро більше або ж при тій же ж потужності часу буде витрачено в десятеро більше.

Пошук ключа доступу з перехопленого пакету рукостискання є ресурсоємною операцією. Кількість усіх можливих ключів хоч і є скінченним числом, та все ж воно досить велике, його можна обчислити за формулою (4.1).

$$n = \sum_{i=8}^{63} 95^i \tag{4.1}$$

Зі збільшенням довжини ключа – розмір словника збільшується експоненційно (рис. 4.8).

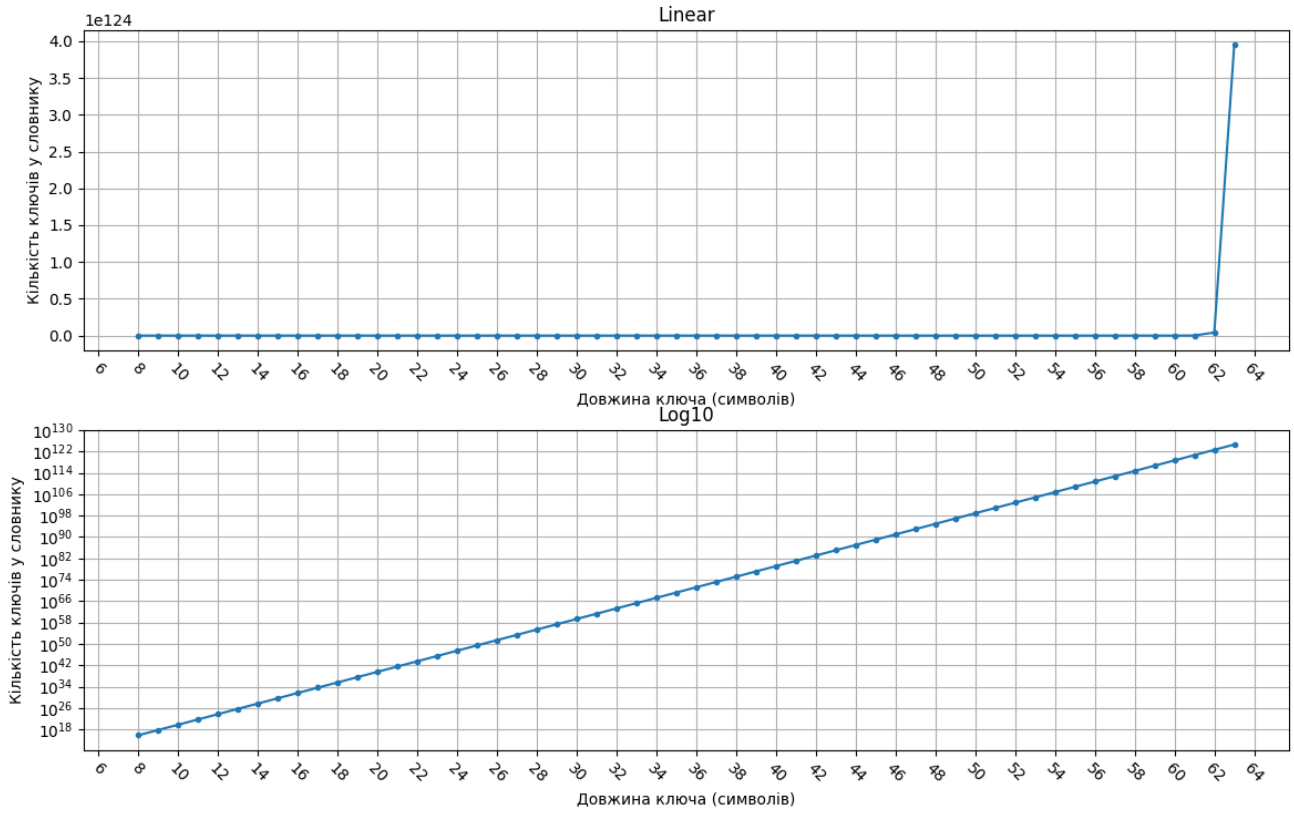


Рис. 4.8. Лінійне та логарифмічне представлення зміни кількості ключів у словнику відносно зміни довжини ключі

Дані на рис 4.8 свідчать про те, що з кожною новою ітерацією обчислювальних потужностей потрібно вдесятеро більше, що в свою чергу дуже важко реалізувати без хмарних обчислень.

Незважаючи на отримані результати, важливо зазначити, що при використанні відмінного апаратного забезпечення результати будуть аналогічно іншими. Проте, у даному дослідженні, це не вплине на вагові коефіцієнти, отримані в результаті методу аналізу ієрархій, оскільки він базується на різниці між точками відліку, які в даному досліджені представлені статичними словниками.

Щоб застосувати метод аналізу ієрархій для даного дослідження, потрібно оцінити характеристики по відношенню одне до одного за шкалою від 1 до 9. Оскільки складність словника збільшується лінійно, тобто, щоразу у десять разів (рис. 4.9). Відповідно на відрізку від 1 до 9 ціною переходу від одного словника до іншого буде додавання до попереднього значення коефіцієнт 0,145454545.

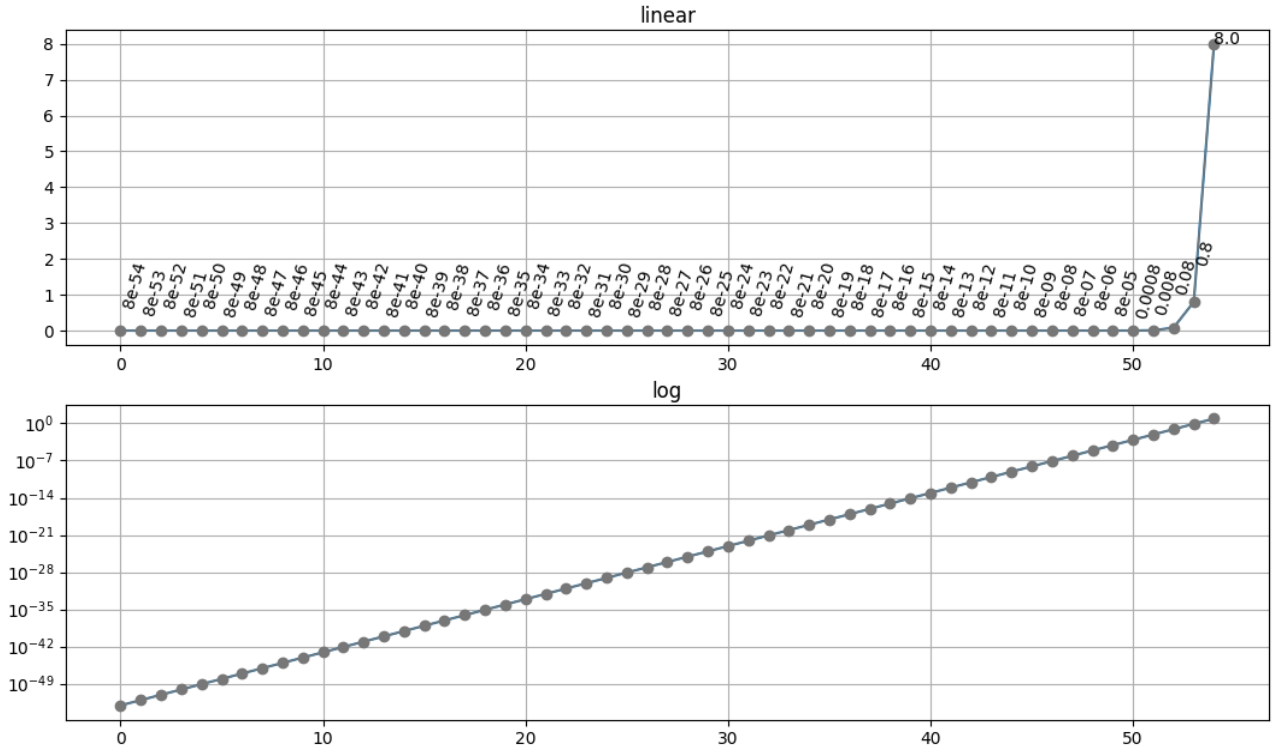


Рис. 4.9. Лінійне та логарифмічне представлення зміни складності словника у методі аналізу ієрархій

Використаємо формулу (3.4) для знаходження вагової матриці:

$$N = \begin{vmatrix} 1 & 1{,}145454545 & \dots & 8{,}854545454 & 9 \\ 0{,}873015873 & 1 & \cdots & 8{,}709090909 & 8{,}854545454 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0{,}112936345 & 0{,}114822547 & \cdots & 1 & 1{,}145454545 \\ 0{,}111111111 & 0{,}112936345 & \cdots & 0{,}873015873 & 1 \end{vmatrix}$$

Використаємо формулу (3.5) для знаходження суми коефіцієнтів для кожного рядка матриці *N*:

$$S = \begin{vmatrix} 280 \\ 271{,}873 \\ \vdots \\ 16{,}70776 \\ 15{,}67342 \end{vmatrix}$$

Використаємо формулу (3.6) для знаходження нормалізованої матриці *N*:

$$|N| = \begin{vmatrix} \frac{1}{280} & \frac{1{,}145454545}{271{,}873} & \cdots & \frac{8{,}854545454}{16{,}70776} & \frac{9}{15{,}67342} \\ \frac{0{,}873015873}{280} & \frac{1}{271{,}873} & \cdots & \frac{8{,}709090909}{16{,}70776} & \frac{8{,}854545454}{15{,}67342} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{0{,}112936345}{280} & \frac{0{,}114822547}{271{,}873} & \cdots & \frac{1}{16{,}70776} & \frac{1{,}145454545}{15{,}67342} \\ \frac{0{,}111111111}{280} & \frac{0{,}112936345}{271{,}873} & \cdots & \frac{0{,}873015873}{16{,}70776} & \frac{1}{15{,}67342} \end{vmatrix}$$

Застосуємо формулу (3.7) для отримання ваги кожного з оцінюваних елементів. Для отримання значень у відсотках матрицю *x* помножимо на 100.

$$x = \begin{vmatrix} 0{,}003011 \\ 0{,}003127 \\ \vdots \\ 0{,}051451 \\ 0{,}053967 \end{vmatrix} \cdot 100\% = \begin{vmatrix} 0{,}3011 \\ 0{,}3127 \\ \vdots \\ 5{,}1451 \\ 5{,}3967 \end{vmatrix}$$

Тобто, вага словника із ключами довжиною у 8 символів складає 0,3011%, вага словника із ключами довжиною в 9 символів складає 0,3128%, вага словника із ключами довжиною в 63 символи складає 5,1451%, а вага словника із ключами довжиною в 64 символи складає 5,3967%.

Як вже було зазначено, довжина ключа не є єдиним критерієм оцінки його складності. Набір символів присутніх у словнику є також важливим критерієм. На

основі табл. 3.5—3.6 можемо зробити висновки про те, які комбінації символів у словниках є логічними для використання. Максимальна кількість символів, які можуть бути використані в паролі становить 95, тобто 95 символів складає 100%. Відповідно до цього отримуємо табл. 4.2.

Таблиця 4.2

Відсоткове співвідношення кількості символів у словниках

Кількість символів	95	94	62	52	36	32	26	10
Відсоткове представлення (*w*)	100	98,95	65,26	54,17	37,89	33,68	27,36	10,5

4.4. Виявлення атак «злий двійник» на мережі стандарту IEEE 802.11 (Wi-Fi) за допомогою моделі класифікації KNN

ЗД – це тип атаки на бездротову мережу, коли зловмисник встановлює фальшиву ТД Wi-Fi із такою ж назвою, що й легітимна ТД, щоб обманом змусити користувачів підключитися до неї. Як тільки користувач підключається до підробленої ТД, зловмисник може перехоплювати та маніпулювати мережевим трафіком користувача, викрадати конфіденційну інформацію та запускати подальші атаки [90].

WPA3 містить нову функцію під назвою Simultaneous Authentication of Equals (SAE), також відому як Dragonfly, яка забезпечує сильніший захист від атаки ЗД. SAE використовує безпечний протокол обміну ключами для встановлення унікального ключа шифрування для кожного сеансу, що значно ускладнює зловмиснику перехоплення та дешифрування мережевого трафіку користувача.

Однак важливо зазначити, що, хоч WPA3 є більш стійким до атаки ЗД, він не повністю захищає від них. Оскільки ще дуже велика кількість клієнтських пристроїв були виготовлені до винаходу протоколу WPA3, то виробниками мережевих пристроїв було закладено транзитивний механізм, який дозволяє застарілим користувацьким пристроям працювати з новим мережевим обладнанням [91]. Згодом, у 2019 році були опубліковані свідчення про те, що деякі

маршрутизатори WPA3 були вразливими до атак із пониженням версії протоколу безпеки, що потенційно могло дозволити зловмиснику обійти захист SAE і здійснити атаку «звий двійник» [92].

Станом на 2021 рік у глобальна економічна вартість Wi-Fi оцінювалась в 3,3 трильйона доларів США, і очікується, що до 2025 року вона зросте до 5 трильйонів доларів [93]. Дана технологія безумовно є рушієм сучасного бізнесу. Та технологія Wi-Fi, як і більшість сучасних, також має певні недоліки, що стосується інформаційної безпеки. Однією із найрозповсюдженіших атак, якщо говорити про бездротові мережі є ЗД. Якщо у дротових мережах, щоб здійснити схожий тип атаки, потрібно мати фізичний доступ до приміщення, в якому функціонує комп'ютерна мережа, то в бездротових мережах такої потреби немає. Зловмисник може знаходитись на відстані від ТД і з легкістю клонувати легітимну мережу. З використанням направлених антен зловмисник може добитись того, що сигнал від нелегітимної ТД може бути сильнішим ніж від легітимної. Таким чином, зловмисники можуть перетягнути клієнтів у мережу, яку вони контролюють. Таким чином користувацькі і корпоративні дані можуть бути викрадено чи модифіковано.

Та як відомо, кожен електронний пристрій, навіть ті, які виготовлені на одному і тому ж заводі за ідентичною технологією – є унікальним. Навіть пристрої, ідентичні за конфігурацією апаратного та програмного забезпечення, все одно можуть мати різні цифровий слід через варіації електронних компонентів. Якщо говорити про мережі стандарту IEEE 802.11, то цифровим відбитком ТД на канальному рівні моделі OSI може виступати потужність сигналу. В мережах Wi-Fi навіть найменше відхилення антени маршрутизатора може змінити зону покриття мережі. Якщо говорити про атаку ЗД, то її зазвичай проводять за допомогою обладнання, яке досить сильно відрізняється від того, яке використовується для роздачі Wi-Fi трафіку. Окрім того, велику роль відіграє розташування обладнання. Якщо ТД Wi-Fi буде знаходитись в певному приміщенні, а атака буде проводитись з-за його меж, то в момент атаки рівень сигналу від ТД на групі клієнтських пристроїв буде зовсім іншим, ніж за відсутності атаки.

Та в сучасному світі, коли більшість клієнтів є мобільними і без будь-яких обмежень можуть змінювати своє місце роботи – це не може бути достовірним джерелом для виявлення атаки. Таким джерелом може бути пристрій, який статично перебуває в одному і тому ж місці і з певною періодичністю перевіряє рівень сигналу від заданої ТД, після чого робить висновок про наявність атаки за рівнем отриманого сигналу. Зазвичай одного такого пристрою може бути не достатньо, оскільки рівень сигналу від легітимної ТД і від ЗД за деяких умов можуть збігтись, і тоді атака буде не поміченою. Отже, чим більше пристроїв, які слідкують за рівнем сигналу від легітимної ТД, тим вища імовірність виявлення атаки, оскільки в зловмисника все менше шансів підібрати правильне розташування і конфігурацію потужності сигналу на пристрої, який виступає в якості ЗД.

Аналіз даних і визначення вторгнення зазвичай є доволі затратною процедурою. Водночас пристрої, які здійснюють моніторинг трафіку не можуть бути громіздкими, принаймні більшими за саме мережеве обладнання, а ціна такої системи не може перевищувати ціну інформації, яка обробляється в легітимній мережі.

Тому в даному дослідженні було представлено метод виявлення атаки під назвою ЗД, яка повністю задовольняє всі вище згадані вимоги [94].

4.4.1. Матеріали та методи дослідження

Об’єктом дослідження виступають мережі стандарту IEEE 802.11, які за своєю природою є вразливими до атаки ЗД. Основною гіпотезою даного дослідження є можливість ідентифікації появи нелегітимної Wi-Fi ТД поряд з легітимною. Під час розробки моделі СВВ було припущено, що атаку можна попередити завдяки алгоритмам машинного навчання з вчителем.

Основний пристрій, за допомогою якого проводилось дослідження – це одноплатний комп’ютер Raspberry Pi 4 Model B, хоча для відтворення даного дослідження може бути використаний будь-який інший комп’ютер із аналогічними характеристиками. Також, для перехоплення пакетів необхідна мережева карта для

роботи у мережах стандарту IEEE 802.11 із можливістю роботи у режимі моніторингу. У досліджені було використано мережеву карту Alfa Network AWUS036NHA із чипсетом AR9271, який було вибрана з переліку мережевого обладнання рекомендованого до застосування програмним засобом aircrack-ng, який в свою чергу заснований на бібліотеці Scapy [95]. На одноплатний комп'ютер було встановлено операційну систему Linux Raspbian, із мінімальним набором додаткового програмного забезпечення, задля уникнення надлишкового споживання ресурсів. Як пристрій, за яким було здійснено спостереження – це будь-який Wi-Fi маршрутизатор, в нашому випадку використовувався Xiaomi Mi 4A.

Програмне забезпечення для перехоплення пакетів з ефіру Wi-Fi було розроблено за допомогою мови програмування Python. Функціонал перехоплення пакетів з ефіру було здійснено за допомогою бібліотеки Scapy [96]. Далі такі пристрої називатимуться сенсорами.

На основний одноплатний комп'ютер було встановлено базу даних на основі часових рядів InfluxDB [97], для запису даних із сенсорів.

У схемі з одним сенсором на нього встановлюється і програмне забезпечення, яке перехоплює пакети і база даних InfluxDB. У схемі із двох і більше сенсорами InfluxDB встановлюється лише на один із сенсорів, а також на ньому розгортається Wi-Fi ТД, яка використовується для доставки даних в базу даних та іншої службової комунікації.

Scapy – це потужна бібліотека Python для обробки та аналізу мережевих пакетів, а саме створення та надсилання мережевих пакетів, перевірки та аналізу мережевого трафіку, тестування та аналізу безпеки мережі. У даному дослідженні наша програма виконувала перехоплення пакетів, в яких був наявний маячок (шар Dot11Beacon, в Scapy). Beacon (маячок) у Wi-Fi – це тип кадру керування, який періодично надсилається ТД, щоб оголосити про свою присутність і надати клієнтам основну інформацію про мережу, а отже є найкращим типом пакету для моніторингу. Мета маячків – дозволити клієнтам виявляти доступні мережі Wi-Fi і надавати основну інформацію про мережу, наприклад назву мережі (SSID),

підтримувані швидкості передачі даних, режими безпеки, а також потужність сигналу від ТД в децибелах помножених на міліват (dBm).

Маячки використовуються на початковій стадії з’єднання Wi-Fi і необхідні для належного функціонування мереж Wi-Fi. Вони надають клієнтам спосіб виявити доступні мережі та прийняти обґрунтовані рішення про те, до якої мережі підключитися. Таким чином, маяки є важливим компонентом мереж Wi-Fi, надаючи інформацію про мережу та дозволяючи клієнтам виявляти мережу та підключатися до неї.

Під час експерименту Beacon пакети збирались з ефіру безперервно (до 10-ти пакетів на секунду). Потужність сигналу вимірюється в децибелах.

Як вже було згадано вище, сенсори працюють на базі одноплатних комп’ютерів, а отже і обчислювальні потужності є доволі обмеженими. Також комунікація між сенсорами в деяких випадках може бути не стабільною через низку причин.

Основною проблемою є те, що кожної секунди в службову мережу може надходити запит на запис в базу даних. Коли кілька малих пакетів передаються окремо, кожен пакет потребує власного заголовка та іншої керуючої інформації. Ці накладні витрати можуть швидко накопичуватися та займати значну частину доступної смуги пропускання, залишаючи менше місця для фактичної передачі даних. Агрегація даних може допомогти зменшити ці накладні витрати, об’єднавши кілька пакетів в один більший пакет, для якого потрібен лише один заголовок і керуюча інформація. Завдяки об’єднанню кількох пакетів в один більший пакет можна скоротити час, необхідний для передачі даних, що може допомогти зменшити затримку та підвищити загальну продуктивність службової мережі. Також існує більший ризик втрати або пошкодження пакетів через такі фактори як шум або перешкоди. Завдяки об’єднанню кількох пакетів в один більший пакет зменшується ймовірність втрати або пошкодження пакетів, оскільки більший пакет є стійкішим і менш схильний до впливу таких факторів.

Загалом агрегація даних може допомогти оптимізувати продуктивність мережі в низькошвидкісних мережах шляхом зменшення накладних витрат,

затримки та ризику втрати або пошкодження пакетів. Зазвичай це покращує роботу клієнтів мережі та забезпечує ефективніше використання доступних мережевих ресурсів.

Отже, задля уникнення перевантаження сервера InfluxDB, який працював на одноплатному комп'ютері, а також уникнення навантаження службової мережі було вирішено відправляти вже агреговані дані один раз на хвилину. Загальну схему збору даних з ефіру і комунікації між сенсорами зображено на рис 4.10.

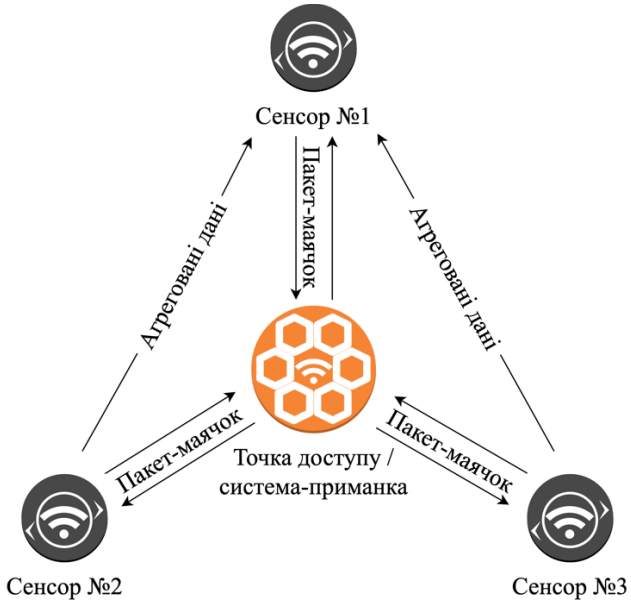


Рис. 4.10. Загальна схема збору даних з ефіру та комунікації між сенсорами

Набір метрик в однохвилинному проміжку – кількість перехоплених маячків, максимальна, мінімальна та середня потужності сигналу потужність сигналу, яка найчастіше з'являлась в ефірі. Середня потужність обчислюється як сума усіх потужностей поділена на їх кількість (4.2).

Потужність сигналу яка найчастіше з'являлась, знаходиться за допомогою статистичної функції мода (4.3).

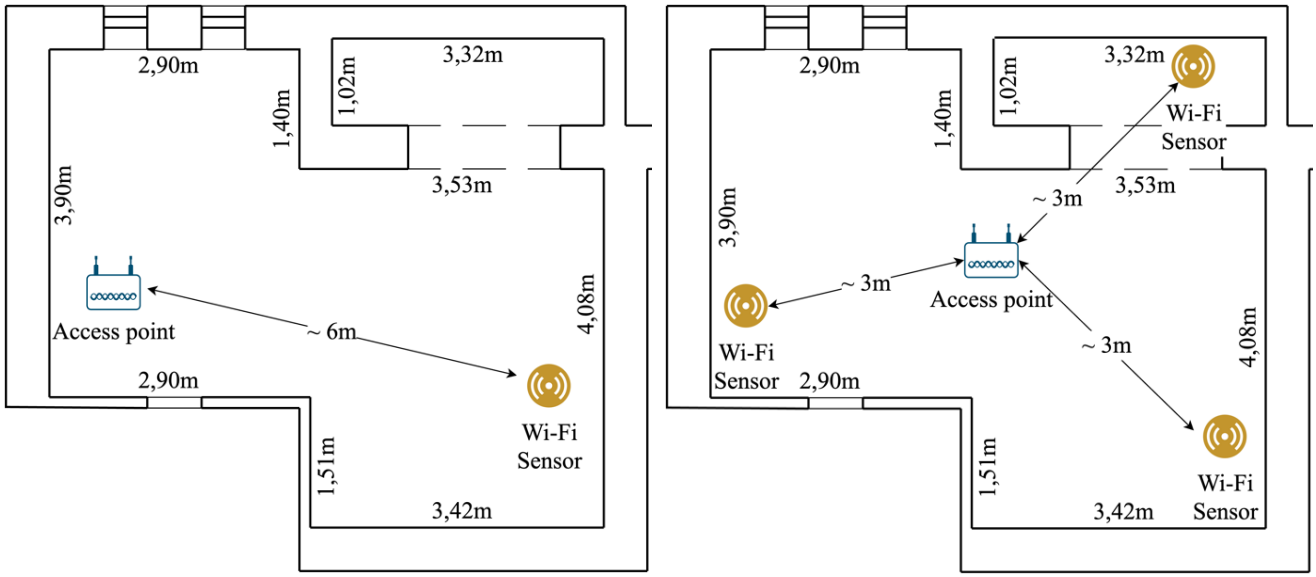
$$pwr_{avg} = \frac{sum(pwr)}{number\ of\ packets} \tag{4.2}$$

$$pwr_{most\ frequent} = mode(pwr) \tag{4.3}$$

Під час замірів ТД і сенсор(и) розташовувались у виділеній лабораторії із відсутніми іншими електронними пристроями, які могли би вплинути на рівень сигналу, хоча не виключається вплив навколишнього середовища, оскільки Wi-Fi пристрої сьогодні дуже розповсюджені. Дані збирались лише в радіочастотному діапазоні Wi-Fi 2.4ГГц (2412МГц – 2472МГц).

Для відтворення атаки в близьких до реальних умов було створено ТД із такою ж MAC адресою і ідентифікатором мережі (SSID) та розташовано в місцях за межами лабораторії в якій проводився дослід із легітимною ТД. Імітація легітимної ТД переміщалась 15 разів в сусідніх приміщеннях до того, в якому були розміщені сенсори і легітимна ТД.

Було проведено дві групи дослідів. У першій групі використовувався один сенсор, який збирав інформацію про потужність сигналу від ТД (рис. 4.11а). У другій, таких сенсорів було три. Сенсори було розставлено в умовний трикутник навколо легітимної ТД, тобто було застосовано підхід так званої тріангуляції (рис. 4.11б).



а) б)

Рис. 4.11. Схема розміщення обладнання з а) одним, б) трьома сенсорами

Після збору даних можна приступати до навчання моделі машинного навчання. Для цього нам необхідно виконати ряд дій, таких як:

– Вибір алгоритму машинного навчання, спираючись на визначену задачу;

– Підготовка даних, що передбачає збір, очищення та попередню обробку даних. Дані мають бути організовані у форматі, який підходить під вибраний алгоритм машинного навчання;

– Розділення даних на тренувальні та тестові дані. Навчальні дані використовуються для навчання моделі, а тестові дані використовуються для оцінки продуктивності моделі;

– На основі тренувальних даних проводиться навчання моделі;

– Для оцінки моделі машинного навчання використовуються тестові дані, щоб її продуктивність моделі. Це допоможе визначити, наскільки добре модель здатна узагальнювати нові дані;

– Якщо модель працює погано, то можна здійснити спробу її вдосконалення, відкоригувавши алгоритм, змінивши параметри моделі або змінивши дані;

Якщо модель задовольняє поставлені перед нею вимоги, то можна розгорнути її у робочому середовищі, щоб робити прогнози на основі нових даних.

4.4.2. Результати досліджень

Для тренування моделі машинного навчання необхідна велика кількість даних. Для того, щоб зрозуміти на скільки зібрані дані готові до обробки візуалізуємо маленькі часові відрізки і порівняємо метрики від легітимної і нелегітимної ТД (рис. 4.12).

На рис. 4.12 відображено зібрані дані одним і тим же ж сенсором, який відображає потужність сигналу від легітимної і нелегітимної точок доступу протягом двох годин. З рисунка видно, що між потужністю сигналів легітимної і нелегітимної точок доступу існує доволі велика прогалина. Це дозволяє нам робити висновок, про те, що ці дані можна використовувати для статистичного аналізу і тренування моделі машинного навчання.

Для аналізу даних було використано мову програмування Python3 із такими бібліотеками, як numpy [98] – для роботи з багатовимірними масивами і матрицями, pandas [99] – для маніпулювання даними та їх подальшого аналізу, matplotlib [100] – для візуалізації двовимірних графіків та seaborn [101] – як розширення до matplotlib.

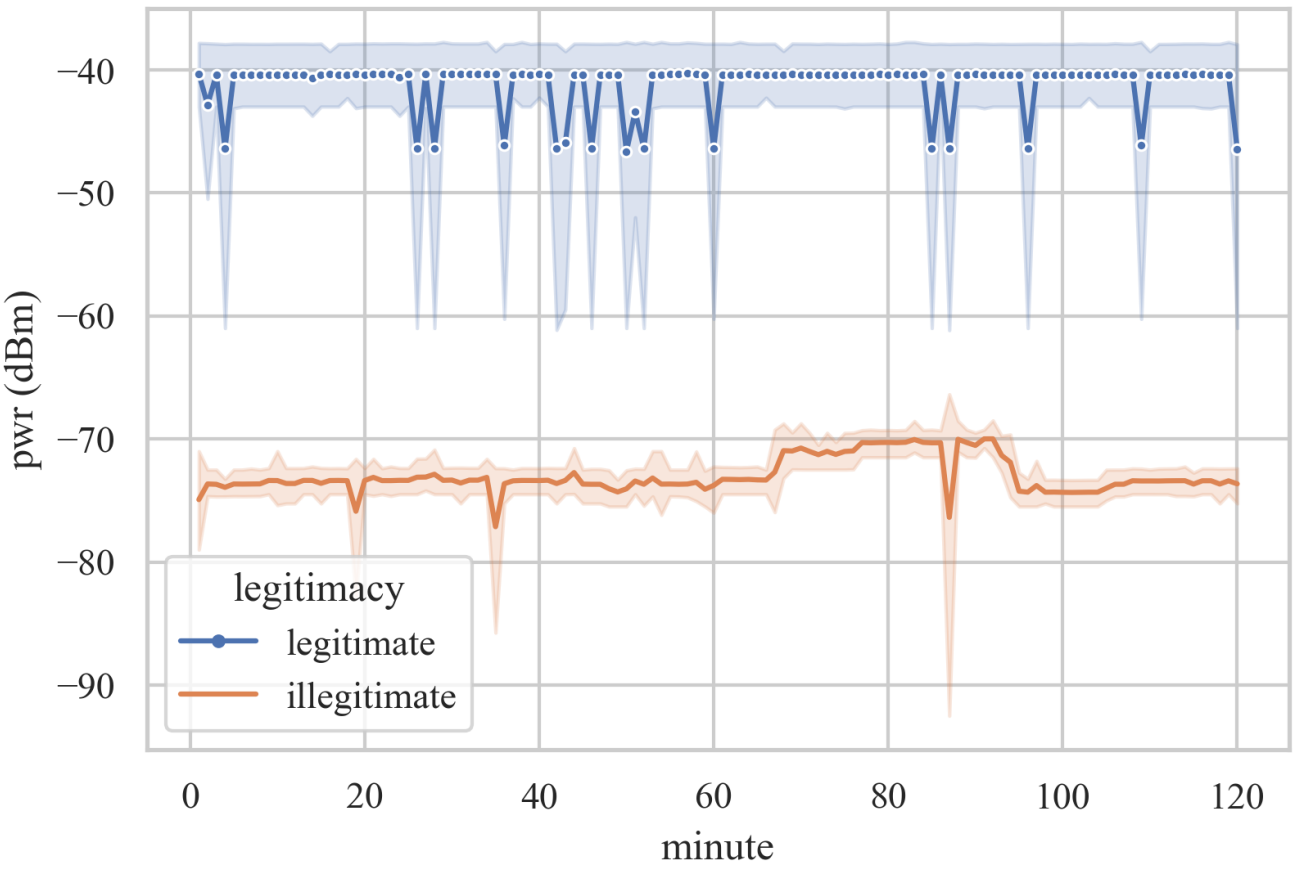


Рис. 4.12. Порівняння потужностей сигналу від легітимної і нелегітимної точок доступу

Загальна кількість в наборах даних склали 14579 рядків для досліду з одним сенсором і 20610 рядків для досліду з трьома сенсорами. Для розуміння того на скільки зібрані дані готові до тренування моделі можемо викликати функцію візуалізації кореляції на тепловій карті за допомогою бібліотеки seaborn, яка покаже, на скільки дані з набору даних корелюються між собою (рис. 4.13 – 4.14).

На рис. 4.13 метрики *min* – мінімальний рівень сигналу; *max* – максимальний рівень сигналу; *avg* – середній рівень сигналу; *mf* – мода, або той, який найчастіше трапляється; *np* – загальна кількість мережевих пакетів.

Відповідно на рис.4.14 перша частина назви метрики *s1* – *sn* відповідає за номер сенсора, а друга частина, назви метрики після нижнього підкреслення відповідає метрикам, згаданим в поясненні до рис. 4.13.

Рис. 4.13. Теплова карта кореляції метрик для набору даних із одним сенсором

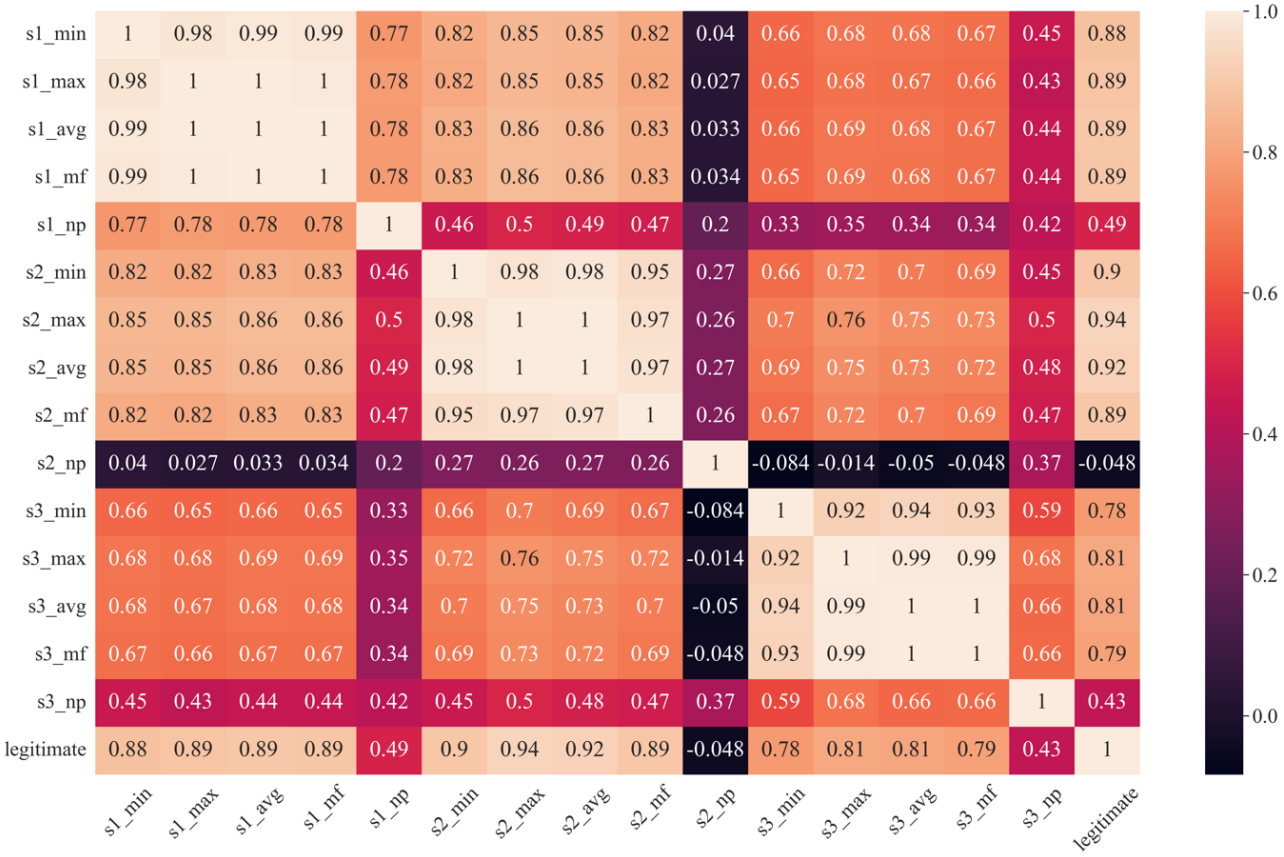


Рис. 4.14. Теплова карта кореляції метрик для набору даних із трьома сенсорами

Як відомо, коефіцієнт кореляції вимірює силу та напрямок лінійного зв’язку між двома змінними та коливається від –1 до +1, де коефіцієнт +1 вказує на ідеальну

позитивну лінійну залежність, а коефіцієнт –1 вказує на ідеальну негативну лінійну залежність. Коефіцієнт 0 означає відсутність лінійного зв'язку.

Поріг для «низької» кореляції може залежати від контексту та конкретного застосування. Однак, загалом, коефіцієнт кореляції менше 0,3 або більше –0,3 часто вважається низькою кореляцією [102].

Та у випадку, якщо в наборі даних є багато змінних і кореляція між певною змінною та іншими змінними стабільно слабка, може бути доречним виключити цю змінну з процесу аналізу чи моделювання.

Одразу ж можемо побачити, що стовпці із суфіксом *np*, що є абревіатурою від number of packets, дуже погано корелюються іншими параметрами, в деяких випадках значення є від'ємним. Це означає, що такі параметри можуть бути шкідливими для моделі передбачення. Отже, ними необхідно знехтувати задля забезпечення точності моделі. На рис. 4.14—4.15 можемо побачити теплову карту кореляції метрик, але вже без метрики, яка відповідає за кількість перехоплених пакетів-маячків.

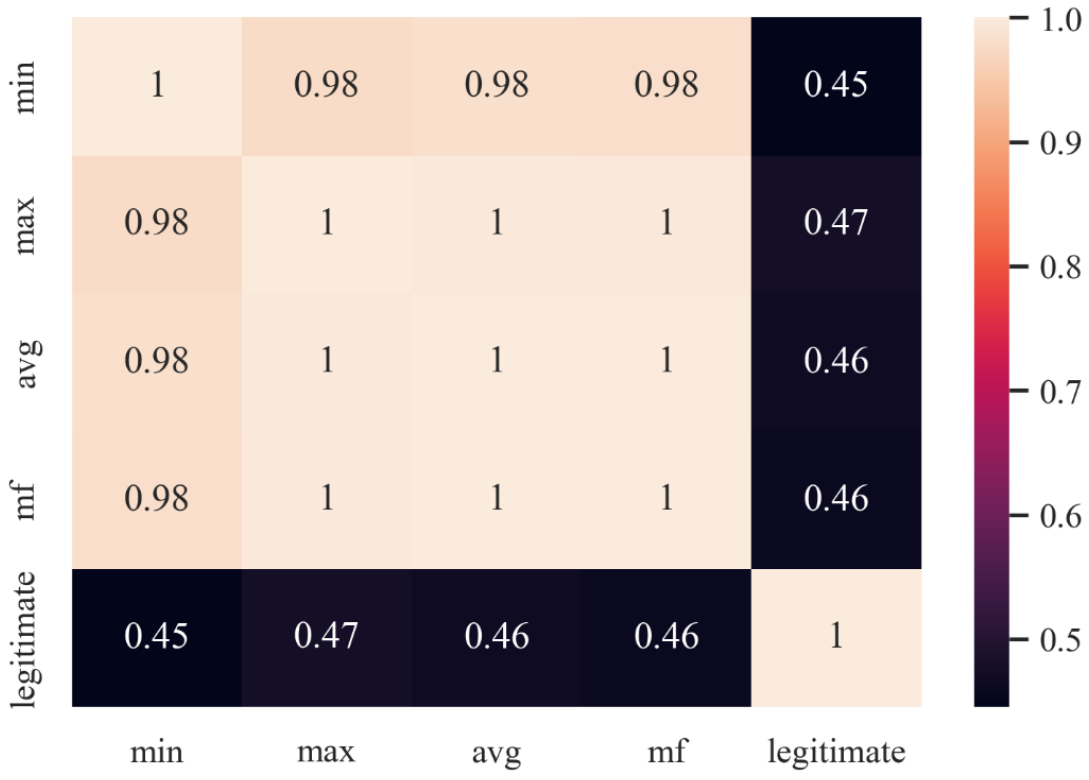


Рис. 4.14. Теплова карта кореляції метрик для набору даних із одним сенсором без метрики кількості перехоплених пакетів-маячків

Як видно на рис. 4.14, мінімальна кореляція між метриками складає не менше 0.45 для набору даних з що є доволі хорошими показниками. Це може означати, що такий набір даних може бути використаний для тренування моделі машинного навчання.

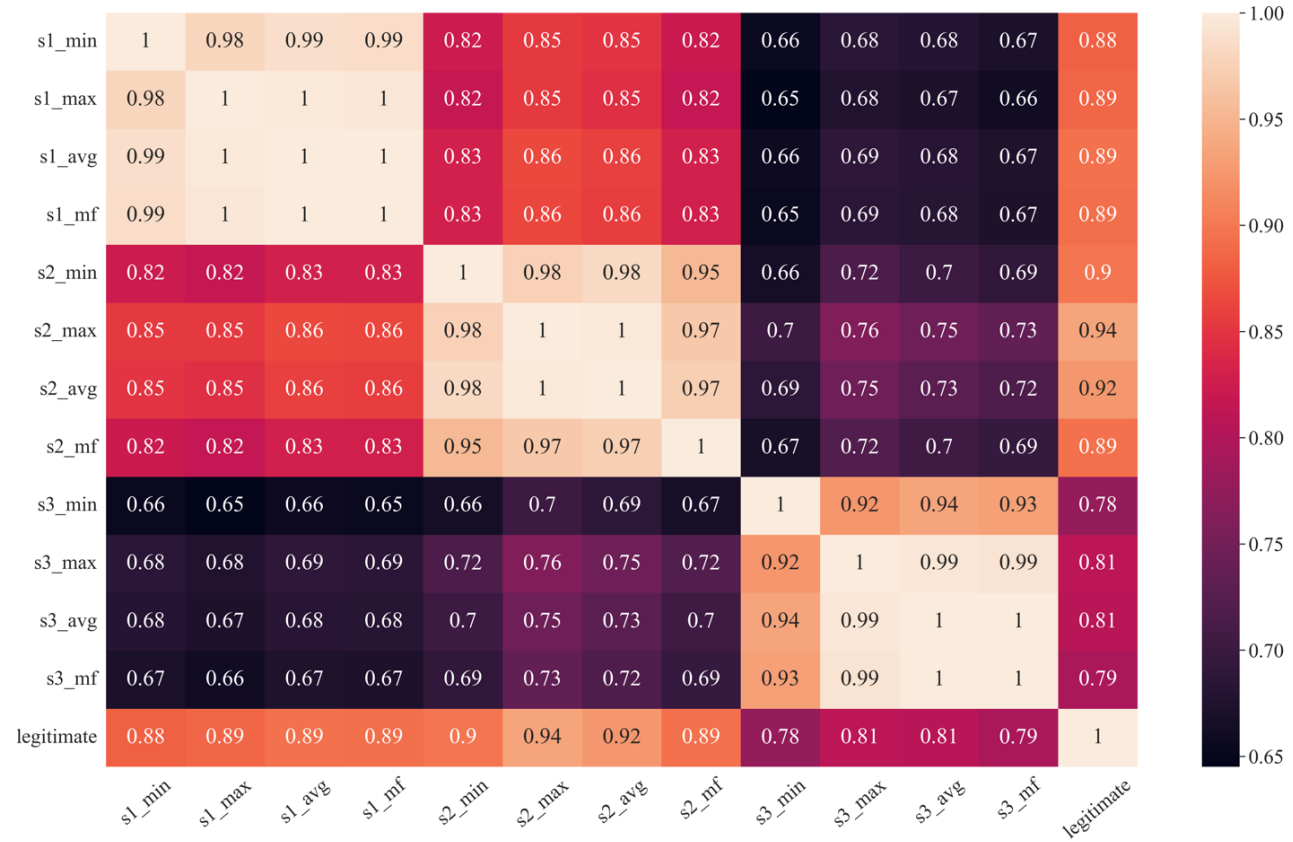


Рис. 4.15. Теплова карта кореляції даних без метрики кількості перехоплених пакетів-маячків

На рис. 4.15, мінімальна кореляція між метриками складає не менше 0.65. Найменше значення кореляції знаходиться на перетині сенсора №1 і його метрики потужності сигналу який найчастіше з'являвся і мінімального значення потужності сигналу від сенсора №3.

Як у випадку з одним сенсором так і у випадку з трьома найменше значення кореляції не входить в діапазон [–0,3÷0,3], тож набори даних можуть бути використані для тренування класифікатора.

Тепер за допомогою функції *plotpair* бібліотеки *seaborn* візуалізуємо кореляцію метрик для групи експериментів з одним сенсором (рис. 4.16) і по

кожному із сенсорів для групи експериментів з трьома сенсорами (рис. 4.17—4.19). Дане співставлення дозволяє наочно побачити чи є перетин даних про потужність сигналу від легітимної та нелегітимної точок доступу між собою.

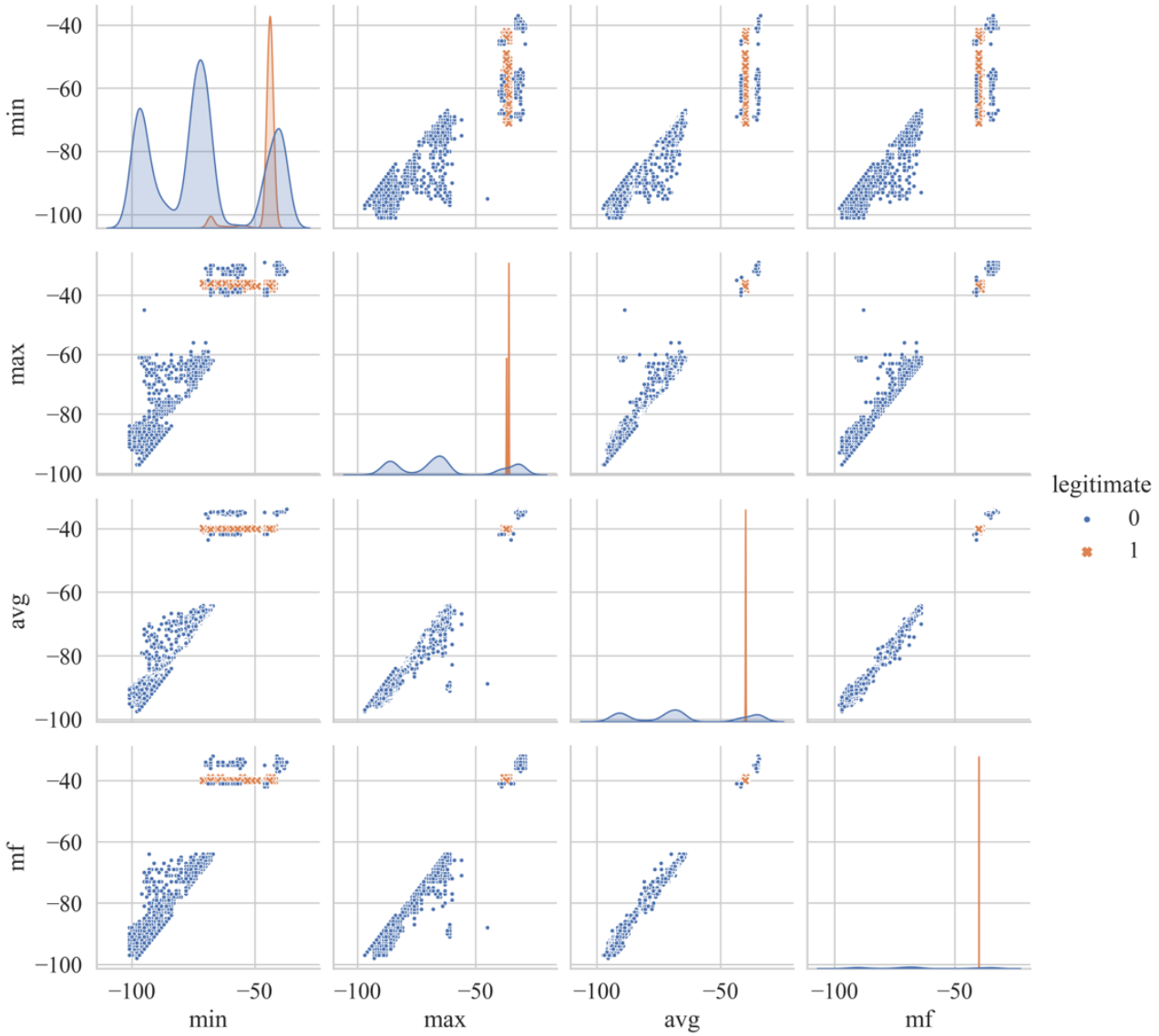


Рис. 4.16. Співставлення метрик легітимної і нелегітимної точок доступу для групи експериментів з одним сенсором

На рис. 4.16 видно доволі значний перетин мінімальної потужності сигналів від легітимної та нелегітимної точок доступу, що звісно може стати проблемою під час тренування моделі машинного навчання. Та все ж такий випадок цілком імовірний в реальних умовах, коли зловмисник розміщує обладнання близько до легітимної ТД або ж збільшує потужність власного обладнання у певному напрямку, у цьому варіанті у напрямку сенсора. Це вказує на те, що застосування

лише одного сенсора в умовах моніторингу бездротової мережі Wi-Fi може бути недостанім.

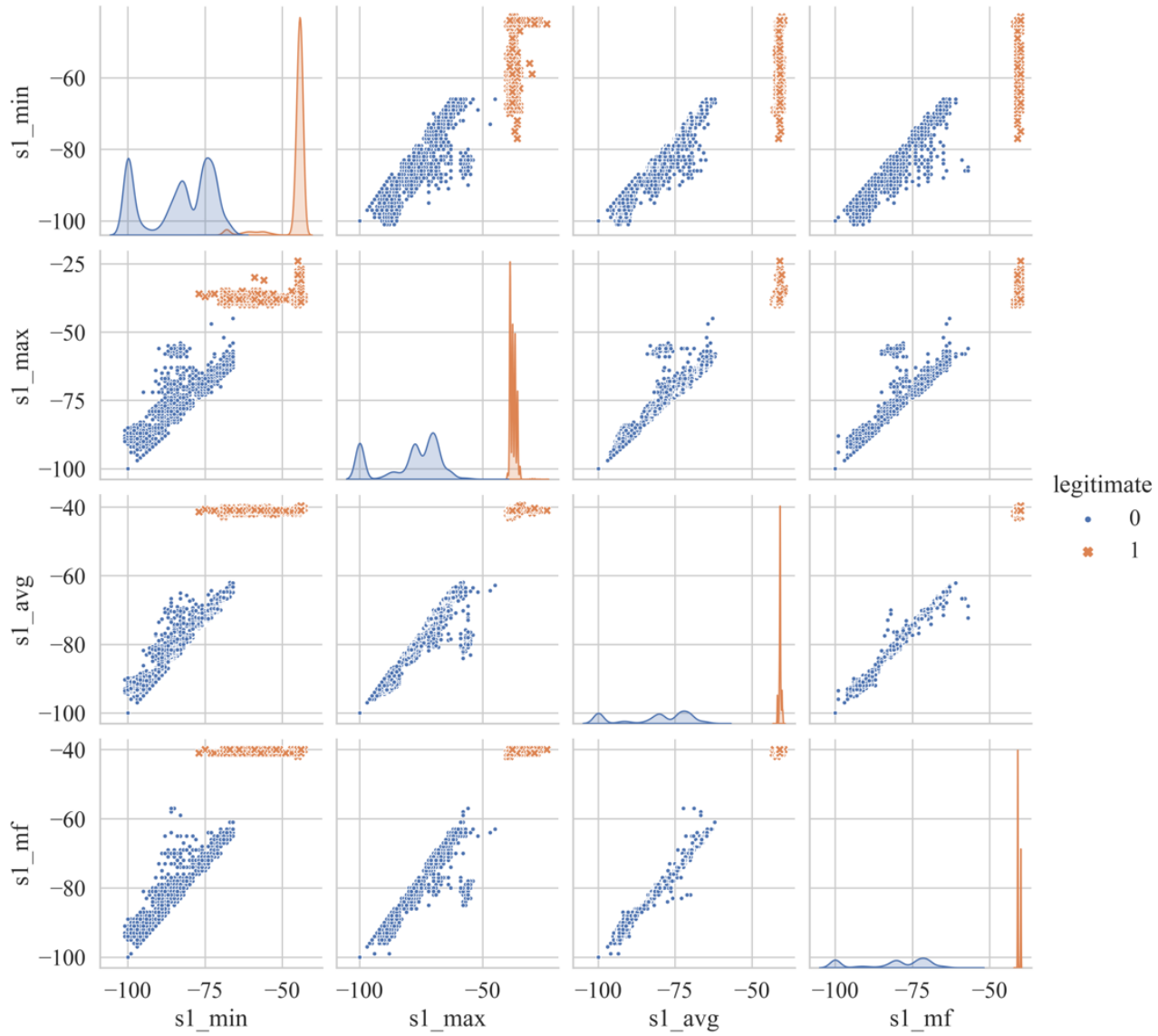


Рис. 4.17. Співставлення метрик легітимної і нелегітимної точок доступу зафіксованих сенсором №1

На рис. 4.17—4.18, відповідно сенсора №1 та №2, видно, що метрики легітимної та нелегітимної ТД не перетинаються, що є доволі хорошим знаком для побудови моделі машинного навчання. У випадку сенсора №3 (рис. 4.18), як і у випадку з експериментом з одним сенсором, видно незначні перетини при порівнянні метрик значень від легітимної та нелегітимної точок доступу. Незважаючи на такий розподіл – це цілком допустиме явище, оскільки за реальних

умов зловмисник може розмістити «злого двійника» в місці, в якому сенсор буде отримувати пакети з рівнем сигналу схожим до рівня сигналу від легітимної ТД.

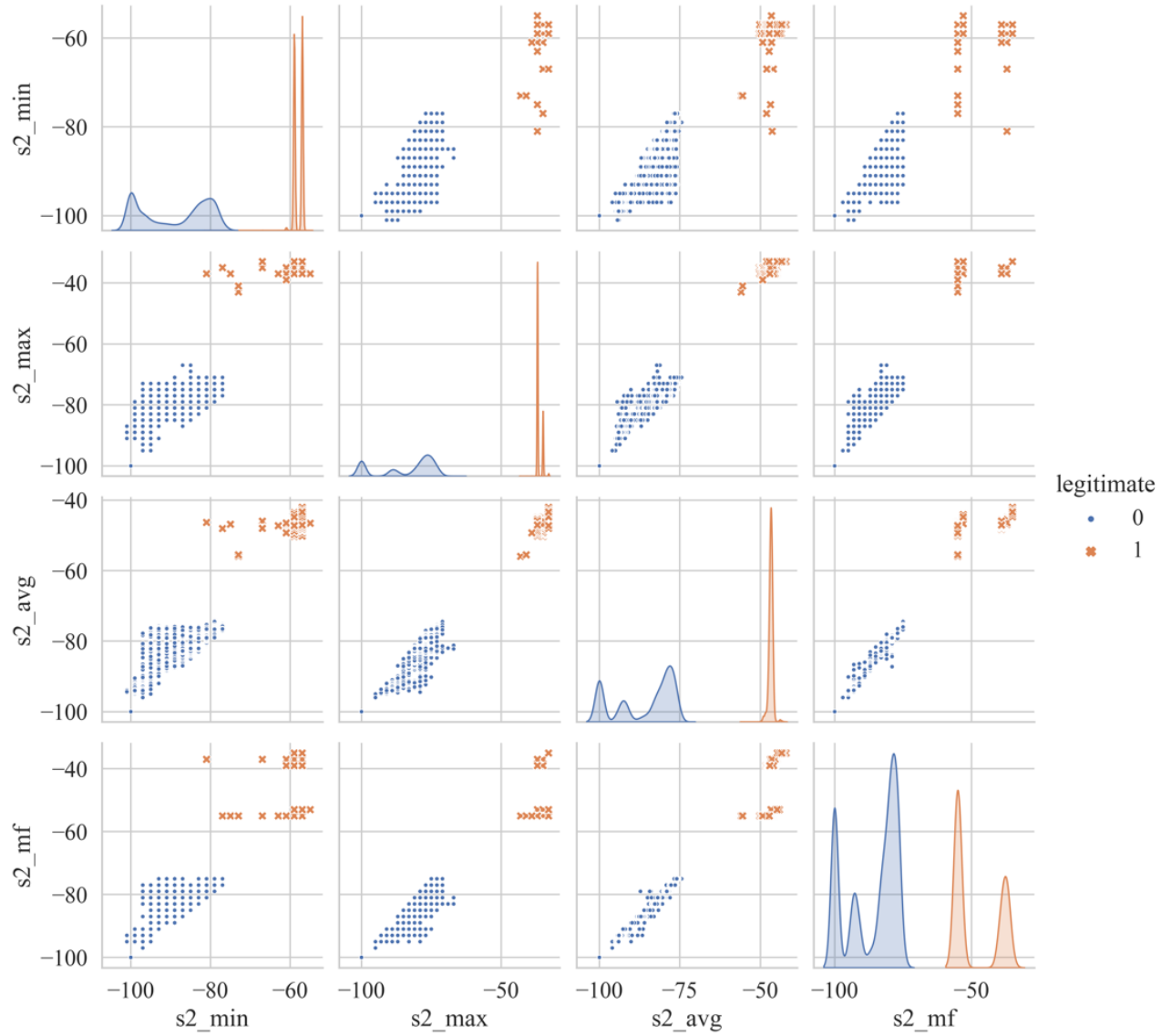


Рис. 4.18. Співставлення метрик легітимної і нелегітимної точок доступу зафіксованих сенсором №2

Для тренування моделі на вхід (*X_train*) було подано такі метрики *min*, *max*, *avg*, *mf* для експерименту з одним сенсором і *s1_min*, *s1_max*, *s1_avg*, *s1_mf*, *s2_min*, *s2_max*, *s2_avg*, *s2_mf*, *s3_min*, *s3_max*, *s3_avg*, *s3_mf* для групи експериментів з трьома сенсорами. Вихідною метрикою (*y_train*) є метрика legitimate, яка і вказує чи належить набір метрик легітимній. Також 20% від усього набору даних було задіяно в тестуванні (*X_test*, *y_test*).Для створення моделі машинного навчання було використано бібліотеку Scikit-learn [103]. Scikit-learn пропонує повний набір

алгоритмів машинного навчання, включаючи як навчання з вчителем, так і методи навчання без вчителя.

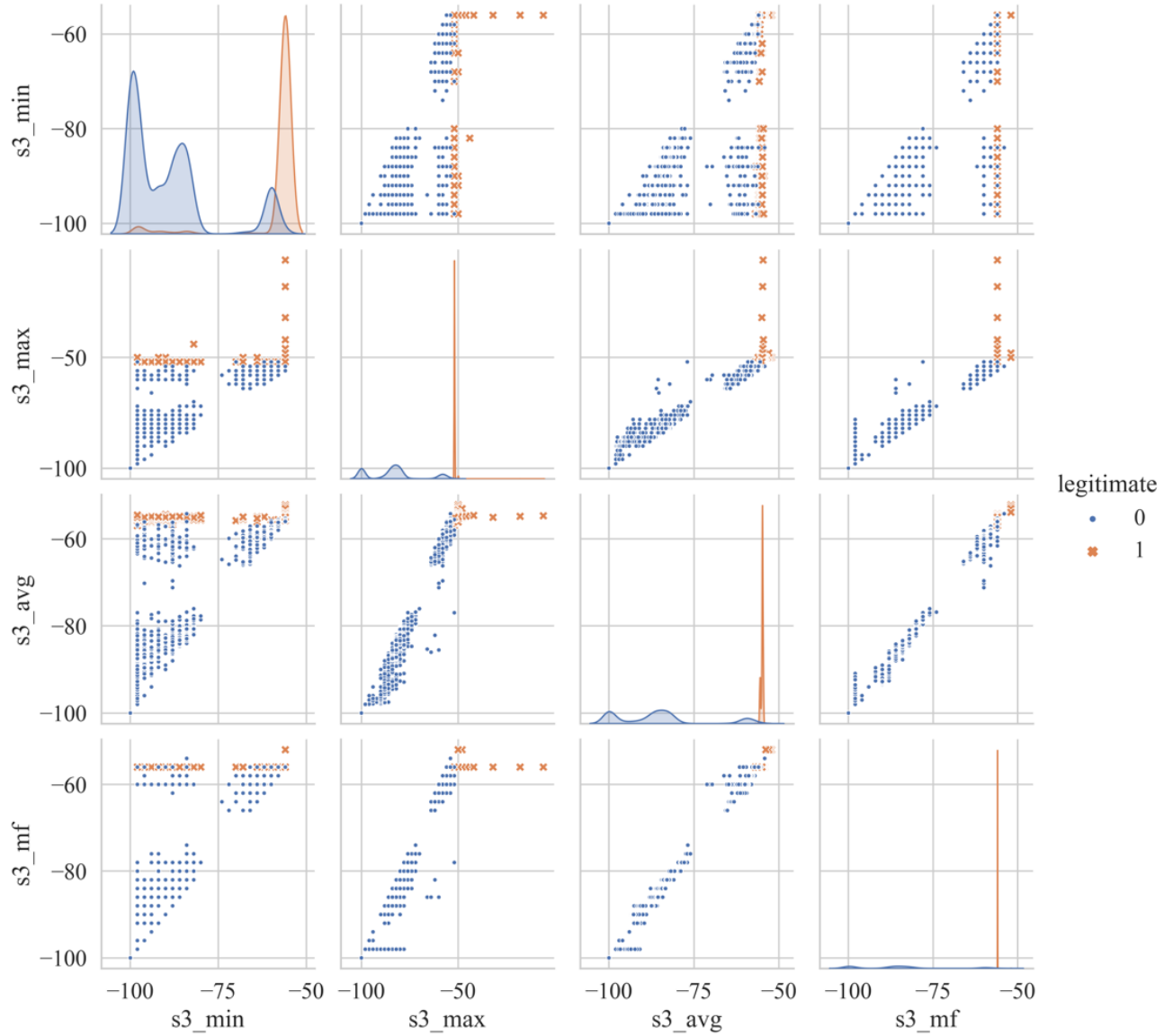


Рис. 4.19. Співставлення метрик легітимної і нелегітимної точок доступу зафіксованих сенсором №3

Деякі з найбільш часто використовуваних алгоритмів у scikit-learn – це лінійна та логістична регресії, дерева рішень, випадкові ліси, *k*-найближчих сусідів, опорні векторні машини та нейронні мережі.

Після навчання моделі проведено тести на двадцяти відсотках від загального набору даних ми отримали результати для схеми з одним сенсором (табл. 4.1) та трьома сенсорами (табл. 4.2). Для цього використаємо функцію *classification_report* з бібліотеки *sklearn* класу *metrics*.

Табл. 4.1.

Класифікаційний звіт для схеми з одним сенсором

	precision	**recall**	**f1-score**	**support**
0	1.00	1.00	1.00	2470
1	1.00	1.00	1.00	446
accuracy			1.00	2916
macro avg	1.00	1.00	1.00	2916
weighted avg	1.00	1.00	1.00	2916

Табл. 4.2.

Класифікаційний звіт для схеми з трьома сенсором

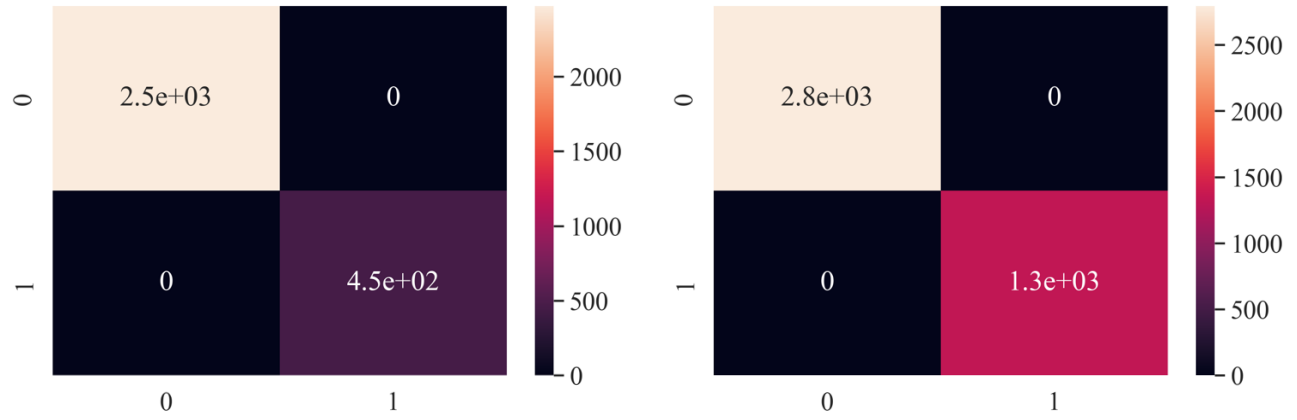
	precision	**recall**	**f1-score**	**support**
0	1.00	1.00	1.00	2792
1	1.00	1.00	1.00	1330
accuracy			1.00	4122
macro avg	1.00	1.00	1.00	4122
weighted avg	1.00	1.00	1.00	4122

де *precision* – це кількість справжніх позитивних результатів, поділена на загальну кількість позитивних прогнозів; *recall* – це кількість справді позитивних зразків, поділена на загальну кількість фактично позитивних зразків; *f1-score* – є гармонійним середнім показником точності та запам’ятовування, який забезпечує баланс між точністю та запам’ятовуванням; *support* – це кількість фактичних входжень класу у вказаному наборі даних. Іншими словами, це кількість зразків у кожному класі [104].

Окрім *precision*, *recall*, *f1-score* та *support*, функція *classification_report* бібліотеки *sklearn* також повідомляє про три інші важливі показники: accuracy, macro avg та weighted avg. Де accuracy – це частка правильно передбачених міток серед усіх зразків у наборі даних. Це показник, який вимірює загальну продуктивність моделі; macro avg – це середнє значення показників (precision, recall

та f1-score) для всіх класів. Цей показник корисний, коли ви хочете оцінити загальну продуктивність моделі в задачі багатокласової класифікації; weighted avg – значення показників (precision, recall та f1-score) для всіх класів, зважене за кількістю зразків у кожному класі. Цей показник корисний, коли у вас є незбалансований набір даних, і ви хочете оцінити загальну продуктивність моделі, беручи до уваги дисбаланс класів.

Як можемо побачити з таблиці 1, з 20% набору даних, а саме з 2916 випадків модель KNN правильно класифікувала усі тестові випадки. Такий же ж результат можемо побачити у випадку з трьома сенсорами, та у цьому випадку як видно кількість тестових випадків вже 4122. На рис. 4.20а— 4.20б зображено матрицю невідповідності моделі машинного навчання KNN для випадку з одним сенсором та трьома сенсорами сенсорами відповідно.



а) б)

Рис. 4.20. Візуалізація матриці невідповідності для моделі машинного навчання KNN для схеми з а) одним сенсором б) трьома сенсорами

У верхньому лівому куті (рис. 4.20а, 4.20б) відображається кількість правильно класифікованих нелегітимних точок доступу; у верхньому правому куті відображено неправильно класифікованих нелегітимних точок доступу; у нижньому правому куті відображено кількість неправильно класифікованих легітимних точок доступу; у нижньому лівому куті відображено кількість правильно класифікованих легітимних точок доступу.

4.5. Висновки до розділу 4

В результаті проведених досліджень у підрозділі 4.1 вдалось виявити критичні недоліки публічних БД, як інструменту пошуку зловмисника за слідами залишеними до, під час та після проведення атаки на Wi-Fi інфраструктуру. Такими недоліками визначено відсутність стандартизації обладнання, яке проводить збір та обробку даних; відсутність валідації даних, які приходять від контриб'юторів; відсутність агрегації даних на основі унікальних екземплярів. Кожен із цих недоліків робить процес пошуку можливих місць перебування зловмисника неефективним. Натомість запропоновано підхід, який дозволяє безперервно покращувати точність геолокації знайдених точок доступу за рахунок метрики потужність сигналу. Як було продемонстровано в досліді підрозділу 4.1, замість сотні виявлень БД WiGLE у нашому досліді було лише одне виявлення, що дозволяє із високою точністю виявляти місця де можна знайти пристрої попередньо зафіксовані на місці кіберзлочину, а відповідно і самого зловмисника.

В межах підрозділу 4.2 застосовано попередньо розроблену діагностичну модель визначено коефіцієнти для усіх наявних механізмів захисту бездротових мереж Wi-Fi. Кожному механізму, в залежності від важкості його подолання було надано коефіцієнти на проміжку від 0 до 1, де при 0 захист повністю відсутній, а при 1 застосовано комбінацію із найстійкіших механізмів. Даний підхід дозволяє підібрати налаштування СП згідно із визначеним профілем зловмисника, що може значно покращити продуктивність у їх застосуванні.

Протокол бездротової безпеки WPA3 представлений як найстійкіший механізм захисту бездротових мереж. Та зважаючи на те, що його використання у СП може бути недоцільним через складність подолання, а також через перехідний механізм для пристроїв, які не підтримують роботи з протоколом WPA3 було вирішено розробити деталізоване дослідження протоколу захисту WPA2, який є легшим до подолання зловмисниками ніж WPA3. В межах підрозділу 4.3 було застосовано модель із підбору параметрів ключа WPA2. Кожному словнику в залежності від його складності надано коефіцієнти на проміжку від 0 до 1, де при 0 довжина ключа становить 8 символів, а при 1 – 64. Для обчислення складності

перебору було використано дві різні технології віртуалізації – повна і контейнеризація і визначено, що контейнеризація є продуктивнішою на 11% за повну віртуалізацію. Окрім того, було встановлено, що контейнеризація краще підходить під задачі з пошуку паролю в оцінці умовної захищеності СП, оскільки запуск контейнерів відбувається за лічені секунди, в той час як у віртуальним машин на це йде більше хвилини. Таким чином контейнеризація дозволяє зберегти час і обчислювальні ресурси.

В межах підрозділу 4.4 було проведено дослід із виявлення атаки «злий двійник» в мережі стандарту IEEE 802.11 (Wi-Fi). У цьому підрозділі пропонується метод виявлення вторгнень за допомогою збору та аналізу даних про потужність сигналу від Wi-Fi точок доступу зібраних з ефіру. В межах імплементації даного метода було розроблено програмно-апаратного комплексу, який дозволяє з високою ефективністю і малим енергоспоживанням здійснює моніторинг службових пакетів в ефірі мереж стандарту IEEE 802.11. В підсумку, можемо констатувати, що за допомогою безперервного моніторингу етеру і застосування алгоритмів машинного навчання на зібраних даних можна значно покращити механізми визначення атак на комп’ютерні мережі Wi-Fi за допомогою аналізу потужності сигналу. В підрозділі 4.4 доведено, що за допомогою алгоритму машинного навчання KNN можна виявити атаку ЗД. Точність у розпізнанні легітимної ТД від не легітимної склала 100%, що дозволяє стверджувати про ефективність даного підходу у визначенні атаки «злий двійник». Виявлення даного типу атаки є доволі важливим у захисті мереж стандарту IEEE 802.11 (Wi-Fi), оскільки атака «злий двійник» є інструментом у спектрі великої кількості векторів атак, а тому числі і атаки на WPA3.

ВИСНОВКИ

В роботі вирішено важливу науково-практичну задачу з покращення ефективності виявлення вторгнень і підвищення ефективності систем-приманок для бездротових комп’ютерних мереж стандарту IEEE 802.11.

У підсумку результати здобуті під час проведення експериментів дозволяють стверджувати, що розроблені підходи значно покращують ефективність у деанонімізації зловмисників систем-приманок.

1. Проведено огляд існуючих рішень та реалізацій систем виявлення вторгнень і систем-приманок для комп'ютерних мереж стандарту IEEE 802.11, а також проаналізовано стан сучасних досліджень у цій галузі. За результатами аналізу встановлено, що сучасні системи виявлення вторгнень переважно базуються на сигнатурних методах, а системи-приманки частіше використовуються як інструменти зловмисників. Також визначено, що виявлення зловмисника, який здійснює атаку на бездротову мережу, може становити проблему через його можливе операційне виходження за межі контрольованої зони. Обґрунтовано актуальність науково-практичного завдання дослідження, включаючи розробку методології оцінки захисту систем-приманок та використання штучного інтелекту для поліпшення ефективності систем виявлення вторгнень.

2. Розроблено та проаналізовано моделі порушника у бездротових мережах стандарту IEEE 802.11 для підприємства. Даний аналіз дозволяє краще зрозуміти можливі ризики і розробляти ефективні методи їх протидії. Досліджено можливі демаскуючі ознаки систем-приманок, зокрема їх можливість виявлення на різних рівнях моделі OSI: канальному, мережевому та прикладному, що дозволяє уникнути виявлення систем-приманок зловмисниками і позитивно впливає як на функціонування як систем-приманок, так і на безпеку бездротової мережі Wi-Fi та інших пов'язаних мережевих ресурсів.

3. Розроблено концептуально нову модель системи захисту інформації з використанням систем-приманок, що відповідає сучасним викликам і вимогам безпеки. У цьому контексті описано мінімальний набір елементів, за допомогою яких можна реалізувати таку систему. Регламентовано правила комунікації між їх

елементами. Для елементів зовнішнього сегменту системи захисту інформації та системи бездротової мережі запропоновано обчислювальні платформи. Для розв'язання проблем масштабованості розробленої системи також запропоновано використання хмарних обчислень.

4. Досліджено критичні недоліки публічних баз даних з геолокації точок доступу Wi-Fi як інструменту пошуку зловмисника за слідами, залишеними до, під час та після проведення атаки на Wi-Fi інфраструктуру. Такими недоліками визначено відсутність стандартизації обладнання, яке проводить збір та обробку даних; відсутність валідації даних, які приходять від контриб'юторів; відсутність агрегації даних на основі унікальних екземплярів. Натомість запропоновано методику, яка дозволяє безперервно покращувати точність геолокації знайдених точок доступу за рахунок метрики потужність сигналу, введення поняття унікальності знайдених екземплярів та стандартизації обладнання контрибюторів. Врезультаті вдалось досягти точності у віднайдені унікальних екземплярів з точністю 90—100% на противагу 0.5—1% у публічних базах даних.

5. Розроблено та застосовано діагностичну модель визначення коефіцієнтів для усіх наявних механізмів захисту бездротових мереж стандарту IEEE 802.11 (Wi-Fi). Даний підхід дозволяє підібрати налаштування системи-приманки згідно із визначеним профілем зловмисника, що може значно покращити продуктивність у їх застосуванні. Зважаючи на актуальність протоколу захисту WPA2 було розроблено деталізовану діагностичну модель відносно складності подолання його ключа. Для обчислення складності перебору було використано дві різні технології віртуалізації – повна і контейнеризація. Визначено, що контейнеризація є продуктивнішою на 11% за повну віртуалізацію і дозволяє швидко масштабувати ресурси.

6. Розроблено та застосовано модель машинного навчання на основі алгоритму KNN для виявлення атаки "злий двійник" в мережі стандарту IEEE 802.11 (Wi-Fi). Розроблено програмно-апаратний комплекс, що забезпечує моніторинг службових пакетів в етері мережі стандарту IEEE 802.11 з високою ефективністю та мінімальним енергоспоживанням. Завдяки безперервному

моніторингу етеру та використанню алгоритмів машинного навчання на зібраних даних моделі вдалося відрізнити легітимні точки доступу від імітованих нелегітимних у 100% випадків. Це свідчить про високу ефективність даного підходу у виявленні атаки "злий двійник". Виявлення цього типу атак є надзвичайно важливим для захисту мереж стандарту IEEE 802.11 (Wi-Fi), оскільки атака "злий двійник" є одним із інструментів у широкому спектрі векторів атак, включаючи атаки на WPA3.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wright, Joshua. “Detecting Wireless LAN MAC Address Spoofing.” (2003). URL: https://www.willhackforsushi.com/papers/wlan-mac-spoof.pdf (дата звернення: 03.03.2024).

2. Дудикевич, В. Б. Комплексний підхід до захисту мовної інформації в технологіях безпровідного зв’язку. / Дудикевич, В. Б., Микитин, Г. В., Ребець, А. І., Банах, Р. І. // Сучасна спеціальна техніка, (2014/4), 75-82 сс.

3. Idamekorala, Rasika. (2009). Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys. 433–438. 10.1109/TIC-STH.2009.5444462.

4. Chen, Jyh-Cheng & Jiang, Ming-Chia & Liu, Yi-wen. (2005). Wireless LAN security and IEEE 802.11i. Wireless Communications, IEEE. 12. 27–36. 10.1109/MWC.2005.1404570.

5. Lee, Jun-Dian & Fan, Chih-Peng. (2007). Efficient low-latency RC4 architecture designs for IEEE 802.11i WEP/TKIP. 56 - 59. 10.1109/ISPACS.2007.4445822.

6. Talab, Samani & Ahmed, Awad & Elgili, Mustafa. (2010). WEP and WPA Improvement. Wireless Sensor Network. 2. 239-242.

7. Sadeghian, Amir. (2013). Analysis of WPS Security in Wireless Access Points. 10.13140/2.1.1869.2164.

8. CVE – CVE-2011-5053. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5053 (дата звернення: 03.03.2024).

9. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // Матеріали Міжнародної науково-практичної конференції “Проблеми і перспективи розвитку ІТ-індустрії”: тези доповідей, 20 – 21 квітня 2017 р. – Х.: ХНЕУ імені Семена Кузнеця, 2017. – 92 с. – 27–28 сс.

10. Банах Р.І. Діагностична модель системи-приманки бездротової мережі стандарту IEEE 802.11 / Р.І. Банах, А.З. Піскозуб // Щоквартальне наукове видання

«Системи обробки інформації» Випуск 2 (148): Харківський національний університет Повітряних Сил імені Івана Кожедуба, 2017. С. 77-83.

11. Reddy, B Indira & Srikanth, V.. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 28-35. 10.32628/CSEIT1953127.

12. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd / Mathy Vanhoef, Eyal Ronen // 41st IEEE Symposium on Security and Privacy, Date: 2020/05/18 - 2020/05/21, Location: San Francisco, USA Proceedings of the 2020 IEEE Symposium on Security and Privacy - S&P 2020); 2020; pp. - 517-533

13. Дудикевич В. Б. Інформаційна модель безпеки технологій зв'язку. / Дудикевич В. Б., Хорошко В. О., Микитин Г.В., Банах Р.І., Ребець А.І. // Інформатика та математичні методи в моделюванні 2014 Том 4. – №2. – 137–148 сс.

14. Банах Р. Перспективи розвитку систем приманок для безпровідних мереж / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Інформація, комунікація, суспільство 2016: матеріали 5-ої Міжнародної наукової конференції ІКС-2016, 19–21 травня 2016 року, Україна, Львів, Славське / Національний університет "Львівська політехніка", Кафедра соціальних комунікацій та інформаційної діяльності. – Львів: Видавництво Львівської політехніки, 2016. – С. 30–31.

15. Development Of the Honeyed Virtual Honeypot. URL: https://www.honeyd.org/ (дата звернення: 03.03.2024).

16. The honeynet project. URL: https://www.honeynet.org/ (дата звернення: 03.03.2024).

17. NMAP: The network mapper – Free Security Scanner. URL: https://nmap.org/ (дата звернення: 03.03.2024).

18. X probe – active OS fingerprinting tool. URL: https://sourceforge.net/projects/xprobe/ (дата звернення: 03.03.2024).

19. Yek, Suen. (2004). Implementing network defence using deception in a wireless honeypot. pp. 4-15.

20. DanMcInerney/fakeAP. URL: https://github.com/DanMcInerney/fakeAP (дата звернення: 03.03.2024).

21. Guan, Yong & Russell, Steve. (2004). SECURING WIRELESS NETWORKS BY WIRELESS HONEYNETS: CHALLENGES AND SOLUTIONS. pp. 1—5. URL: https://www.researchgate.net/publication/282120450_SECURING_WIRELESS_NETWORKS_BY_WIRELESS_HONEYNETS_CHALLENGES_AND_SOLUTIONS (дата звернення: 03.03.2024).

22. Design, A & Overview, Architectural & Siles, Raul. (2007). HoneySpot: The Wireless Honeypot Monitoring the Attacker's Activities in Wireless Networks. URL: https://www.researchgate.net/publication/277295370_HoneySpot_The_Wireless_Honeypot_Monitoring_the_Attacker's_Activities_in_Wireless_Networks (дата звернення: 03.03.2024).

23. Snort – Network Intrusion Detection & Prevention System. URL: https://www.snort.org/ (дата звернення: 03.03.2024).

24. Home – Suricata. URL: https://suricata.io/ (дата звернення: 03.03.2024).

25. Air Marshal – Cisco Meraki Documentation. URL: https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal (дата звернення: 03.03.2024).

26. Aruba. WIRELESS INTRUSION PROTECTION (WIP). URL: https://www.arubanetworks.com/assets/tg/TG_WIP.pdf (дата звернення: 03.03.2024).

27. Provos, Niels. (2003). Honeyd: A Virtual Honeypot Daemon (Extended Abstract). URL: https://researchgate.net/publication/250395424_Honeyd_A_Virtual_Honeypot_Daemon_Extended_Abstract (дата звернення: 03.03.2024).

28. Dong Y., Zampella F., Alsehly F., 2023, Beyond KNN: Deep Neighborhood Learning for WiFi-based Indoor Positioning Systems. arXiv, arXiv:2302.00810. doi:10.48550 /arXiv.2302.00810

29. Lijuan Z. A Network Security Evaluation Method based on FUZZY and RST / Z. Lijuan, W. Qingxin // 2010 2nd International Conference on Education Technology

and Computer (ICETC). 22-24 June 2010 : proceedings. – Shanghai, China : IEEE, 2010. P.40-44.

30. Runfu Z. Security for Wireless Network Based on Fuzzy-AHP with Variable Weight / Z. Runfu, Lianfen H., Mingbo X. // 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 24-25 April 2010 : proceedings. - Wuhan, Hubei, China : IEEE, 2010. Vol. 2. – P.490-493.

31. Ying-Chiang C. Hybrid Network Defense Model Based on Fuzzy Evaluation / C. Ying-Chiang, P Jen-Yi // The Scientific World Journal, 2014. – Vol. 2014. – P. 1-12.

32. Goel R. Wireless Honeypot: Framework, Architectures and Tools / R. Goel, A. Sardana, R. C. Joshi // International Journal of Network Security, 2013. Vol. 15, No.5. – P. 373-383.

33. Дудикевич В.Б. Методи та засоби аналізу систем-приманок в процесі зламу / В.Б. Дудикевич, А.З. Піскозуб, Н.П. Тимошик, Р.П. Тимошик, Т.В. Дуткевич. // Науково-технічний журнал «Захист інформації». – 2009. – №1. – С. 27-31.

34. Ajah I. A. Evaluation of Enhanced Security Solutions in 802.11-Based Networks / I. A. Ajah // International Journal of Network Security & Its Applications (IJNSA). 2014. Vol. 6. No.4. – P. 29-42.

35. FORBES, G., MASSIE, S. and CRAW, S. 2020. Wifi-based human activity recognition using Raspberry Pi. In Alamaniotis, M. and Pan, S. (eds.) Proceedings of Institute of Electrical and Electronics Engineers (IEEE) 32nd Tools with artificial intelligence international conference 2020 (ICTAI 2020), 9-11 Nov 2020, [virtual conference]. Piscataway: IEEE [online], pages 722-730. URL: https://doi.org/10.1109/ICTAI50040.2020.00115 (дата звернення: 03.03.2024).

36. LU, Qian & Qu, Haipeng & ZHUANG, Yuan & LIN, Xi-Jun & OUYANG, Yuzhan. (2018). Client-Side Evil Twin Attacks Detection Using Statistical Characteristics of 802.11 Data Frames. IEICE Transactions on Information and Systems. E101.D. 2465-2473. 10.1587/transinf.2018EDP7030.

37. Modi, Vishwa & Parekh, Asst. (2017). Detection of Rogue Access Point to Prevent Evil Twin Attack in Wireless Network. International Journal of Engineering Research and. V6. 10.17577/IJERTV6IS040102.

38. S., Harsha & Abdus Sattar, Khalid & Sriramulu, Balaji & Rao, Vallabh. (2019). Improving Wi-Fi security against evil twin attack using light weight machine learning application. Compusoft. 8.

39. Kuo, En-Chun & Chang, Ming-Sang & Kao, Da-Yu. (2018). User-side evil twin attack detection using time-delay statistics of TCP connection termination. 1-1. 10.23919/ICACT.2018.8323699.

40. Agarwal, Mayank & Biswas, Santosh & Nandi, Sukumar. (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. 1-16. 10.1007/s10776-018-0396-1.

41. Yang, Chao & Song, Yimin & Gu, Guofei. (2012). Active User-Side Evil Twin Access Point Detection Using Statistical Techniques. Information Forensics and Security, IEEE Transactions on. 7. 1638-1651. 10.1109/TIFS.2012.2207383.

42. Dong Y., Zampella F., Alsehly F., 2023, Beyond KNN: Deep Neighborhood Learning for WiFi-based Indoor Positioning Systems. arXiv, arXiv:2302.00810. doi:10.48550 /arXiv.2302.00810

43. Банах Р.І., Тестування на проникнення як механізм аналізу ефективності системи приманки для мережі Wi-Fi. / Роман Банах, Андріян Піскозуб, Ярослав Стефінко // Тези доповіді ІІ-ої Міжнародної науково-технічної конференції 24-25 листопада 2016 р. «Інформаційна безпека в сучасному суспільстві» 119с., 79—80 сс.

44. Банах Р.І. Збір та обробка метаданих зловмисника для виявлення імовірних місць його перебування з пристроїв стандарту IEEE 802.11 / Банах Р.І., Піскозуб А.З. // 4-th International Conference on Computational Intelligence (ComInt 2017), Taras Shevchenko National University of Kyiv, May 16-18, 2017. – 197–198 сс.

45. Банах Р. І. Створення концепції захищеної хмарної обчислювальної мережі з використанням систем приманок / Банах Р.І., Піскозуб А.З.,Стефінко Я.Я. // Вісник Національного університету “Львівська політехніка”: Серія: Автоматика, вимірювання та керування : збірник наукових праць. – 2015. – № 821. – С. 74–78.

46. IGRSoft/KisMac2. URL: https://github.com/IGRSoft/KisMac2 (дата звернення: 03.03.2024).

47. Kismet – Wi-Fi, Bluetooth, RF, and more. URL: https://www.kismetwireless.net/ (дата звернення: 03.03.2024).

48. Wireshark – Go Deep. URL: https://www.wireshark.org/ (дата звернення: 03.03.2024).

49. Home | TCPDUMP & LIBPCAP. URL: http://www.tcpdump.org/ (дата звернення: 03.03.2024).

50. Банах Р. І. Аналіз подій у безпровідних комп'ютерних мережах для автоматизації тестування на проникнення / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції "Захист інформації і безпека інформаційних систем" – Львів, 2015. – 73–74 сс.

51. Enterprise Trust and Identity Policy System – eTIPS: URL: https://www.opus1.com/nac/vendorwhitepapers/avenda_etips_datasheet.pdf (дата звернення: 03.03.2024).

52. LOIC. A network stress testing application. URL: https://sourceforge.net/projects/loic/ (дата звернення: 03.03.2024).

53. Ivo Petiz. Using Multiscale Traffic Analysis to Detect WPS Attacks / Ivo Petiz, Eduardo Rocha, Paulo Salvador, Antonio Nogueira // IEEE International Conference on Communications 2013: IEEE ICC'13 - 3rd IEEE International Workshop on Smart Communication Protocols and Algorithms (SCPA 2013) - p.1020-1025

54. Wireless distribution system. URL: https://en.wikipedia.org/wiki/Wireless_distribution_system (дата звернення: 03.03.2024).

55. Mesh networking. URL: https://en.wikipedia.org/wiki/Mesh_networking (дата звернення: 03.03.2024).

56. Thorsten Holz. Detecting Honeypots and other suspicious environments / Thorsten Holz, Frederic Raynal // Proceedings of the 2005 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 15–17 June 2005 - p.1555-1563

57. Simon Innes. Honeypots: How do you know when you are inside one? / Simon Innes, Craig Valli // Originally published in the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006. 8 p.

58. Galán, Fermín & Fernández, David. (2006). Use of VNUML in Virtual Honeynets Deployment. 600—615 pp. URL: https://www.researchgate.net/publication/266094954_Use_of_VNUML_in_Virtual_Honeynets_Deployment (дата звернення: 03.03.2024).

59. Банах Р.І. Оцінка надійності елементів системи-приманки у мережі стандарту IEEE 802.11, як розгалуженої системи зі складним підпорядкуванням. / Банах Р.І., Піскозуб А.З. // Вісник Національного університету «Львівська політехніка». Серія «Автоматика, вимірювання та керування». – 2017. – №880. с. 94–98

60. Cloud Computing. URL: https://en.wikipedia.org/wiki/Cloud_computing (дата звернення: 03.03.2024).

61. V. Varadharajan and U. Tupakula, "Security as a Service Model for Cloud Environment," in IEEE Transactions on Network and Service Management, vol. 11, no. 1, pp. 60-75, March 2014.

62. Банах Р. І. Створення концепції захищеної хмарної обчислювальної мережі із застосуванням систем приманок / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Матеріали IV-ої Міжнародної науково-технічної конференції “Захист інформації і безпека інформаційних систем” – Львів, 2015 – 75–76 сс.

63. Банах Р. Одноплатна робоча станція як компонент системи приманки у безпровідних комп'ютерних мережах. / Банах Р., Стефінко Я. // Захист інформації в інформаційно-комунікаційних системах. Тези доповідей І Міжвузівської науково-практичної конф. студентів і курсантів – Львів, 2015 – С. 6-7.

64. Банах Р.І. Автоматизація розгортання Wi-Fi точки доступу, як зовнішнього елементу системи приманки. / Банах Р.І., Піскозуб А.З., Стефінко Я.Я. // Вісник Національного університету «Львівська політехніка». Серія «Автоматика, вимірювання та керування». – 2016. – №852. с. 130–136 сс.

65. Hostapd. URL: https://en.wikipedia.org/wiki/Hostapd (дата звернення: 03.03.2024).

66. Dynamic Host Configuration Protocol. URL: https://uk.wikipedia.org/wiki/DHCP (дата звернення: 03.03.2024).

67. Raspberry Pi OS – Raspberry Pi. URL: https://www.raspberrypi.com/software/ (дата звернення: 03.03.2024).

68. ESP32. URL: https://uk.wikipedia.org/wiki/ESP32 (дата звернення: 03.03.2024).

69. Attackers' Wi-Fi devices metadata interception for their location identification / Roman Banakh, Andrian Piskozub // Proceedings of the 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS-SWS 2018, 2018, pp. 112–116

70. Banakh R. Wi-Fi Honeypot as a service. Conception of business model / Banakh R. // "ENGINEER OF XXI CENTURY": VI INTER UNIVERSITY CONFERENCE OF STUDENTS, PHD STUDENTS AND YOUNG SCIENTISTS. Bielsko-Biała, Poland December 02, 2016. 59-64p.

71. Banakh R. External elements of honeypot for wireless network / Banakh R., Piskozub A., Stefinko Y. // "Modern Problems of Radio Engineering, Telecommunications, and Computer Science": Proceedings of the XIIIth International Conference TCSET'2016. Lviv-Slavsko, Ukraine February 23 – 26, 2016. Lviv Publishing House of Lviv Polytechnic 2016. 480-482p.

72. WiGLE: Wireless Network Mapping. URL: https://wigle.net/index (дата звернення: 03.03.2024)

73. Zhang R. Security for Wireless Network Based on Fuzzy-AHP with Variable Weight / R. Zhang, L. Huang, M. Xiao // 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing. – 490 – 493p.

74. Ajah I. A. Evaluation of Enhanced Security Solutions in 802.11-Based Networks / Ajah I. A. // International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4, July 2014. – 29 - 42 p.

75. Zhang L. Network Security Evaluation through Attack Graph Generation / Zhang L., Tang H., Cui Y.M., Zhang J. // World Academy of Science, Engineering and Technology 30 2009. – 407-410 p.

76. Р. І. Банах. Визначення параметрів ключа методу автентифікації WPA/WPA2 для системи-приманки мережі стандарту IEEE 802.11 / Р. І. Банах // Радіоелектроніка, інформатика, управління. Запорізький Національний технічний університет. с. 110–118.

77. Стефінко Я.Я. Тестування на проникнення з Metasploit і shell скриптами. / Стефінко Я.Я., Піскозуб А.З., Банах Р.І. // Вісник Національного університету “Львівська політехніка”: Серія: Автоматика, вимірювання та керування: збірник наукових праць. – 2015. – № 821. – С. 90—93.

78. Felter, Wes et al. “An updated performance comparison of virtual machines and Linux containers.” 2015 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS) (2015): 171-172.

79. Стефінко Я. "Тестування на проникнення у навчальних лабораторіях з застосуванням контейнеризації" / Стефінко Я., Піскозуб А., Банах Р. // Тези доповідей: Матеріали 8-ї науково-практичної конференції "Інноваційні комп’ютерні технології у вищій школі" . Львів – В-во наук.тов. ім.Т.Г.Шевченка - 2016.- С. 144-151.

80. Manual and Automated Penetration Testing. Benefits and Drawbacks. Modern Tendency» / Yaroslav Stefinko, Andrian Piskozub, Roman Banakh // Modern Problems of Radio Engineering, Telecomunications, and Computer Science: Proceedings of the XIIIth International Conference TCSET’2016 – Lviv-Slavsko, Ukraine, 2016. – 961p. 488-491p.

81. Банах Р.І. Застосування хмарних обчислень для визначення рівня захищеності бездротових мереж стандарту IEEE 802.11. / Банах Р.І., Піскозуб А.З. // Сучасна спеціальна техніка. Науково-практичний журнал №4(67), 2021. с. 5–15.

82. Lu, He-Jun & Yu, Yang. (2021). Research on WiFi Penetration Testing with Kali Linux. Complexity. 2021. 1-8. 10.1155/2021/5570001.

83. Ahmad, N., “Cloud Computing: Technology, Security Issues and Solutions”, Proceedings of the 2nd International Conference on AntiCyber Crimes, pp. 30-35, 2017.

84. Tissir, Najat & El Kafhali, Said & Aboutabit, Noureddine. (2020). Cloud Computing security classifications and taxonomies: a comprehensive study and comparison. 1-6. 10.1109/CloudTech49835.2020.9365884.

85. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers’ devices / Banakh, R., Piskozub, A., Opirskyy, I. // Advances in Intelligent Systems and Computing, 2019, 754, pp. 468–477

86. T. Mladenova and I. Valova, "Analysis of the KNN Classifier Distance Metrics for Bulgarian Fake News Detection," 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021, pp. 1-4, doi: 10.1109/HORA52670.2021.9461333.

87. Taunk, Kashvi & De, Sanjukta & Verma, Srishti & Swetapadma, Aleena. (2019). A Brief Review of Nearest Neighbor Algorithm for Learning and Classification. 1255-1260. 10.1109/ICCS45141.2019.9065747.

88. Банах Р.І. Проблематика використання відкритих джерел даних у розслідувані кіберзлочинів у мережах стандарту IEEE 802.11 / Банах Р.І. // Матеріали II Міжнародної наукової конференції «Теорія модернізації в контексті сучасної світової науки», м.Ужгород, 1 березня, 2024р. / Міжнародний центр наукових досліджень. —Вінниця: ТОВ «УКРЛОГОС Груп, 2024.—244с. – 145–147 сс.

89. Піскозуб А.З. Тестування на проникнення з допомогою open-source OS Linux і shell скриптів / Піскозуб А.З., Стефінко Я.Я., Банах Р.І. // Матеріали п’ятої науково-практичної конференції FOSS Lviv 2015 (23-26 квітня 2015р.), м Львів – 133–136 сс.

90. Jatin Nagpal, Rajesh Patil, Vikas Jain, Rajesh Pokhriyal, Rajveer Rajawat "Evil Twin Attack and Its Detection", International Journal of Emerging Technologies and Innovative Research (www.jetir.org), ISSN:2349-5162, Vol.5, Issue 12, page no.169-171, December-2018

91. Mariusz Bednarczyk, Zbigniew Piotrowski, "Will WPA3 really provide Wi-Fisecurity at a higher level?," Proc. SPIE 11055, XII Conference onReconnaissance and Electronic Warfare Systems, 1105514 (27 March 2019); doi: 10.1117/12.2525020

92. M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 517-533, doi: 10.1109/SP40000.2020.00031

93. Wi-Fi Alliance, “Value of wi-fi,” 2022. URL: https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi (дата звернення: 03.03.2024).

94. Banakh, R., Piskozub, A., Opirskyy, I. 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 (123)) (2023), pp 20–32.

95. Aircrack-ng. Recommended wireless adapters. URL: https://www.aircrack-ng.org/doku.php?id=compatibility_drivers_old (дата звернення: 06.05.2024).

96. Scapy. URL: https://scapy.net/ (дата звернення: 03.03.2024).

97. InfluxDB Time Series Data Platform | InfluxData. URL: https://influxdata.com (дата звернення: 03.03.2024).

98. NumPy. URL: https://numpy.org/ (дата звернення: 03.03.2024).

99. Pandas – Python Data Analysis Library. URL: https://pandas.pydata.org/ (дата звернення: 03.03.2024).

100. Matplotlib – Visualization with Python. URL: https://matplotlib.org/ (дата звернення: 03.03.2024).

101. Seaborn: statistical data visualization. URL: https://seaborn.pydata.org/ (дата звернення: 03.03.2024).

102. Neli J. Salkind, Bruce B. Frey (2019). Statistics for people who (think they) hate statistics. SAGE Publications, Inc., 76-102. https://doi.org/10.7748/nr.12.4.89.s6

103. Scikit-Learn: machine learning in Python. URL: https://scikit-learn.org/ (дата звернення: 03.03.2024).

104. Sklearn, Metrics, Classification Report. URL: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.classification_report. html (дата звернення: 03.03.2024).

ДОДАТОК А. Акти впровадження

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
Національного університету
«Львівська політехніка»
_____ Олег ДАВИДЧАК
«29» 03 2024 р.

АКТ

Про впровадження результатів дисертаційної роботи в навчальний процес

Банаха Романа Ігоровича

«Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» представленої на здобуття наукового ступеня доктора філософії за спеціальністю 125 – *«Кібербезпека та захист інформації»*

Комісія НУ «Львівська політехніка» у складі
Голова комісії – науково-методичної ради інституту комп'ютерних технологій автоматики та метрології, д.т.н., проф. Роман БАЙЦАР.

Члени комісії:

Завідувач кафедри «Безпека інформаційних технологій», д.т.н., с.т.с., професор Ігор ЖУРАВЕЛЬ, д.т.н., проф., професор кафедри «Безпека інформаційних технологій» Олена НЄМКОВА, к.ф.-м.н. доц. доцент кафедри «Безпека інформаційних технологій» Моріка РУСИНКО.

Даним актом підтверджує, що проведені дисертантом наукові дослідження виконувались ним на кафедрі «Безпека інформаційних технологій». Основні положення та результати дисертаційної роботи впроваджені у навчальний процес кафедри «Безпека інформаційних технологій» Національного університету «Львівська політехніка» при вивченні дисциплін:

- «Інформаційно-комунікаційні системи» для студентів 125 «Кібербезпека», спеціалізації «Кібербезпека комп'ютерних систем та мереж», тема №1 «Застосування віртуалізації та контейнеризації в інформаційно-комунікаційних системах» – огляд технологій, переваги та недоліки, масштабованість, застосування технологій віртуалізації та контейнеризації для високонавантажених систем обчислення; тема №5 «Безпека інформації у хмарних обчисленнях» – використання хмарних обчислень та організація безпеки в середовищі хмарного провайдера Amazon Web Services.

Голова комісії,
Колова науково-методичної ради ІКТА
д.т.н., проф. _____ Роман БАЙЦАР

Члени комісії:
проф. каф. БІТ, д.т.н. с.т.с. _____ Ігор ЖУРАВЕЛЬ

проф. каф. БІТ д.т.н. проф. _____ Олена НЄМКОВА

доц. каф. БІТ к.т.н. доц. _____ Моріка РУСИНКО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

НАКАЗ

31.01.2024р. м.Львів № 474-3-10

НДЧ

Для виконання робіт за грантом CRDF «Вдосконалення комплексу динамічної автентифікації кінцевих точок засобами машинного навчання та захисту корпоративних мереж від кібератак» каф.БІТ створити з 01.02.2024р. по 31.07.2024р. тимчасовий творчий колектив у складі:

1.Банах Роман Ігорович - асистент каф.БІТ - виконавець робіт.

2.Лах Юрій Володимирович - доцент каф.ЗІ к.ф.-м.н.- виконавець робіт.

3.Нємкова Олена Анатоліївна - професор каф.БІТ д.т.н., проф.- керівник гранту.

4.Піскозуб Андріян Збігнєвич - доцент каф.ЗІ доц., к.т.н.- виконавець робіт.

Підстава: подання керівника гранту з резолюцією проректора І.В.Демидова, згода працівників.

Ректор Юрій БОБАЛО

Проєкт вносить:

Начальник відділу кадрів Юрій НОВИЦЬКИЙ

Виконавець Ірина ПАСЬКОВИЧ

Погоджено:

Проректор Іван ДЕМИДОВ

Головний бухгалтер Андрій МЕЛЬНИК

Начальник НДЧ Роман НЕБЕСНИЙ

Заступник головного бухгалтера - начальник ПФВ Богдан РАБИК

Начальник юридичного відділу Андрій МОРОЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
КОПІЯ ВІРНА
"___" _____ 20___р.

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного університету
«Львівська політехніка»
проф. _____ Іван ДЕМИДОВ
_____ 2024

АКТ

про використання результатів дисертаційної роботи
Банаха Романа Ігоровича
«Удосконалення технології виявлення вторгнень і систем-приманок у мережах стандарту IEEE 802.11» представленої на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації»

Комісія у складі – голови начальника науково-дослідної частини, д.т.н., ст. досл. Небесного Р. В. та членів: завідувача кафедри захисту інформації, д.т.н., професора Опірського І. Р., завідувача відділу науково-організаційного супроводу наукових досліджень, к.т.н. Лазько Г. В. і заступника начальника планово-фінансового відділу ~~Чулой Т. М.,~~ цим актом підтверджують, що результати дисертаційної роботи Банаха Р. І. використовувались при виконанні науково-дослідної роботи кафедри захисту інформації «Дослідження стійкості біометричних систем автентифікації до атак із застосуванням технології клонування голосу на основі глибинних нейронних мереж» (№ держреєстрації 0124U000407).

Банахом Р. І. було здійснено адаптацію технологій та методів, які були застосовані для виявлення вторгнень у бездротових мережах, для виявлення атак з використанням технології клонування голосу, а саме, методи машинного навчання, які використовуються для аналізу сигналів у бездротових мережах, були використані для аналізу голосових сигналів та виявлення аномалій, пов'язаних із клонуванням голосу.

Голова комісії,
начальник науково-дослідної частини, д.т.н., ст. досл. _____ Роман НЕБЕСНИЙ

Члени комісії:
зав. каф. захисту інформації д.т.н., проф _____ Іван ОПІРСЬКИЙ

зав. відділу науково-організаційного супроводу наукових досліджень, к.т.н. _____ Галина ЛАЗЬКО

в. о. заст. нач. планово-фінансового відділу _____ ~~Тетяна~~ ЧУЛОЙ

intellias
Engineering by people.

ТзОВ «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ «ІНТЕЛЛІАС»
м. Львів, вул. Шафарика, 16/74,
79032 Україна

АКТ

про впровадження результатів дисертаційної роботи

Банаха Романа Ігоровича

«УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВТОРГНЕНЬ І СИСТЕМ-ПРИМАНОК У МЕРЕЖАХ СТАНДАРТУ IEEE 802.11»

Комісія у складі голови – директора Товариства з обмеженою відповідальністю «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ «ІНТЕЛЛІАС», Седлера Віталія Івановича, та члена комісії – начальника відділу кібербезпеки, Чижикова Олександра В'ячеславовича, склала цей акт про те, що запропонований апаратно-програмний комплекс, призначений для збору інформації про потужність сигналів від пристроїв стандарту IEEE 802.11 продемонстрував високу ефективність у виявленні вторгнень. Точність виявлення вторгнень забезпечена розробленою моделлю машинного навчання дозволила виявити 98.7% тестових випадків несанкціонованого доступ до мережевої інфраструктури та забезпечити своєчасне реагування на інциденти. Успішне впровадження наданого апаратно-програмного комплексу підтверджує можливість його подальшої комерціалізації.

Седлер Віталій Іванович
Директор, ТзОВ «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ «ІНТЕЛЛІАС»

Чижиков Олександр В'ячеславович

Начальник відділу кібербезпеки, ТзОВ «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ «ІНТЕЛЛІАС»

www.intellias.com

+38 032 242 05 90
+38 032 290 36 90
info@intellias.com

ДОДАТОК Б. Фрагменти програмних кодів моделей з перехоплення і аналізу даних про геолокацію точок доступу Wi-Fi

1. intercept_beacon_esp32.py

```
import network

wlan_sta = network.WLAN(network.STA_IF)

def get_networks_data():
    networks_data = {}
    wlan_sta.active(True)
    networks = wlan_sta.scan()
    for ssid, bssid, channel, rssi, authmode, hidden in sorted(networks, key=lambda x: x[3], reverse=True):
        ssid = ssid.decode('utf-8')
        bssid = ":".join('%02X' % i for i in bssid)
        networks_data[bssid] = {'ssid': ssid, 'channel': channel, 'rssi': rssi, 'authmode': authmode, 'hidden': hidden}
    return networks_data
```

2. intercept_beacon_raspberry.py

```
from scapy.all import *

def packet_handler(pkt):
    if pkt.haslayer(Dot11Beacon):
        print("Beacon Frame Detected:")
        print("SSID:", pkt.info.decode())
        print("BSSID:", pkt.addr3)
        print("Signal Strength:", -(256 - ord(pkt.notdecoded[-4:-3])))

def main():
    interface = "wlan0"  # Change this to your WiFi interface name
    sniff(iface=interface, prn=packet_handler)
```

```
if __name__ == "__main__":
    main()
```

3. intercept_probe.py

```
import sys
from scapy.all import *

clients_probes = {}

def packetHandler(pkt):
    if pkt.haslayer(Dot11ProbeReq):
        if len(pkt.info) > 0:
            if pkt.addr2 not in clients_probes:
                clients_probes[pkt.addr2] = set()
            clients_probes[pkt.addr2].add(pkt.info.decode('utf-8'))
    for i in clients_probes:
        print(f'Client: {i} | Probes: {clients_probes[i]}')
sniff(iface=sys.argv[1], count=int(sys.argv[2]), prn=packetHandler)
```

4. generate_uuid.py

```
import sys
import hashlib
import uuid

def string_to_uuid(input_string):
    input_bytes = input_string.encode('utf-8')
    hash_bytes = hashlib.md5(input_bytes).digest()
    uuid_str = uuid.UUID(bytes=hash_bytes[:16])
    return uuid_str

ssid = sys.argv[1]
mac_address = sys.argv[2]
uuid_result = string_to_uuid(f'{ssid}_{mac_address}')
print(uuid_result)
```

5. visualization.html

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-
scale=1.0">
  <title>OpenStreetMap with Leaflet.js</title>
  <link rel="stylesheet"
href="https://unpkg.com/leaflet/dist/leaflet.css" />
  <style>
    #map { height: 750px; }
  </style>
</head>
<body>
  <div id="map"></div>
  <div style="display: flex; gap: 10px; margin-top: 10px;">
    <div>
      <label for="ssidFilter">Filter by SSID:</label>
      <input type="text" id="ssidFilter" placeholder="Enter SSID"
onkeyup="applyFilter()">
    </div>
    <div>
      <label for="lat1Filter">Latitude from:</label>
      <input type="number" id="lat1Filter"  placeholder="Enter
Latitude from" onkeyup="applyFilter()">
    </div>
    <div>
      <label for="lat2Filter">Latitude to:</label>
      <input type="number" id="lat2Filter"  placeholder="Enter
Latitude to" onkeyup="applyFilter()">
    </div>
    <div>
      <label for="lon1Filter">Longitude from:</label>
```

```
      <input type="number" id="lon1Filter"  placeholder="Enter
Longitude from" onkeyup="applyFilter()">
    </div>
    <div>
      <label for="lon2Filter">Longitude to:</label>
      <input type="number" id="lon2Filter"  placeholder="Enter
Longitude to" onkeyup="applyFilter()">
    </div>
  </div>

  <script src="https://unpkg.com/leaflet/dist/leaflet.js"></script>
  <script>
    var map = L.map('map').setView([49.7854195, 24.024544833333334],
15);
    var markersLayer = L.layerGroup().addTo(map);

    L.tileLayer('https://{s}.tile.openstreetmap.org/{z}/{x}/{y}.png',
{
      attribution: '&copy; <a
href="https://www.openstreetmap.org/copyright">OpenStreetMap</a>
contributors'
    }).addTo(map);

    var allMarkers = {}; // Store all markers in an object

    // Load the data from data.json
    fetch('data_v6.json')
      .then(response => response.json())
      .then(data => {
        // Function to filter markers by SSID
        window.applyFilter = function() {
          var ssid = document.getElementById('ssidFilter').value;
          var lat1 =
parseFloat(document.getElementById('lat1Filter').value);
```

```
          var lat2 =
parseFloat(document.getElementById('lat2Filter').value);
          var lon1 =
parseFloat(document.getElementById('lon1Filter').value);
          var lon2 =
parseFloat(document.getElementById('lon2Filter').value);

          Object.keys(allMarkers).forEach(macAddress => {
            const marker = allMarkers[macAddress];
            const isInRange = marker.options.latitude >= lat1  &&
marker.options.latitude <= lat2 &&  marker.options.longitude >= lon1
&&  marker.options.longitude <= lon2;
            const isInSsId = marker.options.ssid.includes(ssid);


            if(ssid || (lat1 && lat2 && lon1 && lon2)){
                if (isInSsId && isInRange || !ssid && isInRange ||
!(lat1 && lat2 && lon1 && lon2) && isInSsId) {
                    marker.addTo(map); // Show marker if SSID matches
filter

            } else {
                map.removeLayer(marker); // Hide marker if SSID does
not match filter
            }
            } else {
                return  marker.addTo(map);
            }
          });
        };

        // Add markers to the map
        Object.keys(data).forEach(macAddress => {
          var wifiData = data[macAddress];
```

```
          var marker = L.marker([wifiData.latitude,
wifiData.longitude], { ssid: wifiData.ssid, latitude:
wifiData.latitude,  longitude: wifiData.longitude});
          marker.bindPopup(`<b>${macAddress}</b><br>SSID:
${wifiData.ssid}<br>Power: ${wifiData.pwr}<br>Channel:
${wifiData.channel}<br>Latitude: ${wifiData.latitude}<br>Longitude:
${wifiData.longitude}`);
          allMarkers[macAddress] = marker; // Store marker in
allMarkers object
        });

        applyFilter(); // Apply filter initially
      })
      .catch(error => {
        console.error('Error loading data:', error);
      });
  </script>
</body>
</html>
```